THE QUINTIC GAUSS SUMS

Dissertation
zur Erlangung des Doktorgrades
der
Mathematisch-Naturwissenschaflichen
Fakultäten
der Georg-August Universität zu
Goettingen

vorgelegt von
Léopold Fossi Talom
Aus Bandjoun/ Yom V, Kamerun

Göttingen 2002

D7
Referent: Prof. S.J. Patterson
Korreferentin: Frau Prof. Dr. I. Kersten.
Tag der Disputation:

Contents

List of Figures

CHAPTER 1

INTRODUCTION

In 1801, Gauss in his *Disquisitiones Arithmeticae* introduced the following sum

$$G_2(m;k) = \sum_{n=0}^{k-1} e^{2\pi i m n^2/k}.$$

where m and k are coprime.
This sum has a remarkably simple dependence on its arguments. In the case k odd, it has values as $\pm\sqrt{k}$, or $\pm i\sqrt{k}$. Gauss discovered in 1801 that in fact for k odd:

$$G_2(1;k) = \begin{cases} \sqrt{k} & \text{if} \quad k \equiv 1 \bmod 4 \\ i\sqrt{k} & \text{if} \quad k \equiv -1 \bmod 4 \end{cases}$$

He only found a proof 4 years later, in August 1805. He also determined these values for $k \equiv 0, 2 \bmod 4$. There are nowadays many different proofs of this theorem. See for example [**S.I**], [**K.L**], [**E.T**]
One important property is that Gauss sums generate quadratic subfields of cyclotomic fields. Indeed one can verify easily that for integer k odd,

$$G_2(m,k)^2 = (-1)^{\frac{k-1}{2}} k = k^*.$$

Therefore the quadratic field $\mathbb{Q}(\sqrt{((-1)^{\frac{k-1}{2}}k)})$ is contained in $\mathbb{Q}(e^{\frac{2\pi i}{k}})$. This fact is one of the properties discovered by Gauss before he determined the correct sign for the Gauss sums. He used it to prove the law of quadratic reciprocity. He considers for two distinct primes p, q, and if $(\frac{\cdot}{\cdot})$ is the Legendre symbol, then the expression

$$G_2(1,p)^{q-1} \equiv G(q,p)^{2\frac{q-1}{2}} = {p^*}^{\frac{q-1}{2}} \equiv \left(\frac{p^*}{q}\right) \mod q$$

thus

$$G_2(1,p)^q \equiv G(q,p) \pmod p \tag{0.1}$$

$$\equiv \left(\frac{q}{p}\right) G(1,p) \pmod p \tag{0.2}$$

$$\equiv \left(\frac{p^*}{q}\right) G(1,p) \pmod p \tag{0.3}$$

and so multiply both side of the last equation above by $\left(\frac{q}{p}\right)$ we obtain the desired result:

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{(\frac{q-1}{2})(\frac{p-1}{2})}.$$

Another proof is obtained as follows. The Chinese Remainder Theorem give the values of Gauss sums for composite odd numbers pq and the definition of $G_2(1,p)$

for different values of prime p is known for congruence classes modulo 4 of the odd numbers p, q, and pq so that in plugging in all that within the following identity:

$$G_2(1,pq) = (\frac{p}{q})(\frac{q}{p})G_2(1,p)G_2(1,q);$$

we deduce the law of quadratic reciprocity as:

$$(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

This is another proof of the law of quadratic reciprocity.

A more general Gauss sum is the following.

$$G_n(m;k) = \sum_{\ell=0}^{k-1} e^{(2\pi i m\ell^n/k)}.$$

We see that for k prime and $\gcd(k,m) = 1$

$$G_n(m;k) = \sum_{\chi:\chi\neq 1} \tau_n(\chi),$$

where the χ are all non trivial character modulo k of order ℓ and

$$\tau_n(\chi) = \sum_{a \bmod k} \chi(a)\exp(2\pi i a n/k)$$

The cubic Gauss sum, also called Kummer sum after E.E. Kummer, is

$$G_3(1,p) = \sum_{n=1}^{p-1} \exp(\frac{2\pi i n^3}{p})$$

can be expressed as $G_3 = \tau_3(\chi) + \tau_3(\overline{\chi})$ where χ is a cubic character on $\mathbb{F}_p$, and

$$\tau_3(\chi) = \sum_{n=1}^{p-1} \chi(n)\exp(\frac{2\pi i n}{p}).$$

The sum $G_3(1,p)$is indeed a root of the cubic period polynomial $f_p(X) = X^3 - 3pX - pL$ where $4p = L^2 + 27M^2$. This polynomial has exactly one root in each of the interval $[-2\sqrt{p}, -\sqrt{p}]$, $[-\sqrt{p}, \sqrt{p}]$ and $[\sqrt{p}, 2\sqrt{p}]$, and the question here is to know which of them contains the root G_3. The quotient

$$\frac{\tau_3(\chi)}{|\tau_3(\chi)|}$$

lies on the unit circle. Looking at their arguments θ_p, Kummer observed here that the investigation on the 45 cases of prime p less than 500 gives the frequency 3:2:1 respectively and he suggested that

$$\sum_{\substack{p\equiv 1 \bmod 3,\\ p<x}} \chi_h(|\theta_p|) = \frac{W_h x}{2\log x} + o(\frac{x}{\log x}) \quad h = 1,2,3,$$

where χ_1 (resp. χ_2, χ_3) is the characteristic function of the interval $(0, \frac{\pi}{3}]$ (resp. $(\frac{\pi}{3}, \frac{2\pi}{3}]$, $(\frac{\pi}{3}, \pi]$ and $W_h = \frac{1}{2}, \frac{1}{3}, \frac{1}{6}$ for $h = 1,2,3$ respectively. The study of the frequence

analysis of this arguments was done by Lehmer [**EL**], Goldstine and Von Neumann [**G.VN**]. They found, for $p < 1000$ a different distribution approximately $4 : 3 : 2$. This led one to doubt about the conjecture of Kummer. The same investigation led one observed that the arguments θ_p are likely equidistributed in the interval $(0, \pi)$ for the Lebesgue measure. Then following a suggestion of Davenport [**Da**], Moreno [**MO**] in 1974 proved that if $I \in (0, \pi]$ is a subinterval, then

$$\sum_{p\equiv 1 \bmod 3, p<x} \chi_I(3\theta_p) = \frac{|I|x}{2\log x} + o(\frac{x}{\log x})$$

where $|I|$ is the Lebesgue measure of I. This just proves that the arguments of the $\tau_3(\chi)^3$ are uniformly distributed in the three intervals listed above. The idea of Moreno is that, the character $\chi = \left(\frac{\pi}{\cdot}\right)$ is associated to a factor $\pi|p$, such that $\pi \equiv -1 \bmod 3$ in the field of cubic roots of unity $\mathbb{Q}(\zeta_3)$. He then observed that $\exp(i\theta(\pi)) = p^{\frac{-3}{2}}\tau_3^3(\chi)$ is a Grössencharcter in $\mathbb{Q}(\zeta_3)$, then from Hecke's theory of L-functions, it follows

$$\sum_{N\omega\leq X} \exp(in\theta(\omega)) = o(\frac{X}{\log X})$$

as $X \to \infty$, for each integer $n \neq 0$, and this is equivalent to the uniform distribution of $\tau_3^3(\chi)$. This proof has led one to seriously looking for a proof to disprove the Kummer's conjecture. Kubota [**KB1**] [**KB2**] has indicated a method for obtaining some asymptotic results on the determination of the Gauss sums. This was based mostly on his theory of automorphic functions. Indeed if we define

$$\Gamma = \left\{ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(\mathbb{Z}[\zeta_3]); \quad \gamma \equiv I \mod 3 \right\}$$

then

$$\psi(\gamma) = \begin{cases} \left(\frac{c}{a}\right)_3 & \text{if} \quad c \neq 0, \\ 1 & \text{if} \quad c = 0 \end{cases}$$

We see that ψ is a character on Γ and Γ acts discontinuously on the upper half space $H = \mathbb{C} \times \mathbb{R}_+^\times$ as follows. A point $u = (z, v)$ in H is represented by the matrix

$$\begin{pmatrix} z & -v \\ v & \overline{z} \end{pmatrix}$$

and for $w \in \mathbb{C}$, we write

$$\tilde{w} = \begin{pmatrix} w & 0 \\ 0 & \overline{w} \end{pmatrix}$$

then the action of Γ on H is given by:

$$\gamma(u) = \left(\tilde{a}u + \tilde{b}\right)\left(\tilde{c}u + \tilde{d}\right)^{-1}, \quad \gamma = \begin{pmatrix} a & b \\ c & c \end{pmatrix}.$$

Following Selberg, the Eisenstein series corresponding to the cusp ∞

$$E(u, s) = \sum_{\gamma\in\Gamma_\infty\backslash\Gamma} \overline{\psi(\gamma)} v(\gamma(w))^s$$

for $Re(s) > 2$ and $u = (z, v) \in H$, and where

$$\Gamma_\infty = \{\gamma \in \Gamma; \gamma(\infty) = \infty\}$$

$E(u,s)$ has a meromorphic continuation to the whole s-plane. If we complement $E(u,s)$ by the further three Eisenstein series corresponding to the remaining inequivalent essential cusp, then there is a functional equation connecting the values at s and at $2-s$. On forming the Fourier expansion of $E(u,s)$ with respect to Γ_∞, we find that the coefficients are Dirichlet series satisfying similar functional equations and whose coefficients are cubic Gauss sums. The theory shows that these Dirichlet series are regular in the half-plane $Re(s) > 4/3$. In particular, the regularity at $s = 3/2$ together with a well-known tauberian theorem gives

$$\sum_{N(\alpha)\leq X} \frac{g_3(\alpha)}{|g_3(\alpha)|} = o(X) \quad \text{as} \quad X \to \infty$$

where $\alpha \equiv 1 \bmod 3$ in $\mathbb{Z}[\zeta_3]$ and

$$g_3(\alpha) = \sum_{x \bmod \alpha} \left(\frac{x}{\alpha}\right)_3 \exp(\pi i \mathrm{Tr}_{K/\mathbb{Q}}(\tfrac{x}{\alpha})),$$

where $\mathrm{Tr}_{K/\mathbb{Q}}$ is the trace of the linear map within the $\mathbb{Q}$-vector space

$$K = \mathbb{Q}(\zeta) \to K; \quad y \mapsto yx \text{ for } 0 \neq x, y \in K.$$

The norm $\mathrm{N}_{K/\mathbb{Q}}$ is also defined to be the determinant of the same map. This definition is modified in case $K/\mathbb{Q}$ is a Galois extension.
Patterson [**SJP3**], [**SJP4**] between 1977 and 1978 developed the work of Kubota and established the cubic analogue of the theta series. This enabled Patterson [**SJP1**] in 1978,and later in 1979 Heath-Brown and Patterson(for general result) [**HP**] to prove that the arguments of Gauss sums are uniformly distributed according to the Weyl criterion for uniform distribution on the unit circle. Patterson essentially proved that:

$$\sum_{\substack{N(\pi)\leq X \\ \pi \equiv a \bmod \alpha}} \left(\frac{g_n(\pi)}{|g_n(\pi)|}\right)^m = o(\frac{X}{\log(X)}).$$

for any prime π, and for any integer $m \neq 0$, where

$$g_n(\pi) = \sum_{x \bmod \pi} \left(\frac{x}{\pi}\right)_n e(2\pi i \mathrm{Tr}_{K/\mathbb{Q}}(\tfrac{x}{\pi})).$$

The symbol

$$\left(\frac{\cdot}{\cdot}\right)_n$$

is the n^{th} power residue symbol.
Indeed if we put

$$\tilde{g_n}(\alpha) = \frac{g_n(\alpha)}{|g_n(\alpha)|} \qquad (= 0 \quad if \quad g_n(\alpha) = 0)$$

for any ideal α.
In 1979 Patterson did prove that if one selects α modulo the n^{th} powers of units, then

$$\sum_{N(\alpha)\leq X} \tilde{g_n}(\alpha)\omega(\alpha)\Lambda(\alpha) = o(X).$$

Where Λ is the von Mangoldt function in the field K and here $\omega(c)$ is a Grössencharacter of K i.e a function on the idèle group which is trivial on the field K. This result is

a generalization of the previous one by Heath-Brown and Patterson [**HP**] in 1979 and is up to now known as the latest most outstanding achievement in the theory of Gauss sums. This proof is ingenious and difficult.

Patterson [**SJP3**][**SJP5**], showed that, if we take the Kummer sums $g_3(\alpha)$ for any integer $\alpha \equiv 1 \bmod 3$ in $\mathbb{Z}[\zeta_3]$, then a formal application of the Hardy Littlewood methods suggested the asymptotic formula

$$\sum_{N(\alpha)\leq X} \Re(\frac{g_3(\alpha)}{|g_3(\alpha)|}) \sim \frac{(2\pi)^{2/3}}{5\Gamma(2/3)}\frac{X^{5/6}}{\log X} \quad \text{as} \quad X \to \infty = O(X^{\frac{5}{6}+\epsilon}) \quad \text{for all} \quad \epsilon > 0.$$

In general, if χ is a normalized Hecke character, then for ideal I and prime π we have

$$\sum_{N(I)\leq X} \chi(I) = \alpha(\chi)X + o(X)$$

and

$$\sum_{N(\pi)\leq X} \chi(I) = \beta(\chi)(\frac{X}{\log X}) + o(\frac{X}{\log X}).$$

Using Kummer,s theory of ideal numbers, Stickelberger [**S.L**] in 1890, proved that the ideal generated by the Gauss sums can be factorized as follows: if $\alpha \in \mathbb{Z}[\zeta_m]$ the

$$(g_m(\alpha)) = (\alpha)^\theta$$

where theta is the element of the group ring $\mathbb{Q}[Gal(K/k)]$ defined by

$$\theta = \frac{1}{m}\sum_{\substack{\gcd(t,m)=1 \\ t \bmod m}} t.\sigma_{-t} \quad \text{and the Galois element is such that} \quad \sigma_t(\zeta) = \zeta^t$$

Gauss proof of the quadratic reciprocity law by counting lattice points reappears in the determination of the sign the quadratic Gauss sums. Later, J.W.S. Cassels, in 1969,1970 [**J.W.S**] and [**J.W.S1**], proposed a formula for cubic Gauss sums in terms of values of elliptic functions. A student of him, A. D. McGettrick [**Mc.G1**](1972), reformulated this conjecture in terms of the number of lattice points in certain domain. This conjecture and his biquadratic analogue where proved by C. R. Matthews [**Mat**].
It is a goal of this thesis to investigate the possibility of the analogue of this formula for the quintic Gauss sums.
We define certain roots of unity $\Omega(S_0, \varepsilon, \pi)$ which generalizes the construction of Cassels. It has certain formal properties analogous to those of Gauss sums $\mathfrak{g}(1, \varepsilon, \pi)$. We investigate whether the quotient of this is a simple function in the sens that it can be obtain by information of a finite number of places. the evidence shows that it is probably not the case and the statistical investigation shows evidence of unexpected, but very interesting structure. We give two conjecture on the quintic Gauss sums, namely, on the asymptotic behavior of it partial sums.

In Chapter I, we give a brief description of the cyclotomic fields. We outline the key properties necessary for the introduction of the Gauss sums. We expose the decomposition of prime in general cyclotomic field and define the norm residue symbol. We give a definition of a primary element in the fifth cyclotomic field. We use this kind of prime algebraic integers for the computation.
Chapter II describes the basic properties of the Gauss sums. We outline some key properties of the Gauss sums. We state the Davenport-Hasse Theorems, and introduce the Weil Grössencharacter. We study the asymptotic behavior of powers of Gauss sums (of moment of a Gauss sums) and explain a property on the distribution of Gauss sums. The Gauss sums, after being defined purely algebraically, will be regarded as complex numbers via embeddings into $\mathbb{C}$. This has helped to make computational test through a C program.

In Chapter 3, we describe the fundamental domain. These fields studied here are the prime cyclotomic field. We determine in detail the skeleton of the fundamental domain for the prime cyclotomic field. We find results to characterize the geometry, we prove that there are $\frac{n-1}{2}$ different shapes of faces. This result generalizes the result obtain by Dirichlet for the third cyclotomic field. There are different geometries for the faces of a the fundamental domain. For $n = 3$ and 5 we give a picture for the faces of their fundamental domain. For this, we handle it in a very simple way, just by studying subsets instead of using brute force. This has the advantage of generalizing as far as possible. We give two different methods to construct an n^{th} set for prime n. One of these methods is very elementary, based only on the properties of subsets of the n first positive integers. The combinatorics of these geometries are also studied. We discover that they are related to some numbers $\gamma(n, i)$.

In Chapter 4 we describe some identities that could help us to understand the behavior of the Gauss sums. We fix an n-set, S_0, once and for all. We give identities that reflect the properties of Gauss sums. We specialize on the fifth case to do some computation. The results of the computations would be consistent with a generalization of the Cassels-McGettrick formula. This unfortunately does yield at the present stage a conjecture on the determination of the correct sign for the Gauss sums. However, we can explain more on the distribution of certain functions involving the values of Gauss sums. We attempt to verify a conjecture of Patterson. We study the functions

$$H(X) = \sum_{\substack{N(\pi)<X \\ \pi\equiv 1 \bmod \lambda^3}} \mathfrak{g}(1, \varepsilon, \pi) \log(N(\pi))$$

and

$$\tilde{H}(X) = \sum_{\substack{N(\pi)<X \\ \pi\equiv 1 \bmod \lambda^3}} \frac{\mathfrak{g}(1, \varepsilon, \pi) \log(N(\pi))}{\Omega(\varepsilon, \pi)}$$

Both functions have more or less the same shape and contrary to our expectation, that it would behave like the summation function of the Möbius function, but in fact its behavior is quite different. The observations are graphically consistent with the conjecture that

$$H(X) > 0 \text{ as well as } \tilde{H}(X) > 0$$

for X large. This is would probably behave like other functions, known in the theory of elementary number theory, when we replace $\mathfrak{g}(1, \varepsilon, \pi)$ by the Möbiüs function . We also confirm a suggestion of Patterson, that

$$H(X) \sim c.X^{6/5} + o(X)$$

This conjecture shows numerical evidence however you can't at the moment prove it. We notice that the constant c is of order $\frac{1}{10} = \frac{1}{2.5}$. To do this we represent, in certain range, the functions

$$\frac{H(X)}{X^{6/5}} \quad \text{and} \quad \frac{\tilde{H}(X)}{X^{6/5}}.$$

Another conjecture out of this observation is that, there exists a positive real A such that for $X > A$ neither $H(X)$ nor $\tilde{H}(X)$ never cross the x-axis. This conjecture is stronger that the previous one. We can the summarize both and ask the following in a more general case: We suppose that $H(X) \sim X^{\theta}$ and the problem here is to give an estimate of θ.

In the appendix we give in section 1, a brief description of the Gauss periods (Lagrange resolvents) and then give a result and conditions for these resolvents to be rational integers. This result is less known though. It is known in general that they are algebraic integers in cyclotomic fields. We give also an elementary proof , due to Cauchy, of the determination of the sign for the quadratic Gauss sums. We end up with an algorithm which computes the Gauss sums and run it for some few values. We add at the last end some data, out of our output file.

CHAPTER 2

Generalities on Cyclotomic Fields

1. Introduction

The first investigations of algebraic number fields were made by Gauss, whose study of biquadratic reciprocity led him to introduce the domain $\mathbb{Z}[i]$. Later Eisenstein and Jacobi (not jointly, however), used the domain $\mathbb{Z}[\omega]$ (ω is a primitive cubic root of unity) to study the cubic law of reciprocity. In both cases, the domains have the unique factorization property, and in fact, they are what we call Euclidean domains. Later Kummer and Dirichlet tried to use the domain $\mathbb{Z}[\zeta]$, ζ a primitive root of unity of odd prime degree ℓ to show the impossibility of $x^\ell + y^\ell = z^\ell$ in integers. Kummer prepared a proof which rested on the assumption that $\mathbb{Z}[\zeta]$ has unique factorization and submitted it to Dirichlet who pointed out a mistake. This provoked Kummer to invent his theory of ideal numbers which subsequently grew, among others, in the hands of Kronecker and Dedekind into algebraic number theory as we know it. One can refer to [**K**]. Cyclotomic fields and their subfields, the Abelian fields are thus the first and the most thoroughly studied of the algebraic number fields. This is because Abelian extensions of $\mathbb{Q}$ are the only ones for which the decomposition of primes is determined by their congruence classes to some modulus (called the *conductor* of the field). This chapter is an exposition of the basic algebraic theory of cyclotomic fields. There are two well known results that will appear throughout the thesis. The first one is that every Abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field and the second one is that if C=$\mathbb{Q}(\zeta)$ is the "smallest" cyclotomic field containing a field K, then the trace $tr_{\mathrm{C/K}}(\zeta)$ is a primitive element for K. This is a so called *Lagrange Resolvent or a Gauss sum.*

Let Ω be an algebraically closed field of characteristic zero. We assume that other fields in this section are contained in Ω. Let $E_n = E_n(\Omega)$ denote the set of n^{th} roots of unity contained in Ω ie: $E_n(\Omega) = \{a \in \Omega : a^n = 1\}$. $E_n(\Omega)$ is a group of order n. If $d|n$ then $E_d \subseteq E_n$ is the unique subgroup of order d. Thus E_n is a cyclic group of order n. A generator of $E_n(\Omega)$ is an element of order n. It is a so-called *primitive n^{th} root of unity.* The elements of $E_n(\Omega)$ are solutions of the polynomial equation $X^n - 1 = 0$. In the later steps there is no difference between $\mu_n(\Omega)$ and $E_n(\Omega)$. If $\Omega = \mathbb{C}$ then $\mu_n(\Omega)$ is denoted by μ_n. If $d|n$, then the polynomial $X^{\frac{n}{d}} - 1$ is a factor of $X^n - 1$. There are $\varphi(n)$ primitive n^{th} roots of unity. To see this we simply remark that ζ_n and ζ_n^m are both primitive root of unity whenever $\gcd(m, n) = 1$. Indeed, if $\Phi_n(X) \in \mathbb{Z}[X]$ is the minimal polynomial of ζ_n, then $\Phi_n(X)|X^n - 1$ and it can also be shown that

$$\Phi(X) = \prod_{\gcd(j,n)=1} (X - \zeta_n^j)$$

However if ζ_n^j is another primitive root of unity, then it is a root of the polynomial $X^n - 1$ but not a root of $\gcd(X^j - 1, X^n - 1)$ and therefore $\Phi_n(X)$ can be written as

$$\Phi_n(X) = \frac{X^n - 1}{\gcd(X^n - 1, \prod_{1 \leq j < n}(X^j - 1))}$$

$\Phi_n(X)$ is called the n^{th} *cyclotomic polynomial.*

It follows that

$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

and then the Möbius inversion formula can be applied,

$$\Phi_n(X) = \prod_{d|n}(X^{n/d} - 1)^{\mu(d)}$$

where $\mu(d)$ is the Möbius function.

Definition 2.1. Let k be an arbitrary subfield of Ω. Any extension of k which is of the form $k(E_n(\Omega))$ is called a cyclotomic field of k.

Let ζ_n denote a primitive n^{th} root of unity. Since the coefficients of the above polynomial belong to the prime field of Ω and hence to the field k, the extension $k(\zeta_n) = k(E_n(\Omega))$ is a Galois extension of k and its relative degree does not exceed $\varphi(n)$. Let G=Gal$(k(\zeta_n)/k)$ denote the Galois group of the extension $k(\zeta_n)/k)$. If $x \in k(\zeta_n)/k$, the action of a Galois element $\sigma \in G$ on x is denoted by x^σ for $\sigma(x)$. Since for $\sigma \in G$, we have $\zeta^\sigma \in E_n$, there exits a unique integer $\nu(\sigma)$ mod(n), such that $\zeta_n^\sigma = \zeta_n^{\nu(\sigma)}$. This choice of $\nu(\sigma)$ does not depend on the choice of the primitive n^th root of unity ζ_n. Furthermore we have

$$\sigma, \tau \in G, \quad \zeta_n^{\sigma\tau} = (\zeta_n^\sigma)^\tau = (\zeta_n^{\nu(\tau)})^\sigma = (\zeta_n^{\nu(\sigma)})^{\nu(\tau)} = \zeta_n^{\nu(\sigma)\nu(\tau)}.$$

Hence

$$\nu(\sigma\tau) = \nu(\sigma)\nu(\tau) \mod n.$$

This signifies that the mapping

$$\sigma \longmapsto \nu(\sigma) \mod (n)$$

is a homomorphism sending G onto the group of residue classes modulo n. If m is some integer positive such that

$$\sigma^n(\zeta_n) = \underbrace{\sigma\sigma\cdots\sigma}_{n \quad times}(\zeta_n),$$

then

$$(\zeta_n)^{\sigma^m} = \zeta$$

is equivalent to $m\nu(\sigma) \equiv 1$ modulo(n) which in turn is equivalent to $(\nu(\sigma), n) = 1$ for $\sigma \neq 1_G$. This is to say that $\nu(\sigma)$ is relatively prime to n. The above map is therefore injective and G is an Abelian group, i.e. $k(\zeta_n)/k$ is an Abelian extension.

Theorem 2.1. *Let k be an arbitrary field contained in an algebraically closed field Ω, and let ζ_n be a primitive n^{th} root of unity in Ω (n being not divisible by the characteristic of k). Then the extension $k(\zeta_n)/k$ is an Abelian extension and its Galois group Gal($k(\zeta_n)/k$) is sent isomorphically by the mapping $\sigma \to \nu(\sigma)$, which maps $\zeta_n^{\sigma} = \zeta_n^{\nu(\sigma)}$, to a subgroup of the group of residue classes of $\mathbb{Z}$ modulo m. This isomorphism is given by*

$$\sigma \longmapsto t$$

and consequently the dimension $[L : k] \leq \varphi(m)$.

Remark Suppose $n, m \in N, n, m \geq 2$ and $(n, m) = 1$. Then ζ_n is never a power of ζ_m and vice versa. Therefore, the fields $k(\zeta_n)$ and $k(\zeta_m)$ have as intersection the base field k, and ζ_{nm} is an element of $k(\zeta_m, \zeta_n)$ of order mn i.e. $k(\zeta_{mn}) \subset k(\zeta_n, \zeta_n)$. But $(\zeta_{mn})^n = \zeta_m$ and $(\zeta_{mn})^m) = \zeta_n$ implies that $k(\zeta_n)$ and $k(\zeta_m)$ are both contained in $k(\zeta_{mn})$ and the minimality of $k(\zeta_m, \zeta_n)$ yields the equality .

Note 2.1. From now on, all the fields we use are Galois extensions K of $\mathbb{Q}$.

Definition 2.2. We define for any algebraic integer $a \in K$:
the norm

$$N_{K/\mathbb{Q}}(a) = \prod_{\sigma \in G} \sigma(a)$$

and the trace

$$Tr_{K/\mathbb{Q}}(a) = \sum_{\sigma \in G} \sigma(a)$$

We will sometimes denoted $N_{K/\mathbb{Q}}$ by N and $Tr_{K/\mathbb{Q}}$ by Tr. Both are maps from K to the base field $\mathbb{Q}$.

Definition 2.3. Let O_K be the ring of integers of K, $O_K^{\times}$, is the group of units of K.

Lemma 2.1.

$$u \in O_K^{\times} \iff N_{K/\mathbb{Q}}(u) = \pm 1$$

In the following steps, we shall denote the ring of integers of K, $\mathbb{Z}[\zeta_n]^{\times}$, by O_K and the group of units of K, $O_K^{\times}$, is sometimes denotes by U(K).

Definition 2.4. The *discriminant* $\Delta = \Delta(K/\mathbb{Q})$ of the cyclotomic field $K = \mathbb{Q}(\zeta_n)$ is defined to be $\Delta(\zeta) = \prod_{j \neq i}(\zeta^i - \zeta^j)$ where $\zeta = \zeta_n$ is any primitive root of unity.

$$\Delta(K) = (-1)^{n(n-1)/2} \prod_{j \neq i} (\zeta^i - \zeta^j)$$

Definition 2.5. The O_K-module generated by

$$\{\alpha : \alpha \in K, \mathrm{Tr}_{K/\mathbb{Q}}(\alpha O_K) \subset \mathbb{Z}\}$$

is a fractional ideal $\mathfrak{M}(K/\mathbb{Q})$ containing $\mathbb{Z}$. The *different* $\mathfrak{D} = \mathfrak{D}(K/\mathbb{Q})$ of the extension field $K = \mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ is defined to be the inverse of the $\mathbb{Z}$-module $\mathfrak{M}(K/\mathbb{Q})$:

$$\mathfrak{D} = \mathfrak{M}(K/\mathbb{Q})^{-1}$$

Remark If we replace $\mathbb{Q}$ by $\mathbb{Q}_p$, then K is a local field with maximal prime ideal $\mathfrak{P}$ then

$$\mathfrak{D} = \mathfrak{P}^N$$

for some positive integer N.

Remark

$$\Phi_n(\zeta^a)|n^n \text{ for all integers } a, \quad \text{with } \gcd(a, n) = 1.$$

The discriminant

$$\Delta = \delta(1, \zeta, \cdots, \zeta^{\phi(n)-1})|n^n$$

Remark If $n = p$ is prime, then the Galois group $G = Gal(K/\mathbb{Q})$ of $K/\mathbb{Q}$ is of order $p-1$ and therefore 2 divides $|G|$. Therefore by the elementary theory of finite groups and the Galois connection between subfields of K and subgroups of G, this assures that K contains a quadratic field K_1. Since the Galois group is cyclic, then $G =< \sigma >$ for some generator $< \sigma >$. $K_1/\mathbb{Q}$ is of degree 2 and K/K_1 is of degree $\frac{p-1}{2}$. We will see later that this field is rather easily constructed by using the Gauss sums. This in fact always assures the existence of a quadratic field in a prime power cyclotomic field. This even extends to any cyclotomic field, since the function $\phi(n)$ is even for $n > 2$.
Let t denote the degree of $K/\mathbb{Q}$. Then the homomorphism

$$\varphi : K \to K \otimes_{\mathbb{Q}} \mathbb{R}, \quad x \mapsto x \otimes 1$$

is an injective K-homomorphism. The $\mathbb{R}$-algebra $K \otimes_{\mathbb{Q}} \mathbb{R}$ decomposes as $K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^r \times \mathbb{C}^s$, where (r, s) is called the signature of the field K. In general the component map

$$\varphi_i : K \to \mathbb{R} \quad \text{or} \quad \mathbb{C}$$

is called *real or complex embedding* if its range is $\mathbb{R}$ or $\mathbb{C}$ respectively. That is, φ is written component wise (φ_i) $1 \leq i \leq r + s$ such that the r real first components are real embeddings and the s second components are complex embeddings up to complex conjugacy.

1.1. Decomposition of primes. Let us suppose, as before, that K is an algebraic number field, Galois over $\mathbb{Q}$ of finite degree, and $G = G(K/\mathbb{Q})$ is its Galois group. Denote O_K the ring of integers of K.
Any prime integral ideal $\mathfrak{P}$ of K intersects $\mathbb{Z}$ at some rational prime p and we say that $\mathfrak{P}$ is *above* (p). This also means $\mathfrak{P}|p$ and therefore the norm $N(\mathfrak{P})|N(p)$ implies that $|N(\mathfrak{P})| = p^f$ for some $f \leq n$. $f = f_{\mathfrak{P}}$ is called *the residue class degree* of $\mathfrak{P}/p$. However any other conjugate of a prime ideal above $\mathfrak{P}$ is still a prime above p since

the Galois isomorphism maps primes onto primes and leaves invariant the ideals of the base field. In general, not all the ideals $\sigma(\mathfrak{P}), \sigma \in G$ are distinct. However we are in a situation of a unique factorization domain. Thus, to each prime ideal $\mathfrak{P}$, we associate the Galois subgroup

$$G(\mathfrak{P}) = \{\sigma \in G : \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

$G(\mathfrak{P})$is called *the decomposition group of* $\mathfrak{P}$. The corresponding subfield to this subgroup is called the *decomposition field of* $\mathfrak{P}$. The order $e_{\mathfrak{P}}$ of $G(\mathfrak{P})$ is the exponent of $\mathfrak{P}$ in the factorization of p. It is called *the ramification degree* of $\mathfrak{P}/p$. From the transitivity of the Galois group we see that all the $e_{\sigma(\mathfrak{P})}$ are equal, and we denote it by e. Let r be the number of distinct primes above p, we thus have $ref = n$. The following theorem describes the action of the Galois group on the decomposition:

Theorem 2.2. *Let $K/\mathbb{Q}$ be a Galois extension. Let $p \in \mathbb{Z}$ be a prime number and write $(p) = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$. Then $e = e_1 = \cdots = e_r$ and $f = f_1 = \cdots = f_r$ so that $efr = n$.*

Proof. See [**I.R**], pp 181 − 183 □

Definition 2.6. If $e(\mathfrak{P}/p) > 1$ we say that the prime ideal $\mathfrak{P}$ ramifies in $K/\mathbb{Q}$. i.e $(p) \subset \mathfrak{P}^2$.

Let p, $\mathfrak{P}|p$ be as before, then $\kappa = O_K/\mathfrak{P}$ is a finite field with $N(\mathfrak{P})$ elements. It is the residue class field at $\mathfrak{P}$ and it contains $\mathbb{F}_p = \mathbb{Z}/(p)$ as a subfield. It is also a Galois extension of $\mathbb{Z}/(p)$ with Galois group $\overline{G} = Gal(\kappa/\mathbb{F}_p)$, if we define the homomorphic map from $G(\mathfrak{P})$ to $Gal(\kappa/\mathbb{F}_p) = \overline{G}$ by $\overline{\sigma}(\alpha \pmod{\mathfrak{P}}) = \sigma(\alpha) \pmod{\mathfrak{P}}$. The map $\sigma \mapsto \overline{\sigma}$ is a well defined map and is onto. Let

$$T(\mathfrak{P}) = \{\sigma \in G : \sigma(\alpha) \equiv \alpha \bmod (\mathfrak{P}) \text{ for all } \alpha \in K\}$$

is the kernel of this homomorphism, then $G(\mathfrak{P})/T(\mathfrak{P}) \cong \overline{G}$. $T(\mathfrak{P})$ is called the *inertia group of* $\mathfrak{P}$ and the corresponding field is called the inertia field of $\mathfrak{P}$.
We notice that the order of $G(\mathfrak{P})/T(\mathfrak{P})$ is f and is also a cyclic group of the same order, generated by the homomorphism $\overline{\alpha} \mapsto \overline{\alpha}^p$, $\alpha \in O_K$. The element of the quotient group $G(\mathfrak{P})/T(\mathfrak{P})$ associated by the above isomorphism to the latter operation is called a *Frobenius class* associated with $(K/\mathbb{Q}, \mathfrak{P})$ and is denoted by σ_p.

Lemma 2.2. *Let p be a prime integer such that $p \nmid n$.*
Then σ_p is the element of the Galois group $G(K/\mathbb{Q})$ which maps $\zeta \mapsto \zeta^p$
The equation $\zeta^a \equiv \zeta^b \pmod{p}$ implies that $\zeta^a = \zeta^b$

Proof. $\sigma_p(\zeta) = \zeta^a$ for some $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$
$\sigma_p(\zeta) \equiv \zeta^p \bmod ((p))$ implies that $p|(1 - \zeta^j)$ for some j, $0 < j < n$ and therefore $p|n$ which is a contradiction of the assumption. □

Remark The order of the Frobenius element σ_p is f. Thus an equation of the form $\sigma_p^m = id \in Gal(K/\mathbb{Q})$ is equivalent to saying that $\sigma_p^m(\zeta) = \zeta$. This implies $p^m \equiv 1 \bmod (n)$, therefore f is the smallest positive integer such that $p^f \equiv 1 \bmod (n)$ Moreover if $\sigma_{p_1} = \sigma_{p_2}$ then $\zeta^{p_1} = \zeta^{p_2}$ which is equivalent to $n|(p_1 - p_2)$. Thus,

two primes in the same arithmetic progression with difference n have the same decomposition law. The converse is false. To see this take $K = \mathbb{Q}(\zeta_8)$ and prime $p \equiv 3, 5, 7 \bmod (8)$, which have the same law of decomposition.

Now suppose that n is a power of a prime p, say, $m = p^s$. Then every primitive $p^s th$ root of unity ζ, is a root of $X^{p^s} - 1$ but not that of $X^{p^{s-1}} - 1$. We have, therefore,

$$\prod_{(i,p^s)=1} (X - \zeta^i) = \frac{X^{p^s} - 1}{X^{p^{s-1}} - 1} = X^{p^{(s-1)(p-1)}} + \cdots + X^{p^{(s-1)}} + 1$$

and in particular

$$p = \prod_{(i,p^s)=1} (1 - \zeta^i).$$

For each such i,

$$\frac{1 - \zeta^i}{1 - \zeta} = 1 + \zeta + \cdots + \zeta^{i-1}$$

belongs to O_K. Moreover there exists j such that $ji \equiv 1 \bmod (p^s)$ and $0 < j < p^s$ thus,

$$\frac{1 - \zeta}{1 - \zeta^i} = \frac{1 - \zeta^{ij}}{1 - \zeta^i} = 1 + \zeta^i + \cdots + \zeta^{ij-1} \in O_K.$$

Therefore $1 - \zeta^i$ and $1 - \zeta$ are associates in O_K and we may write

$$p = u(1 - \zeta)^{\phi(p^s)}$$

where u is a unit and $\phi(p^s)$ is the Euler *phi* function.
The prime $\lambda = (1 - \zeta)$ is above p and because of $r = 1$ the equation $ref = \phi(p^s)$ yields $f = 1$ and $e = \phi(p^s)$.

Theorem 2.3. *If $p|m$ and we write $n = p^s m$ with $\gcd(p, m) = 1$, then p factors in O_K in the form*

$$(p) = (\mathfrak{P}_1 \cdots \mathfrak{P}_r)^{\phi(p^s)}$$

where $\mathfrak{P}_1 \cdots \mathfrak{P}_r$ are distinct prime ideals of O_K of degree f, $fr = \phi(m)$ and f is the smallest positive integer such that $p^f \equiv 1 \bmod (m)$.

Proof. This is a double application of both cases where $p \not| m$ follows by $p|p^s$. □

We give an explicit factorization of the primes. This method is due to Dedekind. See [**S.L**] pp 27-28.

Proposition 1.1. Explicit factorization of primes
Let A be a Dedekind domain with quotient field K. Let E be a finite separable extension of K. Let B be the integral closure of A in E and assume that $B = A[\alpha]$ for some element α. Let $f(X)$ be the irreducible polynomial of α over K. Let $\mathfrak{p}$ be a prime of A. Let $\overline{f}$ be the reduction of f and $\mathfrak{p}$, and let

$$\overline{f}(X) = \overline{P}_1(X)^{e_1} \cdots \overline{P}_r(X)^{e_r}$$

be the factorization of $\overline{f}$ into powers of irreducible factors over $\overline{A} = A/\mathfrak{p}$ with leading coefficient 1. then

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

is the factorization of $\mathfrak{p}$ *in* B*, so that* e_i *is the ramification index of* $\mathfrak{P}_i$ *over* $\mathfrak{p}$*, and we have*

$$\mathfrak{P}_i = \mathfrak{p}B + P_i(\alpha)B,$$

if $P_i(X) \in A[X]$ *is a polynomial with leading coefficient 1 whose reduction* mod $\mathfrak{p}$ *is* $\overline{P_i}$.

The main theorem of the unit group is given by,

Theorem 2.4. The Dirichlet Unit Theorem.
Let (r, s) *be the signature of* K *then the group of units is a finitely generated Abelian group of rank* $r + s - 1$*. In other words, we have a group isomorphism*

$$U(K) \cong \mu(K) \times \mathbb{Z}^{r+s-1}$$

and $\mu(K)$ *is the finite cyclic group of the roots of unity in* K*.*

PROOF. See [**P.S**], and [**Min**]. □

Let first define $\varepsilon_1, \cdots, \varepsilon_t$ to be a basis of $\mathbb{Z}^{r+s-1}$, a unit u of K can be written in a unique way as

$$u = \pm\zeta^i \varepsilon_1^{n_1} \cdots \varepsilon_t^{n_t},$$

where ζ is root of unity, $1 \leq i \leq n, n_i \in \mathbb{Z}$. Such a family (ε_i) will be called a *system of fundamental units of* K . It is not unique though, since the changing of a $\mathbb{Z}$-basis of $\mathbb{Z}^{r+s-1}$ results in another basis by a matrix of determinant $+1$ or -1. It is however possible to have the (ε_i) real positive greater than 1, and in this case we have a *system of real fundamental units.*

Remark If K a cyclotomic field, it has even degree over $\mathbb{Q}$, and $r = 0$ and $s = \phi(n)/2$. If n is even then $\#\mu(K) = n$ otherwise $\#\mu(K) = 2n$

Remark The group of units of $K = \mathbb{Q}(\zeta_n)$ is a finitely generated Abelian group of rank $\frac{\phi(n)}{2} - 1$. $\mu(K)$ is the finite cyclic group of the roots of unity in K.

Let $n > 2$ be a prime. Though the existence of a system of $\frac{n-3}{2}$ fundamental units for cyclotomic fields is due to Dirichlet, they have been constructed explicitely and independently by Kronecker and Kummer. If $n > 2$, prime as before, then $N_{K/\mathbb{Q}}(\zeta^i + \zeta^{-i}) = \pm 1$, for $i \neq 0$
Put

$$\varepsilon_i = \zeta^i + \zeta^{-i} \quad \text{for} \quad 1 \leq i \leq \frac{n-3}{2}$$

and apply the above lemma.
Let the power symbol $\overline{x}$ denote the complex conjugate in $\mathbb{C}$. This is an automorphism. It is of order 2, so that the corresponding subfield K_1 is such that K/K_1 is of degree 2 and consequently $K_1/\mathbb{Q}$ is of degree $\phi(n)/2$. The field $\mathbb{Q}(\zeta + \zeta^{-1})$ is a real field which is pointwise fixed under complex conjugate automorphism so that $\mathbb{Q}(\zeta + \zeta^{-1}) \subset K_1$. Since ζ is a root of the polynomial $X^2 - (\zeta + \zeta^{-1})X + 1$ we have $K_1 = \mathbb{Q}(\zeta + \zeta^{-1})$.
K_1 is called the *maximal real subfield of* K and it will be denoted by K^+.

For n = 5, the real (quadratic) subfield is $K_1 = \mathbb{Q}(\zeta + \zeta^{-1})$ and from the equation

$$\zeta + \zeta^2 + \zeta^3 + \zeta^4 + 1 = 0,$$

a unit has the form $\zeta^i \varepsilon_1^k = u_k^i$. We can fix the complex embedding φ such that

$$\tau = \varphi(-\zeta^2 - \zeta^3) = \frac{1+\sqrt{5}}{2} > 1.$$

If p is an odd prime and g a primitive root modulo p, a classical result of Hilbert, [Hilbert Satz 142], says that:

$$\left(\frac{(1-\zeta^{g^{k+1}})(1-\zeta^{-g^{k+1}})}{(1-\zeta^{g^k})(1-\zeta^{-g^k})} \right)^{\frac{1}{2}}$$

form, for $k = 0, 1, 2, \cdots, \frac{p-3}{2}$, a system of fundamental units in the field $\mathbb{Q}(\zeta_p)$. For p not exceeding 161, these units form a system of fundamental units. This is no longer true for $p = 163$. A system of fundamental units related to the above formula was given by H. Vandivier [**V**]. J. Milnor conjectured that if $K = \mathbb{Q}(\zeta_n)$ with $\varphi(n) > 2$, then the units

$$\frac{\zeta_n^s - 1}{\zeta_n - 1}, \quad 2 \leq s < n/2$$

form a system of fundamental units for K. This conjecture was disproved by Ramachandra [**Ram**] who showed that if n has at least two distinct odd prime divisors, then the units from the last formula are multiplicatively dependent. However, if n is prime they are independent and then form together with ζ_n a subgroup of finite index in the group $U(K)$. Similar results were obtained by H. Bass,[**Ba**]

2. Power residue Symbol

We give a definition of the power residue symbol and basic properties that are of use in the definition and computation of Gauss sums. This will be defined in a general situation as possible.
Let k be a number field of finite degree containing ζ_n, a primitive n^{th} root of unity. Let O_k be the ring of integers of k. A prime ideal $\mathfrak{p}$ in O_k is said to be prime to n if and only if $q = N(\mathfrak{p})$ is such that $(q, n) = 1$. The residue class field at $\mathfrak{p}$, $\kappa = O_k/\mathfrak{p}$ is finite of order q. Let α, $\mathfrak{p} \in \mathbb{Z}[\zeta_n]$, where $\mathfrak{p}$ is prime with $\mathfrak{p} \not| \alpha$. Then $\mathbb{Z}[\zeta_n]/(\mathfrak{p})$ is a field with $N(\mathfrak{p})$ elements. Therefore, the analogue of the little Fermat theorem says:

$$\alpha^{N(\mathfrak{p})-1} \equiv 1 \pmod{\mathfrak{p}} \quad \text{and} \quad \mathfrak{p} \not| \alpha.$$

In the following steps we denote ζ_n simply by ζ.

Proposition 2.1. *Let* $\mathfrak{p}, \alpha \in \mathbb{Z}[\zeta]$ *with* $\mathfrak{p}$ *prime, and* $\gcd(N(\mathfrak{p}), n) = 1$ *and* $\mathfrak{p} \not| \alpha$. *Then there exists a unique integer* m, $0 \leq m \leq n-1$, *such that*

$$\alpha^{(N(\mathfrak{p})-1)/n} \equiv \zeta^m \pmod{\mathfrak{p}}.$$

PROOF. Indeed, for all primes $\mathfrak{p} \in \mathbb{Z}[\zeta]$ with $\gcd(N(\mathfrak{p}), n) = 1$ we have

$$n|(N(\mathfrak{p}) - 1).$$

Hence, we can write

$$\alpha^{N(\mathfrak{p})-1} - 1 = \prod_{i=0}^{n} (\alpha^{(N(\mathfrak{p})-1)/n} - \zeta^i).$$

But $\mathfrak{p}|(\alpha^{N(\mathfrak{p})-1} - 1)$ hence $\mathfrak{p}$ divides at least one of the factors on the right hand side. Suppose $\mathfrak{p}$ divides at least two of them, say

$$(\alpha^{(N(\mathfrak{p})-1)/n} - \zeta^i) \text{ and } (\alpha^{(N(\mathfrak{p})-1)/n} - \zeta^j) \text{ with } 0 \leq i < j < n.$$

Then $\mathfrak{p}|\zeta^i(1 - \zeta^{j-i})$, and thus $N(\mathfrak{p})|N(1 - \zeta^{j-i})$, since $\mathfrak{p}$ is not a unit and ζ primitive implies that $N(1 - \zeta^{j-i}) = n$ or ± 1, we deduce that $\gcd(N(\mathfrak{p}), n) \neq 1$ which contradicts the assumption. Therefore, there exists a unique power m such that

$$\alpha^{(N(\mathfrak{p})-1)/n} \equiv \zeta^m \mod (\mathfrak{p}).$$

□

Hence we can define the n^{th} residue symbol $\left(\frac{\alpha}{\mathfrak{p}}\right)_n$ to be the unique n^{th} root of unity such that

$$\alpha^{\frac{q-1}{n}} \equiv \left(\frac{\alpha}{\mathfrak{p}}\right)_n \mod \mathfrak{p},$$

whenever $(\alpha, \mathfrak{p}) = (1)$
We extend $\left(\frac{\alpha}{\mathfrak{p}}\right)_n$ as a multiplicative function of the ideals $\mathfrak{p}$ relatively prime to n i.e if $\mathfrak{a} = \prod \mathfrak{p}$ for such ideals $\mathfrak{p}$ then

$$\left(\frac{\alpha}{\mathfrak{a}}\right)_n = \prod \left(\frac{\alpha}{\mathfrak{p}}\right)_n.$$

Definition 2.7. For $\mathfrak{a}$ such that $(\mathfrak{a}, n) = 1$, $\left(\frac{\alpha}{\mathfrak{a}}\right)_n$ is well defined and is called the n^{th} power residue symbol.

Remark

- The residue symbol is a function of both arguments whenever it is defined.
- From the definition we see that if α is an n^{th} power, then $\left(\frac{\alpha}{\mathfrak{a}}\right)_n = 1$. This shows that, if α and β differ by a factor which is an n^{th} power and satisfy the necessary condition with $\mathfrak{p}$, then $\left(\frac{\alpha}{\mathfrak{p}}\right)_n = \left(\frac{\beta}{\mathfrak{p}}\right)_n$

In order to make this definition more general without any restriction to $(\alpha)+\mathfrak{a} = (1)$, we shall extend the definition to α such that

$$(\alpha) + \mathfrak{a} \neq (1) \text{ by } \left(\frac{\alpha}{\mathfrak{a}}\right)_n = 0$$

Consider furthermore K/k any other finite extension of the number field k. We assume k still contains the n^{th} roots of unity, then the n^{th} power residue symbol is

also a function depending upon the underlined field. The notation becomes $\left(\frac{\cdot}{\cdot}\right)_{n,F}$, where F is the underlying field. If K/k is a normal extension, then the Galois group Gal(K/k) acts on the power residue symbol $\left(\frac{\cdot}{\cdot}\right)_{n,k}$ and $\left(\frac{\cdot}{\cdot}\right)_{n,K}$. As we see it in the next proposition

Proposition 2.2. *Let K/k be a normal extension with Galois group G, and let k/F be a subextension such that a primitive n^{th} root of unity $\zeta_n \in k$.*

1. *For every $\sigma \in G$, we have $\left(\frac{\alpha}{\mathfrak{a}}\right)_{n,K}^{\sigma} = \left(\frac{\alpha^\sigma}{\mathfrak{a}^\sigma}\right)_{n,K}$, for all $\alpha \in K^*$ and all ideals $\mathfrak{a}$ prime to n.*
2. *if $\mathfrak{p}$ has inertia degree 1 in K/k, then $\left(\frac{\alpha}{\mathfrak{P}}\right)_{n,K}^{\sigma} = \left(\frac{\alpha}{\mathfrak{p}}\right)_{n,K}^{\sigma}$, where $\mathfrak{P}$ is a prime ideal in O_K above $\mathfrak{p}$ and $\alpha \in O_k$.*
3. *If K/k is Abelian and $\mathfrak{p}$ is a prime ideal in O_k, then $\left(\frac{\alpha}{\mathfrak{p}}\right)_{n,K} = \left(\frac{\alpha}{N\mathfrak{p}}\right)_{n,k}$, for all $\alpha \in O_K$, where $N = N_{K/k}$ denotes the relative norm.*
4. *Let K/k be a cyclic extension of degree $(K:k) = n$, and suppose that there is a prime ideal $\mathfrak{p} \not| nO_k$ such that $\mathfrak{p} = \mathfrak{P}^n$ is totally ramified in K/k. Then $\left(\frac{N_{K/k}\alpha}{\mathfrak{p}}\right)_{n,k} = 1$ for all $\alpha \in O_K - \mathfrak{P}$.*

Proof. See [**F-Lem**] pp 112. □

3. The primary choice of the prime factor in $\mathbb{Q}(\zeta_5)$

In this small section, we explain the construction of primality factor for prime in the cyclotomic field $\mathbb{Q}(\zeta_5)$. This, in fact turn out to be a general pattern. We will be using this kind of prime factors troughout the dissertation. We specialize the definition as follows:

Definition 2.8. Let $\pi|p$ be a prime above p, then we say that π is primary if

$$\pi \equiv 1 \bmod (1-\zeta)^3.$$

Let ζ be a primitive fifth root of unity in $K = \mathbb{Q}(\zeta_5)$. Then

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{5}) \subset K,$$

and $(\zeta - \zeta^2 - \zeta^3 + \zeta^4)^2 = 5$, therefore we can set $\sqrt{(}5) = (\zeta - \zeta^2 - \zeta^3 + \zeta^4)$. The ring of integer O_K is a unique factorization domain and its units are all of the form $\pm\zeta^i\tau^j$, for some integers i, j and where $\tau = -\zeta^2 - \zeta^3$, is a fundamental unit in $\mathbb{Q}(\sqrt{5})$.
If π is a prime of O_K, then O_π is the completion of O_K at π and K_π the respective fraction field. If we let $\lambda = 1 - \zeta$, thus λ generates the sole prime of O_K above 5. Therefore the λ-adic expansion of τ shows that

$$\tau \equiv -2 \bmod \lambda$$

and

$$\tau^2 \equiv -1 + \lambda^2 \bmod \lambda^3$$

We have the following lemma

Lemma 2.3. • *1 If α is an algebraic integer prime to λ, then there is an associate α^* of α such that*

$$\alpha^* \equiv 1 \bmod \lambda^3$$

- *2 If α_1^* and α_2^* are two associates congruent to 1 modulo λ^3, then their ratio is a fifth power of a unit in O_K.*
- *3 Let $n \in \mathbb{Z}$ be prime to 5. Then any associate n^* of n with*

$$n^* \equiv 1 \bmod \lambda^3$$

is n times a fifth power of a unity in O_K.

PROOF. • 1- Let $\alpha \in \mathbb{Z}[\zeta]$, the λ-adic expansion of α shows that $\alpha \equiv n \bmod \lambda$, $n \in \mathbb{Z}/(5)$ and λ prime to α implies that $n \not\equiv 0 \bmod 5$, thus we can assume $n > 0$. Since τ is a primitive root modulo 5, there exists j, $0 \leq j < 4$ such that

$$\tau^j n \equiv 1 \bmod \lambda.$$

Moreover $\tau^2 \equiv -1 \mod \lambda$ and so, there exist $0 \leq i, j \leq 1$ so that

$$(-1)^i \tau^j \alpha \equiv 1 \bmod \lambda.$$

Then

$$(-1)^i \tau^j \alpha \equiv 1 + m\lambda \bmod \lambda^2$$

and we can assume $0 \leq m \leq 4$. From this restriction follows that

$$\zeta^m (-1)^i \tau^j \alpha \equiv 1 \bmod \lambda^2.$$

Let

$$\zeta^m (-1)^i \tau^j \alpha \equiv 1 + \ell\lambda^2 \bmod \lambda^3.$$

Since $-\tau^2 \equiv 1 - \lambda^2$, we deduce that

$$(-\tau)^{2\ell} \zeta^m (-1)^i \tau^j \alpha \equiv 1 \bmod \lambda^3,$$

for $0 \leq \ell \leq 4$, i.e

$$(-1)i + \ell\zeta^m (-1)^i \tau^{j+2\ell} \alpha \equiv 1 \bmod \lambda^3.$$

- 2- If λ_1^* and λ_2^* are two such associates, then their ratio is a unit. Since both λ_1^* and λ_2^* are congruent to 1 modulo λ^3 their ratio

$$u = \frac{\lambda_1^*}{\lambda_2^*}$$

is also congruent to 1 mod λ^3.
Since $-\tau^{10} \equiv 1 \bmod \lambda^3$ i.e $(-\tau^2)^5 \equiv 1 \bmod \lambda^3$, we consider

$$u = (-1)^i \tau^j \zeta^k (-\tau^2)^l (-\tau^{10})^m$$

modulo λ, λ^2 yields (by 1) $i = j = 0$ and $k = l = 0$ since

$$0 \leq i, j, k, l \leq 4.$$

u is then a tenth power of a unit and a fortiori a fifth power.

- 3- Since $n^4 \equiv 1 \bmod 5$, and $n^{*4} \equiv 1 \bmod \lambda^3$ is an associate of n^4, by 2), $(\frac{n}{n^*})^4$ is a fifth power of a unit, so dividing by $(\frac{n}{n^*})^5$, shows that $\frac{n}{n^*}$ is a fifth power of a unit and therefore 3 falls.

□

The ring $\mathbb{Z}[\zeta]$ is a unique factorization domain and $K^+ = \mathbb{Q}(\sqrt{5})$. Thus every prime $p \equiv 1 \bmod 5$ is the norm of some prime $\pi \in O_K$, and $4p = a^2 - 5b^2$ for some rational integers, a, b.

Lemma 2.4. *If $4p = a^2 - 5b^2$, with a, b in $\mathbb{Z}$, and if $\pi \in O_K$ is a prime divisor of*

$$x = \frac{a + b\sqrt{5}}{2} \qquad \text{in} \qquad O_K$$

then there exists an associate of π in O_K whose norm in K/K^+ is $\pm x$.

Proof. The norm of $x \in K^+/\mathbb{Q}$ is p, which splits as a product of 4 primes in $\mathbb{Z}[\zeta]$. Since $\mathbb{Z}[\zeta]$ is a unique factorization domain, x is, to within a unique factor $u \in K^+$, the product of a prime π and its conjugate $\overline{\pi}$. Thus $x = uN_{K/K^+}(\pi)$, and upon taking the norm of both sides in $K^+/\mathbb{Q}$, one gets $N_{K^+/\mathbb{Q}}(\gamma) = 1$. Since K^+ is a quadratic field in which a generator of the unit group is $\gamma = \zeta + \zeta^{-1}$, one has $u = \pm\gamma^k$ with $k \in \mathbb{Z}$. Also, since $N_{K^+/\mathbb{Q}}(u) = -1$, it follows that $k = 2j$ for some integer j. Noting that $\gamma^2 = \mathrm{N}_{K/K^+}(1-\zeta^2)$, it follows that $x = \pm N_{K/K^+}((1-\zeta^2)^j\pi)$, and hence the result. □

CHAPTER 3

GAUSS SUMS

1. Gauss sums in number fields

Let I be a non zero ideal in the ring of integers O_K and define $\mathfrak{D}(K/\mathbb{Q})$ the different of O_K. The trace of $\alpha \in K$ is

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \textstyle\sum_{\sigma \in Gal(K/\mathbb{Q})} \sigma(\alpha)$$

This is rational integer if $\alpha\mathfrak{D}(K/\mathbb{Q})$ is an integral ideal.
Let a be a fixed number lying in the fractional ideal $(I\mathfrak{D}(K/\mathbb{Q}))^{-1}$. If χ is any character of $G[I]$, the set of invertible elements modulo I, then the Gauss sum corresponding to the pair (χ, a) is:

$$G(\chi, a) = \sum_{x \bmod I} \chi(x) \exp\left(2\pi i Tr_{K/\mathbb{Q}}(ax)\right).$$

Proposition 1.1. *The sum*

$$\sum_{x \bmod I} \chi(x) \exp\left(2\pi i Tr_{K/\mathbb{Q}}(ax)\right)$$

does not depend on the residue classes modulo I.

Proof. Let X and Y be two sets of residues modulo I, then for all $x \in X$ and all $y \in Y$, if x and y are such that $x \equiv y \bmod I$, $x, y \in O_K$ then $\chi(x) = \chi(y)$. But we can write $ax = ay + a(x-y)$, such that $Tr_{K/\mathbb{Q}}(ax) = Tr_{K/\mathbb{Q}}(ay) + Tr_{K/\mathbb{Q}}(a(x-y))$. But $a(x-y) \in \mathfrak{D}(K/\mathbb{Q})^{-1}$ therefore we get $\mathrm{Tr}_{K/\mathbb{Q}}(a(x-y)) \in \mathbb{Z}$.
Thus $\exp\left(2\pi i Tr_{K/\mathbb{Q}}(ax)\right) = \exp(2\pi i \mathrm{Tr}_{K/\mathbb{Q}}(ay))$. □

Remark

- For $K = \mathbb{Q}$ then I is a principal ideal generated by some $n \in \mathbb{Z}$. If $k \in \mathbb{Z}$ and $a \in \mathbb{Q}$ are such that $k = an$, the we denote this sum by

  $$\tau_k(\chi) = \sum_{x \bmod n} \chi(x) exp(2\pi i k x/n).$$

  We denote $\tau_1(\chi)$ simply by $\tau(\chi)$.
- If $a \equiv b \bmod I$ then $\tau_a(\chi) = \tau_b(\chi)$.

Proposition 1.2. *If b is an integer of O_K prime to the ideal I,then*

$$G(\chi, ab) = \overline{\chi}(b) G(\chi, a).$$

In particular, if $K = \mathbb{Q}$, $I = n\mathbb{Z}$ with n a natural number and $a = k/n$ with $(k, n) = 1$, then

$$\tau_a(\chi) = \overline{\chi}(k)\tau(\chi).$$

PROOF. Let b be defined as before. Since b is prime to I then b is invertible modulo I and multiplication by b on the set of residues modulo I is an isomorphism between the two sets both of which are sets of residues modulo I. Furthermore the Gauss sums does not depend on the set of residues modulo I, so that:

$$G(\chi, ab) = \sum_{x \bmod I} \chi(x) \exp(2\pi i \mathrm{Tr}_{K/\mathbb{Q}}(abx)) \tag{1.1}$$

$$= \sum_{y \bmod I} \chi(yb^{-1}) \exp(2\pi i \mathrm{Tr}_{K/\mathbb{Q}}(ay)) \tag{1.2}$$

$$= \chi(b^{-1}) \sum_{y \bmod I} \chi(y) \exp(2\pi i \mathrm{Tr}_{K/\mathbb{Q}}(ay)) \quad y = b^{-1} \tag{1.3}$$

$$= \overline{\chi(b)} G(\chi, a). \tag{1.4}$$

(1.5)

□

Remark From this proposition we know that the Gauss sums for a fixed character χ of $G[I]$ are fully determined by $G(\chi, 1)$.

Proposition 1.3. *Let $I = I_1 \cdots I_r$ be a factorization of I into factors relatively prime in pairs and let $\chi = \chi_1 \cdots \chi_r$ be the factorization of the character χ of $G[I]$. If a lies in $I^{-1}\mathfrak{D}(K/\mathbb{Q})^{-1}$ and for $i = 1, 2, \cdots, r$ the elements a_i belong to $I_i^{-1}\mathfrak{D}(K/\mathbb{Q})^{-1}$ and satisfy $a - a_i \in J_i^{-1}\mathfrak{D}(K/\mathbb{Q})^{-1}$ with $J_i = I/I_i$ then*

$$G(\chi, a) = \prod_{i=1}^{r} G(\chi_i, a_i).$$

PROOF. Let $x \in O_K$, relatively prime to I. Choose $x_i \in O_K$ with $x_i \equiv x \bmod I_i$. Choose $x_i \equiv 1 \bmod I_j$ for $i \neq j$. This is a consequence of the Chinese remainder theorem whose proof is given in the appendix. Then we will have for elements $y_1, \cdots, y_r \in O_K$ such that, $y_i \equiv 1 \bmod I_i$ and $y_i \in I_j$ for $j \neq i$,

$$x_1 y_1 + \cdots + x_r y_r \equiv x \bmod I$$

and thus

$$G(\chi, a) = \sum_{\substack{x \in G[I_i] \\ i=1,\cdots,r}} \chi_1(x_1) \cdots \chi_r(x_r) \exp\left(2\pi i Tr_{K/\mathbb{Q}}(ax)\right)$$

$$= \prod_{i=1}^{r} \sum_{x \in G[I_i]} \chi_1(x_1) \cdots \chi_r(x_r) exp(2\pi \mathrm{Tr}(ax_i y_i)))$$

$$= \prod_{i=1}^{r} \sum_{x \in G[I_i]} \chi_1(x_1) \cdots \chi_r(x_r) exp(2\pi \mathrm{Tr}(a_i x_i y_i))$$

since $ax_iy_i - a_ix_iy_i \in D_{K/\mathbb{Q}}^{-1}$ and consequently, the latest equality is equal

$$\prod_{i=1}^{r} G(\chi_i, a_i)$$

because $\chi_i(y_i) = 1$. □

Corollary 1.4. *Let $n = n_1 \cdots n_r$ be the factorization of a natural number n into mutually prime factors, let χ be a character of $G[n\mathbb{Z}]$ (which group we shall for convenience denote it again by $G[n]$) and let $\chi = \chi_1 \cdots \chi_r$ be its factorization into characters of $G[N]$. Then we have the equality*

$$\tau(\chi) = \prod_{i=1}^{r} \chi_i(n/n_i) \prod_{i=1}^{r} \tau(\chi_i).$$

PROOF. Take $a = 1/n$ and apply the last 3 propositions. □

Corollary 1.5. *If $\gcd(a, I) \neq (1)$ and χ is a primitive character modulo I, then*

$$G(\chi, a) = 0$$

PROOF. Let

$$\gcd(a, I) = I_1 \text{ and } \alpha \equiv 1 \bmod \frac{I}{I_1}, \text{ with } \gcd(\alpha, f) = (1),$$

then

$$a\alpha \equiv a \bmod I.$$

Thus

$$G(\chi, a\alpha) = \overline{\chi}(\alpha) G(\chi, a) = G(\chi, a)$$

therefore it follows that

$$(1 - \chi(\alpha)) G(\chi, a) = 0$$

We have to show that at least one α satisfies $\chi(\alpha) \neq 1$. Now suppose that the conditions on α extend to all residue classes modulo f, then at least one of them satisfies $\chi(\alpha) \neq 1$ otherwise χ is a character modulo $\frac{I}{I_1}$ which contradicts the hypothesis that χ is primitive modulo I. For this value of α we have $(1 - \chi(\alpha))G(\chi, a) = 0$ implies $G(\chi, a) = 0$. □

We define here the local Gauss sum.
Let F be a finite extension of the p-adic field $\mathbb{Q}_p$ and $\mathfrak{P}$ the prime ideal above (p). If we denote $U = U_0 = O_F^{\times}$ the group of local units of F and $U_n = 1 + \mathfrak{P}^n$ $n > 0$ the n^{th} unit group of F, then for any multiplicative character χ of F, $ker(\chi)$ contains at least a U_m for some integer $m \geq 0$. Since the sequence of the (U_n) is decreasing, m is chosen smallest such that $U_m \subset ker(\chi)$ then $f_\chi = \mathfrak{P}^m$ is called *conductor of* χ. If $m = 0$ we say that χ is *unramified, otherwise it is ramified. In both cases we have different consequences for the definition of χ. If χ is ramified, then $\chi(x) = 0$ for all $x \in F$ however for χ unramified, we consider χ as a function on the group of fractional ideals $\mathfrak{I} = F^{\times}/U$.*
If λ is any additive character of F which is trivial on $\mathbb{Z}_p$ then, we define the local Gauss sum as follow:

Definition 3.1. The local Gauss sums is

$$\tau(\chi, a) = \sum_{\substack{x \in U \\ x \bmod 1 + f_\chi}} \chi(x) \exp(2\pi i \lambda(Tr_{F/\mathbb{Q}_p}(a^{-1}x)))$$

where $a \in F^{\times}$ is such that $(a) = f_\chi \mathfrak{D}_F$ and $\mathfrak{D}_F$ is the local different of $F/\mathbb{Q}_p$.

Remark

- $\tau(\chi, a)$ *does not depend on the choice of the residue* $\bmod(1 + f_\chi)$.
- *If* χ *is unramified, then the residue class modulo* $1 + f_\chi$ *is restricted to a single element, therefore* $\tau(\chi, a) = \chi(\mathfrak{D}_F)$. *This means that* $\tau(\chi, a)$ *is a root of unity, since* χ *is of finite order.*

One of the most important properties for these definitions of Gauss sums is the following.

Proposition 1.6. *Let* $\mathfrak{P}$ *be a non zero prime ideal of* O_K *and* χ *a primitive character of* $G[\mathfrak{P}^N]$. *Let* $\mathfrak{P} = \mathfrak{P}_1, \mathfrak{P}_2, \cdots, \mathfrak{P}_g$ *be all the prime ideals of* O_K *lying above the ideal* $p\mathbb{Z} = \mathfrak{P} \cap \mathbb{Z}$, *denote by* $\mathfrak{P}^m$ *the maximal power of* $\mathfrak{P}$ *dividing the different* $\mathfrak{D}(K/\mathbb{Q})$. *We choose an element* Π *of* K *such that* $\Pi O_K = \mathfrak{P}_1 I^{-1}$, $I \subset O_K$, $\mathfrak{P}_1 \nmid I$. *If we denote the character of* $U(K_\mathfrak{P})/U_N(K_\mathfrak{P})$ *induced by* χ *by the same letter and put* $a = \Pi^{-m-N}$, *the Gauss sum* $G(\chi, a)$ *coincides with the Gauss sum* $\tau(\chi, a)$.

Proof. This proof is essentially based on the relation from local to global argument. In fact the global trace is the sum of local traces, such that

$$Tr_{K/\mathbb{Q}}(x) = \sum_{i=1}^{g} T_{K_{\mathfrak{P}_i}/\mathbb{Q}_p}(x).$$

Moreover, for $x \in K$ with $(xO_K, \mathfrak{P}_2 \cdots \mathfrak{P}_g) = (1)$ the quotient x/Π^{m+N} is an integral element in $K_{\mathfrak{P}_i}$ for $i = 2, \cdots, g$; thus

$$exp(2\pi(i\lambda(Tr_{K/\mathbb{Q}}(\Pi^{-m-N}x)))) = 1$$

for $i = 2, \cdots, g$. In fact $Tr_{K/\mathbb{Q}}(\Pi^{-m-N}x)$ is a rational number whose denominator is a power of p, whence $\lambda(Tr_{K/\mathbb{Q}}(\Pi^{-m-N}x))$ coincides with the fractional part of $Tr_{K/\mathbb{Q}}(\Pi^{-m-N}x)$ and this leads to

$$exp(Tr_{K/\mathbb{Q}}(2\pi i\Pi^{-m-N}x)) = exp(2\pi i\lambda(Tr_{K_{\mathfrak{P}_1}/\mathbb{Q}_p}(\Pi^{-m-N}x))).$$

We then apply once more the Chinese Remainder Theorem to choose a suitable set of representatives $x_1, \cdots x_k$ of $G[\mathfrak{P}^N]$ that satisfies $(xO_K, \mathfrak{P}_2 \cdots \mathfrak{P}_g) = (1)$. This representative system of $G[\mathfrak{P}^N]$ is also a representative system of $U(K_{\mathfrak{P}_1})/U_N(K_{\mathfrak{P}_1})$. Thus for $a = \Pi^{-m-N}$, we deduce from the equality above that

$$G(\chi, a) = \sum_{i=1}^{k} \chi(x_i) exp(2\pi i\lambda(Tr_{K_{\mathfrak{P}_1}/\mathbb{Q}_p}(\Pi^{-m-N}x))) = \tau(\chi, a).$$

□

Corollary 1.7. *Let* χ *be a primitive character of* $G[\mathfrak{P}^n]$, *let* $\mathfrak{P}^m$ *be the maximal power of* $\mathfrak{P}$ *which divides* $\mathfrak{D}(K/\mathbb{Q})$ *and finally let* a *be any element of* $\mathfrak{P}^{-m-N} - \mathfrak{P}^{-m-N+1}$. *Then the Gauss sum* $G(\chi, a)$ *differs from* $\tau(\chi, 1)$ *only by a factor which is a root of unity.*

Proof. Let Π be a uniformizer of $\mathfrak{P}$, then if b is an element of $K_\mathfrak{P}$ such that b and b^{-1} are integral in $K_\mathfrak{P}$, then for every c in $\mathfrak{P}^{-m-N}$ the sums $G(\chi, c)$ and $G(\chi, bc)$ differ by a factor which is a root of unity. Thus choose b to be a/Π^{-m-N} and $c = \Pi^{-m-N}$. □

Corollary 1.8. *Let $I = \prod_{i=1}^{r} \mathfrak{P}_i^{N_i}$ and for any $i = 1, \cdots, r$ let $\mathfrak{P}_i^{m_i}$ be the maximal power of $\mathfrak{P}_i$ which divides the different $D_{K/\mathbb{Q}}$. Moreover, let $n_i(\mathfrak{P}_\mathfrak{i})$ be the exponent corresponding to the prime ideal $\mathfrak{P}_i$. If a is an element of $I^{-1}D_{K/\mathbb{Q}}^{-1}$, which satisfies $n_i(a) = -m_i - N_i$ for $i = 1, 2, \cdots, r$ and χ is a primitive character of $G[I]$, then*

$$|G(\chi, a)| = N(I)^{1/2}.$$

Proof. We have proved that $G(\chi, a)$ can split as a product of $G(\chi_i, a_i)$ for suitable primitive characters χ_i defined on $G[{\mathfrak{P}_\mathfrak{i}}^{N_i}]$, and integers a_i. To prove our theorem, you need to do it only locally for $I = \mathfrak{P}_i^N$.

- If χ is unramified, then the conductor of χ is $I = (1)$ and therefore
$$G(\chi, a)\overline{G(\chi, a)} = \chi(\mathfrak{D}_F)\overline{\chi(\mathfrak{D}_F)} = 1.$$
- If χ is ramified, then the conductor of χ is $I = \mathfrak{P}^n$.

$$\begin{aligned} G(\chi, a)\overline{G(\chi, a)} &= \sum_{x,y \in O^\times/U_n} \chi(x) \exp(2\pi i\lambda(Tr_{F/\mathbb{Q}_p}(a^{-1}x)))\overline{\chi(y) \exp(2\pi i\lambda(Tr_{F/\mathbb{Q}_p}(a^{-1}y)))} \\ &= \sum_{x,y \in O^\times/U_n} \chi(xy)\chi^{-1}(ya^{-1}) \exp(2\pi i\lambda(Tr_{F/\mathbb{Q}_p}(a^{-1}(xy - y)))) \\ &= \sum_{x,y \in O^\times/U_n} \chi(x) \exp(2\pi i\lambda(Tr_{F/\mathbb{Q}_p}(a^{-1}y(x - 1)))) \end{aligned}$$

furthermore

$$\begin{aligned} \sum_{y \in O^*/U_n} \exp(2\pi i\lambda(Tr_{F/\mathbb{Q}_p}(a^{-1}y(x - 1)))) &= \sum_{y \in O/\mathfrak{P}^n} \exp(2\pi i\lambda(Tr_{F/\mathbb{Q}_p}(a^{-1}y(x - 1)))) \\ &- \sum_{y \in \mathfrak{P}/\mathfrak{P}^n} \exp(2\pi i\lambda(Tr_{F/\mathbb{Q}_p}(a^{-1}y(x - 1)))). \end{aligned}$$

On the one hand,

$$\begin{aligned} \sum_{y \in O/\mathfrak{P}^n} \exp(2\pi i\lambda(Tr_{F/\mathbb{Q}_p}(a^{-1}y(x - 1)))) &= 0 \quad if x \not\equiv 1 \bmod \mathfrak{P}^n \\ &= N_{F/\mathbb{Q}_p}(\mathfrak{P})^n = N_{F/\mathbb{Q}_p}(I), \quad otherwise. \end{aligned}$$

on the another hand

$$\begin{aligned} \sum_{y \in \mathfrak{P}/\mathfrak{P}^n} \exp(2\pi i\lambda(Tr_{F/\mathbb{Q}_p}(a^{-1}y(x - 1)))) &= \sum_{y \in O/\mathfrak{P}^{n-1}} \exp(2\pi i\lambda(Tr_{F/\mathbb{Q}_p}(a^{-1}y\Pi(x - 1)))) \\ &= 0 \quad if x \not\equiv 1 \bmod \mathfrak{P}^{n-1} \\ &= N_{F/\mathbb{Q}_p}(\mathfrak{P})^{n-1} \quad otherwise. \end{aligned}$$

where Π is a uniformizer for $\mathfrak{P}$.
It then follows that

$$G(\chi, a)\overline{G(\chi, a)} = N_{F/\mathbb{Q}_p}(\mathfrak{P}^n) - \sum_{x \in U_{n-1}/U_n} \chi(x) N_{F/\mathbb{Q}_p}(\mathfrak{P}^{n-1}).$$

Since

$$\sum_{x \in U_{n-1}/U_n} \chi(x) = 0, \qquad \text{by mean of character relation,}$$

the assertion then follows.

□

Corollary 1.9. *If χ is a primitive character of $G[I]$, then*

$$G(\overline{\chi}, a) = \chi(-1)\overline{G(\chi, a)}$$

PROOF. This is just a consequence of the above corollary. □

Remark *Let $\mathfrak{P} = (p)$ prime ideal in $\mathbb{Z}$ and $I = p^r$, χ defined as before. We put again*

$$\zeta = \zeta_{p^r} = \exp(\frac{2\pi i}{p}).$$

Then

$$G(\chi, a) = \sum_{x \bmod p^r} \chi(x)\zeta^{ax}.$$

We then have the following proposition.

Theorem 3.1. *For $a \not\equiv 0 \mod p$ $G(\chi, a) = 0$ if and only if $r > 0$ and χ is not a primitive character modulo p^r.*

PROOF. It is necessary to prove this theorem for $a = 1$.
For $r = 1$, χ must either be primitive or else be a principal character modulo p, where in the later case

$$G(\chi, 1) = \zeta^1 + \zeta^2 + \cdots + \zeta^{p-1} = -1 \neq 0.$$

For the remainder of the proof, we assume that $r \geq 1$ and that χ is primitive if $r = 1$.

$$|G(\chi,1)|^2 = \sum_{x \bmod p^r} \chi(x)^{-1}\zeta^{-x} \sum_{y \bmod p^r} \chi(y)\zeta^{y} \tag{1.6}$$

$$= \sum_{x,y} \chi(x^{-1}y)\zeta^{y-x} \tag{1.7}$$

$$= \sum_{\substack{x \bmod p^r \\ x \not\equiv 0 \bmod p}} \sum_{t \bmod p^r} \chi(t)\zeta^{tx-x} \text{ where } t = x^{-1}y \tag{1.8}$$

$$= \sum_{t} \sum_{x \not\equiv 0 \bmod p} \zeta^{x(t-1)} \tag{1.9}$$

$$= \sum_{t \bmod p^r} \chi(t) \sum_{x \bmod p^r} \zeta^{x(t-1)} - \sum_{t \bmod p^r} \chi(t) \sum_{z \bmod p^{r-1}} \zeta^{pz(t-1)} \tag{1.10}$$

In the first term if $t \not\equiv 0 \bmod p^r$, the sum on x vanishes, therefore the first term sums to p^r. In the same way, when $r > 1$ and $t \not\equiv 0 \bmod p^{r-1}$, the sum on z is zero.

It then follows that,

$$|G(\chi,1)|^2 = p^r - p^{r-1} \sum_{\substack{t \bmod p^r \\ t\equiv 1 \mod p^{r-1}}} \chi(t).$$

When $r = 1$ and χ is primitive, the sum is the same as $\sum_{x \bmod p} \chi(t)$ which is zero. When $r > 1$ and χ is primitive, the sum is again zero, because in this case the restriction of χ on the subgroup $\{t \equiv 1 \bmod p^{r-1}\}$ of $G[P^r]$, is a non trivial character. Finally if $r > 1$ and χ is not primitive, then χ is certainly trivial on $\{t \equiv 1 \bmod p^{r-1}\}$, so that the last sum is p. □

In the next properties we suppose without loss of generality that the ideal I is a prime ideal $\mathfrak{P}$ and χ is Dirichlet character $\bmod \mathfrak{P}$ *of order m. We must then observe that in the Gauss sums, we sum over the set of residues* $\bmod \mathfrak{P}$*, therefore $G[\mathfrak{P}] \equiv (\mathbb{Z}[\zeta]/\mathfrak{P})^*$. Since $\mathbb{Z}[\zeta]/\mathfrak{P}$ is a field with $p^n = q = N_{K(\zeta)/\mathbb{Q}}(\mathfrak{P})$ elements, it is isomorphic to $\mathbb{F}_q$. We then use this isomorphism to look at functions on $\mathbb{Z}[\zeta]/\mathfrak{P}$ as functions defined on $\mathbb{F}_q$, so that we can see characters on $G[\mathfrak{P}]$ as characters on the multiplicative group $\mathbb{F}_q^*$.*

Remark *: Since* $\gcd(q-1,q) = 1$*, then $\mathbb{Q}(\zeta_{q-1},\zeta_q) = \mathbb{Q}(\zeta_{q-1})\mathbb{Q}(\zeta_q)$. Therefore the Galois group $Gal(\mathbb{Q}(\zeta_{q-1},\zeta_q)/\mathbb{Q})$ is equal to the direct product $Gal(\mathbb{Q}(\zeta_{q-1})/\mathbb{Q}) \times Gal(\mathbb{Q}(\zeta_q)/\mathbb{Q})$. This means that a $\mathbb{Q}$-automorphism of $\mathbb{Q}(\zeta_{q-1},\zeta_q)/\mathbb{Q})$ is of the form (σ,τ) where $\sigma \in Gal(\mathbb{Q}(\zeta_{q-1})/\mathbb{Q})$ leaves invariant ζ_q and $\tau \in Gal(\mathbb{Q}(\zeta_q)/\mathbb{Q})$ leaves invariant ζ_{q-1}. This actually has an effect on the Gauss sums.*

Let χ be a non trivial primitive Dirichlet character modulo $\mathfrak{P}$ of order $m|q-1$ and $a \in K$ is such that $a\Pi \in O_K$, where Π generates $\mathfrak{P}$ in $K = \mathbb{Z}[\zeta_m]$.

Proposition 1.10. 1 *- The Gauss sum $G(\chi,a)$ is an algebraic integer in $\mathbb{Q}(\zeta_m,\zeta_q)$.*

2 *- $\sigma.G(\chi,a) = G(\chi^c,a)$ and $\tau.G(\chi,a) = G(\chi,ab)$ where σ is the automorphism of $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ that maps $\zeta_m \to \zeta_m^c$ for $c \in G[m]$ and τ is the isomorphism of $\mathbb{Q}(\zeta_q)/\mathbb{Q}$ that maps $\zeta_q \to \zeta_q^b$ for some $b \in \mathbb{F}_p^*$.*

3 *- $G(\chi,a)^m$ is an algebraic integer in $\mathbb{Q}(\zeta_m)$ independent of $a \neq 0$.*

4 *- $G(\chi,a)^m$ and $G(\chi',a)^m$ are conjugate in $\mathbb{Q}(\zeta_m)$ if χ and χ' are characters of the same order dividing m.*

Proof. 1) It is a simple observation that the Gauss sum is a sum of the product of ζ_m and ζ_q and both are algebraic integers in $\mathbb{Q}(\zeta_m,\zeta_q)$.

2) It is a simple fact. $\chi(x)$ is an m^{th} root of unity which is left invariant under the τ and $\exp(2\pi i \mathrm{Tr}_{K/\mathbb{Q}}(x))$ is a q^{th} root of unity which is invariant under σ. Since $\chi^\sigma(x) = \sigma(\chi(x)) = (\chi(x))^c$ are non-trivial and since $\tau.G(\chi,a) = G(\chi,ba)$ the assertion follows

3) From 2) we see that

$$\tau.(G(\chi,a))^m = (\tau G(\chi,a))^m = (\chi(b)^{-1}G(\chi,a))^m = G(\chi,1)^m,$$

since $\chi(b)$ is an m^{th} root of unity. Therfore $G(\chi,a)$ is invariant under $Gal(\mathbb{Q}(\zeta_p/)\mathbb{Q})$

4) this a consequence of 2) and 3).

□

Remark *From the following propositions, we see that, for primitive characters modulo an ideal I of order m, we know the absolute norm of the Gauss sum, and that its m^{th} power is an algebraic integer in the field $\mathbb{Q}(\zeta_m)/\mathbb{Q}$. Since we know the decomposition law in this cyclotomic field, we would attempt to describe the decomposition of this Gauss sum in this field. According to the multipcative properties, we will do this only for ideals I prime. While looking for the factorization of the m^{th} power of the Gauss sum, we do not need to consider the action of $\tau \in Gal(\mathbb{Q}(\zeta_q)/\mathbb{Q})$, therefore one can describe this when q is a prime.*

2. Factorization of Gauss sums

We have already noticed that for Dirichlet character χ of prime conductor the integral ideal generated by the m^{th} power of Gauss sum lies in the subring of $\mathbb{Z}[\zeta_{p(q-1)}]$, precisely in the ring $O_K = \mathbb{Z}[\zeta_m]$. Its norm is a power of a prime p and therefore factors of p in O_K appear in its decomposition. One should ask the question which of the factors of p and for each of the factors, with what power does it occur. This involves the $\Pi-$adic analysis of the Gauss sums which was completely explained by Stickelberger [**S.L**]*, pp. 6-13.*

Theorem 3.2. *Let $\mathfrak{p}|p$ be a prime ideal in O_K and χ the corresponding Dirichlet character of order m prime to p. Then*

$$(G(\chi,1))^m = \mathfrak{p}^{\sum_{(t,m)=1} t\sigma_t^{-1}},$$

where σ_t maps $\zeta = \zeta_m$ to ζ^t with $\gcd(t,m) = 1$.
We set without loss of generality that $\zeta_m = \exp(2\pi i/m)$

Let $\mathfrak{P}|\mathfrak{p}$ be a prime divisor of the ideal (p) in the ring of integers $\mathbb{Z}[\zeta_{p(q-1)}]$, and consider the residue class field $\kappa = \{0, 1, g, \cdots, g^{q-2}\}$ where $g = \zeta_{q-1} + \mathfrak{P}$. Let $a \in \{1, 2, \cdots, q-2\}$. A theorem of Stickelberger, see [**S.L**] *or* [**I.R**] *chapter 11, states that the highest power of $\mathfrak{P}$ dividing the ideal generated by the Gauss sum*

$$\sum_{i=0}^{q-2} \zeta_{q-1}^{-ai} \zeta_p^{Tr(g^i)}$$

is equal to the digit sum $s_p(a)$ in the p-adic expansion of a. Since $\mathbb{F} = F_q$ and κ are isomorphic fields, there exists a primitive element γ in $\mathbb{F}$ which is mapped onto g under the isomorphism. Now the character χ, defined by $\chi(\gamma) = \zeta_{q-1}$ is a multiplicative character of order $q-1$ of $\mathbb{F}$. Thus the highest power of $\mathfrak{P}$ dividing $(G(\overline{\chi}^a))$ is equal to $s_p(a)$.
Let $a = (q-1)/N$ for some divisor N of $q-1$. Since $G(\overline{\chi}^a) \in \mathbb{Q}(\zeta_N)$ and $G(\overline{\chi}^a)\overline{G(\overline{\chi}^a)} = p^m$, the only possible divisors of the ideal $(G(\chi))$ in $\mathbb{Z}[\zeta_N]$ are the prime divisors of (p). Let $(p) = \prod_{i=1}^{t} P_i$ and $(p) = \prod_{i=1}^{t_1} \mathfrak{P}_i^{p-1}$, with $t = \varphi(N)/ord_N(p)$ and $t_1 = \varphi(q-1)/m$, be the prime ideal decomposition of (p) in $\mathbb{Z}[\zeta_N]$ and in $\mathbb{Z}[\zeta_{p(q-1)}]$, respectively. This refers to the factorization of primes in cyclotomic fields. It then follows that $ord_{\mathfrak{P}_i}(P_i\mathbb{Z}[\zeta_{p(q-1)}]) = p-1$, for $i = 1, \cdots, t$. By lifting the prime ideal decomposition of the ideal $G(\overline{\chi}^a)\mathbb{Z}[\zeta_N]$ into $\mathbb{Z}[\zeta_{p(q-1)}]$, we obtain

$(p-1)ord_P(G(\overline{\chi}^a)) = ord_{\mathfrak{P}}G(\overline{\chi}^a)$ *for some* $P \in \{P_1, \cdots, P_g\}$, *since* $P_i\mathbb{Z}[\zeta_{p(q-1)}]$ *and* $P_j\mathbb{Z}[\zeta_{p(q-1)}]$ *are relatively prime for* $i \neq j$. *Therefore,* $ord_P(G(\overline{\chi}^a)) = s_p(a)/(p-1)$. *Let* P' *be another prime divisor of* $(G(\overline{\chi}^a))$ *in* $\mathbb{Z}[\zeta_N]$. *We know that* $P' = \sigma_i^{-1}(P)$ *for* $\sigma_i \in Gal(K/\mathbb{Q})$ *(see* [**I.R**] *chap.12). Furthermore,* $\sigma_1(P) = \sigma_2(P)$ *if and only if* $\sigma_2^{-1}\sigma_1 \in G_p = \{\sigma \in Gal(K/\mathbb{Q}) | \sigma(P) = P\} \subset Gal(\mathbb{F}/\mathbb{Q})$. *Thus* $P' = \sigma(P)$ *if and only if* $\sigma \in \sigma_i^{-1}G_p$.
Let $S \subset G[N]$ *be a complete set of representatives of the cosets of the principal subgroup* $< p >$ *in* $G[N]$. *Since* $G[N] \cong Gal(\mathbb{F}/\mathbb{Q})$ *by* $i \mapsto \sigma_i : \zeta_N \mapsto \zeta_N^i$, *then* $G_p =< \sigma_p >$ *(*[**I.R**] *chap. 13) and we then have*

$$(G(\overline{\chi}^a)) = \prod_{i \in S} \sigma_i(P)^{b_i}$$

where $b_i = ord_{\sigma_i^{-1}(P)}(G(\overline{\chi}^a))$. *We see without any difficulty that* $b_i = ord_P(\sigma_i(G(\overline{\chi}^a)))$, *and it is easy to see that* $ord_{\mathfrak{P}}\sigma_i(G(\overline{\chi}^a)) = s_p(ai)$ *(*[**I.R**] *chap. 14). Now by similar argument as described above, we get* $b_i = s_p(ai)/(p-1)$. *Thus the highest power of* p *dividing* $G(\overline{\chi}^{\frac{q-1}{N}a})$ *is*

$$h := \frac{1}{p-1} min \left\{ s_p(\frac{q-1}{N}a) | \quad a \in S \right\}.$$

We may replace S *by* $G[N]$ *since* $s_p(j) = s_p(pj)$ *for all integer* $j > 0$. *It also follows that the highest power of a factor of* p *dividing* $G(\chi^{\frac{q-1}{N}a}) = G(\overline{\chi}^{\frac{q-1}{N}(N-a)})$ *is equal to* h, *since* $\gcd(N-a, N) = 1$ *if and only if* $gcd(a, N) = 1$.

We give a table of the factorization of the Gauss sums for some prime cases. Here the ideals $\mathfrak{p}_i$ *are factors of* (p) *in* $\mathbb{Z}[\zeta_m]$.

TABLE 1

m	$p \equiv a \bmod m$	*Factorization of* m^{th} *power Gauss sums*
2	1	$\mathfrak{p}_1 = (p)$
3	1	$\mathfrak{p}_1^2\mathfrak{p}_2$
3	2	$\mathfrak{p}_1^2\mathfrak{p}_2 = (p)^3$
4	1	$\mathfrak{p}_1^3\mathfrak{p}_2$
4	3	$\mathfrak{p}_1^3\mathfrak{p}_2 = (p)^4$
5	1	$\mathfrak{p}_1^4\mathfrak{p}_2^2\mathfrak{p}_3^3\mathfrak{p}_4$
5	2	$\mathfrak{p}_1^4\mathfrak{p}_2^2\mathfrak{p}_3^3\mathfrak{p}_4 = \mathfrak{p}_1^5\mathfrak{p}_2^5 = (\mathfrak{p}_1\mathfrak{p}_2)^5 = (p)^{10}$
5	3	$\mathfrak{p}_1^4\mathfrak{p}_2^2\mathfrak{p}_3^3\mathfrak{p}_4 = \mathfrak{p}_1^5\mathfrak{p}_2^5 = (\mathfrak{p}_1\mathfrak{p}_2)^5 = (p)^{10}$
5	4	$\mathfrak{p}_1^4\mathfrak{p}_2^2\mathfrak{p}_3^3\mathfrak{p}_4 = \mathfrak{p}_1^5\mathfrak{p}_2^5 = (\mathfrak{p}_1\mathfrak{p}_2)^5 = (p)^5$
7	1	$\mathfrak{p}_1^6\mathfrak{p}_2^3\mathfrak{p}_3^2\mathfrak{p}_4^5\mathfrak{p}_5^4\mathfrak{p}_6$
7	2	$\mathfrak{p}_1^6\mathfrak{p}_2^3\mathfrak{p}_3^2\mathfrak{p}_4^5\mathfrak{p}_5^4\mathfrak{p}_6 = \mathfrak{p}_1^{14}\mathfrak{p}_6^7 = (p)^7\mathfrak{p}_1^7$
7	3	$\mathfrak{p}_1^6\mathfrak{p}_2^3\mathfrak{p}_3^2\mathfrak{p}_4^5\mathfrak{p}_5^4\mathfrak{p}_6 = \mathfrak{p}_1^{21} = (p)^{21}$
7	4	$\mathfrak{p}_1^6\mathfrak{p}_2^3\mathfrak{p}_3^2\mathfrak{p}_4^5\mathfrak{p}_5^4\mathfrak{p}_6 = \mathfrak{p}_1^{14}\mathfrak{p}_6^7 = (p)^7\mathfrak{p}_1^7$
7	5	$\mathfrak{p}_1^6\mathfrak{p}_2^3\mathfrak{p}_3^2\mathfrak{p}_4^5\mathfrak{p}_5^4\mathfrak{p}_6 = \mathfrak{p}_1^{21} = (p)^{21}$
7	6	$\mathfrak{p}_1^6\mathfrak{p}_2^3\mathfrak{p}_3^2\mathfrak{p}_4^5\mathfrak{p}_5^4\mathfrak{p}_6 = \mathfrak{p}_1^7\mathfrak{p}_2^7\mathfrak{p}_3^7 = (\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3)^7 = (p)^7$

Remark *From this table, we really see that although the formula of the decomposition looks complicated, it does have a simple shape. This is due to the use of the Galois theory. For more about the factorization of the Gauss sums, see* [**w1**],[**w3**].

If $\mathfrak{p}|p$ is a prime factor and χ the corresponding character, then the prime power decomposition is of the form

$$(G(\chi, a))^m = \mathfrak{p}^{\theta'}$$

where θ' is an element of the group ring $\mathbb{Z}[Gal(k/\mathbb{Q})]$. While still working at prime component $\mathfrak{p}$ prime to m, we extend the result globally by multiplication. Let π be an algebraic integer such that $(\pi) = \mathfrak{p}$. since the ideal generated by $G(\chi, a)^m$ is of the form $\mathfrak{p}^\theta$, there exists a unit $\varepsilon(\pi, a)$ such that,

$$G(\chi, a)^m = \varepsilon(\pi, a)\pi^\theta.$$

Let's fix any embedding, we have

$$|G(\chi, a)^m|^2 = |\varepsilon(\pi, a)|^2 N_{K/\mathbb{Q}}(\pi)^m = N_{K/\mathbb{Q}}(\pi)^m$$

and that implies $|\varepsilon(\pi, a)| = 1$ at all places of K in other words, it is root of unity by a theorem of Kronecker.

3. Gauss sums over finite fields and the Davenport-Hasse relations

One of the most beautiful results on Gauss sums is the Davenport-Hasse relation. Indeed let $m, p, \mathfrak{p}$ and q be as in the preceding sections. Let μ_n the group of m^{th} roots of unity in K. Then the residue class field modulo $\mathfrak{p}$, $O_K/\mathfrak{p}$, is isomorphic to the finite field $\mathbb{F}_q$. Characters on the residue class field modulo $\mathfrak{p}$ are understood to be defined via this isomorphism. The character

$$\chi_{\mathfrak{p}} \quad : \mathbb{F}_q^\times \to \mu_m$$

defined by the relation $\chi_{\mathfrak{p}}(x) \equiv x^{\frac{q-1}{m}} \bmod \mathfrak{p}$ is multiplicative. Any additive character $\lambda_\alpha(x)$ define on the residue classes modulo $\mathfrak{p}$ has the form

$$exp(2\pi i Tr_{K/\mathbb{Q}}(\frac{\alpha x}{\mathfrak{p}}))$$

for some integer α modulo $\mathfrak{p}$. To simplify the computation we will consider

$$\psi_{\mathfrak{p}} : \mathbb{F}_q \to \mu_p$$

be the additive character defined by

$$\psi_{\mathfrak{p}}(x) = exp(2\pi i Tr_{\mathbb{F}q/\mathbb{F}_p}(x)/p).$$

We define the Gauss sums

$$\mathfrak{g}_a(\mathfrak{p}) = \mathfrak{g}(a, \chi_{\mathfrak{p}}, \psi_{\mathfrak{p}}) = \sum_{x \in \mathbb{F}_q^*} \chi_{\mathfrak{p}}(x)^a \psi_{\mathfrak{p}}(x) \qquad (\in K(\mu_p)),$$ *which is known to be non-zero*

We know already that $\mathfrak{g}_a(\mathfrak{p})$ depends only on the congruence class of a modulo m and in particular $\mathfrak{g}_a(\mathfrak{p}) = -1$ if $a \equiv 0 \bmod m$ and otherwise

$$\mathfrak{g}_a(\mathfrak{p})\mathfrak{g}_{-a}(\mathfrak{p}) = \chi_{\mathfrak{p}}(-1)^a q$$

and

$$|\mathfrak{g}_a(\mathfrak{p})| = q^{1/2}.$$

The first Hasse-Davenport relation is as follows.

Theorem 3.3. *Let ℓ be a divisor of m such that $m = \ell d$, then*

$$\prod_{i=0}^{\ell-1} \mathfrak{g}_{a+id}(\mathfrak{p}) = \prod_{\varepsilon:\ \varepsilon^\ell=1} \mathfrak{g}(a, \chi_\mathfrak{p}\varepsilon, \psi_\mathfrak{p}) = \chi_\mathfrak{p}(\ell^{-\ell a}).\mathfrak{g}_{\ell a}(\mathfrak{p}) \prod_{i=1}^{\ell-1} \mathfrak{g}_{id}(\mathfrak{p}).$$

PROOF. □

The second Hasse-Davenport relation is as follow. If $\mathbb{E}$ is a finite extension of $\mathbb{F}$, thes shape of the Hasse Davenport formula relates certain Gauss sums over $\mathbb{E}$ to the Gauss sums over $\mathbb{F}$. Indeed if $\mathfrak{P}$ is a prime above $\mathfrak{p}$ in any extension field K_1 of K. Then $O_{K_1/\mathbb{Q}}/\mathfrak{P} \cong \mathbb{E}$ as finite field, is such that E is a finite extension of $\mathbb{F}$. We define

$$\chi'_\mathfrak{P} = \chi_\mathfrak{p} \circ N_{\mathbb{E}/\mathbb{F}_q}, \text{ and } \psi'_\mathfrak{P} = \psi_\mathfrak{p} \circ tr_{\mathbb{E}/\mathbb{F}_q}.$$

$\chi'_\mathfrak{P}$ and $\psi'_\mathfrak{P}$ are respectively multiplicative and additive characters on $\mathbb{E}$.

Theorem 3.4. *Let $tr_{\mathbb{E}/\mathbb{F}}$ and $N_{\mathbb{E}/\mathbb{F}}$ be the relative trace and relative norm respectively, mappings from $\mathbb{E}$ onto $\mathbb{F}$. Then*

$$\mathfrak{g}_a(\mathfrak{P})' = (-1)^{m-1}\mathfrak{g}_a(\mathfrak{p})^m,$$

where $\mathfrak{P}|\mathfrak{p}$ in $\mathbb{E}/\mathbb{F}$ of degree m and $\mathfrak{g}_a(\mathfrak{P})'$ is the corresponding Gauss sum for the characters $\chi'_\mathfrak{P}, \psi'_\mathfrak{P}$

PROOF. □

4. The Gauss sum and Jacobi sum as complex numbers

In this section we give the main relation between Gauss and Jacobi sums.

We introduce a small modification on the definition of the Gauss sum. This version is the computable version where the Gauss sums are embedded in the field of complex number. In fact $\mathbb{Q}(\mu_n)/\mathbb{Q}$ is an extension of degree $\varphi(n)$. $K = \mathbb{Q}(\mu_n) \otimes_\mathbb{Q} \mathbb{R} \cong \mathbb{C}^{\varphi(n)/2}$ and the ring of integers $\mathbb{Z}[\mu_n]$ is a lattice in K.
From here on, we choose the characters to be the power residue symbol $\left(\frac{\cdot}{\alpha}\right)_n$ for α and algebraic integer coprime to n. Let ε be any embedding of $\mathbb{Q}(\mu_n)$ into $\mathbb{C}$, then we rewrite the Gauss sums as

$$\mathfrak{g}(r, \varepsilon, \alpha) = \sum_{x \in G[\alpha]} \varepsilon(\left(\frac{x}{\alpha}\right)_n)\mathbf{e}(\frac{rx}{\alpha}),$$

where $\mathbf{e}(x) = exp(2\pi i \mathrm{Tr}_{K/\mathbb{Q}}(x))$, and r is an algebraic integer in K. we will not make any difference between $\mathrm{Tr}_{K/\mathbb{Q}}$ and its unique extension to $\mathbb{C}^{\varphi(n)/2}$.
All the properties we have described remain unchanged. We will work only at prime algebraic integer argument since multiplicative relations allow one to do so.

Then, $\mathfrak{g}(r, \varepsilon, \pi)$ depends only on the ideal $\mathfrak{p}$ generated by π. Indeed if we replace π by $u\pi$ where u is a unit, then

$$\mathfrak{g}(r, \varepsilon, u\pi) = \varepsilon(\left(\frac{u}{\pi}\right)_n)\mathfrak{g}(r, \varepsilon, \pi)$$

implies $(\mathfrak{g}(r,\varepsilon,\pi))^n$ *does not depend on* π *itself but on the ideal* $\mathfrak{p}$ *generated by* π. *Furthermore if* π_1 *and* π_2 *are primes and coprime then for* r *coprime to* π_1 *and* π_2

$$\varepsilon(\left(\frac{\cdot}{\pi_1\pi_2}\right)_n) = \varepsilon(\left(\frac{\cdot}{\pi_1}\right)_n)\varepsilon(\left(\frac{\cdot}{\pi_2}\right)_n)$$

$$\mathfrak{g}(r,\varepsilon,\pi_1\pi_2) = \varepsilon(\left(\frac{\pi_2}{\pi_1}\right)_n)\varepsilon(\left(\frac{\pi_1}{\pi_2}\right)_n)\mathfrak{g}(r,\varepsilon,\pi_1)\mathfrak{g}(r,\varepsilon,\pi_2).$$

Moreover we have the following lemma:

Lemma 3.1. *Let* α *be an algebraic integer prime to* n. *The function* $\mathfrak{g}(r,\varepsilon,\alpha)$ *vanishes as the Möbiüs function* $\mu(\alpha)$ *does.*

From the multiplicative properties of the Gauss sums, we must suppose that α *is a prime* π *and that* $r = 1$ *such that the function* $\mathfrak{g}(1,\varepsilon,\pi^r)$ *vanishes as the Möbiüs function* $\mu(\pi^r)$ *does.*

Proof.

$$\begin{aligned}
(4.1)\ \mathfrak{g}(1,\varepsilon,\pi^r) &= \sum_{x \bmod \pi^r} \varepsilon(\left(\frac{x}{\pi^r}\right)_n)\mathbf{e}(\frac{x}{\pi^r}) \\
(4.2) &= \sum_{\substack{x \bmod \pi^r \\ gcd(\pi x)=1}} \varepsilon^r(\left(\frac{x}{\pi}\right)_n)\mathbf{e}(\frac{x}{\pi^r}) \\
(4.3) &= \sum_{\substack{x_0 \bmod \pi, \\ x_1,\cdots,x_{r-1} \bmod \pi}} \varepsilon^r(\left(\frac{x_0}{\pi}\right)_n)\mathbf{e}(\frac{x_0}{\pi^r} + \frac{x_1}{\pi^{r-1}} + \cdots + \frac{x_{r-1}}{\pi}) \\
(4.4) &= \sum_{x_0 \bmod \pi} \varepsilon^r(\left(\frac{x_0}{\pi}\right)_n)\mathbf{e}(\frac{x_0}{\pi^r}) \sum_{x_1,\cdots,x_{r-1} \bmod \pi} \mathbf{e}(\frac{x_1}{\pi^{r-1}} + \cdots + \frac{x_{r-1}}{\pi}) \\
(4.5) &= 0
\end{aligned}$$

□

Another important lemma is giving the relation for $\mathfrak{g}(\pi^\ell,\varepsilon,\alpha\pi^r)$. *By the same arguments as before we will consider only this case:*

$$\mathfrak{g}(\pi^\ell,\varepsilon,\alpha\pi^r),$$

and the lemma is as follows:

Lemma 3.2. *Let* $\ell < r$ *both integers, the function* $\mathfrak{g}(\pi^\ell,\varepsilon,\pi^r)$ *has the form*

$$\mathfrak{g}(\pi^\ell,\varepsilon,\pi^r) = \begin{cases} 0 & \text{if} \quad r-\ell > 1 \\ -\phi(\pi^r) & r \equiv 0 \bmod n \text{ and } r = \ell \\ 0 & r \not\equiv 0 \bmod n \text{ and } r = \ell \\ -N(\pi^{r-1}) & \text{if} \quad r \equiv 0 \bmod n \quad \text{and} \quad r-l = 1 \\ N(\pi^{r-1})\mathfrak{g}(1,\varepsilon^r,\pi) & \text{if} \quad r \not\equiv 0 \bmod n \quad \text{and} \quad r-l = 1 \end{cases}$$

Proof. The crucial point is to write down a simple shape of the elements of the set of residues modulo π^r which are coprime to π^r. In the following step, we choose this set to be

$$x_0 + x_1\pi + x_2\pi^2 \cdots + x_{r-1}\pi^{r-1}$$

where the x_i are taken modulo π and $x_0 \not\equiv 0 \bmod \pi$, $0 \leq i \leq r-1$.

$$\mathfrak{g}(\pi^\ell, \varepsilon, \pi^r) = \sum_{x \bmod \pi^r} \varepsilon(\left(\frac{x}{\pi^r}\right)_n)\mathbf{e}(\frac{\pi^\ell x}{\pi^r}) \tag{4.6}$$

$$= \sum_{\substack{x \bmod \pi^r \\ gcd(\pi x)=1}} \varepsilon^r(\left(\frac{x}{\pi}\right)_n)\mathbf{e}(\frac{x}{\pi^{r-\ell}}) \tag{4.7}$$

$$= \begin{cases} 0 & \text{if} \quad r-\ell > 1 \\ -\phi(\pi^r) & \text{if} \quad \varepsilon^r \equiv 1 \text{ and } r = \ell \\ 0 & \text{if} \quad \varepsilon^r \not\equiv 1 \text{ and } r = \ell \\ -N(\pi^{r-1}) & \text{if} \quad \varepsilon^r \equiv 1 \quad \text{and} \quad r-l = 1 \\ N(\pi^{r-1})\mathfrak{g}(1, \varepsilon^r, \pi) & \text{if} \quad \varepsilon^r \not\equiv 1 \quad \text{and} \quad r-l = 1 \end{cases} \tag{4.8}$$

□

The Galois action of $Gal(K/\mathbb{Q})$ on $\mathfrak{g}(r, \varepsilon, \pi)$ is as follow: If $\sigma \in Gal(K/\mathbb{Q})$ is the Galois elements that maps $\zeta_n = \zeta$ to ζ^a for some integer a, then

$$\mathfrak{g}(r, \varepsilon, \pi)^\sigma = \mathfrak{g}(r, \varepsilon^\sigma, \pi) = \mathfrak{g}(r, \varepsilon^a, \pi) = \mathfrak{g}(r, \varepsilon, \pi^\sigma).$$

thus

$$\mathfrak{g}(r, \varepsilon, \pi\pi^\sigma) = \varepsilon(\left(\frac{\pi^\sigma}{\pi}\right)_n)\varepsilon(\left(\frac{\pi}{\pi^\sigma}\right)_n)\mathfrak{g}(r, \varepsilon, \pi)\mathfrak{g}(r, \varepsilon, \pi^\sigma).$$

We see that, if instead of the prime factor π of the prime p, we take p itself, then p factors as $p = \prod_{i=1}^r \pi_i$. It then follows that:

$$\mathfrak{g}(r, \varepsilon, p) = \prod_{\substack{i=1, j=1 \\ j \neq i}} \varepsilon(\left(\frac{\pi_i}{\pi_j}\right)_n) \prod_{i=1}^r \mathfrak{g}(r, \varepsilon, \pi_i)$$

Remark *This formula looks rather simple but it is a very important one. Since it makes use of the Chinese Remainder Theorem which plays a key role in the the multiplicative relations among the Gauss sums. We also notice that $\mathfrak{g}(r, \varepsilon, p)$ is invariant under all complex embeddings.*

Definition 3.2. Let χ and ψ denote two characters modulo an integral prime π. The Jacobi sum $J(\chi, \psi)$ is defined by

$$J(\chi, \psi) = \sum_{x \bmod \pi} \chi(x)\psi(1-x)$$

Its order is the least common multiple n of the order of χ and ψ, such that the Jacobi sum $J(\chi, \psi) \in \mathbb{Q}(\zeta_n)$.

Note 3.1. The Jacobi sum $J(\chi, \psi)$ defines a symmetric pairing.
The most important properties of the Jacobi sums can be listed as follows.

Theorem 3.5. *Let χ and ψ denote two characters modulo an integral prime π.*

- *If χ and ψ are both trivial, then $J(\chi, \psi) = N_{K/\mathbb{Q}}(\pi)$*
- *If exactly one of the $\chi's$ or one of the $\psi's$ is trivial, then $J(\chi, \psi) = 0$.*
- *If χ is nontrivial, then $J(\chi, \overline{\chi}) = -\chi(-1)$.*

- *If χ and ψ are such that $\chi, \psi,$ and $\chi\psi$ are nontrivial, then*

$$J(\chi,\psi) = \psi(-1)J(\overline{\chi}\overline{\psi},\psi) = \chi(-1)J(\overline{\chi}\overline{\psi},\chi)$$

PROOF. see [**B1**] *pp* 57, 59 □

Now as we did for the Gauss sums, we reformulate the Jacobi sums at prime argument for power residue symbol with embedding into the field of complex numbers and extend it as a multiplicative function of π

$$J((a,b);\varepsilon_1,\varepsilon_2,\pi) = \sum_{x \bmod \pi} \varepsilon_1(\left(\frac{x}{\pi}\right)_n)^a \varepsilon_2(\left(\frac{1-x}{\pi}\right)_n)^b.$$

where a and b are taken modulo n and $\varepsilon_1, \varepsilon_2$ are two fixed complex embeddings of $K = \mathbb{Q}(\zeta_n)$ into $\mathbb{C}$ as before.
We denote $J((a,b);\varepsilon_1,\varepsilon_2,\pi)$ by $J(\varepsilon_1,\varepsilon_2,\pi)$ if $a = b = 1$.

The most important relation between Gauss an Jacobi sums is as follows.

Lemma 3.3. *Let $\varepsilon_1, \varepsilon_2$ be two complex characters of μ_n. If $\varepsilon_1\varepsilon_2$ is nontrivial then*

$$\mathfrak{g}(r,\varepsilon_1,\pi)\mathfrak{g}(r,\varepsilon_2,\pi) = J(\varepsilon_1,\varepsilon_2,\pi)\mathfrak{g}(r,\varepsilon_1\varepsilon_2,\pi).$$

$$|J(\varepsilon_1,\varepsilon_2,\pi)|^2 = N_{K/Q}(\pi)$$

PROOF. Indeed,

$$\mathfrak{g}(r,\varepsilon_1,\pi)\mathfrak{g}(r,\varepsilon_2,\pi) = \sum_{x \bmod \pi} \sum_{y \bmod \pi} \varepsilon_1(\left(\frac{x}{\pi}\right)_n)\varepsilon_2(\left(\frac{y}{\pi}\right)_n)\mathbf{e}(x+y)$$

Then put $\gamma = x + y$ and the summation above becomes

$$\begin{aligned}
&\sum_{\gamma \bmod \pi} \sum_{x \bmod \pi} \mathbf{e}(\gamma)\varepsilon_1(\left(\frac{x}{\pi}\right)_n)\varepsilon_2(\left(\frac{\gamma-x}{\pi}\right)_n) \\
&= \sum_{\substack{x \bmod \pi,\\ \gamma=0}} \varepsilon_1(\left(\frac{x}{\pi}\right)_n)\varepsilon_2(\left(\frac{-x}{\pi}\right)_n) + \sum_{\substack{\gamma \bmod \pi\\ \gamma\neq 0}} \sum_{x \bmod \pi} e(\gamma)\varepsilon_1(\left(\frac{x}{\pi}\right)_n)\varepsilon_2(\left(\frac{\gamma-x}{\pi}\right)_n) \\
&= \varepsilon_2(\left(\frac{-1}{\pi}\right)_n) \sum_{x \bmod \pi} \varepsilon_1\varepsilon_2(\left(\frac{x}{\pi}\right)_n) + \sum_{\substack{\gamma \bmod \pi\\ \gamma\neq 0}} \sum_{\gamma x \bmod \pi} \mathbf{e}(\gamma)\varepsilon_1(\left(\frac{\gamma x}{\pi}\right)_n)\varepsilon_2(\left(\frac{\gamma-\gamma x}{\pi}\right)_n) \\
&= \sum_{\substack{\gamma \bmod \pi\\ \gamma\neq 0}} \varepsilon_1\varepsilon_2(\left(\frac{\gamma}{\pi}\right)_n)\mathbf{e}(\gamma) \sum_{x \bmod \pi} \varepsilon_1(\left(\frac{x}{\pi}\right)_n)\varepsilon_2(\left(\frac{1-x}{\pi}\right)_n) \\
&= \mathfrak{g}(r,\varepsilon_1\varepsilon_2,\pi)J(\varepsilon_1,\varepsilon_2,\pi).
\end{aligned}$$

For the module of $J(\varepsilon_1,\varepsilon_2,\pi)$, we use the known formula for the module of the Gauss sums:

$$|J(\varepsilon_1,\varepsilon_2,\pi)| = \frac{|\mathfrak{g}(r,\varepsilon_1,\pi)||\mathfrak{g}(r,\varepsilon_1,\pi)|}{|\mathfrak{g}(r,\varepsilon_1\varepsilon_2,\pi)|} = \frac{N_{K/\mathbb{Q}}(\pi)^{1/2}N_{K/\mathbb{Q}}(\pi)^{1/2}}{N_{K/\mathbb{Q}}(\pi)^{1/2}} = N_{K/\mathbb{Q}}(\pi)^{1/2}$$

□

Remark Suppose that $c = \pi^k$ with $k > 1$ then

$$\left(\frac{x}{\pi^k}\right)_n = \left(\frac{x}{\pi}\right)_n^k$$

and is never a primitive character on $G[\pi^k]$ and therefore $\mathfrak{g}(r, \varepsilon_1, \pi^k) = 0$. This generalizes to

$$\mathfrak{g}(r, \varepsilon_1, \alpha) = 0 \quad \text{if} \quad \mu(\alpha) = 0,$$

where α is any algebraic integer, coprime to r and $\mu(\alpha)$ is the Möbiüs function on K. For this reason, a much more generalized theorem of Eisenstein [**E**] and Weil [**w2**],[**w3**] is as follows:

Theorem 3.6. *Let $\varepsilon_1, \varepsilon_2$ be two homomorphisms of $\mu_n(K) \to \mu_n(\mathbb{C})$. Then there exists a Grössencharakter $\omega(\varepsilon_1, \varepsilon_2, c)$ of K such that, if c is coprime to r and n then*

$$\mathfrak{g}(r, \varepsilon_1, c)\mathfrak{g}(r, \varepsilon_2, c) = \mu(c)\omega(\varepsilon_1, \varepsilon_2, c)\mathfrak{g}(r, \varepsilon_1\varepsilon_2, c).$$

Where μ is the Möbius function in K.

We therefore see that if ε is a generator of order n of the group of complex characters of $\mu_n(K)$, then

$$\mathfrak{g}(r, \varepsilon, c)\mathfrak{g}(r, \varepsilon, c) = \mu(c)\omega(\varepsilon, \varepsilon, c)\mathfrak{g}(r, \varepsilon^2, c).$$
$$\mathfrak{g}(r, \varepsilon, c)\mathfrak{g}(r, \varepsilon^2, c) = \mu(c)\omega(\varepsilon, \varepsilon^2, c)\mathfrak{g}(r, \varepsilon^3, c).$$

$$\cdots$$

$$\cdots$$

$$\mathfrak{g}(r, \varepsilon, c)\mathfrak{g}(r, \varepsilon^{n-1}, c) = \mathfrak{g}(r, \varepsilon, c)\mathfrak{g}(r, \varepsilon^{-1}, c)$$

$$= \mu(c)\omega(\varepsilon, \varepsilon^{n-1}, c)\mathfrak{g}(r, \varepsilon^n, c) = \mu(c)\varepsilon\left(\frac{-1}{c}\right)_n |\mathfrak{g}(r, \varepsilon, c)|^2 = \mu(c)\varepsilon\left(\frac{-1}{c}\right)_n N_{K/\mathbb{Q}}(c).$$

It then follows that

$$\mathfrak{g}(r, \varepsilon, c)^n = \mu(c)^n\varepsilon\left(\frac{-1}{c}\right)_n N_{K/\mathbb{Q}}(c)\omega(\varepsilon, \varepsilon^2, c)\omega(\varepsilon, \varepsilon^3, c)\cdots\omega(\varepsilon, \varepsilon^{n-2}, \pi)$$

Now let us go back to the fifth cyclotomic field and state the following lemma:

Lemma 3.4. *If π is a prime element of $\mathbb{Z}[\zeta_5]$ dividing the prime $p \in \mathbb{Z}$ and let χ be a primitive Dirichlet character modulo π of order 5, then $\rho = \pi\sigma_3(\pi)$ is an associate of the Jacobi sum $J(\chi, \chi)$. More precisely, $\rho = \pm\zeta^j J(\chi, \chi)$, for some integer i between 0 and 4. Moreover if π is primary, then $\rho = \pm J(\chi, \chi)$.*

Proof. By the uniqueness of the factorization of p in $\mathbb{Z}[\zeta]$, any α in K/K^+ whose norm is p has the form $\alpha = u.\sigma_i(\pi)\sigma_j(\pi)$ where u is a unit of K and i, j are integers between 1 and 4, with $i \not\equiv \pm j \bmod 5$. Hence $\alpha = u\sigma_k(\rho)$ for a unique k, $1 \leq k \leq 4$. Also since

$$|\alpha| = |\sigma_k(\rho)| = \sqrt{p}$$

we have $|u| = 1$ and for all $\mathbb{Q}-$conjugates $\sigma_j(u)$ of u, $|\sigma_j(u)| = 1$, therefore u is a root of unity in K by the Kronecker theorem; i.e $u = \pm\zeta^i$. Let χ_0 be another Dirichlet

character modulo 5, then put $\alpha = J(\chi_0, \chi_0)$. We know that $N(J(\chi_0, \chi_0)) = \sqrt{p}$, then $\rho = \pm\zeta^i \sigma_j(J(\chi_0, \chi_0))$; i.e

$$\rho = \pm\zeta^i J(\chi_0^j, \chi_0^j)$$

for unique integers $0 \leq i \leq 4$, $1 \leq j \leq 4$. We then conclude by taking $\chi = \chi_0^j$.
Now we suppose that π is primary, therefore $\rho \equiv 1 \bmod (1-\zeta)^3$ for all j, since π and $\sigma_j(\pi)$ satisfies the same requirements. If g is a primitive root modulo p such that $\chi(g) = \zeta^h$, with $h \in \mathbb{Z}$. For any $m \in \mathbb{Z}$ prime to p we denote $ind_g(m)$ the index of m with respect to g. Then

$$J(\chi, \chi) = \sum_{t=2}^{p-1} \zeta^{h(ind_g(t) + id_g(1-t))} \tag{4.9}$$

$$\equiv \sum_{t=2}^{p-1} (1 - h(ind_g(t) + id_g(1-t)))(1-\zeta) \tag{4.10}$$

$$\equiv p - 2 + h(2\sum_{k=1}^{p-2} k)(1-\zeta) \bmod (1-\zeta)^3 \tag{4.11}$$

$$\equiv -1 \bmod (1-\zeta)^3, \text{ since } \quad p - 1 \equiv 0 \bmod (1-\zeta)^4. \tag{4.12}$$

Since

$$\rho = \pm\zeta^i J(\chi, \chi) \equiv \pm(1 - i(1-\zeta))(-1) \bmod (1-\zeta)^3 \equiv 1 \bmod (1-\zeta)^3$$

implies that $i \equiv 0 \bmod 5$ and therefore $\rho = \pm J(\chi, \chi)$. □

5. The moment Gauss sums and the uniform distribution

Here the notations differ slidely from the previous, but they are essentially the same. The field we consider here is of the form $K = \mathbb{Q}(\zeta_{q-1})$ where q is of the form p^f and $n|q-1$. A consequence of this fact is that $\mathbb{Q}(\zeta_n) \subset K$.
We define ε as before as an injective homomorphism

$$\varepsilon : \mu_{q-1}(K) \to \mu_{q-1}(\mathbb{C}).$$

We furthermore suppose ε is an isomorphism.
Then $\chi = \chi_\pi$ is a Dirichlet character modulo π so that $\varepsilon \circ \chi(x)$ has values in $\mathbb{C}$. We also put

$$\mathbf{e}(x) = \exp(2\pi \mathrm{Tr}_{K/\mathbb{Q}}(x))$$

where $\mathrm{Tr}_{K/\mathbb{Q}}$ is the trace of $K/\mathbb{Q}$. We then reformulate the Gauss sum as follow:

$$\mathfrak{g}(a, \varepsilon \circ \chi, \pi) = \sum_{x \pmod{\pi}} \varepsilon(\chi(x)) \mathbf{e}(\frac{a.x}{\pi})$$

and with this definition, all the properties of Gauss sums are satisfied.

Definition 3.3. Under the assumption above and for any positive integer m we define the m^{th} moment of the Gauss sum $\mathfrak{g}(a, \varepsilon \circ \chi, \pi)$, as follows:

$$M_m\mathfrak{g} := M_m\mathfrak{g}(a, \varepsilon \circ \chi, \pi) = \sum_{a \neq 0 \pmod{\pi}} \sum_{\chi \neq 1} \mathfrak{g}(a, \varepsilon \circ \chi, \pi)^m$$

In the next lines, we are going to give a non trivial estimate of the module $|M_m\mathfrak{g}|$. The trivial estimate is obtained by using the properties involving the module of the Gauss sums.
In fact $|\mathfrak{g}(a, \varepsilon \circ \chi, \pi)| \leq \sqrt{q}$ therefore

$$|M_m\mathfrak{g}| \leq \sum_{a\neq 0} \sum_{\chi\neq 1} |\mathfrak{g}(a, \varepsilon \circ \chi, \pi)|^m = (q-1)(q-2)q^{m/2}$$

One can perform this estimate as follows:

Another property of the Gauss sum for a non trivial character states that for any $a \not\equiv 0 \pmod{\pi}$,

$$\mathfrak{g}(a, \varepsilon \circ \chi, \pi) = \varepsilon(\overline{\chi}(a))\mathfrak{g}(1, \varepsilon \circ \chi, \pi),$$

and then taking into account the character relation on the residues class modulo π we obtain

$$|\sum_{a \pmod{\pi}} \mathfrak{g}(a, \varepsilon \circ \chi, \pi)^m|$$

$$= \quad 0 \quad \text{if} \quad \chi^m \neq 1 \tag{5.1}$$

$$= \quad (q-1)q^{m/2} \quad \text{if} \quad \chi^m = 1 \tag{5.2}$$

then the characters with significant effect in the sum are those whose order divides m. The number of such chararcters is $d = \gcd(m, q-1)$.
Therefore

$$|M_m\mathfrak{g}| \leq \sum_{\chi\neq 1} |\sum_{a \pmod{\pi}} \mathfrak{g}(a, \varepsilon \circ \chi, \pi)^m| = \sum_{\substack{\chi^d=1 \\ \chi\neq 1}} (q-1)q^{m/2} = (d-1)(q-1)q^{m/2}.$$

We summarize this result in the following theorem:

Theorem 3.7. *Let $m \geq 1$, and let $d = gcd(m, q-1)$, the greatest common divisor of m and $q-1$. Then we have*

$$|M_m\mathfrak{g}| \leq (d-1)(q-1)q^{m/2}.$$

The next step consists of the equidistribution properties of the arguments of the Gauss sums.
In fact

$$|\mathfrak{g}(a, \varepsilon \circ \chi, \pi)| = \sqrt{q}$$

implies that

$$\frac{\mathfrak{g}(a, \varepsilon \circ \chi, \pi)}{\sqrt{q}}$$

lies on the unit circle in the complex plane. It is important to consider the equidistribution properties of the following sequence in the interval $[0, 1]$ as $q \to \infty$

$$\frac{1}{2\pi} arg(\mathfrak{g}(a, \varepsilon \circ \chi, \pi))$$

whenever $\pi \not| a$ and $\chi \neq 1$. Here $arg(z)$ stands for the argument of the complex number z.
We want to establish the equidistribution estimate for the above sequence with a

good error term.
Let α_1 and α_2 be any real numbers with $0 \leq \alpha_1 < \alpha_2 \leq 1$ and let

$$L(\alpha_1, \alpha_2) := \#\left\{(a, \chi) : \pi \not| a, \quad \chi \neq 1 \quad and \quad \alpha_1 \leq \frac{1}{2\pi} arg(\mathfrak{g}(a, \varepsilon \circ \chi, \pi)) \leq \alpha_2\right\}$$

We are now looking for an estimate of $L(\alpha_1, \alpha_2)$. We first recall the Erdös-Turan discrepancy theorem [**KuNi**] pp. 112 on the uniform distribution. If $\{a_m\}$ is a sequence of reals in the interval $[0, 1]$. Then for any positive integer N, denote the discrepancy

$$D_N = \sup_{0 \leq \delta_1 < \delta_2 \leq 1} \left| \left(\frac{1}{N} (\sum_{\substack{1 \leq m \leq N \\ \delta_1 \leq a_m \leq \delta_2}} 1 \right) - (\delta_1 - \delta_2) \right|.$$

for any positive integer K, from [**MON**] pp. 8, the estimate for D_n is as follows:

$$ND_N \leq \frac{N}{K+1} + 3 \sum_{1 \leq m \leq K} \frac{1}{m} \left| \sum_{1 \leq j \leq N} e^{2\pi i m a_j} \right|.$$

Therefore replace N by $(q-1)(q-2)$ in D_N and use the definition of $L(\delta_1, \delta_2)$ we get

$$|L(\delta_1, \delta_2) - (q-1)(q-2)(\delta_1 - \delta_2)|$$

$$\leq \frac{(q-1)(q-2)}{K+1} + 3 \sum_{1 \leq m \leq K} \frac{1}{mq^{m/2}} \left| \sum_{\chi \neq 1} \sum_{a \neq 0} \mathfrak{g}(a, \varepsilon \circ \chi, \pi)^m \right| \tag{5.3}$$

$$\leq \frac{(q-1)(q-2)}{K+1} + 3 \sum_{1 \leq m \leq K} \frac{|M_m \mathfrak{g}|}{mq^{m/2}} \tag{5.4}$$

we take $K = q - 1$ and then using the estimate for $M_m \mathfrak{g}$ we deduce that

$$|L(\delta_1, \delta_2) - (q-1)(q-2)(\delta_1 - \delta_2)|$$

$$\leq (q-2) + 3(q-1) \sum_{1 \leq m \leq q-1} \frac{\gcd(m, q-1) - 1}{m}.$$

We give now an estimate to the sum $\sum_{1 \leq m \leq q-1} \frac{\gcd(m, q-1)}{m}$. In fact

$$\sum_{1 \leq m \leq q-1} \frac{\gcd(m, q-1)}{m} = \sum_{n | q-1} \sum_{\substack{1 \leq m \leq (q-1)/n \\ \gcd(m, (q-1)/n) = 1}} \frac{1}{m} \tag{5.5}$$

$$\leq (1 + \log q) \sum_{n | q-1} 1 = (1 + \log q D(q-1)) \tag{5.6}$$

$$\leq 2D(q-1) \log q \tag{5.7}$$

where $D(n)$ is the number of positive divisor of n.
Thus we finally have

$$|L(\delta_1, \delta_2) - (q-1)(q-2)(\delta_1 - \delta_2)| \leq 7qD(q-1)\log q.$$

We can now state the theorem as follows:

Theorem 3.8. *we have*

$$|L(\delta_1, \delta_2) - (q-1)(q-2)(\delta_1 - \delta_2)| \leq 7(q-1)D(q-1)\log q$$

Remark The m-moment of the Gauss sum would certainly be simplify if we introduce the properties from the Davenport-Hasse theorem. At least it would give a much better result in term of congruences modulo n the order of the character χ. This is not the place to undertake that. Both theorems would certainly lead to alike ones in the theory of Jacobi sums, since both sums are related.

CHAPTER 4

CYCLOTOMIC CRYSTAL

1. Introduction

We denote by K an algebraic number field of finite degree over $\mathbb{Q}$ and we assume K contains μ_n, the group of the n^{th} roots of unity. Let $V = K \otimes_{\mathbb{Q}} \mathbb{R}$ (as algebra, $V \cong \mathbb{R}^N, N = dim_{\mathbb{Q}}(K)$) and regard V as a topological algebra, that is, V is also a linear space. For K=$\mathbb{Q}(\mu_n)$, the space V is also viewed as the infinite component of the adéle ring $K_{\mathbb{A}}$ of K and N is the absolute degree of K.

Definition 4.1. (1) The mapping

$$z \otimes x \mapsto (\zeta z) \otimes x,$$

for $\zeta \in \mu_n, z \in K, x \in \mathbb{R}$ is called a rotation(the rotation by ζ).

(2) The mapping $z \mapsto z + b$ ($b \in \mathfrak{R}$ the ring of integers of K) is the translation by b.

(3) For $a \in K - \{0\}$ and $b \in \mathfrak{R}$, a transformation $\sigma(a, b)$ is the mapping $z \mapsto az + b$

Definition 4.2. Let

$$\Gamma = \{\sigma(a, b); a \in \mu_n, b \in \mathfrak{R}\}$$

We call Γ a cyclotomic crystallographic group. To see that Γ is a group , we define the composition as follows

$$\sigma(a, b)\sigma(c, d) = \sigma(ac, ad + b)$$

and

$$\sigma(a, b)^{-1} = \sigma(a^{-1}, -a^{-1}b)$$

with this definition, Γ is a discrete group which acts discontinuously on V; furthermore, Γ is isomorphic to $\mu_n \rtimes \mathfrak{R}$.

In general, there is a fundamental domain of a crystallographic group which is a polyhedron. This is the case of our group Γ, where the fundamental domain is given by parallelotopes. Here, a parallelotope is the generalization of a higher dimensional parallelogram. In general it is not always possible to obtain a fundamental domain of Γ by a single parallelotopes, but we need a finite number of them. This construction of the fundamental domain is very useful in the geometric point of view in the algebraic number theory. one uses it to find absolute residue system for an ideal $\mathfrak{a}$ of $\mathfrak{R}$ and one derives a generalization of the Gauss lemma which leads to the definition of the Legendre symbol, and therefore, give another proof to the reciprocity law. ([**R-H**] , Kubota). The idea behind it is that it can also help in determining Euclidean algorithm for certain number fields. This will appear in this

chapter throughout as a consequence of some combinatoric facts. We give a complete description of the skeleton of the fundamental domain for cyclotomic fields of prime order.
Our investigation on the geometric aspect of the fundamental domain for Γ leads to some combinatorial results for certain values of n, precisely when n is an odd and prime. We shall also derive for $n = 5$, and for general n an interesting property concerning the Euclidean property of the corresponding field. The geometric definition of the fundamental domain for Γ is that of Dirichlet. For, one needs in general to endow the space V with some quadratic function d, positive definite. Let d to be any norm function defined on V, which preserved by Γ, that is

$$d(\gamma x, \gamma y) = d(x, y)$$

for all $x, y \in V$ and $\gamma \in \Gamma$.

Definition 4.3. See [**A. Bear**] pp 204.
A *fundamental set* for Γ is a subset D of V which contains exactly one point from each orbit in V. Thus no two points in D are Γ-equivalent and

$$\bigcup_{\gamma \in \Gamma} \gamma F = V$$

Definition 4.4. See [**A. Bear**] pp 204.
A subset F of the metric space (V, d) is a *fundamental domain* for the group Γ if and only if

- (1) F is a domain.
- (2) There is some fundamental set D with $F \subset D \subset \overline{F}$.
- (3) The $d-\text{vol}(\partial(F)) = 0$

Remark If F is a fundamental domain, then for $\gamma \in \Gamma$ ($\gamma \neq I$, I is the identity element of Γ),

$$(\gamma F) \cap F = \emptyset, \quad \bigcup_{\gamma \in \Gamma} \gamma \overline{F} = V.$$

Definition 4.5. (Dirichlet fundamental domain.)
Let $x \in V$ fixed. Then

$$F_x = \{y : d(x, y) < d(\gamma x, y), \text{ for all } \gamma \in \Gamma\}$$

is the Dirichlet fundamental domain centered at x.

We denote F_0 by F.
The set Γ, which is a subgroup of transformations of V preserving d is of the form $Ort_d \times V$, where $Orth_d$ is the orthogonal group associated with the quadratic form defining d. The stabilizer of a point is compact. It follows that the set:

$$\{\gamma, \quad \gamma \in \Gamma : d(x, y) = d(x, \gamma y) \ \ for \ \ y \in \overline{F}\}$$

is compact and discrete in $Orth_d \times V$ and therefore finite. $V = \Gamma F$, thus for all $x \in V$ there exists $\gamma \in \Gamma$ and $y \in F$ with $x = \gamma y$.

Theorem 4.1. *There exists a finite number of elements $\gamma_1, \cdots, \gamma_m$ of Γ such that $\overline{F_x}$ can be given by a finite number of inequalities*

$$d(x-y) \leq d(\gamma_i x - y) \qquad i = 1, \cdots, m.$$

PROOF. See [**I.M. Gel**]pp 8-9. □

Remark This theorem is well known, but it is sometimes hard to find the minimal set for the $\gamma_i's$. In finding this minimal set, one can describe the geometry of the fundamental domain for a fixed metric. One notices that different metrics will give different shape of the fundamental domain even if they are equivalent metrics. We will explicitely solve this problem for the cyclotomic fields generated by a primitive n^{th} root of unity, for n prime and odd.

2. The cyclotomic case

In the case of number fields, we have said that V is an algebra such that we can impose some linear conditions on its basis elements. In fact is not necessary to use the algebraicity of V for that , since any linear relation correspond to equivalence class with respect to the corresponding hyperplane.
Let ζ be a primitive n^{th} root of unity. The field $K = \mathbb{Q}(\zeta)$ is the n^{th} cyclotomic field.

Let e_i denote the element $\zeta^i \otimes 1$ in $K \otimes_{\mathbb{Q}} \mathbb{R}$. Then $\sum_{i=1}^{n} e_i = 0$, we obtain a map:

$$\mathbb{R}^n \to V : \quad (x_1, x_2, \cdots, x_n) \mapsto \sum_{i=1}^{n} x_i e_i$$

with kernel $W = \mathbb{R}(1, 1, \cdots, 1)$. The dual space to $\mathbb{R}^n/W$ is the subspace

$$\{\underline{x} = (x_1, x_2, \cdots, x_n) \in \mathbb{R}^n : \quad x_1 + x_2 + \cdots + x_n = 0\}$$

and $V \cong \mathbb{R}^n/W$.
We define the quadratic form

$$q(\underline{x}) = \sum_{i<j} (x_i - x_j)^2 \quad \text{on} \quad \mathbb{R}^n/W.$$

We transfer this quadratic form to V and called it d.
Then for $x \in V; x = \sum_{i=1}^{i=n} x_i e_i$ where $x_i \in \mathbb{R}$ for all i

$$d(x) = \sum_{1 \leq i < j \leq n} (x_i - x_j)^2 = \frac{1}{2} \sum_{i,j=1}^{n} (x_i - x_j)^2 = n \sum_{i=1}^{n} x_i^2 - \left(\sum_{i=1}^{n} x_i \right)^2,$$

(V, d) is a quadratic space and the corresponding bilinear symmetric form is

$$(\ ,\ ) : V \times V \to \mathbb{R}; \quad (x, y) \mapsto \tfrac{1}{2}[d(x+y) - d(x) - d(y)] \tag{2.1}$$

The Dirichlet fundamental domain for d is

$$F = \{x \in V : |(x, y)| \leq \frac{1}{2} d(y), y \in L\} \tag{2.2}$$

F is a compact convex symmetric subset of V.

The aim of our work here is to find a suitable finite set of points such that F is

the convex hull of these points. This set is chosen to be minimal in such a way that its elements are exactly the vertices of F. We will also give a complete combinatoric description of its geometric structure. We prove that this combinatoric structure is related to certain numbers. The symmetric group plays a key role. The Euler relation for polyhedron is satisfied.

The following properties hold:

Lemma 4.1.
- *(1)* $(e_i, e_i) = n - 1, \quad 1 \leq i \leq n.$
- *(2)* $(e_i, e_j) = -1, \quad 1 \leq i \neq j \leq n.$
- *(3)* $\sum_{i=1}^{n} x_i e_i = 0 \Leftrightarrow x_i$ *constant for all* $\quad i, 1 \leq i, j \leq n.$
- *(4) For* $x \in V$, *there exists a representation of* x *in the form* $x = \sum_{i=1}^{n} x_i e_i$ *with* $x_i \geq 0$ *for all* i.
- *(5) Let* $x = \sum_{i=1}^{n} x_i e_i \in V$ *be an integral point, there exists a representation of* x *of the form* $x = \sum_{i=1}^{n} \lambda_i e_i$ *and* $0 \leq \sum_{i=1}^{n} \lambda_i < n$;

PROOF. (1),(2) and (3) are clear.
(4). If all the $x_i \geq 0$ then, we are done, otherwise, let $z_i = x_i + \lambda \geq 0$ where $\lambda \geq max\{|x_i|, 1 \leq i \leq n\}$ is any real number. Then $x = \sum_{i=1}^{n} z_i e_i$.
(5) Put $\lambda = [\frac{1}{n} \sum_{i=1}^{n} x_i] - 1$ the $x = \sum_{i=1}^{n} (x_i - \lambda) e_i$

□

Definition 4.6.
- For $A \subset N = \{1, 2, \cdots, n\}$ an element $v_A = \sum_{i \in A} e_i$ is called an elementary vector.
- $x_1, x_2 \in V$ are said to be equivalent if they are congruent modulo the subspace generated by $(1, 1, \cdots, 1)$

Lemma 4.2. *Let* N *be as before, and* $A, B \subset N$. *The notation* A^C *stands for* $N - A$, *the complementary of* A *in* N, *then:*
- *(1)* $e_N = 0$
- *(2)* $e_A + e_B = e_{A \cup B} + e_{A \cap B}$
- *(3)* $e_{A \cup B} = e_{A - B} + e_{A \cap B} + e_{B - A}$
- *(4)* $e_{A^C} = -e_A$
- *(5)* $(e_A, e_A) = |A|(n - |A|)$
- *(6)* $(e_A, e_B) = -|A||B|$ *if* $A \subset B^C$
- *(7)* $(e_A, e_B) = n|A \cap B| - |A||B|$
- *(8)* $(e_A, e_{A \cup B}) = |A|(n - |A|) - |A||B| + |A||A \cap B|)$
- *(9)* $(e_{A \cap B}, e_{A \cup B}) = (e_A, e_B) + |B - A||A - B|$
- *(10)* $(v, e_A) = -(v, e_{A^C})$ *for* $v \in V$

PROOF. (1),(2),(3),(4) fall from the definition of the elementary vectors and the Morgan's laws.

(5). From the definition of the quadratic form,

$$(e_A, e_A) = \sum_{i\in A}\sum_{j\in A}(e_i, e_j) = \sum_{i\in A}(n - |A|) = |A|(n - |A|).$$

(6). Since $A \subset B^C$, $(e_i, e_j) = -1$ for $i \in A$ and $j \in B$, therefore

$$(e_A, e_B) = \sum_{i\in A}\sum_{j\in B}(e_i, e_j) = \sum_{i\in A}(-|B|) = -|A||B|.$$

(7). We decompose the sets A and B as follow

$$A = (A \cap B) \cup (A - B) \text{ and } B = (B \cap A) \cup (B - A).$$

then

$$\begin{aligned}
(2.3)\quad (e_A, e_B) &= (e_{A\cap B} + e_{A-B}, e_{A\cap B} + e_{B-A}) \\
(2.4)\quad &= n|A \cap B| - |A \cap B|(|A - B| + |B - A|) - |A - B||B - A| \\
(2.5)\quad &= n|A \cap B| - |A \cap B|(|A| + |B| - |A \cap B|) \\
(2.6)\quad &- (|A| - |A \cap B|)(|B| - |B \cap A|) \\
(2.7)\quad &= n|A \cap B| - |A||B|
\end{aligned}$$

The (8) is a direct consequence of (7).
The (9). From (7) we have on the one hand

$$\begin{aligned}
(2.8)\quad (e_{A\cap B}, e_{A\cup B}) &= n|A \cap B| - |A \cap B||A \cup B| \\
(2.9)\quad &= n|A \cap B| - |A \cap B|(|A| + |B| - |A \cap B|)
\end{aligned}$$

and on the other hand, we have

$$\begin{aligned}
(e_A, e_B) + |A - B||B - A| &= n|A \cap B| - |A||B| + (|A| - |A \cap B|)(|B| - |A \cap B|) \\
&= n|A \cap B| - |A \cap B|(|A| + |B| - |A \cap B|)
\end{aligned}$$

The (10), follows from (1). □

Theorem 4.2. *Let $y \in F$ with $d(y)$ maximal.*
Let $S = \{A \subset N : (x, e_A) = \frac{1}{2}d(e_A)\}$
Then S is totally ordered under inclusion.

Proof. $N \in S$ and therefore S is not empty .
Let $A, B \in S$. We have to prove that either $A \subset B$ or $B \subset A$
Put $C = A - B, D = B - A$, then
if $D = \emptyset$ or $C = \emptyset$ we are done.
Otherwise, we have $C \neq \emptyset \neq D$

Since $A, B \in S$ we have $(x, e_A) = \frac{1}{2}d(e_A)$ and $(x, e_B) = \frac{1}{2}d(e_B)$

$$(x, e_A + e_B) = \frac{1}{2}(d(e_A) + d(e_B)) \tag{2.10}$$

$$= (x, e_{A\cap B}) + (x, e_{A\cup B}) \text{ by lemma } 4.2(2) \tag{2.11}$$

$$= \frac{1}{2}d(e_A + e_B) - (e_A, e_B) \text{ because } d \text{ is a quadratic form} \tag{2.12}$$

$$> \frac{1}{2}(d(e_{A\cap B} + e_{A\cup B})) - (e_{A\cap B}, e_{A\cup B}) \text{ by lemma } 4.2(9) \tag{2.13}$$

$$= \frac{1}{2}d(e_{A\cap B}) + \frac{1}{2}d(e_{A\cup B}) \tag{2.14}$$

Therefore

$$(x, e_{A\cap B}) + (x, e_{A\cup B}) > \frac{1}{2}d(e_{A\cap B}) + \frac{1}{2}d(e_{A\cup B})$$

implies that at least one of the following inequalities holds:

$$(x, e_{A\cap B}) > \frac{1}{2}d(e_{A\cap B})$$

or

$$(x, e_{A\cup B}) > \frac{1}{2}d(e_{A\cup B})$$

Which contradicts the fact that $x \in F$, and hence

$$x \in F \text{ implies that } (C = \emptyset \text{ or } D = \emptyset) \text{ so that it follows that } (A \subset B \text{ or } B \subset B)$$

□

Remark We know that the fundamental domain is defining by a finite set of inequalities. By proving that $F = F_1$, we can explicitely determine all the inequalities since we know all the e_A's.

Theorem 4.3. *We have:*

$$F = \{x \in V : (x, e_A) \leq \frac{1}{2}d(e_A), \quad \emptyset \neq A \subset N\}$$

Proof. Let F_1 be the set defined in the statement of the theorem. By the definition of F, we have $F \subset F_1$; thus the only inclusion to be proved is that $F_1 \subset F$. Let $y \in L$ so that y is not an elementary vector. Since we are considering lattice points, we can introduce a recurrence relation on the function d. From the lattice point y, we consider the neighboring points of the form $y \pm e_i$. Then for $y \in L$ and $y \neq e_A$, $A \in N$ there exists an element $u = \pm e_i \in L$ such that $d(u)+d(y-u) < d(y)$. To see that, take

$$y = \sum_{i=0}^{n} m_i e_i, \quad m_i \in \mathbb{Z} \text{ and } 0 \leq \sum_{i=0}^{n} m_i < n.$$

This is always possible since $\sum_{i=1}^{i=n} e_i = 0$.
Then

$$(y, u) - (u, u) = \frac{1}{2}(d(y) - d(u) - d(y-u)) = \pm(nm_i - \sum_{j=1}^{n} m_j) - (n-1)$$

i.e $\frac{1}{2}(d(y)-d(u)-d(y-u)) = \pm(nm_i - \sum_{j=1}^{n} m_j) - (n-1)$. This expression has no constant sign, precisely it is positive for at least one value of i. Suppose that for all i

$$\pm(nm_i - \sum_{j=1}^{n} m_j) - (n-1) < 0$$

is negative; then

- (1)
$$nm_i \leq \sum_{j=1}^{n} m_j - (n-1) \leq 2n-2 < 2n$$
implies that $m_i < 2$ for all i.
- (2)
$$nm_i \geq \sum_{j=1}^{n} m_j - (n-1) \geq -n+1 > -n$$
implies that $m_i > -1$ for all i.

From (1) and (2), follows that $m_i \in \{0,1\}$, and hence y is an e_B for some $B \subset N$, which contradicts our assumption that y is not an elementary vector.
Let $x \in F_1$ then we have to prove that $x \in F$. This is done by induction as follows. We know that $(x, e_A) \leq \frac{1}{2}d(e_A)$ for all $A \subset N$. Let $y \in L$. There exists u such that $d(u) + d(y-u) < d(y)$ and $u = \pm e_i$ for some i.
Suppose first that $y - u = e_A$ and $y \neq e_B$ for all $B \subset N$, and u is solution to the inequality $d(u) + d(y-u) < d(y)$. In this case we have:

$$(x,y) = (x, e_A + u) = (x, e_A) + (x, u) \leq \frac{1}{2}(d(e_A) + d(u)) < \frac{1}{2}d(y),$$

since $x \in F_1$. Consequently

$$(x,y) < \frac{1}{2}d(y),$$

by the choice of u. Hence in this case the inequalities corresponding to y which define F are satisfied. Next, suppose that $y - u$ is not of the form e_A.
Suppose $y \in L$ and suppose that for all z with $d(z) < d(y)$, the inequality $(x,z) < \frac{1}{2}d(z)$ is satisfied. Then we can write $y = z + u$ with $d(z) + d(u) < d(y)$. In this case

$$(x,y) = (x,z) + (x,u) < \frac{1}{2}(d(z) + d(y))$$

since z satisfies $d(z) < d(y)$. Therefore the inequality

$$(x,y) < \frac{1}{2}d(y)$$

follows as a consequence. □

Example. For $n = 3$, $N = \{1,2,3\}$ and since $e_1 + e_2 + e_3 = 0$
Then $F = \{x \in V : 2|(x, e_i)| \leq d(e_i), i = 1,2,3\}$
F is defined by 6 inequalities.

To describe F fully , we have to determine all its vertices, so that F is nothing else but the convex hull of its vertices.

3. The vertices

Put $b = \max\{d(x); x \in \overline{F}\}$.
Then the value b exists and is attained because of the continuity property of d on the one hand , and on the other hand because F is compact.

Lemma 4.3. *Let $x_0 \in V$ and $d(x_0) = b$ then x_0 is a vertex of F.*

PROOF. see [**?**]in The geometry of discrete groups. □

Theorem 4.4. *Let $S = \{A \subset N : (x_0, e_A) = \frac{1}{2}d(e_A)\}$*
The span of $\{e_A, A \in S\}$ over $\mathbb{R}$ has dimension $n-1$ and possesses a basis :
$\{e_{A_i}, 0 < i \leq n-1\}$ with $\emptyset \neq A_i \subsetneq A_{i+1} \subsetneq N$.

PROOF. Suppose that W, the $\mathbb{R}$-span of $\{e_A, A \in S\}$ has codimension ≥ 1. Then for some suitable $u \in V - \{0\}$, we have $(u, e_A) = 0$ for all $A \in S$. Then without lost of generality we can suppose $(u, x_0) \geq 0$ otherwise we multiply u by -1.

By replacing u by tu, for real t small enough, we can consider $w \in V$ such that $w = x_0 + u$ is in some neighborhood of x_0 with the property that

$$0 \leq (w, e_B) < \frac{1}{2}d(e_B) \quad \text{for} \quad B \notin S$$

. Hence we can take $w = x_0 + u$ with the conditions above, so that for $B \notin S$,

$$(w, e_B) = (x_0+u, e_B) \leq \frac{1}{2}d(e_B), \quad \text{implies that:} \quad (u, e_B) \leq \frac{1}{2}d(e_B) - (x_0, e_B) \leq d(e_B)$$

for $B \subset N$ and $B \notin S$.

However, if $B \subset N$ then $(w, e_B) = (x_0 + u, e_B) \leq \frac{1}{2}d(e_B)$.
That implies that for $A \subset N$ we have $x_0 + u \in F$ by the definition of F.
But $(x_0, u) > 0$ and so

$$d(x_0 + u) \geq d(x_0) + d(u) + 2(x_0, u) > d(x_0) \tag{3.1}$$

$$\text{and from this follows that} \quad x_0 + u \notin F \tag{3.2}$$

by the defining property of x_0. This implies $u = 0$.
The linear span of $\{e_A, A \in S\}$ is therefore of dimension $n-1$. We conclude that there are $n-1$ different proper subsets A_i such that $\{e_{A_i}, 0 < i < n; A_i \in S\}$ forms a basis of V.
If $A, B \in S$ then

$$(x_0, e_A) = \frac{1}{2}d(e_A) \text{ and } (x_0, e_B) = \frac{1}{2}d(e_B)$$

then by the above lemma, this implies that either $A \subset B$ other $B \subset A$ and hence S is totally ordered. □

Remark Indeed we can deduce that the vertex x_0 is the unique solution to the linear equations

$$(x, e_B) = \frac{1}{2}d(e_B)$$

for exactly $n-1$ elements B of S.

Remark Since S is totally ordered, $A_1 \subsetneq A_2 \subsetneq \cdots \subsetneq A_{n-1} \subsetneq N$.
The set A_i must contain at least i elements. and since all of them are proper subsets, A_i has exactly i elements. There are many ways of classifying such a sequence, but we will choose one of them in that we define

$$A_i = \{i+1, i+2, \cdots, n\} \quad 1 \leq i \leq n-1$$

and the corresponding elementary vector

$$e_{A_i} = \sum_{j=i+1}^{n} e_j$$

Theorem 4.5. *The vertices of F are the points*

$$x_\sigma = \frac{1}{n}\sum_{i=1}^{n} \sigma(i) e_i$$

where σ is a permutation of N. In particular there are $n!$ vertices.

Proof. Before we start the proof, we make the following remark. If σ is a permutation of $\{1, 2, \cdots, n\}$ then the action of σ on A_i is done elementwise, so that $A_i^\sigma = B_i$ and $|A_i| = |B_i|$. For this reason we consider at most only one chain $A_1 \subsetneq A_2 \subsetneq \cdots \subsetneq A_n = N$ of subsets of N up to a permutation. Furthermore, if we consider $x_0 = \sum_{i=1}^n \frac{i}{n} e_i$ then put $x_0^\sigma = \sum_{i=1}^n \frac{\sigma(i)}{n} e_i$, such that $x_\sigma = x_0^\sigma$. We deduce that

$$(x_0, e_{A_i}) = \frac{1}{2} d(e_{A_i}) \quad \text{implies} \quad (x_0^\sigma, e_{A_i^\sigma}) = (x_\sigma, e_{A_i^\sigma}) = \frac{1}{2} d(e_{A_i^\sigma})$$

for any permutation σ.
The proof of the theorem reduces to any particular case. In fact if

$$(x_0, e_{A_i}) = \frac{1}{2} d(e_{A_i}), \qquad \text{then} \qquad \sum_{j=i+1}^{n} (x_0, e_j) = \frac{1}{2} i(n-i).$$

We define explicitely the components of x_0.
Let $x_0 = \sum_{i=1}^n x_i e_i$ we have $(x_0, e_i) = nx_i - \sum_{j=1}^n x_j$ so that if we suppose $\sum_{i=1}^n x_i = 0$ then $(x_0, e_j) = nx_j$.
This implies $\sum_{j=i+1}^n nx_j = i(n-i)$ for $0 \leq i \leq n-1$.
Since

$$\sum_{k=i+1}^{n} (k - \frac{n+1}{2}) = i(n-i)$$

then

$$\sum_{k=i+1}^{n} nx_k = \sum_{k=i+1}^{n} (k - \frac{n+1}{2}).$$

Put $nx_i = i - \frac{1}{2}(n+1)$ then $x_i = \frac{2i-n-1}{2n}$ and it follows that

$$x_0 = \sum_{i=1}^{n} \frac{2i-n-1}{2n} e_i = \frac{1}{n}\sum_{i=1}^{n} i e_i$$

since

$$\sum_{i=1}^{n} e_i = 0$$

and

$$b = d(x_0) = \sum_{0<i<j\leq n} \frac{(i-j)^2}{n^2} = \frac{n^2-1}{12} = d(x_0^\sigma)$$

□

Example. For $n = 3$ the situation is as follows.
The generating system is (e_1, e_2, e_3) with $e_1 + e_2 + e_3 = 0$.
$N = \{1, 2, 3\} = \{i, j, k\}$. The proper subsets are

$$\{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}.$$

It follows that $e_i + e_j = -e_k$ and $e_i e_j = e_{i+j}$. The index is taken modulo 3.

$$\mathfrak{S}_3 = \{(1, 2, 3), (2, 1, 3), (3, 2, 1), (1, 3, 2), (3, 1, 2), (3, 2, 1)\}$$

The vertices are

$$\text{Vert}_3 = \left\{\frac{1}{3}(e_1 + 2e_2 + 3e_3), \frac{1}{3}(2e_1 + e_2 + 3e_3), \frac{1}{3}(3e_1 + 2e_2 + e_3),\right. \tag{3.3}$$

$$\left.\frac{1}{3}(e_1 + 3e_2 + 2e_3), \frac{1}{3}(3e_1 + e_2 + 2e_3), \frac{1}{3}(3e_1 + 2e_2 + e_3)\right\} \tag{3.4}$$

$$= \left\{-\frac{1}{3}(2e_1 + e_2), -\frac{1}{3}(e_1 + 2e_2), \frac{1}{3}(2e_1 + e_2), \frac{1}{3}(-e_1 + e_2),\right. \tag{3.5}$$

$$\left.\frac{1}{3}(e_1 - e_2), \frac{1}{3}(2e_1 + e_2)\right\} \tag{3.6}$$

3.1. Generating integral points from the vertices. We just have to show how one can construct $e_1, \cdots, e_n$ from the vertices, since they generate the $\mathbb{Z}$-module of integral elements.
Let $e_j, \quad 1 \leq j \leq n$ and σ, τ are permutations of $\{1, 2, , \cdots, n\}$ such that $\sigma(j) = n$, $\tau(i) = n - \sigma(i)$ if $i \neq j$ and $\tau(j) = n$, then define

$$v_j = \sum_{i=1}^{n} \frac{\sigma(i)}{n} e_i \quad \text{and} \quad v_j^* = \sum_{i=1}^{n} \frac{\tau(i)}{n} e_i.$$

$$\text{It follows that} \quad e_j = v_j + v_j^*.$$

This solution is not unique. However an integral point can be represented as

$$\alpha = \sum_{i=1}^{n} m_i e_i = \sum_{i=1}^{n} m_i (v_i + v_i^*)$$

4. The geometry and the combinatoric of the fundamental domain for n = 3,5

4.0.1. *Case n=3.* In this case, $N = \{1, 2, 3\}$ so that for $\emptyset \neq A \subset N$, we have $d(e_A) = 2$
for $v \in Vert_3$ then inequality for the fundamental domain is

$$F = \{x : (x, e_A) \leq \frac{1}{2} d(e_A) = 1 \quad \text{for all} \quad \emptyset \neq A \subset N\}.$$

For a fixed A we look at all vertices that is solution to the above equation. It is relevant to notice that $(v, e_A) \in \{-1, 0, 1\}$. The 0-dimensional faces described by A, are the solutions to the system of equations

$$\begin{cases} (v, e_A) &= 1 \\ (v, e_B) &= 0 \text{ for A} \subset \text{B} \end{cases}$$

and the 1-dimensional faces, are solutions to

$$(x, e_A) = 1 \text{ for all } A \subset N.$$

The fundamental domain has a very simple shape. It has 6 vertices the so-called 0-dimensional faces and 6 1-dimensional faces, that are segments. This domain is also called the *Dirichlet hexagon.*

4.0.2. **The Euler relations.** This relation is taken from the [**WR**] pp 127 theor 3.5.1]
Let P be a non empty r-dimensional polytope in $\mathbb{R}^n$. Then

$$f_{-1}(P) - f_0(P) + f_1(P) + \cdots + (-1)^{r+1} f_r(P) = 0$$

Where $f_k(P), k \geq 0$ denotes the number of k-faces of P and $f_{-1}(P) = 1$, hence for $r = 3$ one verifies that $1 - 6 + 6 - 1 = 0$

4.1. Case n=5. In this case $N = \{1, 2, 3, 4, 5\}$ so that for the subset A such that

$$\emptyset \neq A \subset N, d(e_A) = 4$$

for $v \in Vert_5$, the inequality for the fundamental domain is

$$(x, e_A) \leq d(e_A) = 2.$$

The fundamental domain is the convex hull of the vertices

$$\{ \sum_{i=1}^{5} \frac{\sigma(i)}{5} e_i, \quad \text{with } \sigma \in \mathfrak{S}_5 \ \}$$

If A is a proper subset of N, there exists at least one $v = \sum_{i=1}^{5} \frac{\sigma(i)}{5} e_i$ such that $(v, e_A) = \frac{1}{2} d(e_A)$.
Suppose $v_0 = \frac{1}{5}(e_1 + 2e_2 + 3e_3 + 4e_4 + 5e_5)$. For A consists of one element we have

A	{1}	{2}	{3}	{4}	{5}
v_0, e_A	-2	-1	0	1	2

and therefore for $\sigma \in \mathfrak{S}_5$ (v_0^σ, e_A) does not lead to change in the range of the set $\{-1, -2, 0, 1, 2\}$. We obtain v_0 in solving the system of linear equation for $A = \{1\} \subset B = \{1, 2\} \subset C = \{1, 2, 3\} \subset D = \{1, 2, 3, 4\} \subset E = \{1, 2, 3, 4, 5\}$.

Any other permutation $\sigma \in \Sigma_5$ on this sequence yields a permutation on the entries such that F is an invariant set and hence any vertex is defined by exactly 5 linear equations.

Remark
We recall that there are exactly $5! = 120$ vertices

We do not give the proof since it falls from the above description which involves the cardinality of the permutation group, but we will later find this proof in a combinatorial way.

4.1.1. **determination of the 3-dimensional faces.** From the above description, there are as many vertices as possible sequences of subsets in N and each proper subset determines a linear equation in such a way that the fundamental domain is the intersection of convex half-spaces. A linear equation in V determines a hyperplane and its interaction with F describe a 3-dimensional face of F.
From the relation $\sum_{i=1}^{5} e_i = 0$ we notice that the faces are classified in pairs of parallel faces. It will follow that the lower dimensional faces are paired in a similar fashion.

Lemma 4.4. *There are* $30 = 2^5 - 2$ *3 dimensional faces.*

PROOF. To see that we just notice that each face of F is defined via

$$(x, e_A) = \frac{1}{2} d(e_A)$$

, where A is a proper subset of N. □

They are as many faces as non trivial subsets of N; These are

$$A_1 = \{1\}, A_2 = \{1,2\}, A_3 = \{1,3\}, A_4 = \{1,4\}, A_5 = \{1,5\}, A_6 = \{2\}$$

$$A_7 = \{2,3\}, A_8 = \{2,4\}, A_9 = \{2,5\}, A_{10} = \{3\}, A_{11} = \{3,4\},$$

$$A_{12} = \{3,5\}, A_{13} = \{4\}, A_{14} = \{4,5\}, A_{15} = \{5\},$$

$$A_{16} = \{2,3,4,5\}, A_{17} = \{3,4,5\}, A_{18} = \{2,3,5\}, A_{19} = \{2,4,5\}$$

$$A_{20} = \{2,3,4\}, A_{21} = \{1,3,4,5\}, A_{22} = \{1,4,5\},$$

$$A_{23} = \{1,3,5\}, A_{24} = \{1,3,4\}, A_{25} = \{1,2,4,5\},$$

$$A_{26} = \{1,2,5\}, A_{27} = \{1,2,4\}, A_{28} = \{1,2,3,5\},$$

$$A_{29} = \{1,2,3\}, A_{30} = \{1,2,3,4\}.$$

What is interesting for the combinatorics of this domain, is that we can study completely all the geometric structure using only subsets. That is what we will be doing in the next steps. The notation $F_3(A), F_2(A), F_1(A), F_0(A)$ will denote successively the 3-dimensional, 2-dimensional, 1-dimensional and 0-dimensional faces which are contained in the face associated to the underlying subset A.

4.1.2. **Determination of the 2-dimensional faces.** A 2-dimensional face is the intersection of two 3-dimensional faces. Let $v \in F_A \cap F_B$, Then v satisfies simultaneously

$$2(v, e_A) = d(e_A)$$

and

$$2(v, e_B) = d(e_B).$$

Then consequently, it means either $A \subset B$ or $B \subset A$. Therefore the intersection of two 3-dimensional faces exists if their underlying subsets satisfy inclusion property. This reduces considerably the testing for the distinct 2-dimensional faces.

For example $F_3(\{1,2\}) \cap F_3(\{1,5\})$, $F_3(\{1,2\}) \cap F_3(\{3,5\})$ are not 2-dimensional faces. One notices that distinct subset with the same cardinality does not satisfy the inclusion property and so their inetersection does not yield a lower dimensional face.
We notice also that if $A \cap B = \emptyset$ then $F_3(A)$ and $F_3(B)$ are parallel and therefore have no common lower dimensional face.
However, to find the number of different 2-dimensional objects we will replace $\{1,2,3,4,5\}$ by $\{a,b,c,d,e\}$ where each of them can play the same role as the others do. We are going to give different description for A and B and then count the number of different possibilities.

- $A = \{a\}$ and $B = \{a,b\}$ then one has
$$\binom{5}{1}\binom{4}{1} = 5 \times 4 = 20 \text{ faces}$$
- $A = \{a\}$ and $B = \{a,b,c\}$ then one has
$$\binom{5}{1}\binom{4}{2} = \frac{5 \times 4 \times 3}{2} = 30 \text{ faces}$$
- $A = \{a\}$ and $B = \{a,b,c,d\}$ then one has
$$\binom{5}{1}\binom{4}{3} = 5 \times 4 = 20 \text{ faces}$$
- $A = \{a,b\}$ and $B = \{a,b,c\}$ then one has
$$\binom{5}{2}\binom{3}{1} = 5 \times 6 = 30 \text{ faces}$$
- $A = \{a,b\}$ and $B = \{a,b,c,d\}$ then one has
$$\binom{5}{2}\binom{3}{2} = 30 \text{ faces}$$
- $A = \{a,b,c\}$ and $B = \{a,b,c,d\}$ then one has
$$\binom{5}{3}\binom{2}{1} = 20 \text{ faces}$$

Therefore the number of 2-dimensional faces are

$$\binom{5}{1}\binom{4}{1} + \binom{5}{1}\binom{4}{2} + \binom{5}{1}\binom{4}{3} + \binom{5}{2}\binom{3}{1} + \binom{5}{2}\binom{3}{2} + \binom{5}{3}\binom{2}{1} = 20+30+20+30+30+20 = 150$$

Lemma 4.5. *We have shown that the fundamental domain F has* 150 *2-dimensional faces.*

PROOF. □

Now we are going to describe the geometric structure of the 2-dimensional faces. Suppose $\emptyset \neq A \subset B$ to find the number of vertices one has to play with the construction of possible distinct chains from the subchain $A \subset B$

- $A = \{a\}$ and $B = \{a, b\}$
  then put $C = \{a, b, c\}$ and $D = \{a, b, c, d\}$ $A \subset B \subset C \subset D$.
  there are $\binom{1}{3} = 3$ such C and 2 such D, therefore there are exactly 6 possible constructions each of which results in uniquely determining a vertex. Such a 2-dimensional face is a hexagon.
  $A = \{a\}$ and $B = \{a, b, c\}$
  in putting $C = \{a, b\}$ and $D = \{a, b, c, d\}$ then $A \subset C \subset B \subset D$.
  there are $\binom{1}{2} = 2$ such C and 2 such D, therefore there are exactly 4 possible constructions each of which results in uniquely determining a vertex. Such a 2-dimensional face is a parallelogram.
  $A = \{a\}$ and $B = \{a, b, c, d\}$
  then put $C = \{a, b\}$ and $D = \{a, b, c\}$ $A \subset C \subset D \subset B$.
  there are $\binom{1}{3} = 3$ such C and 2 such D, therefore there are exactly 6 possible constructions each of which results in uniquely determined a vertex. Such a 2-dimensional face is a hexagon.
- $A = \{a, b\}$ and $B = \{a, b, c\}$
  then put $C = \{a\}$ and $D = \{a, b, c, d\}$, $C \subset A \subset B \subset D$.
  there are 2 such C and 2 such D, therefore there are exactly 4 possible constructions each of which results in uniquely determined a vertex. Such a 2-dimensional face is a parallelogram.
  $A = \{a, b\}$ and $B = \{a, b, c, d\}$
  then put $C = \{a\}$ and $D = \{a, b, c\}$, $C \subset A \subset D \subset B$.
  there are 2 such C and 2 such D, therefore there are exactly 4 possible constructions each of which results in uniquely determined a vertex. Such a 2-dimensional face is a parallelogram.
- $A = \{a, b, c\}$ and $B = \{a, b, c, d\}$
  Then the situation is just symmetric if one supposes $A = \{a\}$ and $B = \{a, b\}$ Therefore we still have a hexagon.
- $A = \{a, b, c, d\}$ and $B = \{a\}$
  Then the situation is just symmetric if one supposes $A = \{a\}$ and $B = \{a, b, c, d\}$ and we have a hexagon.

Remark

- We have observed that there are two different types of geometries of the surfaces. They are either hexagon or parallelogram. This idea suggests one that in higher dimension this geometry becomes quiet complicated.
- The following sequence of vertices taken in this order forms a parallelogram:
  $\frac{1}{5}(5, 4, 1, 3, 2), \frac{1}{5}(5, 4, 3, 1, 2), \frac{1}{5}(5, 4, 3, 2, 1),$
  $\frac{1}{5}(5, 4, 2, 3, 1), \frac{1}{5}(5, 4, 2, 1, 3), \frac{1}{5}(5, 4, 1, 2, 3),$

4.1.3. **Determination of the 1-dimensional faces.** A 1-dimensional face is the intersection of two 2-dimensional faces whenever it is not empty. As we have done in the preceeding cases, we are going to evaluate the number of different chains of subsets with 3 components $\emptyset \neq A \subset B \subset C$

- $A = \{a\}$ and $B = \{a, b\}, C = \{a, b, c\}$
  their cardinality is
$$\binom{5}{1}\binom{4}{1}\binom{3}{1} = 5 \times 4 \times 3 = 60$$
- $A = \{a\}$ and $B = \{a, b\}, C = \{a, b, c, d\}$
  their cardinality is
$$\binom{5}{1}\binom{4}{1}\binom{3}{2} = 5 \times 4 \times 3 = 60$$
- $A = \{a\}$ and $B = \{a, b, c\}, C = \{a, b, c, d\}$
  their cardinality is
$$\binom{5}{1}\binom{4}{2}\binom{3}{1} = 5 \times 6 \times 2 = 60$$
- $A = \{a, b\}$ and $B = \{a, b, c\}, C = \{a, b, c, d\}$
  their cardinality is
$$\binom{5}{2}\binom{3}{1}\binom{2}{1} = 10 \times 3 \times 2$$

The total number of $1-$ dimensional faces is

$$\binom{5}{1}\binom{4}{1}\binom{3}{1} + \binom{5}{1}\binom{4}{1}\binom{3}{2} + \binom{5}{1}\binom{4}{2}\binom{3}{1} + \binom{5}{2}\binom{3}{1}\binom{2}{1} = 240.$$

4.1.4. **Determination of the 0-dimensional faces.** With this method we can determine the 0-dimensional face, that are vertices,if we consider chains of subsets of length 4.

$$A = \{a\} \subset B = \{a, b\} \subset C = \{a, b, c\} \subset D = \{a, b, c, d\}$$

Their number is

$$\binom{5}{1}\binom{4}{1}\binom{3}{1}\binom{2}{1} = 5 \times 4 \times 3 \times 2 = 120 = 5!$$

4.1.5. **The Euler relation.** Let P be a non empty 4-dimensional polytope in $\mathbb{R}^n$. Then

$$f_{-1}(P) - f_0(P) + f_1(P) - f_2(P) + f_3(P) - f_4(P) = 0$$

Where $f_k(P)$ denotes the number of k-faces of P , then one verifies that

$$1 - 120 + 240 - 150 + 30 - 1 = 0.$$

4.1.6. **The geometric structure of the 3-faces.**

Lemma 4.6. *There are two different kinds of a 3-dimensional face. It is either a convex hull of* 24 *vertices or a convex hull of* 12 *vertices.*

Remark We notice that for a face related to a subset A the symmetry imposed by the complement A^C of A yields in determining a symmetric face which of course has the same number of vertices . That is, in fact, the general case within this respect such that the number of non-trivial faces appears as even numbers. Having said that we take $A = \{a\}$ then we determine the vertices of $F_3(A)$ in constructing the sequences of length 4.

$$A = \{a\} \subset B = \{a, b\} \subset C = \{a, b, c\}, D = \{a, b, c, d\}$$

Then the dual sequence with respect to the complement results in a symmetric vertex.
Then for $A = \{a\}$ fixed, we have

$$\binom{4}{1}\binom{3}{1}\binom{2}{1} = 24$$

For $B = \{a, b\}$ we have

$$\binom{2}{1}\binom{3}{1}\binom{2}{1} = 12$$

We say that a 3-dimensional object is of type I if the corresponding subset is $A = \{a\}$ or $A = \{a, b, c, d\}$ and of type II if the underlined subset is $A = \{a, b\}$ or $A = \{a, b, c\}$. We now ask the question to know how many surface are there in a 3-dimensional face.

- **type I** $A = \{a\}$
  either $B = \{a, b\}$ or $B = \{a, b, c\}$ or $B = \{a, b, c, d\}$
  then we have

  $$\binom{4}{1} + \binom{4}{2} + \binom{4}{3} = 4 + 6 + 4 = 14$$

  A 3-face of type I has 14 2-dimensional faces of which we have 8 hexagons and 6 parallelograms.
- **type II** $A = \{a, b\}$
  either $B = \{a\}$ or $B = \{a, b, c\}$ or $B = \{a, b, c, d\}$
  then we have

  $$\binom{2}{1} + \binom{3}{1} + \binom{3}{1} = 2 + 3 + 3 = 8$$

  A 3-face of type II has 8 2-dimensional faces of which we have 2 hexagons and 6 parallelograms.

Remark For the pictures of these 3-faces, see figure 2 and figure 3

5. Generalization

We suppose that n is a prime number as before and

$$N = \{1, 2, \cdots n\}.$$

Then $\{0,1\}^N = \{A : A \subset N\}$ is the power set.
Let K be an $\mathbb{R}$-algebra of dimension $n-1$ generated by a basis $(e_1, e_2, \cdots, e_n)$ subject to the relation $e_n = -\sum_{i=1}^{n-1} e_i$ and $e_i * e_j = e_{i+j}$. All indices are taken modulo n.
Define on K the quadratic form

$$d(x) = n\sum_{i=1}^{n} x_i^2 - (\sum_{i=1}^{n} x_i)^2 = \sum_{i<j}(x_i - x_j)^2,$$

where $x = \sum_{i=1}^{n} x_i e_i$.
Define

$$L = \{x = \sum_{i=1}^{n} n_i e_i, \quad n_i \in \mathbb{Z}\},$$

L is a $(n-1)$-dimensional lattice in K.
The fundamental domain for d if

$$F = \{x \in K : d(x) \leq d(x-y) \text{ for all } y \in L\}$$

All the propositions above are still valid in this general case, we are going to prove a general combinatoric properties using the knowledge of certain partition set identities.
We denote by $\mathfrak{F}_k, 0 < k \leq n-2$ the set of all k-dimensional faces of F. Let $\mathfrak{S}$ be the set of all strictly monotonic (increasing) sequence of subsets of N.
if $s \in \mathfrak{S}$ then $l(s)$ is number of proper subsets of s. It is also called the length of s. Taking into account the length of $s \in \mathfrak{S}$ we can form subset $\mathfrak{I}_l = \{s : l(s) = l\}$, l standing for the length of the sequences, we see that

$$\mathfrak{S} = \bigcup_{0<i<n} \mathfrak{I}i$$

Theorem 4.6.

$$|\mathfrak{F}_{n-k-1}| = |\mathfrak{I}_k|$$

Proof. Take first $k = n-1$. Since $n = |N|$, to any sequence of length $n-1$ correspond a sequence of length n.
A sequence of length $n-1$ is just a renumbering of $\{x_1\} \subset \{x_1, x_2\} \subset \cdots \subset \{x_1, x_2, \cdots, x_n\}$ where $x_j \in \{1, 2, \cdots, n\}, 1 \leq j \leq n$. Their cardinality correspond to the number of different permutations of $(1, 2, \cdots, n)$ and this corresponds to the number of vertices of F, i.e the x_σ of theorem 17.
Before we go any further we notice that for $k = 1$, $|\mathfrak{F}_{n-2}| = 2^n - 2$. However if A and B are disjoint proper sets, then there is no chain containing both A and B and therefore $F_A \cap F_B = \emptyset$. If A determines uniquely a $(n-2)$ dimensional face of F, such that two $(n-2)$dimensional faces are not disjoint exactly when their corresponding subsets have non empty intersection. This generalizes to disjoint $s_1 = (A_1 \subset A_2 \subset \cdots \subset A_k)$ and $s_2 = (B_1 \subset B_2 \subset \cdots \subset B_k)$ sequences of length k such that none of the A_i'appears in the B_i's and vice versa, then if $A_1 \cap B_1 = C \neq \emptyset$

then a sequence of $\mathfrak{I}_{k+1}$ is obtaining from anyone of both if we add C to. And this chain obviously corresponds to a face of dimension $(k-2)$ in $\mathfrak{F}_{n-k-2}$. Furthermore if B is a subset of N of length k the number of sequences containing B is $k!(n-k)!$. But in general

$$|\mathfrak{F}_{n-k-1}| = \sum_{i_1=1}^{n-1}\sum_{i_2=1}^{n_1-i_1-1}\cdots\sum_{i_k=1}^{n_{k-1}-i_{k-1}-1}\binom{n}{i_1}\binom{n_1-i_1}{i_2}\cdots\binom{n_k-i_{k-1}}{i_k} \tag{5.1}$$

$$= \sum_{i_1+\cdots+i_k<n}\frac{n!}{i_1!.\cdots.i_k!(n-\sum_{j=1}^{k}i_j)!}. \tag{5.2}$$

where $n_i = n - \sum_{k=1}^{i-2} i_k$ and $\binom{n}{m} = 0$ if $m > n$ □

Theorem 4.7. *There are exactly* $\frac{n-1}{2}$ *classes of different non congruent* $(n-1)$*-faces.*

Proof. This theorem is illustrated in the case $n = 3$ and $n = 5$ by figure 2 and figure 3 respectively.
To prove it, observe that, on one hand, two subsets A and B with the same cardinality have the same number of vertices as solutions to finding different sequences of length n containing A . Then replace elements of A by that of B yield a bijective map on the sets of vertices. On another hand, subsets with different cardinalities have of course different number of vertices and consequently determine two different geometries. Finally if $A \subset N$, the underlined face of A and A^C have the same geometry since they are parallel and F is a symmetric convex set. □

Theorem 4.8.

$$|\mathfrak{F}_k| = \sum_{i=0}^{k+1}(-1)^i(k+1-i)^n\binom{k+1}{i}$$

Proof. The formula

$$\sum_{i_1=1}^{n-1}\sum_{i_2=1}^{n_1-i_1-1}\cdots\sum_{i_k=1}^{n_{k-1}-i_{k-1}-1}\binom{n}{i_1}\binom{n_1-i_1}{i_2}\cdots\binom{n_k-i_{k-1}}{i_k}$$

is just

$$\sum_{i_1=1}^{n-1}\sum_{i_2=1}^{n_1-i_1-1}\cdots\sum_{i_k=1}^{n_{k-1}-i_{k-1}-1}\frac{n!}{i_1!i_2!\cdots i_k!(n-i_1-\ldots i_k)} = \tag{5.3}$$

$$\sum_{i_0+i_1+\cdots+i_k=n}^{n-1}\frac{n!}{i_0!i_1!\cdots i_k!} \tag{5.4}$$

$$= n! \tag{5.5}$$

times coefficient of X^n in $(e^X-1)(e^X-1)\cdots(e^X-1)$ $(k+1)$ times

$$= (k+1)^n - \binom{k+1}{1}k^n + \binom{k+1}{2}(k-1)^n - \cdots + (-1)^k\binom{k+1}{k}1^n$$

$$= \sum_{i=0}^{k+1}(-1)^i(k+1-i)^n\binom{k+1}{i}$$

where $i_0 = n - (i_1 + \cdots + i_k)$ □

Put

$$\gamma(n,m) = \sum_{i=0}^{m} (-1)^i (m-i)^n \binom{n}{i}$$

and

$$\Gamma(n,m) = \frac{1}{m!}\gamma(n,m) = \frac{1}{m!}\sum_{i=0}^{m} (-1)^i (m-i)^n \binom{m}{i}$$

Then we have $\gamma(n,m) = |\mathfrak{F}_k|$.

Lemma 4.7.

$$m^n = \sum_{j=1}^{n} \binom{m}{j} j!\Gamma(n,j)$$

PROOF. Let's take two sets A and B having n and m elements respectively. Every function $f : A \to B$ can be reviewed as a surjective function if we suitably change its codomain . That is if we consider $f : A \to f(A) = \{y = f(x), x \in A\} \subset B$. Therefore the total number of functions from A to B equal to m^n is also equal to the number of the functions in the set

$$\{f : A \to B with \quad |f(A)| = \gamma_j, \quad j = 1, 2, \cdots, m\}.$$

These functions are pairwise disjoint. The number of surjection from a set of n elements onto a set of $\gamma_j \leq n$ elements is equal to $\gamma(n,j) = j!\Gamma(n,j)$. Since j elements can be chosen out of the m elements of B in $\binom{m}{k}$ possible ways, the lemma then follows. □

Lemma 4.8.

$$\Gamma(n+1,m) = \Gamma(n,m-1) + m\Gamma(n,m)$$

PROOF. □

With this one can tabulate the γ's and Γ's. Moreover $|\mathfrak{F}_{n-k-1}| = \gamma(n,k)$

Example This is a table of $\gamma(n,j)$

	1	2	3	4	5	6	7	
1	1							
2	1	2						
3	1	6	6					
4	1	14	42	24				
5	1	30	150	240	120			
6	1	62	540	1560	1800	720		
7	1	126	1806	8400	16800	15120	5040	

Lemma 4.9. *For $n > 1$*

$$\sum_{m=1}^{n}(-1)^{m-1}(m-1)!\Gamma(n,m) = 0$$

PROOF. Observe that $k!\gamma(n,k)$ is the coefficient of x^n in $(e^x-1)^k$. But

$$\frac{1}{k!}(e^x-1)^k = \sum_{n=k}^{\infty}\frac{\Gamma(n,k)}{n!}x^n$$

$$(-1)^{k-1}(k-1)!\frac{(e^x-1)^k}{k!} = \sum_{n=k}^{\infty}(-1)^{k-1}(k-1)!\frac{\Gamma(n,k)}{n!}x^n$$

and therefore

$$\sum_{k=1}^{\infty}(-1)^{k-1}\frac{(e^x-1)^k}{k!} = \sum_{k=1}^{\infty}\sum_{n=k}^{n}(-1)^{k-1}(k-1)!\Gamma(n,k)\frac{x^n}{n!}$$

But

$$log(1+(e^x-1)) = \sum_{k=1}^{\infty}\frac{x^n}{n!}\sum_{k=1}^{n}(-1)^{k-1}(k-1)!\Gamma(n,k)$$

This implies that

$$x = \sum_{k=1}^{\infty}\frac{x^n}{n!}\sum_{k=1}^{n}(-1)^{k-1}(k-1)!\Gamma(n,k)$$

hence for $n > 1$

$$\sum_{k=1}^{n}(-1)^{k-1}(k-1)!\Gamma(n,k) = 0$$

□

We now state the well-known result in the combinatorial theory of polytopes, Euler's relation. $\Gamma(n,0) = (-1)^{n-1}$

Theorem 4.9. The Euler relation

$$\sum_{k=0}^{n}(-1)^{k+1}k!\Gamma(n,k) = 0$$

PROOF. We give a very simple proof base on the recurrence relation for $\Gamma(n,m)$. Suppose $\mathbf{n = 2}$ then we have $-(-1)+1-2!\Gamma(2,1) = 1+1-2 = 0$ and we are done. Suppose $\mathbf{n > 2}$ then the relation

$$\Gamma(n+1,m) = \Gamma(n,m-1) + m\Gamma(n,m)$$

implies that

$$(-1)^m m!\Gamma(n+1,m) = (-1)^m m((m-1)!\Gamma(n,m-1) + m!\Gamma(n,m))$$

then

$$\sum_{m=1}^{n}(-1)^m m!\Gamma(n+1,m) = \sum_{m=1}^{n}(-1)^{n-1}(m-1)!\Gamma(n,m)$$

and finally use the above lemma and the facts that $\Gamma(n,n) = 1$ and $\Gamma(n,0) = (-1)^{n-1}$ □

Remark We observe that the $\Gamma(n,m)$'s are increasing in the first instance and then decrease with respect to m. It reaches its maximal value at about $[\frac{n+1}{2}]$. it then easy to see that it has link with the behavior of $m!(n-m)!$. The symbol $[x]$ stands for the largest integer less than the real number x.

6. Cyclotomy revisited

Here we are going to describe some implications which have a link to the determination of the fundamental domain. These facts are known and proved by different methods.
Let K be as before a cyclotomic number field. We define the measure μ on K as follows:

$$\mu(x) = \sum_{\sigma} |\sigma(x)|^2,$$

where $x \in K$ and σ runs over the different $\mathbb{R}$-algebra homomorphisms $\sigma : K \to \mathbb{C}$. We extend μ to $K \otimes_{\mathbb{Q}} \mathbb{R}$ by d as $d(x) = Tr_{K/\mathbb{Q}}(xx^{-1})$. Here the x^{-1} is suitably defined as $\sigma(x^{-1}) := \overline{\sigma(x)}$. In fact Gauss used this as metric to prove that the ring $\mathbb{Z}[i]$ is an Euclidean ring. My aim here is to prove that this also works for other cases such as 3, 5, 4, 7 and may also work in many others. Gauss used a classical inequality between the arithmetic mean and the geometric mean of finite number of positive real numbers.

Lemma 4.10. *Let $x_1, \cdots, x_n \in \mathbb{R}$, positive and*
$\alpha_1, \cdots, \alpha_n > 0$ with $\alpha_1 + \cdots + \alpha_n = 1$
Then

$$x_1^{\alpha_1}.\cdots.x_n^{\alpha_n} \leq \alpha_1 x_1 + \cdots + \alpha_n x_n$$

This lemma generalizes the geometric arithmetic mean inequality. This is:

Lemma 4.11. *We have*

$$N(x)^2 = \left(\prod_{\sigma} |\sigma(x)|\right)^2 \leq \left(\frac{d(x)}{n}\right)^n$$

where σ runs over all $n = \frac{1}{2}(K : \mathbb{Q})$ different complex embeddings of K in $\mathbb{C}$ and $N(x)$ is the norm function.

Definition 4.7. An integral domain R is called Euclidean with respect to a given function $f : R \to \mathbb{N}$ if f has the following properties:

- $f(\alpha) = 0$ if and only if $\alpha = 0$
- For all $\alpha, \beta \in R - \{0\}$ there exists a $\gamma \in R$ such that $f(\alpha - \beta\gamma) < f(\beta)$
- For every $\kappa > 0$ the set $\{f(\alpha) : \alpha \in R, f(\alpha) < \kappa\}$ is finite. We call such an f an Euclidean function on R.

Equivalent definitions are given in [**H.W.L**]. However certain authors restrict their definition to the first two properties. Here the (absolute) norm function N stands for f and satisfies all the properties. We note that $d_{K/\mathbb{Q}}$ the distance function defined above and that is related to the field K/$\mathbb{Q}$. We have the following proposition:

Proposition 6.1. *Let $K \subset L$ be a number fields, and put $n = (K : \mathbb{Q})$ and*

$$d(\alpha) = \sum |\sigma(\alpha)|^2 \quad \text{for} \quad \alpha \in L$$

Then

- *(1)*

$$d_L(\alpha) - d_L(\alpha - \beta) = (L : K) \left(d_K \left(\frac{1}{(K : L)} Tr_{L/K}(\alpha) - \beta \right) - d_K(\frac{1}{(L : K)} Tr_{L/K}(\alpha) - \beta) \right)$$

  for all $\alpha \in L, \beta \in K$.
- *(2) if $L = K(\zeta_m)$ then*

$$d_L(\alpha) = \frac{1}{m} \sum_{j=1}^{m} d_K(Tr_{L/K}(\alpha \zeta_m^j)).$$

PROOF. [**F-L**] □

In fact if

$$F_K = \{x \in K : d_K(x) < d_K(x - \gamma) \text{ for all } \gamma \in R\}$$

then $b_K = sup\{d_K(x) : x \in F_K\}$ and for every $x \in K$ there is a $\gamma \in R$ such that $d_K(x - \gamma) \leq b_K$. Thus K is norm Euclidean if $b_K < 1$ and sometimes $b_K = 1$ is sufficient.

Definition 4.8. We call $b' \in \mathbb{R}$ a usable bound if $b' \geq b_K$ and if for all $x \in F_K$ such that $d(x) = b'$ there is a root of unity $\zeta \in R$ and $\gamma \in R$ such that

$$d(x - \gamma) = d(x - \gamma - \zeta) = b'.$$

We see that every $b' > b_K$ is a usable bound and therefore if b' is a usable bound for K , then K is norm Euclidean.

Theorem 4.10. *Let ζ_m be a primitive m^{th} root of unity, and $L = K(\zeta_m)$. Then $b_L \leq (L : K) b_K$, and if b' is a usable bound for K then so is $(L : K)b'$ for L.*

We then remark that we have $b_{\mathbb{Q}} = \frac{1}{4}$ as simple exercise. Then we see that any cyclotomic field $K/\mathbb{Q}$ with degree $\varphi(n)$ satisfies the bound condition $b_K \leq \frac{\varphi(n)}{4}$ and therefore:

Lemma 4.12. *For $n = 1, 3, 4, 5, 8, 12$ $K = \mathbb{Q}(\zeta_n)$ is norm Euclidean.*

PROOF. Since $\frac{1}{4}$ is a usable bound for $\mathbb{Q}$ we conclude from the theorem that $\frac{\varphi(n)}{4}$ is a usable bound for any n. hence for $\varphi(n) \leq 4$, $\varphi(n)$ is a usable bound for any n. □

Remark The case $n = 5$ was long time ago proved by Ouspensky, see [**O**].

Theorem 4.11. *For $n = 1, 3, 4, 5, 7, 8, 9, 11, 12, 15, 20$ $K = \mathbb{Q}(\zeta_n)$ is norm Euclidean.*

PROOF. To see this we just have to evaluate $b_K = \frac{n^2-1}{2}$ for primes 3,5,7,11 and then use the transition property defining a usable bound for composite number. For $n = 20 = 4 \times 5$

$$b_{\mathbb{Q}(\zeta_{20})} = 2^2 b_{\mathbb{Q}(\zeta_5)} = 8 = (\mathbb{Q}(\zeta_{20}) : \mathbb{Q}).$$

The same argument applies to $n = 15$. Then we see that $b_K \leq 1$ for all these values. □

Remark . This results are not known from different authors, like [**H.W.L**], but we don't simply know how to extend the result for larger m. We therefore still know very few cyclotomic fields which are norm Euclidean.

6.1. The construction of n^{th} set. In this part of the paper we intend to provide a very simple way of determining an n^{th} set.

Definition 4.9. Let $\mathfrak{a}$ be an integral ideal of $\mathbb{Z}[\zeta_n]$ the ring of integers of $\mathbb{Q}[\zeta_n]$ and μ_n be as before the group of the n^{th} roots of unity. A finite set S of integer of $\mathbb{Z}[\zeta_n]$ is called a $\frac{1}{n}$-set (or $\frac{1}{n}$-representative system) modulo $\mathfrak{a}$ if the set of ζx,($\zeta \in \mu_n, x \in$ S) forms together with 0 a complete representative system of residues modulo $\mathfrak{a}$.

We intend to give, in case where n is prime, a simple construction of such an S. We must notice that there is not only one way of constructing an n-th set. A very simple way is obtained for example, as follows. For $\mathfrak{a}$ prime to n, take any system of representatives modulo $\mathfrak{a}$. Pick up an element x, put it in S and delete all elements which are congruent to $\zeta^i x$, $1 \leq i < n$ and repeat the process with any non deleted element until all elements are deleted.
The difficulties here are that we can not really make a practical computation. For example, for ideals with the same absolute prime norm one may use the same n-th set. But by using the geometry one can fix this in a canonical way such that it does depend on the action of the unit group and therefore depends no more on the ideal itself, but on each representative of it. This enables one to handle practical computation. We then make use of a fundamental domain F we have constructed so far.

Definition 4.10. Let F be the fundamental domain constructed above, and π an algebraic integer , then $F_\pi = \pi F \cap \mathbb{Z}[\zeta_n] \otimes_{\mathbb{Z}} \mathbb{R}$ is called a set of residues modulo π.

F_π is just a homothetic deformation of F and therefore both have the same geometry. This set of residues was called by Habicht [**Ha**] "absolute" set of residues modulo π in place of "smallest". He used this definition to give a geometric proof of the law of cubic reciprocity.

- We have classified the $(n-2)$-dimensional faces according to the length of the corresponding subset. If A^k is the set of all subsets of cardinality k, then for $k = n-2$, there are exactly $\frac{n-1}{2}$ different incongruent $(n-2)-$faces. This is an equivalence relation i.e $A \cong B$ if and only if $|A| = |B|$ or $|A| = n-|B|$. We easily see that the cardinal of $A^k = (card(A^{n-k}))$ is a multiple of n, hence in each class A^k we choose $2\frac{|A^k|}{n}$ faces, and for this choice, consider the union of the cones at the origin, each containing the $(n-2)$-dimensional

face as section. From this point of view we can construct symmetric $\frac{1}{n}$-set as Mc Gettrick, C.R. Matthews did in their Ph. D dissertations. This is sometimes useful, but is not enough to have a $\frac{1}{n}$-sets, we need to know how to count points in it. For a subset of $\mathfrak{D} \subset A^k$ of cardinality $2\frac{|A^k|}{n}$, then for $A \in \mathfrak{D}$, $F_{n-2}(A)$ has an even number of $F_{n-3}(A)$ then we keep a half of them in $F_{n-2}(A)$ as boundaries, and then consider the section of the cone containing the origin and limited by the remainder from the $F_{n-2}(A)$. We should also make sure that the $F_{n-2}(A)$'s, by rotation, do not match with any other remaining $F_{n-2}(A)$, $A \notin \mathfrak{D}$. This indeed is very difficult, but since all the faces are defined by linear equations, this amounts to saying that half of the inequalities have to be strict.

- Furthermore we have another description of a $\frac{1}{n}$-set.
  See the permutation group $\mathfrak{S}_n$ as acting on the set N. We have already seen that this action runs over the set of vertices. That is, the natural action of $\mathfrak{S}_n$ onto N is transitive and we may write N as a homogeneous space:

$$N \cong \mathfrak{S}_n/\mathfrak{S}_{n-1}.$$

  Then we take any of the number in N and consider all neighboring face. Here a neighbor face of A is any subset B containing (or is contained in) A. Choose for example $A = \{1\}$ then A has $(n-1)!$ vertices and $2^{n-1} - 2$ neighbors. Then the n^{th} set must contain only F_A as a proper face and half of each of the neighboring faces. We have the defining equation

$$F_{\frac{1}{n}} = \{x \cong (x_1, \cdots, x_{n-1}, 0) \in F : x_1 \geq 0, \cdots, x_{\frac{n-1}{2}} \geq 0, x_{\frac{n+1}{2}} > 0, \cdots, x_{n-1} > 0\}$$

Remark We notice that for the first case we have more vertices of the original fundamental domain and many equations than in the second case where we only simple inequalities, and fewer vertices.

6.2. The Gauss Lemma. Another application of the $\frac{1}{n}$-set is the Gauss lemma. Let $\mathfrak{a}$ be an integral ideal of K=$\mathbb{Q}(\zeta_n)$ prime to n and let S be an $\frac{1}{n}$-set modulo $\mathfrak{a}$. If α is any integer of K prime to $\mathfrak{a}$, there exists a unique n^{th} root of unity $\varepsilon(\alpha, x)$ such that

$$\alpha x \equiv \varepsilon(\alpha, x)x' \bmod \mathfrak{a}, \qquad \text{with} \qquad x' \in S \text{ for a given} \quad x \in S.$$

If $\mathfrak{a} = \mathfrak{p}$ is a prime ideal, then the power residue symbol $(\frac{\alpha}{\mathfrak{p}})_n$ of degree n is defined by

$$\alpha^{\frac{N(\mathfrak{p})-1}{n}} \equiv \left(\frac{\alpha}{\mathfrak{p}}\right)_n \bmod \mathfrak{p}, \quad \text{and is an } n^{th} \text{ root of 1.}$$

Here $N(\mathfrak{p}) = (\mathbb{Z}[\zeta_n] : \mathfrak{p})$. If $\mathfrak{a}$ is not a prime, then the power residue symbol is defined multiplicatively as

$$\left(\frac{\alpha}{\mathfrak{a}_1\mathfrak{a}_2}\right)_n = \left(\frac{\alpha}{\mathfrak{a}_1}\right)_n \left(\frac{\alpha}{\mathfrak{a}_2}\right)_n.$$

Theorem 4.12. Generalization of the Gauss-Schering Lemma[R-H],[KB2]

$$\prod_x \varepsilon(\alpha, x) = \left(\frac{\alpha}{\mathfrak{p}}\right)_n, \quad (x \in S).$$

PROOF. If $\mathfrak{a} = \mathfrak{p}$ is a prime ideal, then $\prod x = \prod x' \mod \mathfrak{p}$ entails

$$\prod_x \varepsilon(\alpha, x) \equiv \alpha^{\frac{N(\alpha)-1}{n}} \mod \mathfrak{p}.$$

The proposition is true by the definition.
If $\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2$ We are going to prove the theorem by induction on the number of ideals factors of $\mathfrak{a}$. Thus let S_2 be the set of elements of S, which are divisible by $\mathfrak{a}_1$, and let $\beta_1 \in K$ be an integer such that $(\beta_1, \mathfrak{a}) = \mathfrak{a}_1$. Then for each $x \in S_2$, there exists an integer $\gamma(x) \in K$ such that $\beta_1\gamma(x) \equiv x \bmod \mathfrak{a}$, and the set of all $\gamma(x)$ forms a $\frac{1}{n}$-set of residues modulo$(\mathfrak{a}_2)$. Since $\alpha x \equiv \varepsilon(\alpha, x)x' \mod \mathfrak{a}$ yields $\alpha\beta_1\gamma(x) \equiv \varepsilon(\alpha, x)\beta_1\gamma(x) \mod \mathfrak{a}$. and consequently $\alpha x \equiv \varepsilon(\alpha, x)\gamma(x') \mod \mathfrak{a}_2$. We then have $\prod_x \varepsilon(\alpha, x) = (\frac{\alpha}{\mathfrak{a}_2})_n, x \in S_2$.
consider next $S_1 = S - S_2$. Here we see that S_1 is the union of $norm(\mathfrak{a}_2)$ sets, each of which is a $\frac{1}{n}$-set of residues system mod$(\mathfrak{a}_1)$. Since $norm(\mathfrak{a}_2) \equiv 1 \mod (n)$ we have

$$\prod_x \varepsilon(\alpha, x) = \left(\frac{\alpha}{\mathfrak{a}_1}\right)_n^{N(\mathfrak{a}_2)} = \left(\frac{\alpha}{\mathfrak{a}_1}\right)_n, x \in S_1.$$

□

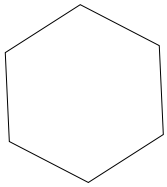

Fig 1. Fundamental domain for n=3.

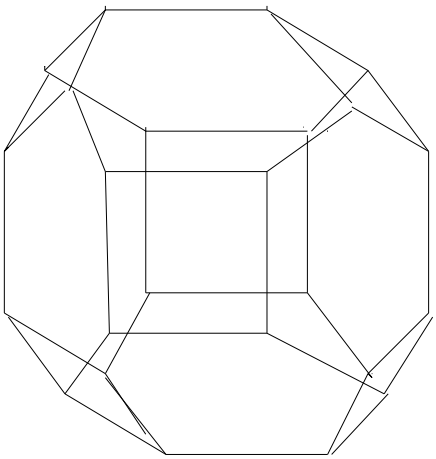

fig 2. 3 Dim face for A={a} or A={a,b,c,d}

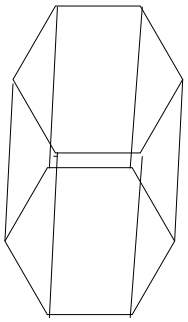

Fig 3. 3 Dim face for A={a,b} or A={a,b,c}

FIGURE 1. Fundamental domain for n=3 and 3-faces for n=5

CHAPTER 5

THE GAUSS SUMS AND THE FUNDAMENTAL DOMAIN

In this chapter we intend to extend the idea of McGettrick and Cassels in making use of the fundamental domain to find identities linked to the understanding of the Cassels' conjecture. We do not deal explicitely with elliptic functions; we mostly think of that in terms of a 2-dimensional lattice in a quadratic number field. We seek such identities in general algebraic number fields.

Definition 5.1. Let Γ be the lattice of the algebraic integers in an algebraic number field K. Let α be an integer of K. We say that $\beta \in K$ is an $\alpha-$ division point modulo Γ if $\alpha\beta \equiv 0 \bmod \Gamma$.
We shall consider henceforth the field $K = \mathbb{Q}(\zeta)$ where ζ is an n^{th} root of unity, $n > 2$ prime. We consider $\mathbb{Z}[\zeta]$ as a subring of $\mathbb{Q}(\zeta) \otimes_{\mathbb{Q}} \mathbb{R}$.
We have already proved that

$$F_\alpha \cap (\mathbb{Z}[\zeta] \otimes 1)$$

is a complete set of residues modulo α. It has $N_{K/\mathbb{Q}}(\alpha)$ elements. We shall denote this set again by F_α. This should cause no confusion.
Let $\pi|p$ be a prime not dividing n with norm q, then a fortiori $n|(N_{K/\mathbb{Q}}(\pi) - 1)$, therefore $\mathbb{F}_q$ contains an n^{th} root of unity ζ. If S_π is any n^{th} set modulo π, then:

Theorem 5.1.

$$\prod_{x \in S_\pi} x = -\zeta_{S_\pi}$$

Where ζ_{S_π} is an n^{th} root of unity depending on S_π

Proof. From Wilson's Theorem, we have

$$\prod_{x \in F_\pi - \{0\}} x \equiv -1 \qquad (\text{mod } \pi).$$

But since

$$F_\pi = (\bigcup_{i=1}^{n} \zeta^i S_\pi) \cup \{0\},$$

then

$$\prod_{x \in F_\pi - \{0\}} x = \prod_{x \in S_\pi} x \prod_{x \in S_\pi} x\zeta \cdots \prod_{x \in S_\pi} x\zeta^{n-1} = \zeta^{\frac{(q-1)}{n}(1+2+\cdots+n-1)}(\prod_{x \in S_\pi} x)^n = (\prod_{x \in S_\pi} x)^n = -1;$$

then the result follows. □

Remark The construction of ζ_S . The ζ_S is constructed such that it satisfies action of the Galois group as the Gauss sum does. Indeed: Let n be an odd prime, an n^{th} set is of the form

$$S_0 = \frac{1}{1-\zeta} F_0$$

where F_0 is invariant under the Galois group and is contained in $[0,1]e_1 \times [0,1]e_2 \cdots \times [0,1]e_{n-1}$ and both have the same volume, for the Lebesgue measure.
For an ideal α,

$$S_\alpha = \alpha S_0 = \frac{\alpha}{1-\zeta} F_0.$$

The Galois group operates on S_α elementwise. For g a fixed primitive root modulo n, and for σ a generator of the Galois group such that $\sigma(\zeta) = \zeta^\sigma = \zeta^g$ and then, this implies that

$$\sigma(S_\alpha) = \frac{\sigma(\alpha)}{1-\sigma(\zeta)} F_0 = (\sum_{i=0}^{g-1} \zeta^i)^{-1} \ \frac{\sigma(\alpha)}{1-\zeta} F_0.$$

therefore $S_{\sigma(\alpha)} = \sum_{i=0}^{g-1} \zeta^i \sigma(S_\alpha)$. Let us define

$$R(\alpha) = \prod_{x \in S_\alpha} x \qquad (\text{mod } \alpha)$$

then

$$R(\sigma(\alpha)) = \left(\frac{\sum_{i=0}^{g-1} \zeta^i}{\sigma(\alpha)} \right)_n R(\alpha)^\sigma.$$

Remark If g' is the inverse of the primitive root of g modulo n, then replace α by $\sigma^{-1}(\alpha)$ to have

$$R(\alpha) = \left(\frac{\sum_{i=0}^{g'-1} \zeta^i}{\alpha} \right)_n R(\sigma^{-1}(\alpha))^\sigma = \left(\frac{\sum_{i=0}^{g'-1} \zeta^i}{\alpha} \right)_n R(\sigma^{-1}(\alpha))^g.$$

We easily see that if g is primitive root modulo n, then g' is also a primitive root modulo n thus we have:

Lemma 5.1. Identity 0
Let g be any primitive root modulo n and $\sigma : \zeta \mapsto \zeta^g$ the element of the Galois group G associated to g. Let α be an algebraic integer such that $\alpha \equiv 1 \bmod n$, then we have the following identity:

$$R(\alpha) = \left(\frac{\sum_{i=0}^{g-1} \zeta^i}{\alpha} \right)_n R(\sigma(\alpha))^{g'}.$$

Where g' is the inverse of g modulo n.

PROOF. The proof is the consequence of the last identity for $R(\alpha)$. □

We observe that since we have $\phi(n-1)$ pairs (g, g') of primitive roots modulo n we therefore have $\phi(n-1)$ such identities for $R(\alpha)$

We notice that there is an extra factor in the formulation of$R(\alpha)$, therefore we will prefer another formulation $\Omega_0(S_0,\alpha)$ which avoids this perturbation. furthermore $\Omega_0(S_0,\alpha)$ will satisfy complex conjugate transformation, i.e $\Omega_0(S_0,\overline{\alpha}) = \overline{\Omega_0(S_0,\alpha)}$. This refers to a property of the Gauss sums.
We can sumarize these properties as follows:

$$\sigma(\Omega_0(S_0,\alpha)) = \Omega_0(S_0,\sigma(\alpha)) \quad \text{and} \quad \sigma^{-1}(\Omega_0(S_0,\alpha)) = \Omega_0(S_0,\alpha)^{-1}.$$

Remark : We have to show how to construct $R(\pi)$ set from the above description. It would be invariant under the complex conjugate action. It therefore needs a correction factor. This is due to the fact that the $n-$set attached to π, S_π and the $n-$set attached to $\pi^{\sigma^{-1}}$, $S_{\pi^{\sigma^{-1}}}$, are not necessary conjugate sets. We give explanations and solutions in the next section.

1. First identity

We fix a n^{th}-set S_0 once and for all, such that $S_\pi = \pi S_0$.
Let u be a unit in $K = \mathbb{Q}(\zeta) \otimes_{\mathbb{Q}} \mathbb{R}$, if we replace π by $u\pi$ then the lemma follows:

Lemma 5.2. *The function $R(\pi)$ satisfies for u a unit of K;*

$$R(u\pi) = \left(\frac{u}{\pi}\right)_n R(\pi)$$

PROOF. Indeed, if $x \in S_{u\pi}$ then $u^{-1}x \in S_\pi$

$$R(\pi) = \prod_{x\in S_{u\pi}} u^{-1}x = u^{-\frac{q-1}{n}} \prod_{x\in S_{u\pi}} x = \left(\frac{u}{\pi}\right)_n^{-1} R(u\pi)$$

□

The correction factor is done as follows. Before we study a general case, we go through the case $n = 5$ first.

Lemma 5.3. *Let the prime $\alpha \equiv 1 \bmod 5$ be an algebraic integer in $\mathbb{Z}[\zeta]$ and S_α a fifth set modulo α, chosen as before. Choose σ to be the generator of the Galois group of $\mathbb{Q}[\zeta]/\mathbb{Q}$ such that $\sigma(\zeta) = \zeta^2$. If we define*

$$\Omega_0(S_0,\alpha) = \left(\frac{\zeta^2}{\alpha}\right)_5 R(\alpha)$$

then $\Omega_0(S_0,\alpha)^{\sigma^2} = \Omega_0(S_0,\alpha^{\sigma^2})$

PROOF. We do this proof only for prime π and extend this multiplicatively.

If σ maps $\zeta \to \zeta^2$ then σ^2 is the complex conjugate, so that

$$x \in \frac{\pi}{1-\zeta}F_0 \quad \text{implies that} \quad x^\sigma \in \frac{\pi^\sigma}{1-\zeta^\sigma}F_0^\sigma = \frac{\pi^\sigma}{1-\zeta^\sigma}F_0 = \frac{\pi^\sigma}{1-\zeta^2}F_0 \quad \text{since}$$

F_0 is invariant under the Galois group.
Then from $S_{\pi^\sigma} = (1+\zeta)S_\pi$ follows that

$$R(\pi^\sigma) \equiv \prod_{x\in S_\pi}(1+\zeta)x^\sigma \equiv \left(\frac{1+\zeta}{\pi^\sigma}\right)_5 \prod_{x\in S_\pi} x^\sigma = \left(\frac{1+\zeta}{\pi^\sigma}\right)_5 R(\pi)^\sigma \pmod{\sigma(\pi)}.$$

In replacing π by π^σ we have

$$R(\pi^{\sigma^2}) = \left(\frac{1+\zeta}{\pi^{\sigma^2}}\right)_5 R(\pi^\sigma)^\sigma = \left(\frac{1+\zeta}{\pi^{\sigma^2}}\right)_5 \left(\frac{1+\zeta}{\pi^{\sigma^2}}\right)_5^\sigma R(\pi)^{\sigma^2} \qquad \text{since} \qquad \sigma^2$$

is the complex conjugate map we have

$$R(\pi)R(\pi^{\sigma^2}) = \left(\frac{1+\zeta}{\pi^{\sigma^2}}\right)_5 \left(\frac{1+\zeta}{\pi^{\sigma^2}}\right)_5^\sigma.$$

On the one hand, we have:

$$\left(\frac{1+\zeta}{\pi^{\sigma^2}}\right)_5 = \left(\frac{1+\zeta^{\sigma^2}}{\pi}\right)_5^{-1} = \left(\frac{1+\zeta^{-1}}{\pi}\right)_5^{-1} = \left(\frac{1+\zeta}{\pi}\right)_5^{-1} \left(\frac{\zeta}{\pi}\right)_5.$$

On the another hand, we have:

$$\left(\frac{1+\zeta}{\pi^{\sigma}}\right)_5^\sigma = \left(\frac{1+\zeta^{\sigma}}{\pi^{\sigma^2}}\right)_5 = \left(\frac{1+\zeta^{\sigma^{-1}}}{\pi}\right)_5^{-1} = \left(\frac{1+\zeta^{-1}}{\pi}\right)_5^{-1} = \left(\frac{1+\zeta^{3}}{\pi}\right)_5^{-1}.$$

Therefore if we put

$$B = \frac{\zeta}{(1+\zeta)(1+\zeta^3)} = \frac{\zeta}{1+\zeta+\zeta^3+\zeta^4} = -\zeta^{-1} \quad \text{then} \quad R(\pi)R(\pi^{\sigma^2}) = \left(\frac{B}{\pi}\right)_5.$$

If we put $A = \zeta^2$ then

$$A/A^{\sigma^2} = -\zeta^{-1} \times u^5, \qquad \text{where u is an algebraic integer.}$$

and so

$$R(\pi)R(\pi^{\sigma^2}) = \left(\frac{A}{\pi}\right)_5 \left(\frac{A}{\pi^{\sigma^2}}\right)_5$$

we determine A up to a fifth power. This solution is no way unique but we choose it as simple as possible. For example we take $A = \zeta^2$ then we have

$$\frac{A}{A^{\sigma^2}} = \frac{\zeta^2}{\zeta^3} = -\zeta^{-1}$$

and with this choice we have

$$\Omega(S_0, \pi) = \left(\frac{\zeta^2}{\pi}\right)_5 R(\pi),$$

then the assertion of lemma follows □

Remark We notice that the choice for $A = \zeta^2$ can be obtained by solving the congruence equation $2x \equiv -1 \pmod 5$ which has the solution $x \equiv 2 \bmod 5$.
we can generalize it as follows.

Theorem 5.2. *Let p and n be prime numbers such that $p \equiv 1 \bmod n$ and $\pi|p$ is a prime factor of p. Then there exists m, $0 \leq m \leq n$, so that*

$$\Omega(S_0, \pi) = \left(\frac{\zeta^m}{\pi}\right)_n R(\pi)$$

satisfies

$$\overline{\Omega(S_0,\pi)} = \Omega\left(S_0, \pi^{\sigma^{\frac{n-1}{2}}}\right)$$

PROOF. Let g be a primitive root modulo n. Then $\sigma : \zeta \to \zeta^g$ generates the Galois group of $\mathbb{Q}(\zeta_q)$.

$$R(\pi^\sigma) = \left(\frac{1+\zeta}{\pi^\sigma}\right)_n R(\pi)^\sigma$$

therefore, we obtain inductively

$$R(\pi^{\sigma^{\frac{n-1}{2}}}) = \left(\prod_{i=1}^{\frac{n-1}{2}} \left(\frac{1+\zeta^{\sigma^{-}i}}{\pi}\right)_n^{-1}\right) R(\pi)^{-1}.$$

Put

$$u = \prod_{i=1}^{\frac{n-1}{2}} \left(\frac{1+\zeta^{\sigma^{-}i}}{\pi}\right)_n^{-1}.$$

By the definition of the n^{th} power residue symbol, u is a root of unity i.e $u = \zeta^k$, for some $0 \leq k \leq n$.
It follows that

$$R(\pi^{\sigma^{\frac{n-1}{2}}}) = \left(\frac{\zeta^k}{\pi}\right)_n^{-1} R(\pi)^{-1} = \left(\frac{\zeta}{\pi}\right)_n^{-k} R(\pi)^{-1}.$$

We are now looking for a formula $\Omega(S_0,\pi) = \left(\frac{\zeta^t}{\pi}\right)_n R(\pi)$ which satisfies

$$\Omega(S_0, \pi^{\sigma^{\frac{n-1}{2}}}) = \overline{\Omega(S_0,\pi)}$$

as we have done in the case $n = 5$, this amount to solving the congruence equation

$$2m \equiv -k \mod n,$$

since n is prime and $\gcd(2,n) = 1$ we see that this equation has the unique solution $m = -2^{-1}k$ where 2^{-1} is the inverse of 2 modulo n. □

Finally, by combining lemma 5.2 and lemma 5.3, we can sate the first identity as follows.
Identity

$$\Omega(S_0, u\pi) = \left(\frac{u}{\pi}\right)_n \Omega(S_0,\pi)$$

$$\Omega(S_0, \pi^{\sigma^{-1}}) = \Omega(S_0,\pi)^{\sigma^{-1}}$$

2. Second identity

There is a similar identity with the Gauss sum.

Lemma 5.4.

$$\mathfrak{g}(1,\varepsilon,u\pi) = \varepsilon(\left(\frac{u}{\pi}\right)_n)\mathfrak{g}(1,\varepsilon,\pi)$$

Remark We see that the first and the second identity have the same configuration. Then, if we suppose that the unit u is an n^{th} power, then the first and second identity are invariant under the unit group U_0^n.
For $n = 5$ we have chosen prime π to be primary, i.e $\pi \equiv 1 \bmod \lambda^3$. We fortunately prove that if π_1 and π_2 are associate primary primes then their ratio is a fifth power unit. The consequence it that in this class of primary primes there is exactly one value of $\mathfrak{g}(1, \varepsilon, u\pi)$ and $\Omega(S_0, u\pi)$. As Patterson suggested to me, if the Gauss sums are to be considered as congruence functions, it would be better to work them in this class of primes.

3. Third identity

We will denote the complex root of unity $\varepsilon\left(\Omega(S_0, \alpha)\right)$ by $\Omega(S_0, \varepsilon, \alpha)$.

Lemma 5.5. *The function*

$$\frac{\mathfrak{g}(1, \varepsilon, \pi)}{\Omega(S_0, \varepsilon, \pi)}$$

is independent of the generator of the ideal. It is a function of ideals.

Proof. This follows from the first and second identity. □

We extend this formula multiplicatively to obtain

$$\tilde{g}(1, \varepsilon, (\alpha)) = \frac{\mathfrak{g}(1, \varepsilon, \alpha)}{\Omega(S_0, \varepsilon, \alpha)}$$

for suitable choice of α, i.e for example when $N(\alpha) \equiv 1 \pmod{n}$

We remark that $\tilde{g}(1, \varepsilon, (\alpha))$ does not depend on the n^{th} set we choose. In fact if we replace S_0 by uS_0 for a unit u this is equivalent to replace α by $u\alpha$.

Remark We then notice that $\tilde{g}(1, \varepsilon, (\alpha))^n = \mathfrak{g}(1, \varepsilon, (\alpha))^n$. However the n^{th} power is given by the Stickelberger relations.

Theorem 5.3. *Let (α) be a principal ideal in O_K which is supposed to be prime to n, and let ε be as before. Then*

$$\mathfrak{g}(1, \varepsilon, \alpha)^n = \mu(\alpha)^n \chi(\alpha) \varepsilon \left(\alpha^{\sum_{(t,n)=1} t\sigma_t^{-1}} \right),$$

where $\sigma_t \in Gal(K/\mathbb{Q})$ maps ζ to ζ^t with $\gcd(t, n) = 1$ and where χ is a character of order n.

Let us put

$$\omega(\varepsilon, \alpha) = \varepsilon \left(\alpha^{\sum_{(t,n)=1} t\sigma_t^{-1}} \right)$$

and

$$\Phi(\alpha) = \mu(\alpha)^n \mathfrak{g}(1, \varepsilon, \alpha)^n$$

then, from Weil we know that Φ is a Grossencharacter with defining ideal n^2. The Galois group acts on ϕ as follows.

$$\Phi(\alpha^\sigma) = \Phi(\alpha)^\sigma.$$

From this relation we see that

$$\chi(\alpha^\sigma) = \chi(\alpha)^\sigma.$$

We want determine χ explicitly for $n = 5$. This result has been suggested by the computation. Let $\lambda = 1 - \zeta$ and τ the real fundamental unit $\frac{1+\sqrt{5}}{2}$. we prove that:

Proposition 3.1. *Let π a prime ideal in $\mathbb{Z}[\zeta]$. $\Phi(\pi) = -\chi(\pi)\varepsilon(\omega(\pi))$ where*
$\chi(\pi) = 1 \quad If \quad \pi \equiv 1 \bmod \lambda^3$
$\chi(\tau) = -1$
$\chi(\zeta) = \zeta$

Proof. From Weil, χ is a character of conductor at most λ^8 where $\lambda = 1 - \zeta$. Define

$$U_k = \{x : \quad x \equiv 1 \bmod \lambda^k\} \quad .$$

$$\chi((1 + a\alpha^k)(1 + b\alpha^k)) = \chi(1 + (a + b)\lambda^k)$$

Let $\sigma \in Gal(K/Q)$ such that $\zeta^\sigma = \zeta^2$ then $\lambda^\sigma = 1 - \zeta^2 = \lambda(2 - \lambda)$
If $\alpha \in U_8, \quad \chi(\alpha) = 1.$
If $\alpha \in U_7 \quad$ and $\quad \alpha \notin U_8$
then $\chi(1+\lambda^7)^\sigma = \chi(1+(\lambda^7)^\sigma) = \chi(1+3\lambda^7)$ implies that $\chi(1+\lambda^7)^2 = \chi(1+3\lambda^7) = \chi(1+\lambda^7)^3$ and then follows that $\chi(1 + \lambda^7) = 1$.
This idea works for $k = 6, 5, 4, 3$. For $k = 3$, we notice in general that

$$\left(1 + a\lambda^k\right) \equiv (1 + \lambda^k)^a \bmod (\lambda^{k+1})$$

and therefore we obtain

$$\chi(1 + (\lambda^3)^\sigma) = \chi(1 + 2^3\lambda^3) = \chi(1 + 3\lambda^3) = \chi(1 + \lambda^3)^3 = \chi(1 + \lambda^3)^\sigma$$

and therefore we have $\chi(1 + \lambda^3) = 1$.
Since $\tau^\sigma = -1/\tau, \quad \chi(\tau^\sigma) = \chi(-1/\tau) = \chi(-1)\chi(1/\tau) = \chi(\tau)^2$. This implies that $\chi(\tau)^3 = \chi(-1) = -1$. It follows that $\chi(\tau) = -1$.
From $\Phi(\zeta) = 1 = \chi(\zeta)\zeta^\theta = \chi(\zeta)\zeta^4$ follows that $\chi(\zeta) = \zeta$. □

This suggests that we can give a simple formulation of the $\Phi(\pi)$ and of course of $\Phi(\alpha)$ whenever it is defined.

Lemma 5.6. *For $m = 5$*

$$\mathfrak{g}(1, \varepsilon, \pi)^5 = \mu(\pi) \left(\frac{-\mathrm{Tr}_{K/\mathbb{Q}}(\pi)}{5}\right)_2 \chi(\pi/\pi^*)\pi^\theta$$

where π^* is primary associate of π.

$$\chi(\pi) = 1 \text{ if } \pi \equiv 1 \bmod \lambda^3$$

$$\chi(\tau) = -1$$

$$\chi(\zeta) = \zeta$$

Proposition 3.2. *Let π be a prime integer in $\mathbb{Q}(\zeta)$ and π^* any primary associate of π such that $\pi^* \equiv 1 \bmod (1 - \zeta)^3$, then*

$$\Phi(\pi) = \chi(\pi^*/\pi)^{-1}\Phi(\pi^*) = \chi(\pi^*/\pi)^{-1}(\pi^*)^\theta$$

4. Cassels' formula

4.1. The Cassels conjecture. The Cassels conjecture is related to the cubic and quartic case of Gauss sums. We can state the cubic case as follows.
The elliptic curve

$$y^2 = 4x^3 - 1$$

over the complex numbers is parameterized by the Weierstrass function

$$x = \wp(z), \quad y = \wp'(z)$$

with periods

$$\theta\mathbb{Z}[\zeta]$$

where $\theta = 3.0599087..$ is the smallest positive real period. Then for prime $\pi|p$ of degree 1, the result of Eisenstein says that

$$\prod_{r=1}^{p-1} \wp(\theta r/\pi) = 1/\pi^2$$

Since

$$\wp(\zeta z) = \zeta\wp(z), \quad \wp(\zeta^2 z) = \zeta^2\wp(z) \quad \text{and } p = 3n+1$$

then for S any third set of residues $\bmod \pi$ we have:

$$P_S = \prod_{x\in S} \wp(\theta x/\pi)$$

which satisfies

$$P_S^3 = \prod_{x\in S} \wp(\theta x\pi)\wp(\theta\zeta x/\pi)\wp(\theta\zeta^2 x/\pi) = 1/\pi^2$$

The Cassels formula is as follows:

$$\mathfrak{g}(1,\varepsilon,\pi) = -\frac{\varepsilon(\pi)p^{\frac{1}{3}}P_S}{\Omega(S,\varepsilon,\pi)}$$

where $p^{\frac{1}{3}}$ is the real cubic root of p and $\pi \equiv 1 \bmod 3$.

P_S gives a canonical way of extracting a cubic root of π, which, in turn, is necessary in the Stickelberger formula,

$$\mathfrak{g}(1,\varepsilon,\pi)^3 = -\pi^2\overline{\pi} = -p\pi$$

If this would have not been the case, that P_S exists, one would have had for a fixed $i; 1 \le i \le 3$,

$$\mathfrak{g}(1,\varepsilon,\pi) = \frac{\varepsilon(\zeta^{i_0})p^{\frac{1}{3}}\varepsilon(\pi)^{\frac{1}{3}}}{\Omega(S,\varepsilon,\pi)}$$

with $0 \le \arg(\varepsilon(\pi)^{1/3}) < 2\pi/3$
Remark We notice that we can rewrite this formula as in a very general shape.

5. A generalized of a formula of Cassels' type

We shall investigate the possibility of a formula of Cassels'type for $n = 5$; if such a formula exists, it could serve as a prototype for formulae for more general n.
Let ε, p, $\pi|p$, S and $\Omega(S, \varepsilon, \pi)$ be as before.

$$P(1, \varepsilon, \pi) = -\frac{\mathfrak{g}(1, \varepsilon, \pi)}{\Omega(S, \varepsilon, \pi)}.$$

We notice that $P(1, \varepsilon, \pi)$ lies in a much more bigger field than K.
Remark Let $K_1 = K = \mathbb{Q}(\zeta_n)$ and $K_2 = \mathbb{Q}(\zeta_p)$ the we denote F the join of K_1 and K_2, i.e $F = K_1K_2$ then

$$F/K_2 = K_1K_2/K_2 \equiv K_1/\mathbb{Q}$$

so that F/K_2 is a Galois extension of $\mathbb{Q}$. Since n and p are relatively prime, the Galois group of $F/\mathbb{Q}$ is just the product of the underlying Galois groups i.e $Gal(F/\mathbb{Q}) = Gal(K_1/\mathbb{Q}) \times Gal(K_2/\mathbb{Q})$. The Galois group $Gal(K/\mathbb{Q})$ acts on $P(1, \varepsilon, \pi)$ as follows

$$P(1, \varepsilon, \pi)^\sigma = P(1, \varepsilon^\sigma, \pi) = P(1, \varepsilon, \pi^\sigma)$$

for $\sigma \in Gal(K/\mathbb{Q})$.
We have furthermore,

$$\overline{P(1, \varepsilon, \pi)} = P(1, \varepsilon^{-1}, \pi).$$

Moreover $P(1, \varepsilon, \pi)$ satisfies

$$P(1, \varepsilon, u\pi) = P(1, \varepsilon, \pi).$$

so that P is invariant under the action of the unit group.

$$P(1, \varepsilon, \pi)^n = -\mathfrak{g}(1, \varepsilon, \pi)^n = \omega(\varepsilon, \pi).$$

This know by the Stickelberger decomposition of Gauss sums. $\omega(\varepsilon, \pi)$ is a complex number and we can extract its roots. Then we can fix $\arg(\omega(\varepsilon, \pi)^{1/n}) \in [-\pi/n, \pi/n[$. We then classify the pair of complex numbers $(P(1, \varepsilon, \pi), \omega(\varepsilon, \pi)^{1/n})$ according to their arclength. In fact they differ one from another by a complex n^{th} root of unity. The numerical computation shows that

$$\sum_{N(\pi)\leq 4.10^4 \quad \pi\equiv 1 \pmod{\lambda^3}} P(1, \varepsilon, \pi) = -149.738678 - 0.000079i$$

TABLE 1

	$sector0$	$sector1$	$sector2$	$sector3$	$sector4$
$\mathfrak{g}(1, \epsilon, \pi)$	744	848	868	868	848
$P(1, \varepsilon, \pi)$	862	882	775	775	882
$Total$					

there 4176 gauss sums, 744 in sector 0, 848 in sector 1, 868 in sector 2, 868 in sector3, 848 in sector 4 there 4176 corrected gauss sums , 862 in sector 0 , 881 in sector 1, 776 in sector 2, 776 in sector3, 881 in sector 4

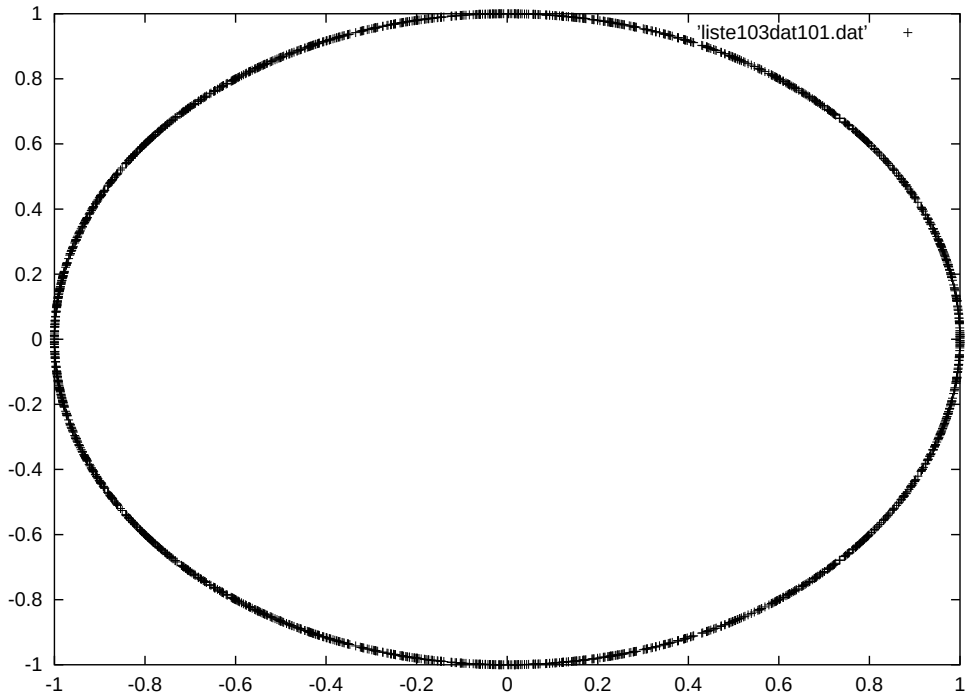

FIGURE 1. Graphic of the arguments of Gauss sums for $\pi \equiv 1 \pmod{\lambda^3}$ $N(\pi) \leq 20000$

Figure 1, figure 2 and figure 3 show the distribution of the arguments of Gauss sums. There are points which are very accurate than the other but this does not however says anything about the distribution. As has been proved by Patterson, this distribution is uniform. This graphs are consistent with the fact that the normalized Gauss sums are uniformly distributed on the unit circle, as was proved by Patterson. Note that there is no obvious bias as can be observed in the cubic case [**SJP5**]

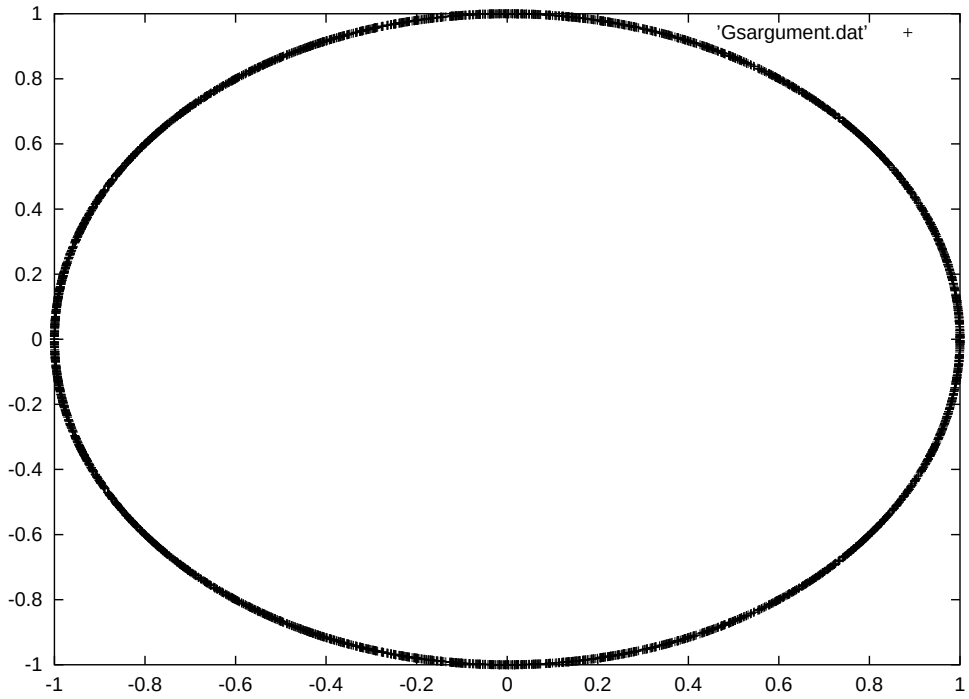

FIGURE 2. Graphic of the arguments of Gauss sums for $\pi \equiv 1 \pmod{\lambda^3}$ $N(\pi) \leq 40000$

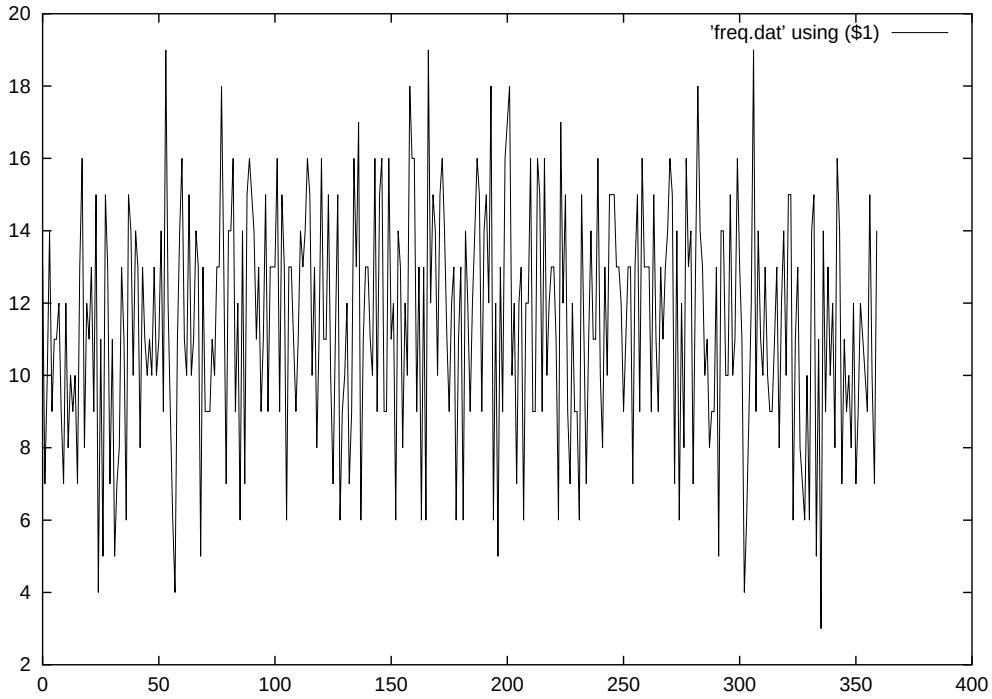

FIGURE 3. frequency in each 1 degree on the circle

This figure is the histogram of the frequency distribution of the argument of Gauss sums on intervals of arc-length one degree.

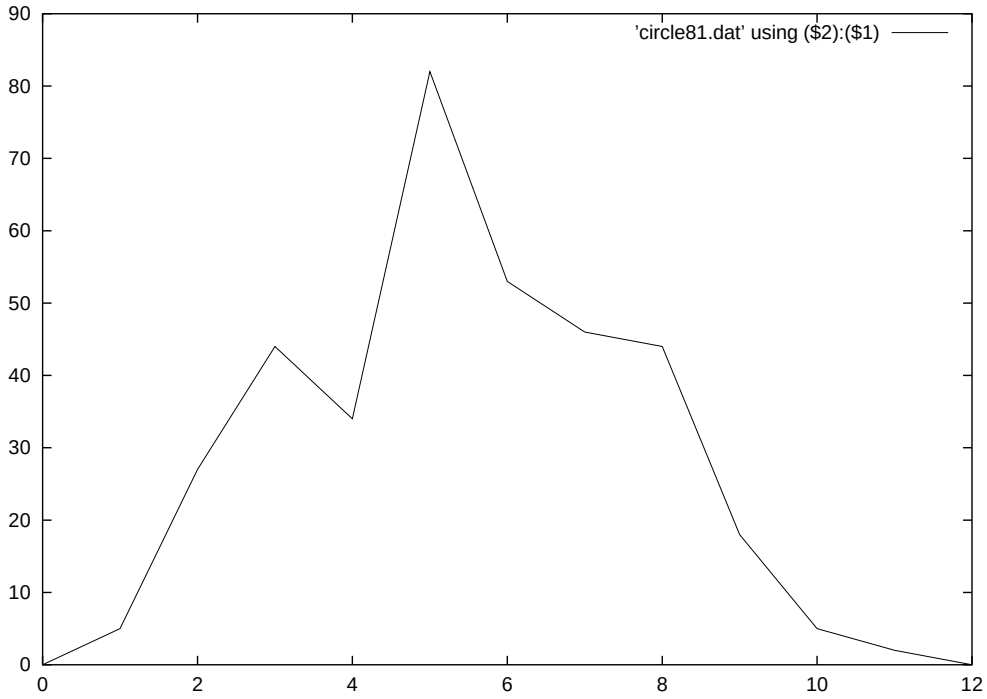

FIGURE 4. frequency in each 1 degree on the circle

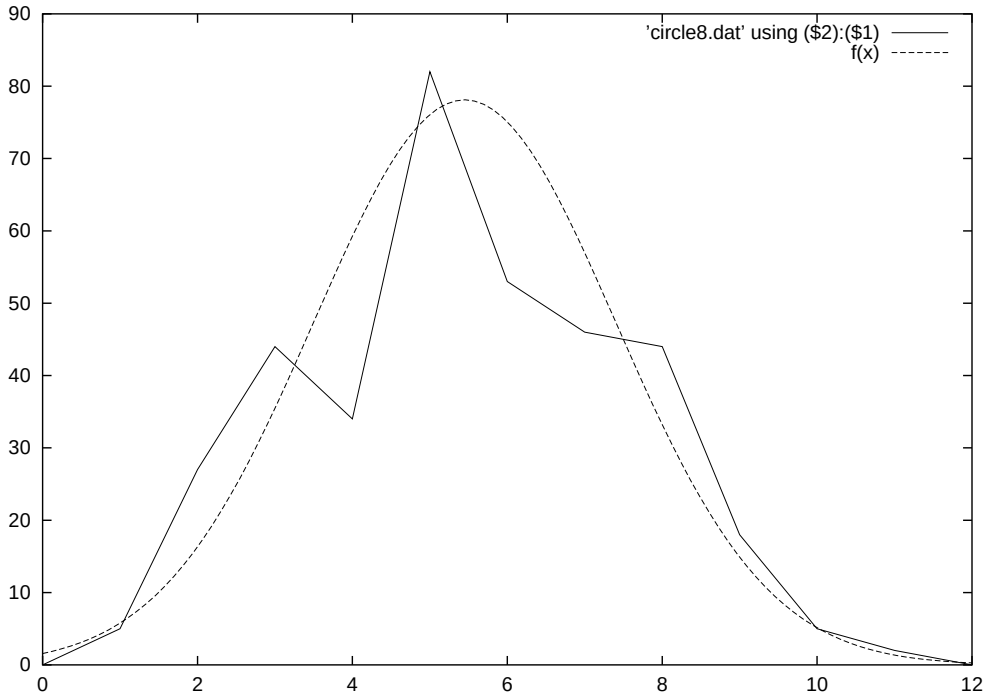

FIGURE 5. both graphs plotted one against another

The plot of the graph shows some properties. The "tailing off" is observed. The graph of the frequencies shows that there is a symmetry on the distribution. We then classify, instead of the arguments of the Gauss sums, but the intervals of one degree arc length with respect to their frequencies. This has been done for different values of primes $p \equiv 1 \pmod 5$, $p < X$. For example when

$$X = 2.10^4$$

we understand this through the table as follows: in the first line we have the number of frequencies with which an interval of the form $[n^0, (n+1)^0)$ appears and the second line gives number of the Gauss sums with argument in the corresponding range. from this table, we see that out of a sample of 1963 Gauss sums for the selected

TABLE 2

different values of the frequency	1	2	3	4	5	6	7	8	9	10	11
Number of sectors of 1 degree	5	27	44	34	82	53	46	44	18	5	2

value of $\pi \equiv 1 \mod \lambda^3$, we notice that some sectors have a higher frequency rate while others just have a very few. From the computation, the sector $[249, 250[$ first appears when we go over 20.000. In looking at the three first pictures, we preconize this fact by noticing that some points on the unit circle tend to be darker than others. This does not disprove the uniformly distribution of the arguments of Gauss sums proved by Patterson, it is, however,consistent with the uniform distribution proved by him. In this restricted range there is no sign of the same sort of biais as on sees in the cubic case. The statistical analysis makes such a bias unlikely. We have known it first from Kummer about this result. See comment about this fact from [**HP**]. However, the shape of the plot of the above distribution is really meaningful. The bell shape shows a tendency that this distribution looks like a Gauss normal distribution $N(\mu, \sigma)$, where μ is the mean and σ is the variance. Here the computed estimate values are

$$\mu = 5.45278 \quad \text{and} \quad \sigma = 2.02$$

Remark We could even find the mean μ without any computation. Since for primes $\pi \equiv 1 \pmod \lambda)^3$ there is at most 1 ,2, 3 or $4 = \phi(5)$ different Gauss sums. This is a consequence of the decomposition of primes in cyclotomic fields. Then if $p \equiv 1 \pmod 5$ then the Prime Number Theorem suggests that there is at most $c\frac{X}{\log X}$ primes of the sort. Some estimates of the constant c says it is very close to 1. Therefore

$$\mu = \mu(X) = 4.\frac{1}{360}\frac{X}{4\log X} = \frac{1}{360}\frac{X}{\log X}$$

so that for $X = 20.000$ we obtain $\mu = 5.61$ which may be considered to be closed to the estimated value 5.45278.

6. Conjectures on the partial sums of the Gauss sums

We are now interested in some partial summations. Some of this results are know from the elementary number theory. We use the computational result to support conjecture on partial sums. First we look at the following partial sums. We put them in pair so that we can discuss case after case. We first refresh our mind with partial summation Theorem.

Theorem 5.4. *Let $f(n)$ and $g(n)$ be arithmetic functions. Consider the sum function*

$$F(x) = \sum_{n \leq x} f(n).$$

Let a and b be non negative integers with $a < b$. Then

$$\sum_{n=a+1}^{b} f(n)g(n) = F(b)g(b) - F(a)g(a+1) - \sum_{n=a+1}^{b-1} F(n)(g(n+1) - g(n)).$$

Let x and y be non negative real numbers with $[y] < [x]$, and let $g(t)$ be a function with a continuous derivative on the interval $[y, x]$. Then

$$\sum_{y<n\leq x} f(n)g(n) = F(x)g(x) - F(y)g(y) - \int_y^x F(t)g'(t)dt.$$

In particular, if $x \geq 2$ and $g(t)$ is continuously differentiable on $[1, x]$, then

$$\sum_{n<x} f(n)g(n) = F(x)g(x) - \int_1^x F(t)g'(t)dt.$$

Proof. [**Na**] pp. 211. □

From this theorem we deduce the following:
In the particular case of the statement, if we replace $g(n)$ by $\frac{1}{n}$, then

$$\sum_{n\leq X} \frac{f(n)}{n} = \frac{F(X)}{X} + \int_0^X \frac{F(x)}{x^2} dx$$

and we furthermore obtain

$$\frac{1}{X}\int_0^X F(y)dy = \frac{1}{X}\sum_{n\leq X} f(n)\int_n^X dy \tag{6.1}$$

$$= \frac{1}{X}\sum_{n\leq X} f(n)(X-n) \tag{6.2}$$

$$= \sum_{n\leq X} f(n)(1-\frac{n}{X}) \tag{6.3}$$

Let $\mu(n)$ be the Möbiüs function,

$$\mu(n) = \begin{cases} 1 & \text{if} \quad n = 1 \\ (-1)^k & \text{if} \quad n \text{ is the product of k distinct primes} \\ 0 & \text{if n is divisible by a square} \end{cases}$$

We define the functions:

$$F(X) = \sum_{n \leq X} \mu(n) n^{\frac{1}{2}}.$$

we contrast

$$F(X) = \sum_{n \leq X} \mu(n) n^{\frac{1}{2}} \quad \text{and} \quad H(X) = \sum_{\substack{N(\pi) \leq X \\ \pi \equiv 1 \bmod \lambda^3}} \mathfrak{g}(1, \varepsilon, \pi) \log(N(\pi)).$$

Here the reason for which we decide this form is as follows. The Gauss sum has the modulus $|\mathfrak{g}(1, \varepsilon, \pi)| = \sqrt{N(\pi)}$ and for the powers of π the Gauss sums vanish, therefore it is better to use the Von Mangoldt Λ function.
In fact if we put

$$M(X) = \sum_{n \leq X} \mu(n),$$

then $M(X)$ is a function which is on average $O(\sqrt{X})$ therefore

$$\sum_{n \leq X} \mu(n) n^{\frac{1}{2}} = O(X),$$

In contrary $\sqrt{n}$ can be replaced by any other arithmetic function, then we cannot easily determine the estimate. In replacing $\sqrt{n}$ by the Gauss sum, we are consistent with this conjecture.

6.1. Conjecture I.

$$H(X) = \sum_{\substack{N(\pi) \leq X \\ \pi \equiv 1 \bmod \lambda^3}} \mathfrak{g}(1, \varepsilon, \pi) \log(N(\pi)) = c.X^{6/5} + O(X^{1+\epsilon})$$

Where c is a constant and ε is a positive real number.

Note that $H(X)$ is a real function. Because at the primes, which are primary $\pi^* \equiv 1 \pmod{\lambda}^3$ there is at most one Gauss sum $\mathfrak{g}(1, \varepsilon, \pi^*)$, because any other primary associate prime differs from the previous one by a fifth power of a unit. This is not necessary the case for other primes. Moreover the inverse of a Galois element yields complex conjugate on the Gauss sums, so that in each congruent class of primes, the Gauss sums appear in simultaneously pair of complex conjugates and therefore the function $H(X)$ is real. At each prime factor $\pi | p$, if $\mathfrak{g}(1, \varepsilon, \pi^*)$ is not real the sum

$$\mathfrak{g}(1, \varepsilon, \pi^*) + \mathfrak{g}(1, \varepsilon^{-1}, \pi^*)$$

is either positive or negative.
We would expect this sign appears totally at random so that it would behave like the Möbius function. For this reason the function $H(X)$ would cross the x-axis infinitely many times as X tends to ∞. This is however a surprising result that let us to conjecture.

6.2. Conjecture II. The function $H(X)$ has the following property: there exists a positive real A, such that for all $X > A$, $H(X) > 0$.

All of them are derived from the theorem 5.4. We will consider successively functions

$$f_1(p) = \sum_{\substack{p\equiv 1 \pmod 5 \\ \pi|p, \quad \pi\equiv 1 \pmod{\lambda^3}}} \mathfrak{g}(1,\varepsilon,\pi)\log(N(\pi))$$

and

$$f_2(p) = f_1(p) \times \frac{1}{p}.$$

Since

$$H(X) = \sum_{\substack{N(\pi)\leq X \\ \pi\equiv 1 \pmod{\lambda}^3}} \mathfrak{g}(1,\varepsilon,\pi)\log(N(\pi))$$

then

$$H_1(X) = \frac{1}{X}\int_1^X H(Y)dY = \sum_{N(\pi)=p\leq X} f_1(p)\left(1-\frac{N(\pi)}{X}\right)$$

and for

$$K(X) = \sum_{\substack{N(\pi)\leq X \\ \pi\equiv 1 \pmod{\lambda}^3}} \frac{\mathfrak{g}(1,\varepsilon,\pi)\log(N(\pi))}{N(\pi)}$$

we have

$$K_1(X) = \frac{1}{X}\int_1^X K(Y)dY = \sum_{N(\pi)=p\leq X} f_2(p)\left(1-\frac{N(\pi)}{X}\right)$$

so that we obtain if we assume the conjecture I, that:

$$H_1(X) = \frac{1}{X}\int_1^X H(Y)dY = c.\frac{5}{11}X^{\frac{6}{5}} + O(X^{1+\epsilon})$$

from theorem 5.4,

$$K(X) = \frac{H(X)}{X} + \int_1^X \frac{H(Y)}{Y^2}dY = c.X^{1/5} + O(X^{-1+\epsilon})$$

and then it follows that

$$K_1(X) = \frac{1}{X}\int_1^X K(Y)dY = c.\frac{5}{6}X^{\frac{1}{5}} + O(X^{-1+\epsilon})$$

The same observation is valid for

$$\tilde{H}(X) = \sum_{\substack{N(\pi)\leq X \\ \pi\equiv 1 \pmod{\lambda}^3}} \frac{\mathfrak{g}(1,\varepsilon,\pi)\log(N(\pi))}{\Omega(S_0,\varepsilon,\pi)}$$

and

$$\tilde{K}(X) = \sum_{\substack{N(\pi)\leq X \\ \pi\equiv 1 \pmod{\lambda}^3}} \frac{\mathfrak{g}(1,\varepsilon,\pi)\log(N(\pi))}{\Omega(S_0,\varepsilon,\pi)N(\pi)}$$

In the next pages, we explain here a sample of different graphs we have described.

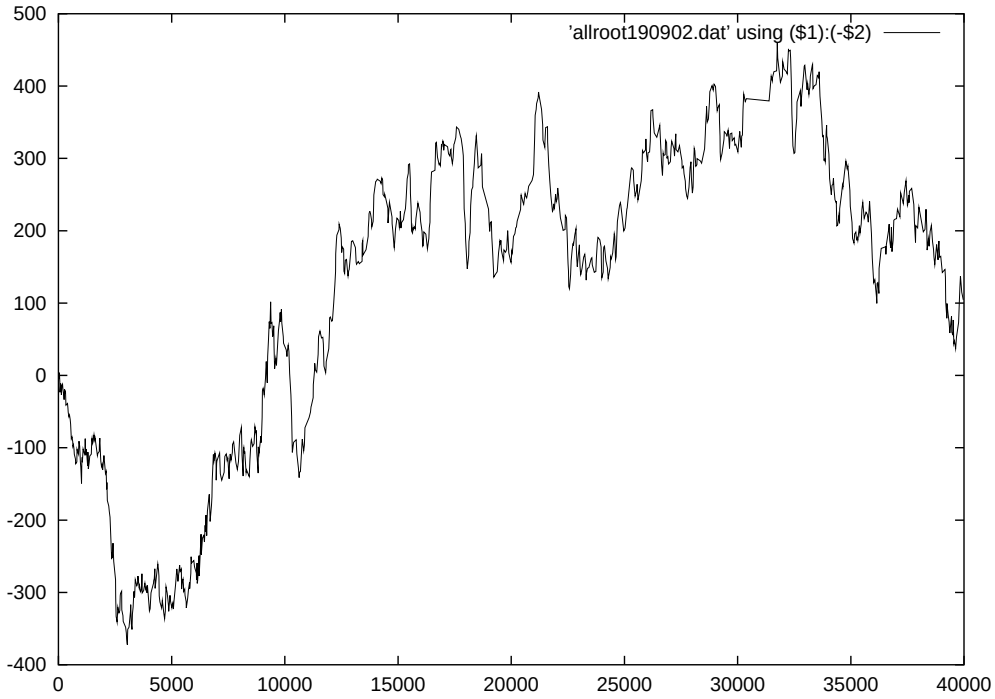

FIGURE 6. $g(X) = \sum_{\substack{n \leq X \\ 0<X<40.000}} \Omega(S_0, \varepsilon, \pi) \log(N(\pi))$

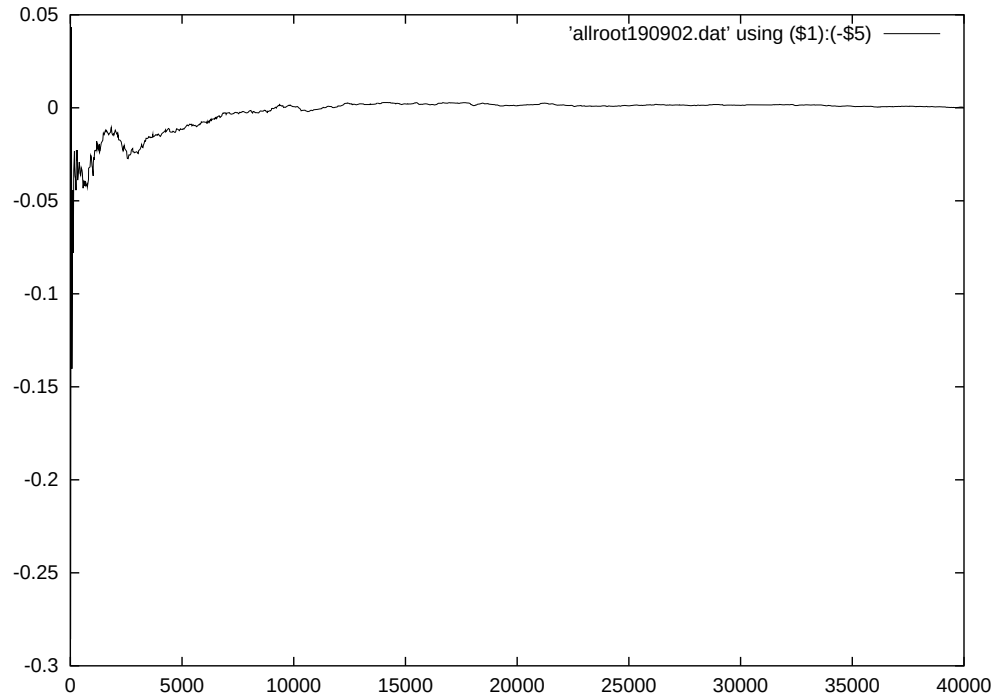

FIGURE 7. $g(X) = \frac{1}{X^{6/5}} \sum_{\substack{n \leq X \\ 0<X<40.000}} \Omega(S_0, \varepsilon, \pi) \log(N(\pi))$

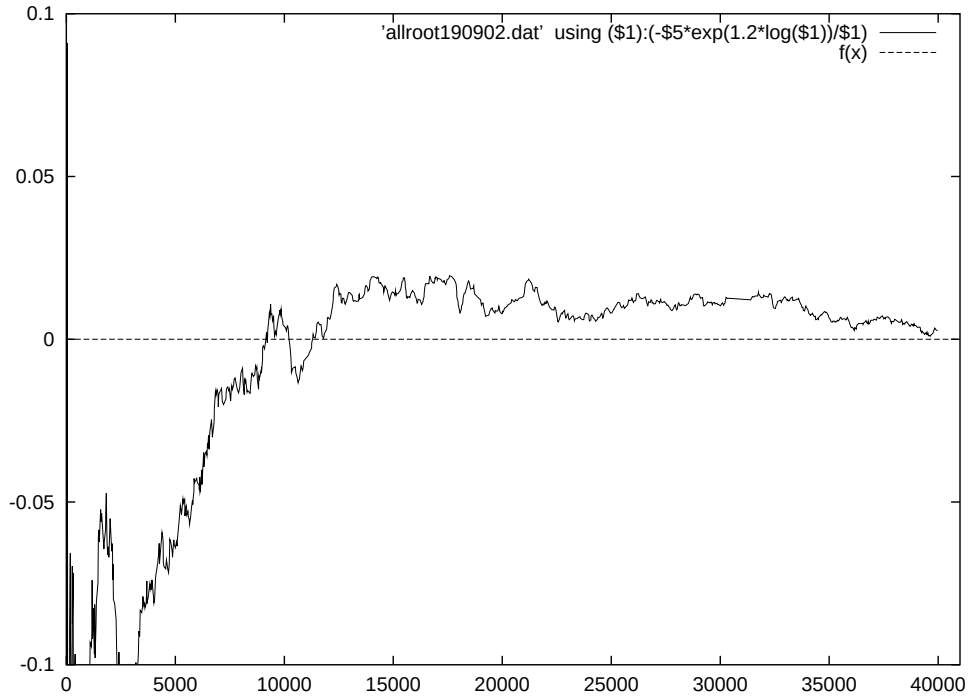

FIGURE 8. $g(X) = \frac{1}{X} \sum_{\substack{n \leq X \\ 0<X<40.000}} \Omega(S_0, \varepsilon, \pi) \log(N(\pi))$

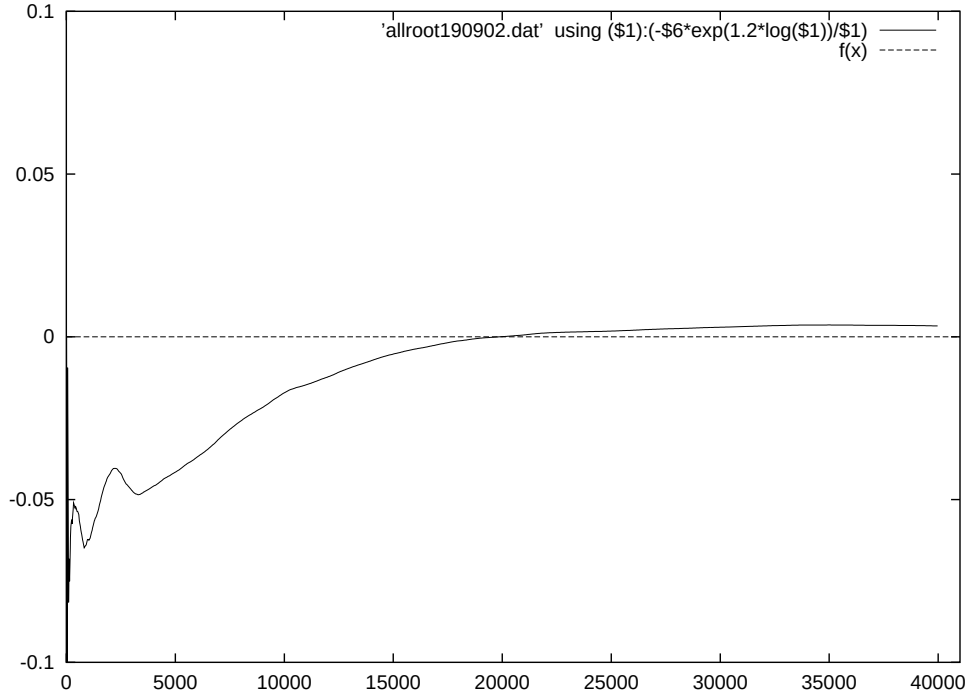

FIGURE 9. $g(X) = \frac{1}{X} \sum_{\substack{n \leq X \\ 0<X<40.000}} \Omega(S_0, \varepsilon, \pi) \log(N(\pi))(1 - \frac{N(\pi)}{X})$

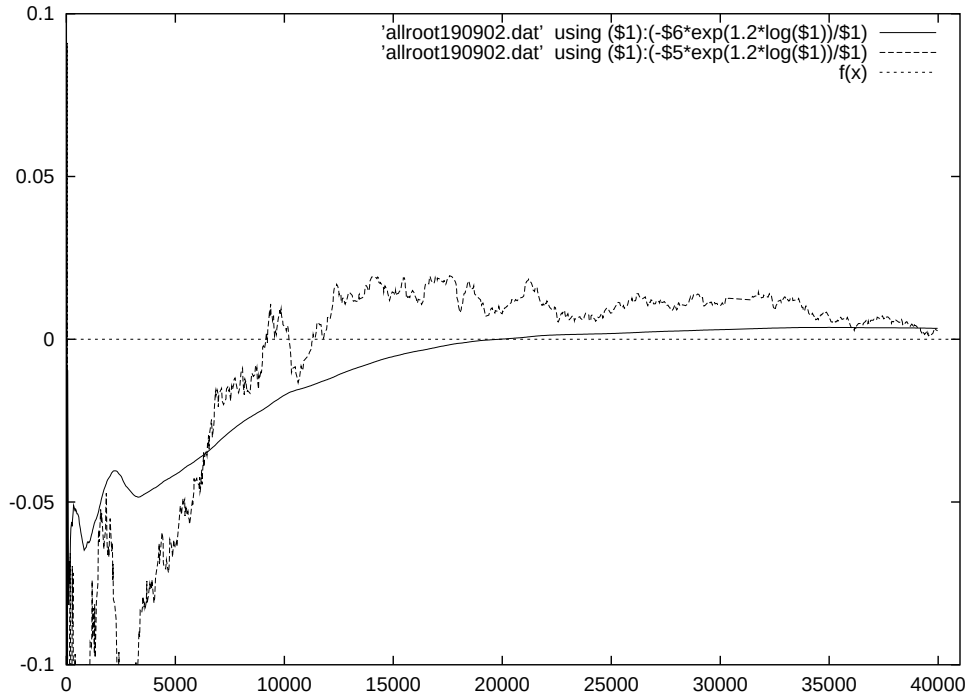

FIGURE 10. $g(X) = \frac{1}{X}\sum_{\substack{n\leq X\\ 0<X<40.000}} \Omega(S_0,\varepsilon,\pi)\log(N(\pi))$ and $f(X) = \frac{1}{X}\sum_{\substack{n\leq X\\ 0<X<40.000}} \Omega(S_0,\varepsilon,\pi)\log(N(\pi))(1-\frac{N(\pi)}{X})$

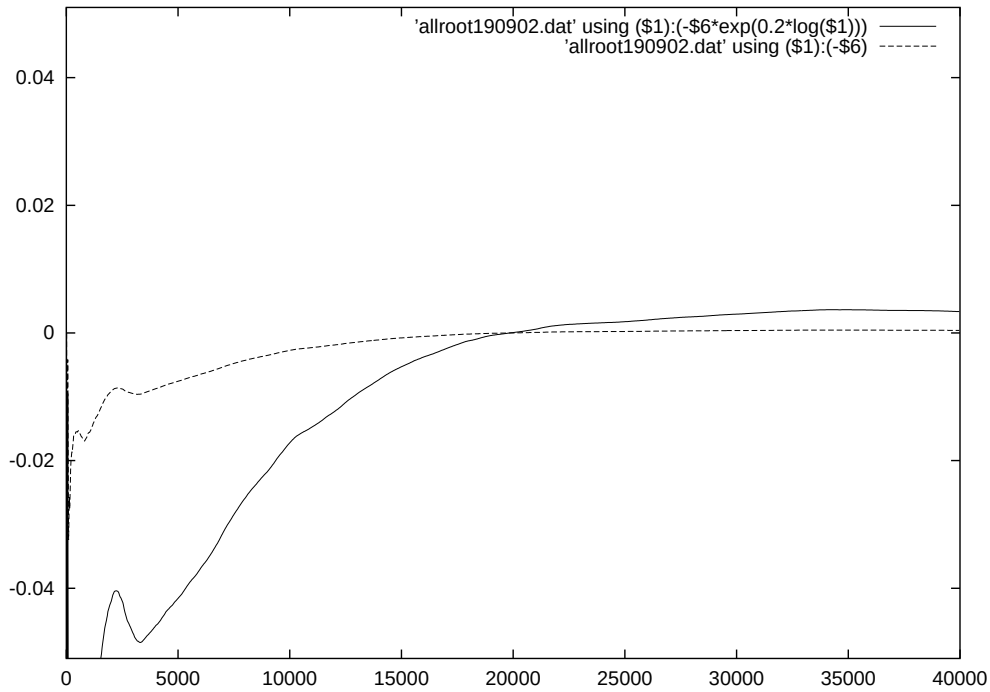

FIGURE 11. $g(X) = \frac{1}{X}\sum_{\substack{n\leq X\\ 0<X<40.000}} \Omega(S_0,\varepsilon,\pi)\log(N(\pi))\left(1-\frac{N(\pi)}{X}\right)$ and $\sum_{\substack{n\leq X\\ 0<X<40.000}} \Omega(S_0,\varepsilon,\pi)\log(N(\pi))\left(1-\frac{N(\pi)}{X}\right)$

We observe that if $\frac{1}{X}\sum_{\substack{n\leq X\\ 0<X<40.000}} \Omega(S_0,\varepsilon,\pi)\log(N(\pi))$ would behave like X or $X^{6/5}$ then the constant would be very small if it is not 0.

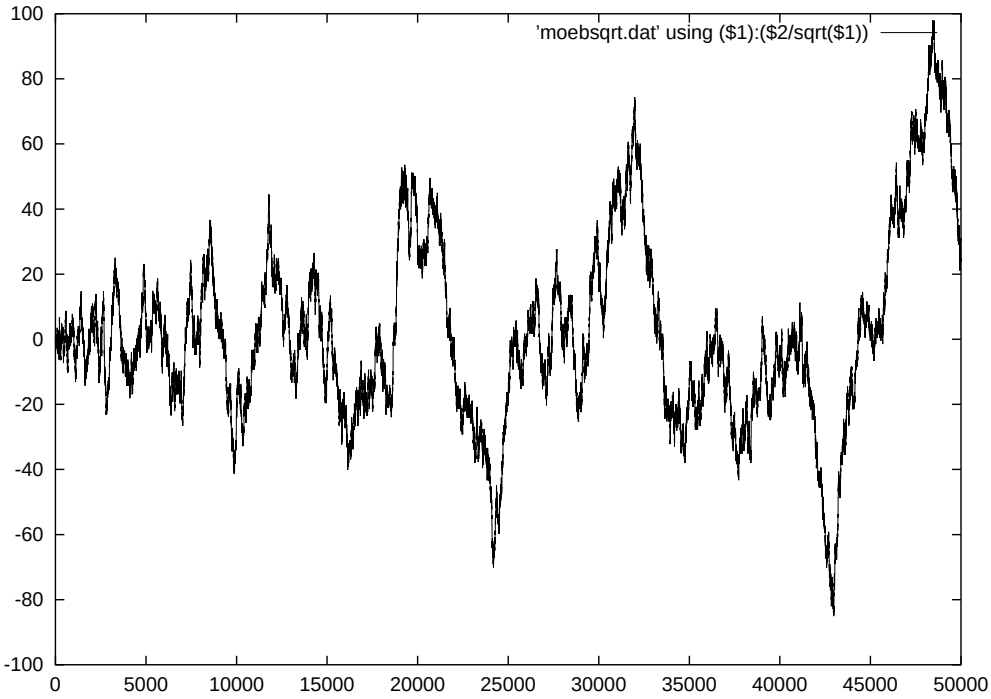

FIGURE 12. $f(X) = X^{-1/2} \sum_{\substack{n \leq X, \\ 0<X<50.000}} \mu(n) n^{1/2}$

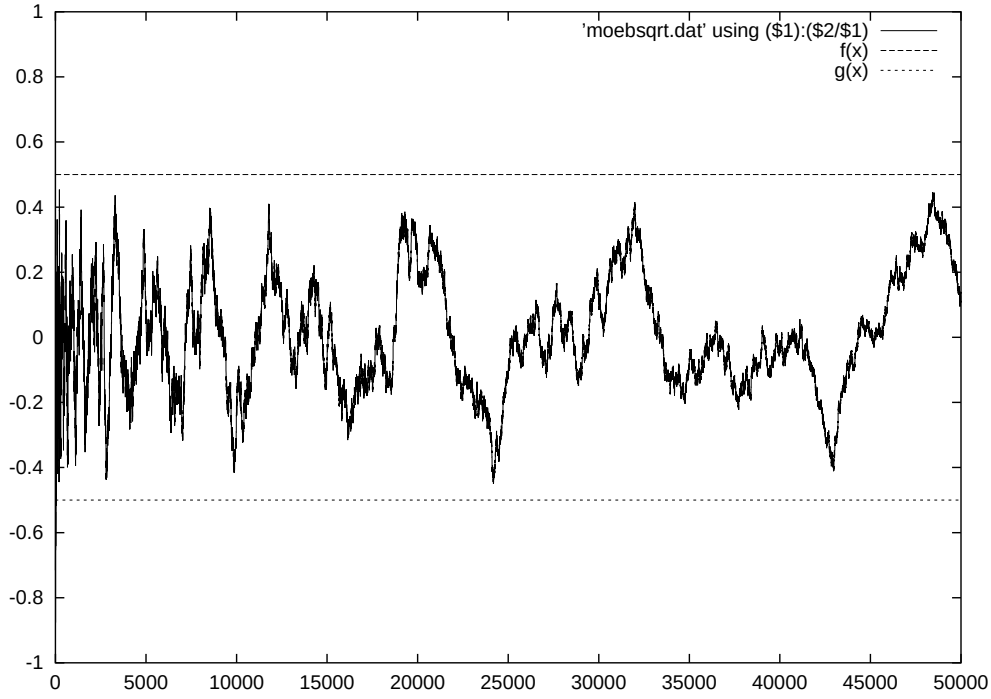

FIGURE 13. $f(X) = \frac{1}{X} \sum_{\substack{n \leq X, \\ 0<X<50.000}} \mu(n) n^{1/2}$

This in fact suggests that the constant term would be 0.5. It is known that

$$\sum_{n<X} \mu(n) = O(X^{1/2})$$

so that

$$\sum_{n<X} \mu(n)\sqrt{n} = O(X) \quad \text{i.e} \quad \frac{1}{X}\sum_{n<X} \mu(n)\sqrt{n} = O(1)$$

The Mertens conjecture suggested that the absolute values of the constant would be at most 1, but it has been disprove by A. M. Odlyzko and H. J. J. te Riele, where they showed that for $X > exp(3.21.10^{64})$, the constant is unfortunately greater that 1.

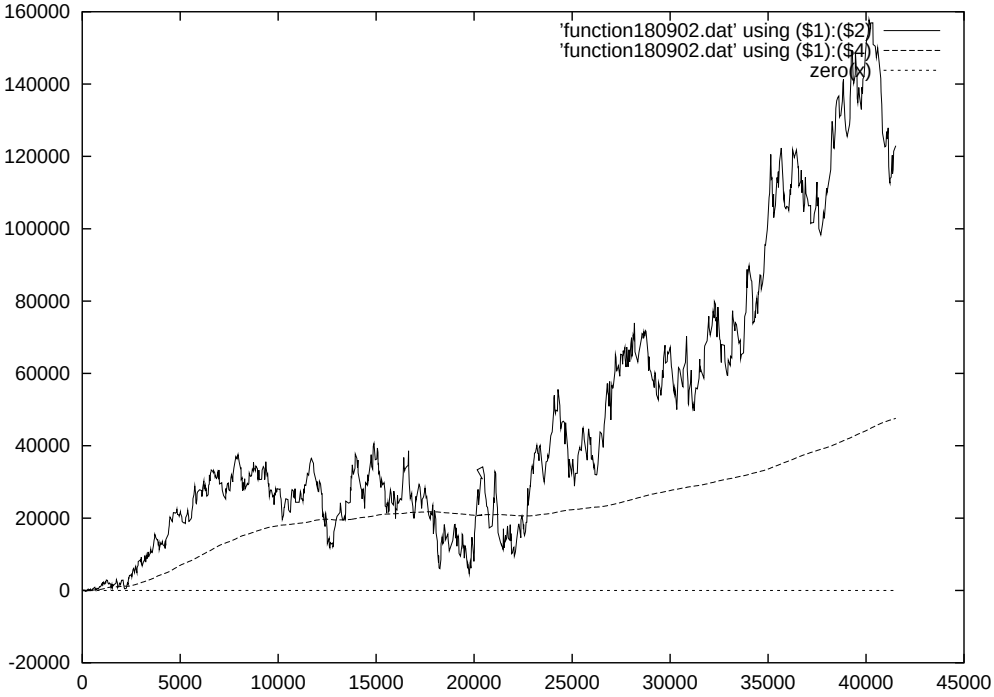

FIGURE 14. $\sum_{\substack{\pi\equiv 1 \pmod{\lambda^3},\\ N(\pi)\leq X, X\leq 40000}} \mathfrak{g}(1,\varepsilon,\pi)\log(N(\pi))$
and $\sum_{\substack{\pi\equiv 1 \pmod{\lambda^3},\\ N(\pi)\leq X, X\leq 40000}} \mathfrak{g}(1,\varepsilon,\pi)\log(N(\pi))(1-\frac{N(\pi)}{X})$

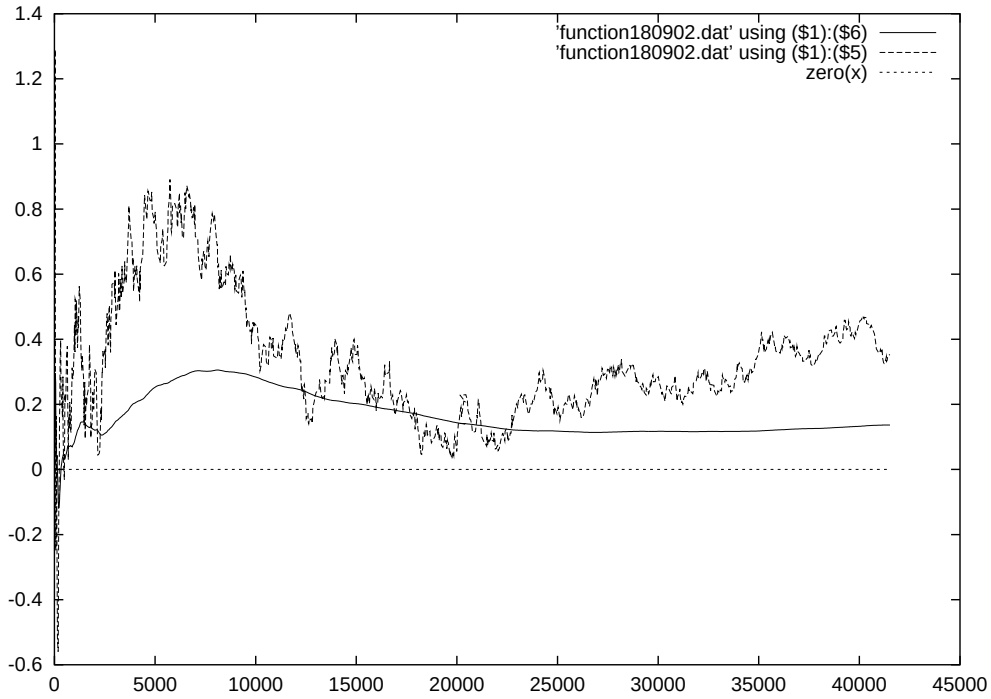

FIGURE 15. $\frac{1}{X^{6/5}} \sum_{\substack{\pi \equiv 1 \pmod{\lambda^3}, \\ N(\pi) \leq X, X \leq 40000}} \mathfrak{g}(1, \varepsilon, \pi) \log(N(\pi))$ and $X^{-\frac{6}{5}} \sum_{\substack{\pi \equiv 1 \pmod{\lambda^3}, \\ N(\pi) \leq X, X \leq 40000}} \mathfrak{g}(1, \varepsilon, \pi) \log(N(\pi))(1 - \frac{N(\pi)}{X})$

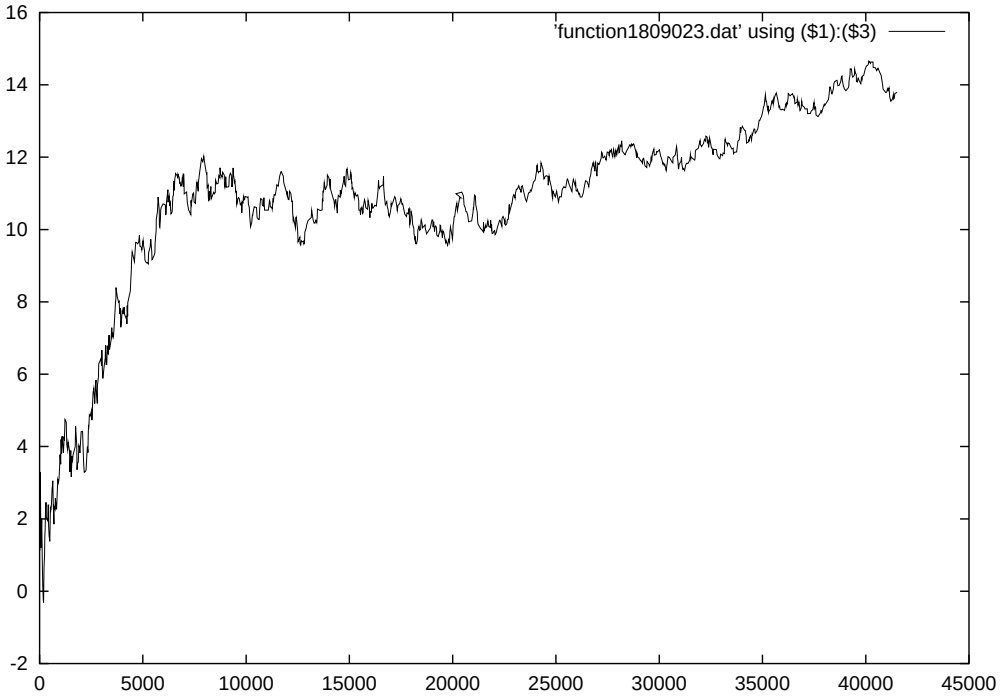

FIGURE 16. $\sum_{\substack{\pi \equiv 1 \pmod{\lambda^3}, \\ N(\pi) \leq X, X \leq 40000}} \frac{\mathfrak{g}(1, \varepsilon, \pi) \log(N(\pi))}{N(\pi)}$

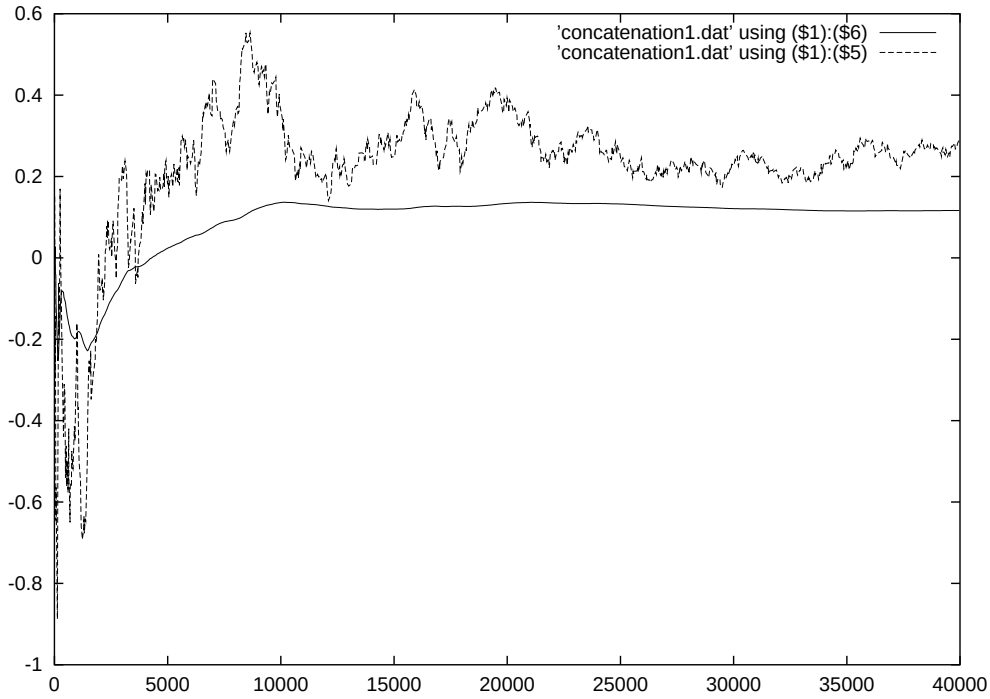

FIGURE 17.

$$f(X) = X^{-\frac{6}{5}} \sum_{\substack{\pi \equiv 1 \pmod{\lambda^3}, \\ N(\pi) \leq X, X \leq 40000}} \frac{\mathfrak{g}(1, \varepsilon, \pi) \log(N(\pi))}{\Omega(S_0, \varepsilon, \pi)}$$

$$\text{and} \quad X^{-\frac{6}{5}} \sum_{\substack{\pi \equiv 1 \pmod{\lambda^3}, \\ N(\pi) \leq X, X \leq 40000}} \frac{\mathfrak{g}(1, \varepsilon, \pi) \log(N(\pi))}{\Omega(S_0, \varepsilon, \pi)} \left(1 - \frac{N(\pi)}{X}\right)$$

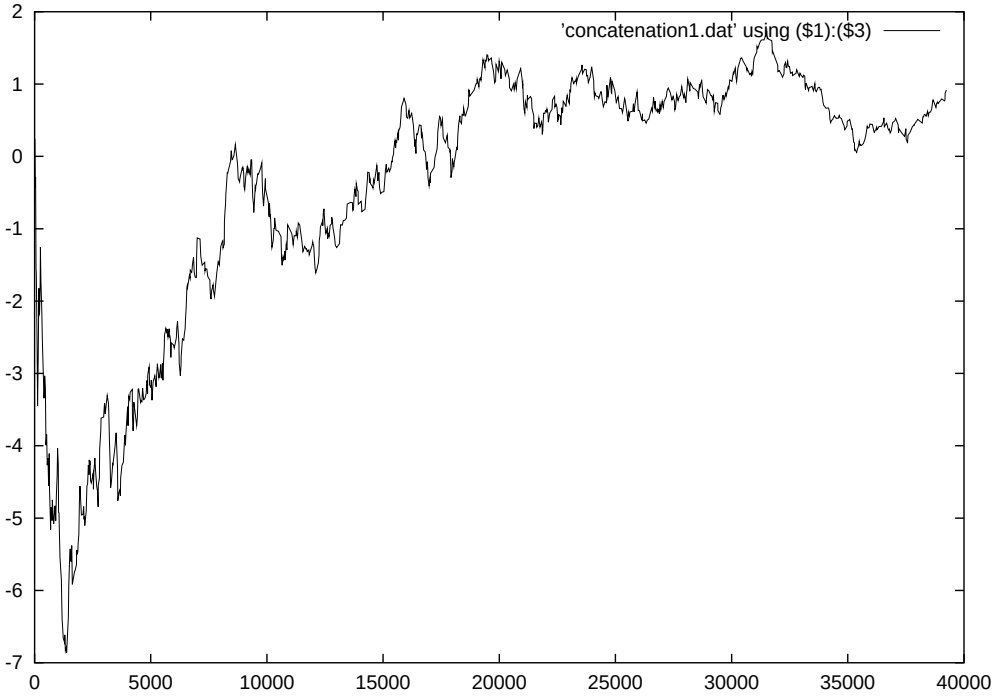

FIGURE 18. $\sum_{\substack{\pi\equiv 1 \pmod{\lambda^3},\\ N(\pi)\leq X, X\leq 40000}} \frac{\mathfrak{g}(1,\varepsilon,\pi)\log(N(\pi))}{\Omega(S_0,\varepsilon,\pi)N(\pi)}$

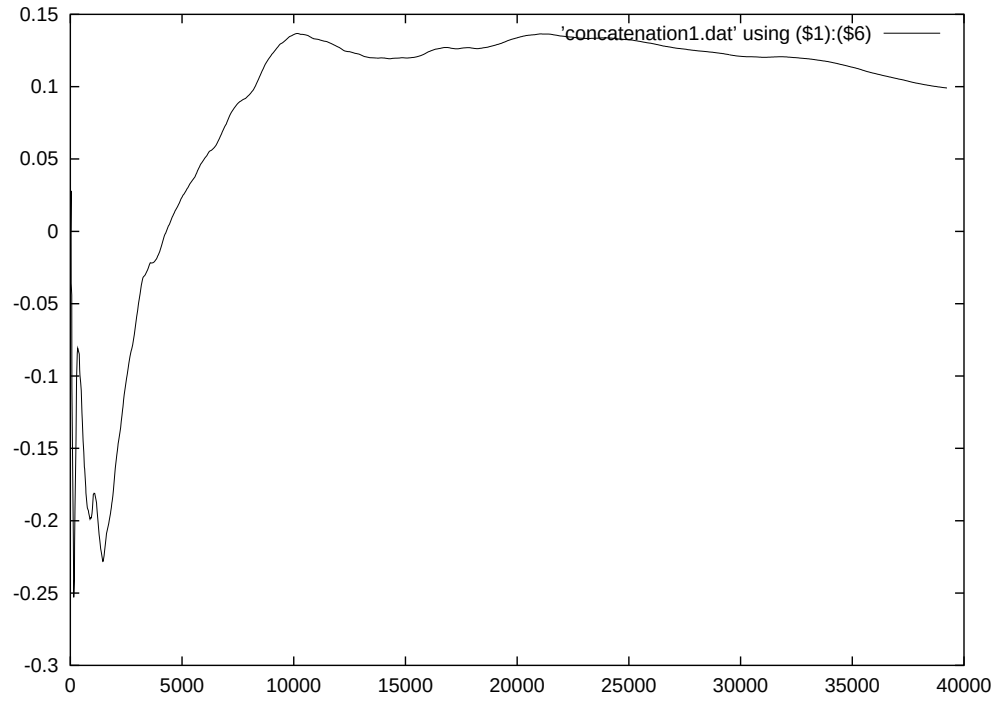

FIGURE 19.

$$X^{-\frac{6}{5}} \sum_{\substack{\pi\equiv 1 \pmod{\lambda^3},\\ N(\pi)\leq X, X\leq 40000}} \frac{\mathfrak{g}(1,\varepsilon,\pi)\log(N(\pi))}{N(\pi)} \text{ and}$$

6.3. Conclusion. The phenomenon observed near the origin is very common to such a question.
All the pictures drawn with the Gauss sums are different from the pictures drawn with the Möbiüs function. We expected to see all of them behave the same way. This is far from our expectation. The partial sumation involving Gaus sums have a tendency to have a constant sign for large values of X. This means that the sign of Gauss sums is far from being totally random.

We also notice that the integral version of any of the functions involving Gauss sums, is very smooth.

The quotient of Gauss sums multiply by a suitable root of unity, which would represent a generalization of the determination of the sign of the quadratic Gauss sums, does not have effect on the functions we plotted. Nevertheless, they have a very much elegant asymptotic behaviour that one would expect.
We have numerically confirmed a conjecture of Patterson within the range of computation.

In the earlier chapter, we simply come to the conclusion that the test for the validity of a possible Cassels-McGettrick formula, that would represent a generalization of the determination of the sign of the quadratic Gauss sums, does not hold. The statistical evidence indicates that even with a broad interpretation of the formulation of such a formula, no such formula exists.

Since the choice of the root of unity is done with respect to some geometry, one may think of modifying the fundamental region as to succeed. This is not done here and this would be hard to undertake surgery beyond the 3-dimensional space. Our result is also a warning, that one would need a different approach in the theory of Gauss sums. Patterson introduced his inaugural lecture at Goettingen in 1981, with a title " Gaussschen Summe: ein Thema mit Variationen" and 20 years later in another talk on the recent development in this theory, came to the conclusion that one may need more means and strategies than that one actually has.

CHAPTER 6

APPENDIX

1. The Gauss periods or the Lagrange resolvents

This section has nothing to do with the discussion about the origin of Gauss periods or Lagrange resolvents. If the latter appears earlier than the Gauss sums, the contemporary scientists extended the research on problems raised up by Gauss and may have named these sums after Gauss. However any computation of Gauss sum induces an implicit dermination of the Lagrange resolvents. However, Hilbert used the expression " Würzelzahl " to refer to the term used by Lagrange in his famous *Rflexions sur la rsolution algbrique des quations.*
In this step we are not taking part to this discussion, but we will emphasize on a particular case, which is more or less less obvious. In general the Lagrange resolvents are algebraic integers in a certain field $K/\mathbb{Q}$. Here we prove that upon certain conditions, all the Lagrange resolvents are rational integers such that the corresponding Gauss sum has a very simple shape. We give a simple example to explain this fact.

Let $p \geq 3$ and $q \neq p$ be prime numbers and ζ_p, ζ_q are respectively a p^{th} and q^{th} primitive root of 1. Let $n \geq 2$ be the order of q mod p such that

$$p(q-1)|(q^n-1) \quad \text{and} \quad n|p-1.$$

Put$f = (q^n-1)/p$ and $e = (p-1)/n$. In the field $K = \mathbb{Q}(\zeta_p)$, any finite prime ideal $\mathfrak{q}$ above q yields a finite residue class field $\mathbb{F} = \mathbb{Z}[\zeta_p]/\mathfrak{q}$, and $\mathbb{F} \cong \mathbb{F}_{q^n}$.

Definition 6.1. Let $\alpha \in \mathbb{Z}[\zeta_p]$ be a generator of $\mathbb{F}^\times$ such that $\alpha^f \equiv \zeta_p \pmod{\mathfrak{q}}$. The p elements

$$\eta_i = \sum_{j=0}^{f-1} \zeta_q^{\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^{i+pj})}, \quad 0 \leq i \leq p-1$$

are called Gauss periods, and the Gauss sum is nothing else but

$$G = \sum_{i=0}^{q^n-2} \zeta_p^i \zeta_q^{\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^i)} = \sum_{i=0}^{p-1} \eta_i \zeta_p^i.$$

Remark This form of the Gauss sums is the computable version. One has to find a method to compute the η_i and then use its properties to perform a good algorithm. See [**F.T1**], [**F.T2**], [**G.M**],[**H**].

We can extend the index of η_i to $\mathbb{Z}$ as follows: define

$$\eta_{i+kp} := \eta_i.$$

Let g be a primitive root modulo q such that

$$g \equiv \alpha^{\frac{q^n-1}{q-1}} \bmod \mathfrak{q}$$

and let τ be the automorphism of $\mathbb{Q}(\zeta_q)/\mathbb{Q}$ such that $\tau(\zeta_q) = \zeta_q^g$.

$$\tau(\eta_i) = \sum_{j=0}^{f-1} \zeta_q^{g\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^{i+pj})} = \sum_{j=0}^{f-1} \zeta_q^{\mathrm{Tr}_{K/\mathbb{Q}}(g\alpha^{i+pj})} = \sum_{j=0}^{f-1} \zeta_q^{\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^{\frac{p(q^n-1)}{p(q-1)}+i+pj})} = \eta_i$$

for each i. Since τ generated $Gal(\mathbb{Q}(\zeta_q)/\mathbb{Q})$, this proves that:

Lemma 6.1. *Let $p \geq 3$ and $q \neq p$ be prime numbers such that there exits $n \geq 2$ factor of $p-1$ and $p(q-1)|q^n-1)$. Let η_i defined as before, then for*

$$0 \leq i \leq p-1 \qquad \eta_i \in \mathbb{Z}$$

and

$$\eta_{qi} = \eta_i$$

Proof. We have already proved that $\tau(\eta_i) = \eta_i$ for all $\tau \in Gal(\mathbb{Q}(\zeta_q)/\mathbb{Q})$ so that η_i is invariant under $Gal(\mathbb{Q}(\zeta_q)/\mathbb{Q})$.

$$\eta_{qi} = \sum_{j=0}^{f-1} \zeta_q^{\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^{qi+pj})} = \sum_{j=0}^{f-1} \zeta_q^{\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^{i+pj})}, \quad 0 \leq i \leq p-1$$

□

We define the polynomial in one indeterminate

$$G(X) = \sum_{i=0}^{q^n-2} X^i \zeta_q^{\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^i)}$$

then

$$G(X) \equiv \sum_{i=0}^{p-1} \eta_i X^i \bmod (X^p - 1)$$

so that $G = G(\zeta_p)$ and a direct computation shows that

$$G(1) = \sum_{i=0}^{p-1} \eta_i = -1 \quad \text{and} \quad G(\zeta_p^i)G(\zeta_p^{-i}) = q^n, \quad 1 \leq i \leq p-1$$

.

$G(1) = -1$ has generated discussion about the real definition of Gauss sums. Thus in [**w1**] we see that one can correct the sign by introducing the Möbiüs function.

If n is even, then from $\eta_{qi} = \eta_i$ we deduce that $\eta_{-i} = \eta_{q^{\frac{n}{2}}i} = \eta_i$ so that $G(\zeta_p^i) = G(\zeta_p^{-i})$, thus $G = \pm q^{n/2}$. Then working modulo $(\zeta_p - 1)$, we obtain

$$G = q^{\frac{n}{2}}$$

If n is odd, then $e = (p-1)/n$ is even. We then define the Gaussian periods

$$\theta_i = \sum_{l=0}^{n-1} \zeta_p^{g^{i+el}}, \quad 0 \leq i \leq e-1.$$

This results in the well-known lemma

Lemma 6.2. *$\{\theta_0, \theta_1 \cdots \theta_{e-1}\}$ forms a normal integral basis of $\mathbb{Q}(\theta_0)/\mathbb{Q}$, the subfield of $\mathbb{Q}(\zeta_p)$ of degree e.*

We also notice that

$$\theta_{g^{i+e}} = \theta_i \text{ for } i \geq 0.$$

this observation is a consequence of the fact that $q^n \equiv g^{p-1} \equiv 1 \bmod p$ implies that $g^e \equiv q^t \bmod p$ for some t prime to n. We have therefore

$$G(\zeta_p) = \theta_0 + \sum_{i=0}^{p-2} \theta_{g^i} \zeta_p^{g^i} = \theta_0 + \sum_{i=0}^{e-1} \theta_{g^i} \sum_{j=0}^{n-1} \zeta_p^{g^{i+ej}}$$

i.e

$$G(\zeta_p) = \theta_0 + \sum_{i=0}^{e-1} \theta_{g^i} \theta_i$$

The multiplication among the θ_i yields the following facts. Since $(\theta_i)_{(0 \leq i \leq e-1)}$ form a basis there is matrix A with coefficients $a_{(i,j)}$ such that

$$\theta_0 \theta_i = \sum_{j=0}^{e-1} a_{i,j} \theta_j$$

for $0 \leq i, j \leq e-1$. Since $\theta_{i+ke} = \theta_i$ we see that $a_{(i+ke,j+le)} = a_{(i,j)}$, however, one notices that if $\sigma \in Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is such that $\sigma(\zeta_p) = \zeta_p^g$ then $\sigma(\theta_0\theta_i) = \theta_1\theta_{i+1}$. Therefore by taking the conjugates of $\theta_0\theta_i$ we have

$$\theta_i \theta_j = \sum_{k=0}^{e-1} a_{(j-i,k-i)} \theta_k = \sum_{k=0}^{e-1} a_{(i-j,k-j)} \theta_k = \theta_j \theta_i.$$

This proves that

$$a_{(i,j)} = a_{(-i,j-i)}.$$

Finally we have

$$\theta_i \theta_j = A \begin{pmatrix} \theta_j \\ \theta_{j+1} \\ \cdots \\ \cdots \\ \cdots \\ \theta_{j+e-1} \end{pmatrix} = \theta_j \begin{pmatrix} \theta_j \\ \theta_{j+1} \\ \cdots \\ \cdots \\ \cdots \\ \theta_{j+e-1} \end{pmatrix}.$$

We have therefore proved that the gauss periods $\theta_0, \cdots, \theta_{e-1}$ are exactly the eigen values of the matrix A, and $det(XI - A)$ is the minimal polynomial of the periods. Thus $\mathbb{Q}(\theta_0) \cong \mathbb{Q}(A)$ by $\theta_0 \longmapsto A$.

Example

We take $p = 3$ and $q = 5$, then $K = \mathbb{Q}(\zeta_3)$. The order of 5 modulo 3 is 2, so that 5 does not split in $\mathbb{Z}[\zeta_3]$. The residue class field at 5 is

$$\mathbb{Z}[\zeta_3]/(5) = \{a + b\zeta_3; \quad 0 \leq a, b \leq 5\}.$$

and the element $\alpha = 1 + 3\zeta_3$ is a generator. Furthermore $f = 8$ and $e = 1$.

$$\eta_0 = \sum_{j=0}^{7} \zeta_q^{\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^{0+3j})} = \zeta_5^2 + \zeta_5^0 + \zeta_5^4 + \zeta_5^0 + \zeta_5^3 + \zeta_5^0 + \zeta_5 + \zeta_5^0 \quad = \quad 3$$

$$\eta_1 = \sum_{j=0}^{7} \zeta_q^{\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^{1+3j})} = \zeta_5^4 + \zeta_5^0 + \zeta_5^3 + \zeta_5^2 + \zeta_5 + \zeta_5^4 + \zeta_5^2 + \zeta_5^3 \quad = \quad -2$$

$$\eta_2 = \sum_{j=0}^{7} \zeta_q^{\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^{2+3j})} = \zeta_5^2 + \zeta_5^4 + \zeta_5^4 + \zeta_5^3 + \zeta_5^3 + \zeta_5 + \zeta_5 + \zeta_5^2 \quad = \quad -2$$

One verifies that:

$$\eta_0 + \eta_1 + \eta_2 \quad = \quad -1$$

$$\eta_2 = \eta_{-1} = \eta_1.$$

$$G(\zeta_3) = \eta_0 + \zeta_3\eta_1 + \zeta_3^2\eta_2 = \eta_0 + \eta_1(\zeta_3 + \zeta_3^2) = 3 + (-2)(-1) = 5 = 5^{\frac{2}{2}}.$$

$$G(\zeta_3^{-1}) = \eta_0 + \zeta_3\eta_2 + \zeta_3^2\eta_1 = \eta_0 + \eta_1(\zeta_3 + \zeta_3^2) = 3 + (-2)(-1) = 5 = 5^{\frac{2}{2}}.$$

then follows

$$G(\zeta_3)G(\zeta_3^{-1}) = 5 \times 5 = 5^2$$

2. The quadratic Gauss sums

The first Gauss sum ever computed is

$$G_2 = \sum_{r \bmod p} \left(\frac{r}{p}\right) \exp\left(\frac{2\pi i r}{p}\right),$$

where p is an odd prime and $\left(\frac{r}{p}\right)$ is the unique quadratic character modulo p. We see at once that

$$G_2^2 = \sum_{r,s \bmod p} \left(\frac{rs}{p}\right) \exp\left(\frac{2\pi i(r+s)}{p}\right) = \sum_{t \bmod p} \left(\frac{t}{p}\right) \sum_{s \bmod p} \exp\left(\frac{2\pi i s(t+1)}{p}\right),$$

under the substitution $r \equiv st \bmod p$, and the inner sum is $p-1$ if $t \equiv -1 \bmod p$ and -1 otherwise. We therefore obtain

$$G_2^2 = (-1)^{\frac{p-1}{2}} p.$$

The problem here is to determine the right sign for G_2. Indeed

Theorem 6.1. *For the quadratic Gauss sum, we have the following result:*

$$G_2 = \begin{cases} p^{1/2} \text{ if } p \equiv 1 \bmod 4 \\ ip^{1/2} \text{ if } p \equiv -1 \bmod 4 \end{cases},$$

where $p^{1/2}$ is the positive square root.

Proof. There are many proofs of this theorem. We outline here that of Cauchy. Put $\zeta = \exp(2\pi i/p)$.
If we consider the product

$$\sigma_2 = \prod_{r=1}^{(p-1)/2} (\zeta^{2r-1} - \zeta^{-2r+1}).$$

We then see the above product as follows. In the field $\mathbb{Q}$ the roots of unity we have are ± 1 then σ can be obtained just by selecting a half set modulo p and build the product over this half set. If we choose as a half set to be the odd numbers modulo p then a factor of this product $\zeta^{2r-1} - \zeta^{-2r+1}$ is seeing as $(1)\zeta^{2r-1} + (-1)\zeta^{-2r+1}$. Any other choice of another half set results in multiplying σ_2 by a suitable sign. Since the half set modulo p, $\{1, 3, \cdots, p-2\}$ has as symmetric $\{-1, -3, \cdots, -p+2\} = \{2, 4, \cdots, p-1\}$ we therefore deduce that:

$$\sigma_2^2 = (-1)^{(p-1)/2} \prod_{r=1}^{p-1} (\zeta^r - \zeta^{-r}) = (-1)^{p-1)/2} p.$$

this product is just the values of the cyclotomic polynomial of order p at 1, so that

$$\sigma_2 = \pm G_2.$$

In fact

$$\sigma_2 = G_2.$$

The sign of σ_2^2 is easily determined by writing it in the form

$$\sigma_2 = (2i)^{(p-1)/2} \prod_{r=1}^{\frac{p-1}{2}} \sin(2\pi(2r-1)/p),$$

and then counting the number of negative factors in the product. Considering the congruence relations it could be enough to prove that $\sigma_2 = \pm G_2$. The prime p ramifies totally in $\mathbb{Q}(\zeta)$ and if $\lambda = 1-\zeta$, we then have the prime ideal factorization $(p) = (\lambda)^{p-1}$. On the one hand we have $(\frac{r}{p}) \equiv r^{\frac{p-1}{2}} \bmod p$, so

$$G_2 \equiv \sum_{r \bmod p} r^{\frac{p-1}{2}}(1-\lambda)^r = \sum_{s=0}^{\frac{p-1}{2}} (-\lambda)^s \sum_{r \bmod p} r^{\frac{p-1}{2}} \binom{r}{s} \mod \lambda^{\frac{p-1}{2}}.$$

However $\sum_{r \bmod p} r^n$ is either 0 or -1 mod$p$ according to whether $(p-1)|n$ or not, so that only the term $s = \frac{p-1}{2}$ contributes to the sum. By Wilson's Theorem, the result is

$$G_2 \equiv (\frac{p-1}{2})! \lambda^{\frac{p-1}{2}} \mod \lambda^{\frac{p-1}{2}}.$$

On the other hand, by similar arguments,

$$\zeta^{2r-1} - \zeta^{-2r+1} = -\zeta^{-2r+1}(1-\zeta^{2(2r-1)}) \equiv -2(2r-1)\lambda \mod \lambda^2,$$

so that

$$\sigma_2 \equiv \prod_{r=1}^{\frac{p-1}{2}} (-2(2r-1)\lambda) \equiv (\frac{p-1}{2})! \lambda^{\frac{p-1}{2}} \mod \lambda^{\frac{p+1}{2}}$$

Thus $G_2 \equiv \sigma_2 \bmod lambda^{\frac{p-1}{2}}$. To finish the proof one has to determine the sign of σ_2.
$\sin(\frac{2(2r-1)\pi}{p}) < 0$ if $\frac{p+2}{2} < r \leq \frac{p-1}{2}$, therefore the product in σ_2 has $\frac{p-1}{2} - [\frac{p+2}{4}]$ negative terms and this is either $\frac{p-1}{4}$ or $\frac{p-3}{4}$ according to whether $p \equiv 1 \bmod 4$ or $p \equiv 3 \bmod 4$ respectively. We then deduce that the sign of σ_2 is $(i)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{4}} = +1$ for $p \equiv 1 \bmod 4$ or $(i)^{\frac{p-1}{2}}(-1)^{\frac{p-3}{4}} = +i$ for $p \equiv i \bmod 4$ □

There are number of proofs of this theorem in the literature, [**J.W.S**].
Loxton attempted to generalize the relation between G_m and σ_m, for higher order Gauss sums. He proved [**Lox**][**Lox1**] that there exits an algebraic integer α such that $\sigma_m = \alpha G_m$ The problem here to determine the magnitude of such α. This question is still open.

3. Algorithm for the computation of the Gauss sums

Let $K = \mathbb{Q}(\zeta_m)$ and p prime integer such that $p^f \equiv 1 \bmod m$. Let $\pi | p$ be a prime such that $N_{K/\mathbb{Q}}(\pi) = p^f \equiv 1 \bmod (m)$

- 1. Find a primitive root modulo π
  Let g be a primitive root modulo π. That is , the cyclic group$< g >$ generated by g together with $\{0\}$ is a complete set of residues modulo p. Then if $x \in \mathbb{Z}[\zeta_m]$, there exists an integer $k > 0$ so that $x = g^k$. In practice we just take a primitive root, whose absolute norm is the smallest, although this magnitude is related to the Riemann Hypothesis, our computation shows that they are relatively small. Th searching for a primitive root has a bad complexity and therefore the as $N(\pi) \to \infty$ the computation is very slow

- Computation of the Legendre symbol:
  Put $N = \frac{p^f - 1}{m}$ and $t = g^N \bmod \pi$ with $t^m \equiv 1 \pmod{\pi}$.
  Since π is a polynom $f(\zeta_m)$ in ζ_m with integer coefficients, then test the power of t such that $f(t^\ell) \equiv 0 \bmod \pi$, $1 \leq \ell \leq m$, say a.
  Evaluate $r = a^{-1} \bmod m$.
  Define $\left(\frac{g}{\pi}\right)_m = \zeta_m^r$.
- Thus if $\chi = \chi_\pi = \left(\frac{\div}{\pi}\right)$ is the Dirichlet character associated to π, then its values at the non zero residue classes modulo π are fully determined by its values at g.
  We then notice that the determination of the values of the Gauss sums is related to the determination of the primitive roots $\bmod \pi$. At this stage the slower the algorithm of finding a primitive root, the slower the computation of the values of the gauss sums is.
  From the Wilson's Theorem:

$$g^{p^f - 1} \equiv 1 \bmod \pi$$

we have the following facts:

- $g^{\frac{p^f - 1}{2}} \equiv -1 \bmod \pi$
- $\chi(g^{am}) = 1$
- $\chi(g^{a+m}) = \chi(a)$

Let $S^* = \left\{x_1, \cdots, x_{p^f-1}\right\}$ be any set of non zero residues modulo π, then

$$G(\chi,1) = \sum_{k=1}^{p^f-1} \chi(g^k)e(g^k) = \sum_{k=1}^{\frac{p^f-1}{2}} \chi(g^k)(e(g^k)+e(-g^k)) \tag{3.1}$$

$$= 2\sum_{\ell=0}^{m-1}\sum_{k=1}^{\frac{p^f-1}{2m}} \chi(g^\ell)\cos\left(2\pi \mathrm{Tr}_{K/\mathbb{Q}}\left(\tfrac{g^{km+\ell}}{\pi}\right)\right) \tag{3.2}$$

$$= 2\sum_{\ell=0}^{m-1}\chi(g)^\ell \sum_{k=1}^{\frac{p^f-1}{2m}} \cos\left(2\pi \mathrm{Tr}_{K/\mathbb{Q}}\left(\tfrac{g^{km+\ell}}{\pi}\right)\right) \tag{3.3}$$

$$= \sum_{\ell=0}^{m-1}\chi(g)^\ell G_\ell(\pi) \tag{3.4}$$

(3.5)

where

$$G_\ell(\pi) = 2\sum_{k=1}^{\frac{p^f-1}{2m}} \cos\left(2\pi \mathrm{Tr}_{K/\mathbb{Q}}\left(\tfrac{g^{km+\ell}}{\pi}\right)\right); \quad G_\ell(\pi) \text{ is called in appendix 1, a Gauss period .}$$

If $\chi(g) = \zeta^r = \zeta_m^r$ then

$$G(\chi,1) = \sum_{l=1}^{m-1} \zeta^{rl} G_l(\pi)$$

Thus if ε is any injection that maps $\mu_m(K)$ into $\mu_m(\mathbb{C})$ then

$$\mathfrak{g}(1,\varepsilon,\pi) = G(\varepsilon\circ\chi,1).$$

Example
$p = 11$ $m = 5$ $g = 2$. Then $(11) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$ where $\mathfrak{p}_i = (11, \zeta_5 - 4^i)$.
One of these ideal factors has $\pi = -5\zeta_5 + 16\zeta_5^2 - 13\zeta_5^3 + 13\zeta_5^4$ as a uniformizer.
$(\pi) = (11, \zeta_5 - 5)$. $\mathbb{Z}[\zeta_5]/(\pi) \cong \mathbb{F}_{11}$, but $\mathbb{Z}/(11) \subset \mathbb{Z}[\zeta_5]$ implies that $\{0,1,2,\cdots,10\}$ is a complete set of residues modulo (π).
since

$$e\left(\frac{x}{\pi}\right) = e\left(\frac{x\sigma(\pi)\sigma^2(\pi)\sigma^3(\pi)}{11}\right)$$

and since $\mathrm{Tr}_{K/\mathbb{Q}}$ is $\mathbb{Q}$-linear we have

$$\mathrm{Tr}_{K/\mathbb{Q}}\left(\tfrac{x\sigma(\pi)\sigma^2(\pi)\sigma^3(\pi)}{11}\right) = \frac{x}{11}\mathrm{Tr}_{K/\mathbb{Q}}(\sigma(\pi)\sigma^2(\pi)\sigma^3(\pi)) \tag{3.6}$$

$$= \frac{x}{11}\mathrm{Tr}_{K/\mathbb{Q}}(23\zeta_5 - 23\zeta_5^2 - 74\zeta_5^3 - 60\zeta_5^4) \tag{3.7}$$

$$= \frac{2x}{11} \tag{3.8}$$

therefore

$$e\left(\frac{x}{\pi}\right) = \exp\left(\frac{4x\pi i}{11}\right) \text{ and } \left(\frac{2}{\pi}\right)_5 = \zeta_5^3$$

$$G_l(\pi) = 2\sum_{k=1}^{\frac{11-1}{10}} \cos\left(2\pi \mathrm{Tr}_{K/\mathbb{Q}}\left(\frac{2^{5k+l}}{\pi}\right)\right) \tag{3.9}$$

$$= 2\cos\left(2\pi \mathrm{Tr}_{K/\mathbb{Q}}\left(\frac{2^{5k+l}}{\pi}\right)\right) \tag{3.10}$$

$$= 2\cos\left(2.2\pi\left(\frac{2^{5k+l}}{11}\right)\right) \tag{3.11}$$

the Gauss sums

$$G\left(\left(\frac{\cdot}{\pi}\right)_5, \pi\right) = \sum_{k=1}^{10}\left(\frac{2^i}{\pi}\right)_5 \exp\left(\frac{4.2^k.i\pi}{11}\right) \tag{3.12}$$

$$= \sum_{k=1}^{10}\zeta_5^{2k}\exp\left(\frac{4.2^k i\pi}{11}\right) \tag{3.13}$$

$$= \sum_{l=1}^{4}\zeta_5^{2l} 2\cos\left(\frac{2^{5l+1}.2\pi}{11}\right) \tag{3.14}$$

$$= 2\left(\zeta_5^2\cos\left(\frac{2\pi}{11}\right) + (\zeta_5^4\cos\left(\frac{10\pi}{11}\right) + \zeta_5\cos\left(\frac{6\pi}{11}\right)\right) \tag{3.15}$$

$$+ 2\left(\zeta_5^3\cos\left(\frac{8\pi}{11}\right) + \zeta_5^0\cos\left(\frac{4\pi}{11}\right)\right). \tag{3.16}$$

Let's take $\varepsilon(\zeta_5) = exp(2i\pi/5)$ and we find that

$$\mathfrak{g}(\pi, \varepsilon, 1) = -0.151714534668630627524904404 2+3.313152984691512984920560792*i$$

$$p = 31, \quad m = 5, \quad g = 3$$

Then $(31) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$ where $\mathfrak{p}_i = (31, \zeta_5 - 16^i), \quad 1 < i < 5$.
One of these ideal factors has $\pi = -63\zeta_5 + 5\zeta_5^2 - 42\zeta_5^3 - 34\zeta_5^4$ as a uniformizer.
$(\pi) = (31, \zeta_5 - 8)$. $\mathbb{Z}[\zeta_5]/(\pi) \cong \mathbb{F}_{31}$ but $\mathbb{Z}/(31) \subset \mathbb{Z}[\zeta_5]$ implies that $\{0, 1, 2, \cdots, 30\}$ is a complete set of residues modulo (π).
$e\left(\frac{x}{\pi}\right) = e\left(\frac{x\sigma(\pi)\sigma^2(\pi)\sigma^3(\pi)}{31}\right)$ and since $\mathrm{Tr}_{K/\mathbb{Q}}$ is $\mathbb{Q}$-linear we have

$$\mathrm{Tr}_{K/\mathbb{Q}}\left(\frac{x\sigma(\pi)\sigma^2(\pi)\sigma^3(\pi)}{31}\right) = \frac{x}{31}\mathrm{Tr}_{K/\mathbb{Q}}(\sigma(\pi)\sigma^2(\pi)\sigma^3(\pi)) \tag{3.17}$$

$$= \frac{x}{31}\mathrm{Tr}_{K/\mathbb{Q}}(-49\zeta_5 + 58\zeta_5^2 + 335\zeta_5^3 + 237\zeta_5^4) \tag{3.18}$$

$$= \frac{-681x}{31} \tag{3.19}$$

therefore $e\left(\frac{x}{\pi}\right) = \exp\left(\frac{-2x\pi i}{31}\right)$ and $\left(\frac{3}{\pi}\right)_5 = \zeta_5^3$

$$G_l(\pi) = 2\sum_{k=1}^{\frac{31-1}{10}} \cos\left(2\pi \mathrm{Tr}_{K/\mathbb{Q}}\left(\frac{2^{5k+l}}{\pi}\right)\right) \tag{3.20}$$

$$= 2\sum_{k=1}^{3} \cos\left(2\pi \mathrm{Tr}_{K/\mathbb{Q}}\left(\frac{3^{5k+l}}{\pi}\right)\right) \tag{3.21}$$

$$= 2\left(\cos\left(-2\pi\frac{3^{5.1+l}}{31}\right) + \cos\left(-2\pi\frac{3^{5.2+l}}{31}\right) + \cos\left(-2\pi\frac{3^{5.3+l}}{31}\right)\right) \tag{3.22}$$

$$= 2\left(\cos\left(2\pi\frac{3^{5+l}}{31}\right) + \cos\left(2\pi\frac{3^{10+l}}{31}\right) + \cos\left(2\pi\frac{3^{15+l}}{31}\right)\right) \tag{3.23}$$

The Gauss sums

$$G\left(\left(\frac{\cdot}{\pi}\right)_5, \pi\right) = \sum_{k=1}^{30}\left(\frac{3^i}{\pi}\right)_5 \exp\left(\frac{-2.3^k.i\pi}{31}\right) = \sum_{k=1}^{30}\zeta_5^{3k}\exp\left(\frac{2.3^k i\pi}{31}\right) \tag{3.24}$$

$$= \sum_{l=1}^{5}\zeta_5^{3l} 2\sum_{k=1}^{3}\cos\left(\frac{3^{5k+l}.2\pi}{31}\right) \tag{3.25}$$

$$= 2\left(\zeta_5^3\left(\cos\left(\frac{6\pi}{31}\right) + \cos\left(\frac{32\pi}{31}\right) + \cos\left(\frac{26\pi}{31}\right)\right)\right) \tag{3.26}$$

$$+ 2\left(\zeta_5\left(\cos\left(\frac{18\pi}{31}\right) + \cos\left(\frac{34\pi}{31}\right) + \cos\left(\frac{16\pi}{31}\right)\right)\right) \tag{3.27}$$

$$+ 2\left(\zeta_5^4\left(\cos\left(\frac{54\pi}{31}\right) + \cos\left(\frac{40\pi}{31}\right) + \cos\left(\frac{48\pi}{31}\right)\right)\right) \tag{3.28}$$

$$+ 2\left(\zeta_5^2\left(\cos\left(\frac{38\pi}{31}\right) + \cos\left(\frac{58\pi}{31}\right) + \cos\left(\frac{20\pi}{31}\right)\right)\right) \tag{3.29}$$

$$+ 2\left(\zeta_5^0\left(\cos\left(\frac{52\pi}{31}\right) + \cos\left(\frac{50\pi}{31}\right) + \cos\left(\frac{60\pi}{31}\right)\right)\right) \tag{3.30}$$

For distinct values of $\varepsilon(\zeta_5)$ we obtain the following results $\varepsilon(\zeta_5) = exp(2i\pi/5)$

$G(\pi, \varepsilon, 1) = 5.226579352648107065417247109 - 1.919080058380184951993603231 \times I$

$\varepsilon(\zeta_5) = exp(4i\pi/5)$

$G(\pi, \varepsilon, 1) = 4.552416669473279118809518850 - 3.205542460723585071329278448 \times I$

$\varepsilon(\zeta_5) = exp(6i\pi/5)$

$G(\pi, \varepsilon, 1) = 4.552416669473279118809518850 + 3.205542460723585071329278448 \times I$

$\varepsilon(\zeta_5) = exp(8i\pi/5)$

$G(\pi, \varepsilon, 1) = 5.226579352648107065417247109 + 1.919080058380184951993603231 \times I$

4. data

This is just a sample of the output file we have. The algebraic numbers are given in the basis $\zeta, \cdots, \zeta^4$. On the rows, v stands for a prime factor of P. Under v there are successively four lines, each corresponding to a conjugate of primary v^* up to a fifth power of a unit, v^*, the $(1-\zeta)$-adic extension of v^*, the value of Gauss sums as a complex number, the angle corresponding to the Gauss sum, and the root of unity $\Omega(S_0, v^*)$ obtained from the fundamental domain with respect to S_0.

```
v=  -1,0,0,2
31  -63 5 -42 -34   1 0 0 3 3   5.2266  -1.9191   -20.162067  -1 0 0 0
31  -2 -3 1 -5   1 0 0 4 2   4.5524  -3.2055   -35.150921  -1 0 0 0
31  -5 1 -3 -2   1 0 0 1 0   4.5524  3.2055   35.150963  0 0 0 -1
31  -34 -42 5 -63   1 0 0 2 4   5.2266  1.9191   20.162107  0 0 0 -1

v=  -2,-1,1,-2
41  1 3 0 2   1 0 0 2 1   2.5685  -5.8654   -66.351456  0 0 0 -1
41  0 1 2 3   1 0 0 1 2   -5.0581  3.9262   142.180450  0 0 0 -1
41  3 2 1 0   1 0 0 4 4   -5.0581  -3.9263   -142.180389  -1 0 0 0
41  2 0 3 1   1 0 0 3 0   2.5684  5.8654   66.351532  -1 0 0 0

v=  -2,1,1,1
61  3 2 1 5   1 0 0 4 3   -4.9170  -6.0682   -129.017731  0 0 -1 0
61  -34 63 -60 42   1 0 0 2 0   -6.6959  -4.0205   -149.017487  0 0 -1 0
61  42 -60 63 -34   1 0 0 3 -1   -6.6959  4.0205   149.017532  0 -1 0 0
61  5 1 2 3   1 0 0 1 1   -4.9170  6.0682   129.017776  0 -1 0 0

v=  -2,-2,1,-1
71  42 5 23 31   1 0 0 3 1   2.6149  8.0101   71.921021  0 -1 0 0
71  -12 2 -9 -5   1 0 0 4 0   -3.2575  -7.7710   -112.742767  0 0 -1 0
71  -5 -9 2 -12   1 0 0 1 3   -3.2575  7.7710   112.742836  0 -1 0 0
71  31 23 5 42   1 0 0 2 2   2.6149  -8.0101   -71.920937  0 0 -1 0

v=  -3,-1,-1,1
101  -34 -2 -20 -23   1 0 0 2 3   9.8919  -1.7748   -10.171501  1 1 1 1
101  20 1 12 13   1 0 0 1 4   -1.0453  9.9954   95.970375  -1 0 0 0
101  13 12 1 20   1 0 0 4 1   -1.0453  -9.9954   -95.970291  0 0 0 -1
101  -23 -20 -2 -34   1 0 0 3 2   9.8919  1.7748   10.171578  1 1 1 1

v=  -3,-2,-1,2
131  -4 -2 0 -3   1 0 0 2 4   -4.7380  10.4188   114.453888  0 0 -1 0
131  -110 81 -118 13   1 0 0 1 0   -11.1907  2.4019   167.885941  0 -1 0 0
131  13 -118 81 -110   1 0 0 4 2   -11.1907  -2.4020   -167.885864  0 0 -1 0
131  -3 0 -2 -4   1 0 0 3 3   -4.7380  -10.4188   -114.453835  0 -1 0 0

v=  -3,-1,3,2
151  -3 0 -2 1   1 0 0 3 2   -8.5591  -8.8171   -134.149353  1 1 1 1
151  13 157 -89 165   1 0 0 4 1   -1.2623  -12.2232   -95.895943  0 0 0 -1
151  165 -89 157 13   1 0 0 1 4   -1.2623  12.2232   95.895988  -1 0 0 0
151  1 -2 0 -3   1 0 0 2 3   -8.5591  8.8171   134.149429  1 1 1 1

v=  -1,-1,3,0
181  -9 8 -10 2   1 0 0 2 4   5.9452  -12.0688   -63.774700  0 -1 0 0
181  -45 -24 -13 -52   1 0 0 1 0   -13.0977  3.0741   166.791382  1 1 1 1
181  -52 -13 -24 -45   1 0 0 4 2   -13.0977  -3.0741   -166.791336  1 1 1 1
181  2 -10 8 -9   1 0 0 3 3   5.9452  12.0688   63.774769  0 0 -1 0
```

```
v=  -3,2,-1,-2
191  71 -2 45 42   1 0 0 2 1   5.1231  12.8356   68.241318  -1 0 0 0
191  10 6 2 13   1 0 0 1 2   -6.3175  12.2918   117.201408  0 0 -1 0
191  13 2 6 10   1 0 0 4 4   -6.3175  -12.2918   -117.201370  0 -1 0 0
191  42 45 -2 71   1 0 0 3 0   5.1232  -12.8356   -68.241272  0 0 0 -1

v=  -2,0,0,3
211  -1 9 -6 9   1 0 0 0 2   5.7477  -13.3403   -66.690941  0 0 -1 0
211  -16 34 -31 24   1 0 0 0 2   12.8835  6.7093   27.509060  -1 0 0 0
211  24 -31 34 -16   1 0 0 0 2   12.8835  -6.7093   -27.508987  0 0 0 -1
211  9 -6 9 -1   1 0 0 0 2   5.7477  13.3403   66.690987  0 -1 0 0

v=  -3,-3,-1,3
241  -9 -17 5 -23   1 0 0 2 1   -1.2352  15.4750   94.563652  -1 0 0 0
241  -5 -24 12 -27   1 0 0 1 2   9.2728  -12.4505   -53.322437  0 0 -1 0
241  -27 12 -24 -5   1 0 0 4 4   9.2728  12.4505   53.322475  0 -1 0 0
241  -23 5 -17 -9   1 0 0 3 0   -1.2352  -15.4750   -94.563622  0 0 0 -1

v=  -4,-3,0,-2
251  -4 3 -5 2   1 0 0 2 3   -2.1786  15.6925   97.904053  -1 0 0 0
251  60 81 -13 118   1 0 0 1 4   14.4796  -6.4298   -23.944149  0 0 -1 0
251  118 -13 81 60   1 0 0 4 1   14.4796  6.4298   23.944191  0 -1 0 0
251  2 -5 3 -4   1 0 0 3 2   -2.1786  -15.6925   -97.904037  0 0 0 -1

v=  -4,-2,1,-4
271  241 63 110 212   1 0 0 2 2   13.0712  10.0071   37.437107  1 1 1 1
271  0 1 -3 3   1 0 0 1 3   -9.4517  13.4783   125.040001  -1 0 0 0
271  3 -3 1 0   1 0 0 4 0   -9.4517  -13.4784   -125.039932  0 0 0 -1
271  212 110 63 241   1 0 0 3 1   13.0712  -10.0071   -37.437042  1 1 1 1

v=  -4,-1,1,0
281  -16 -71 34 -81   1 0 0 0 1   -0.1217  16.7626   90.415955  0 -1 0 0
281  -1 -6 4 -6   1 0 0 0 1   11.4050  -12.2852   -47.127842  0 0 0 -1
281  -6 4 -6 -1   1 0 0 0 1   11.4050  12.2852   47.127903  -1 0 0 0
281  -81 34 -71 -16   1 0 0 0 1   -0.1217  -16.7626   -90.415871  0 0 -1 0

v=  -4,-1,2,4
311  -4 -2 -5 -3   1 0 0 2 0   -0.3871  -17.6309   -91.257736  0 -1 0 0
311  335 81 157 288   1 0 0 1 1   8.7925  -15.2870   -60.094284  1 1 1 1
311  288 157 81 335   1 0 0 4 3   8.7924  15.2870   60.094360  1 1 1 1
311  -3 -5 -2 -4   1 0 0 3 4   -0.3871  17.6309   91.257812  0 0 -1 0

v=  -3,-3,3,4
331  0 6 7 3   1 0 0 1 0   0.2367  18.1919   89.254608  0 -1 0 0
331  7 0 3 6   1 0 0 3 3   -12.1057  13.5813   131.712173  0 -1 0 0
331  6 3 0 7   1 0 0 2 4   -12.1057  -13.5813   -131.712082  0 0 -1 0
```

```
331  3 7 6 0   1 0 0 4 2   0.2367  -18.1919   -89.254562  0 0 -1 0

v=  -4,-3,1,-3
401  -5 -49 27 -52   1 0 0 1 4   14.2760  -14.0426   -44.527699  1 1 1 1
401  17 5 8 16   1 0 0 3 2   -17.4865  9.7581   150.836884  0 0 -1 0
401  16 8 5 17   1 0 0 2 3   -17.4865  -9.7582   -150.836792  0 -1 0 0
401  -52 27 -49 -5   1 0 0 4 1   14.2760  14.0426   44.527775  1 1 1 1

v=  -3,2,0,2
421  -1 -16 9 -16   1 0 0 0 4   8.3003  18.7645   66.138268  -1 0 0 0
421  24 34 -6 49   1 0 0 0 4   7.3545  19.1549   68.995842  0 -1 0 0
421  49 -6 34 24   1 0 0 0 4   7.3545  -19.1549   -68.995728  0 0 -1 0
421  -16 9 -16 -1   1 0 0 0 4   8.3003  -18.7645   -66.138176  0 0 0 -1

v=  -3,2,4,3
431  31 -2 20 17   1 0 0 2 4   -20.6775  -1.8552   -174.873062  -1 0 0 0
431  35 -9 27 13   1 0 0 1 0   1.5296  -20.7041   -85.774612  0 0 -1 0
431  13 27 -9 35   1 0 0 4 2   1.5296  20.7041   85.774696  0 -1 0 0
431  17 20 -2 31   1 0 0 3 3   -20.6775  1.8552   174.873138  0 0 0 -1

v=  -4,-3,2,1
461  4 4 -1 4   1 0 0 0 2   -3.2293  -21.2267   -98.650375  0 0 0 -1
461  89 -136 139 -81   1 0 0 0 2   -8.7992  19.5851   114.193428  0 0 -1 0
461  -81 139 -136 89   1 0 0 0 2   -8.7992  -19.5851   -114.193367  0 -1 0 0
461  4 -1 4 4   1 0 0 0 2   -3.2294  21.2267   98.650459  -1 0 0 0

v=  -4,-2,4,3
491  -2 7 -4 5   1 0 0 4 4   14.6961  -16.5839   -48.453827  1 1 1 1
491  -139 -42 -60 -128   1 0 0 2 1   -20.8132  7.6035   159.931702  0 -1 0 0
491  -128 -60 -42 -139   1 0 0 3 0   -20.8132  -7.6035   -159.931671  0 0 -1 0
491  5 -4 7 -2   1 0 0 1 2   14.6960  16.5839   48.453854  1 1 1 1

v=  -1,-1,-1,4
521  -1 -1 -1 4   1 0 0 0 4   15.8837  -16.3924   -45.902981  0 0 -1 0
521  -1 -1 4 -1   1 0 0 0 4   22.1453  5.5303   14.021482  -1 0 0 0
521  -1 4 -1 -1   1 0 0 0 4   22.1454  -5.5302   -14.021399  0 0 0 -1
521  4 -1 -1 -1   1 0 0 0 4   15.8836  16.3924   45.903049  0 -1 0 0

v=  -4,-3,4,4
541  0 -4 -8 -7   1 0 0 1 2   -16.7955  16.0907   136.227661  0 0 -1 0
541  -8 0 -7 -4   1 0 0 3 0   14.5042  18.1832   51.421513  0 0 0 -1
541  -4 -7 0 -8   1 0 0 2 1   14.5043  -18.1831   -51.421432  -1 0 0 0
541  -7 -8 -4 0   1 0 0 4 4   -16.7955  -16.0908   -136.227615  0 -1 0 0

v=  -4,-2,-1,3
571  13 -3 11 5   1 0 0 4 0   -18.2526  15.4221   139.804718  0 0 -1 0
571  -99 -2 -60 -63   1 0 0 2 2   23.5897  3.8110   9.177059  0 0 -1 0
```

```
571  -63 -60 -2 -99   1 0 0 3 1   23.5897  -3.8110   -9.176973  0 -1 0 0
571  5 11 -3 13   1 0 0 1 3   -18.2526  -15.4221   -139.804688  0 -1 0 0

v=  -3,-2,-2,3
601  5 6 2 8   1 0 0 1 4   19.8339  14.4089   35.997551  1 1 1 1
601  -233 -60 -107 -204   1 0 0 3 2   2.1889  -24.4174   -84.877411  0 0 -1 0
601  -204 -107 -60 -233   1 0 0 2 3   2.1889  24.4174   84.877472  0 -1 0 0
601  8 2 6 5   1 0 0 4 1   19.8339  -14.4089   -35.997490  1 1 1 1

v=  -2,-1,4,0
631  -23 -5 -12 -19   1 0 0 3 3   -14.2569  20.6819   124.580086  0 0 0 -1
631  78 12 41 60   1 0 0 4 2   21.7721  12.5290   29.918814  0 -1 0 0
631  60 41 12 78   1 0 0 1 0   21.7721  -12.5290   -29.918758  0 0 -1 0
631  -19 -12 -5 -23   1 0 0 2 4   -14.2569  -20.6819   -124.580040  -1 0 0 0

v=  -5,-1,1,1
641  -19 -2 -10 -13   1 0 0 2 1   23.9704  -8.1498   -18.777819  -1 0 0 0
641  -45 41 -53 13   1 0 0 1 2   -20.4908  -14.8704   -144.031219  0 0 -1 0
641  13 -53 41 -45   1 0 0 4 4   -20.4908  14.8703   144.031296  0 -1 0 0
641  -13 -10 -2 -19   1 0 0 3 0   23.9704  8.1499   18.777925  0 0 0 -1

v=  -5,-3,0,4
661  -23 45 -42 31   1 0 0 3 4   -22.5968  12.2631   151.511597  0 0 -1 0
661  -2 12 -9 10   1 0 0 4 3   -8.2239  24.3592   108.655190  1 1 1 1
661  10 -9 12 -2   1 0 0 1 1   -8.2239  -24.3592   -108.655144  1 1 1 1
661  31 -42 45 -23   1 0 0 2 0   -22.5968  -12.2632   -151.511536  0 -1 0 0

v=  -5,-2,0,3
691  9 9 -1 14   1 0 0 0 3   -4.9105  25.8241   100.766335  0 0 0 -1
691  89 -31 74 24   1 0 0 0 3   -26.2800  0.6007   178.690598  0 0 -1 0
691  24 74 -31 89   1 0 0 0 3   -26.2800  -0.6007   -178.690598  0 -1 0 0
691  14 -1 9 9   1 0 0 0 3   -4.9105  -25.8242   -100.766273  -1 0 0 0

v=  -5,-2,2,1
701  3 7 6 5   1 0 0 4 1   22.1071  14.5697   33.386806  0 -1 0 0
701  6 3 5 7   1 0 0 2 3   3.8662  -26.1926   -81.603371  -1 0 0 0
701  7 5 3 6   1 0 0 3 2   3.8662  26.1926   81.603424  0 0 0 -1
701  5 6 7 3   1 0 0 1 4   22.1072  -14.5696   -33.386726  0 0 -1 0

v=  -3,-2,3,-2
751  -10 -4 -3 -12   1 0 0 1 4   -10.6823  25.2366   112.942238  0 0 -1 0
751  -63 -100 23 -139   1 0 0 3 2   6.0766  -26.7222   -77.188889  0 0 0 -1
751  -139 23 -100 -63   1 0 0 2 3   6.0766  26.7222   77.188919  -1 0 0 0
751  -12 -3 -4 -10   1 0 0 4 1   -10.6823  -25.2366   -112.942215  0 -1 0 0

v=  -5,-1,0,2
761  136 23 70 107   1 0 0 2 0   -1.7902  -27.5281   -93.720734  -1 0 0 0
```

```
761  -15 -4 -8 -12   1 0 0 1 1   19.6068  -19.4055   -44.704449  0 0 -1 0
761  -12 -8 -4 -15   1 0 0 4 3   19.6068  19.4055   44.704472  0 -1 0 0
761  107 70 23 136   1 0 0 3 4   -1.7902  27.5281   93.720779  0 0 0 -1

v=  -5,-3,1,-2
811  -74 -17 -35 -63   1 0 0 2 0   -19.2056  21.0272   132.407578  0 -1 0 0
811  -20 -14 -3 -27   1 0 0 1 1   2.3924  -28.3774   -85.181046  1 1 1 1
811  -27 -3 -14 -20   1 0 0 4 3   2.3924  28.3774   85.181076  1 1 1 1
811  -63 -35 -17 -74   1 0 0 3 4   -19.2056  -21.0273   -132.407501  0 0 -1 0

v=  -5,2,-2,1
821  -262 -118 -89 -280   1 0 0 4 0   -4.1373  28.3528   98.302040  0 0 0 -1
821  1 -2 5 -3   1 0 0 2 2   3.3161  -28.4606   -83.354042  1 1 1 1
821  -3 5 -2 1   1 0 0 3 1   3.3161  28.4605   83.354073  1 1 1 1
821  -280 -89 -118 -262   1 0 0 1 3   -4.1372  -28.3528   -98.301994  -1 0 0 0

v=  -5,-4,0,5
881  4 9 4 -1   1 0 0 0 1   28.8634  -6.9211   -13.484297  0 -1 0 0
881  4 4 -1 9   1 0 0 0 1   23.6963  -17.8741   -37.027210  0 0 0 -1
881  9 -1 4 4   1 0 0 0 1   23.6963  17.8742   37.027328  -1 0 0 0
881  -1 4 9 4   1 0 0 0 1   28.8634  6.9212   13.484399  0 0 -1 0

v=  -5,-1,2,0
911  -7 2 -4 -5   1 0 0 4 3   -28.2321  -10.6747   -159.288116  0 0 0 -1
911  -139 -147 5 -233   1 0 0 2 0   22.3766  20.2556   42.151749  1 1 1 1
911  -233 5 -147 -139   1 0 0 3 4   22.3766  -20.2555   -42.151661  1 1 1 1
911  -5 -4 2 -7   1 0 0 1 1   -28.2321  10.6747   159.288193  -1 0 0 0

v=  -5,1,1,-1
941  27 15 8 31   1 0 0 3 0   -17.6746  -25.0721   -125.181870  0 0 0 -1
941  -52 -38 -9 -70   1 0 0 4 4   25.6601  -16.8094   -33.228027  0 -1 0 0
941  -70 -9 -38 -52   1 0 0 1 2   25.6601  16.8095   33.228096  0 0 -1 0
941  31 8 15 27   1 0 0 2 1   -17.6746  25.0721   125.181870  -1 0 0 0

v=  -5,-4,1,-1
971  2 15 -7 16   1 0 0 3 1   -9.5159  -29.6723   -107.780998  0 -1 0 0
971  -92 -13 -49 -70   1 0 0 4 0   30.7724  4.9049   9.056336  0 0 -1 0
971  -70 -49 -13 -92   1 0 0 1 3   30.7724  -4.9049   -9.056272  0 -1 0 0
971  16 -7 15 2   1 0 0 2 2   -9.5159  29.6723   107.781044  0 0 -1 0

v=  -5,-5,-5,1
991  -1 -6 -6 -6   1 0 0 0 3   -5.4346  -31.0075   -99.941132  -1 0 0 0
991  -6 -1 -6 -6   1 0 0 0 3   31.3929  2.3415   4.265628  0 -1 0 0
991  -6 -6 -1 -6   1 0 0 0 3   31.3930  -2.3415   -4.265582  0 0 -1 0
991  -6 -6 -6 -1   1 0 0 0 3   -5.4346  31.0075   99.941132  0 0 0 -1

v=  -5,-1,-4,1
```

```
1021  -19 13 -20 2   1 0 0 2 2   -18.6410  -25.9521   -125.689102  0 0 -1 0
1021  20 41 -13 53   1 0 0 1 3   -1.1150  -31.9336   -91.999771  0 -1 0 0
1021  53 -13 41 20   1 0 0 4 0   -1.1151  31.9336   91.999832  0 0 -1 0
1021  2 -20 13 -19   1 0 0 3 1   -18.6410  25.9521   125.689171  0 -1 0 0

v=  -5,-3,-3,2
1031  -41 -31 -6 -56   1 0 0 0 1   22.4913  22.9159   45.535759  1 1 1 1
1031  -16 19 -21 9   1 0 0 0 1   27.0916  17.2350   32.463615  1 1 1 1
1031  9 -21 19 -16   1 0 0 0 1   27.0916  -17.2350   -32.463570  1 1 1 1
1031  -56 -6 -31 -41   1 0 0 0 1   22.4914  -22.9159   -45.535698  1 1 1 1

v=  -4,-4,2,-3
1051  27 -10 23 6   1 0 0 3 2   31.7162  6.7142   11.952858  -1 0 0 0
1051  -12 -38 16 -45   1 0 0 4 1   -30.0030  -12.2809   -157.739594  -1 0 0 0
1051  -45 16 -38 -12   1 0 0 1 4   -30.0030  12.2809   157.739655  0 0 0 -1
1051  6 23 -10 27   1 0 0 2 3   31.7162  -6.7142   -11.952776  0 0 0 -1

v=  -4,-4,4,5
1061  7 -5 8 1   1 0 0 3 4   -8.4050  31.4699   104.953575  0 0 0 -1
1061  -52 92 -89 60   1 0 0 4 3   -21.8761  -24.1337   -132.190948  0 -1 0 0
1061  60 -89 92 -52   1 0 0 1 1   -21.8761  24.1337   132.190979  0 0 -1 0
1061  1 8 -5 7   1 0 0 2 0   -8.4050  -31.4699   -104.953514  -1 0 0 0

v=  -4,-2,3,-1
1091  5 1 2 -2   1 0 0 1 2   7.4134  32.1876   77.029930  -1 0 0 0
1091  2 5 -2 1   1 0 0 3 0   30.3305  -13.0791   -23.326700  1 1 1 1
1091  1 -2 5 2   1 0 0 2 1   30.3305  13.0792   23.326771  1 1 1 1
1091  -2 2 1 5   1 0 0 4 4   7.4134  -32.1876   -77.029861  0 0 0 -1

v=  -5,2,-3,2
1151  -81 -71 -6 -121   1 0 0 0 0   -4.1482  33.6718   97.023094  0 0 0 -1
1151  -16 4 -11 -6   1 0 0 0 0   -33.6943  3.9614   173.294571  0 0 -1 0
1151  -6 -11 4 -16   1 0 0 0 0   -33.6943  -3.9614   -173.294510  0 -1 0 0
1151  -121 -6 -71 -81   1 0 0 0 0   -4.1481  -33.6718   -97.023018  -1 0 0 0

v=  -4,2,3,0
1171  0 -4 2 3   1 0 0 1 3   25.6239  22.6807   41.513306  1 1 1 1
1171  2 0 3 -4   1 0 0 3 1   -5.3276  33.8026   98.956581  0 0 -1 0
1171  -4 3 0 2   1 0 0 2 2   -5.3275  -33.8026   -98.956482  0 -1 0 0
1171  3 2 -4 0   1 0 0 4 0   25.6239  -22.6807   -41.513256  1 1 1 1

v=  -5,-2,2,-4
1181  3 7 1 5   1 0 0 4 2   4.3246  34.0925   82.770638  0 0 0 -1
1181  1 3 5 7   1 0 0 2 4   13.1627  31.7450   67.479149  1 1 1 1
1181  7 5 3 1   1 0 0 3 3   13.1628  -31.7450   -67.479088  1 1 1 1
1181  5 1 7 3   1 0 0 1 0   4.3247  -34.0925   -82.770546  -1 0 0 0
```

```
v=  -4,-3,3,0
1201  0 -4 -3 3   1 0 0 1 4   -20.1002  28.2309   125.450554  0 -1 0 0
1201  -3 0 3 -4   1 0 0 3 2   11.0004  -32.8632   -71.492851  0 -1 0 0
1201  -4 3 0 -3   1 0 0 2 3   11.0004  32.8632   71.492897  0 0 -1 0
1201  3 -3 -4 0   1 0 0 4 1   -20.1001  -28.2309   -125.450516  0 0 -1 0

v=  -3,-1,0,5
1231  0 -4 2 -7   1 0 0 1 0   17.2045  -30.5778   -60.635899  0 0 0 -1
1231  42 -165 128 -139   1 0 0 3 3   32.6080  12.9508   21.661312  -1 0 0 0
1231  -139 128 -165 42   1 0 0 2 4   32.6080  -12.9507   -21.661264  0 0 0 -1
1231  -7 2 -4 0   1 0 0 4 2   17.2045  30.5779   60.635956  -1 0 0 0

v=  -6,-2,1,-2
1291  12 5 3 11   1 0 0 3 0   -6.8007  -35.2810   -100.910339  0 -1 0 0
1291  118 -78 121 -5   1 0 0 4 4   0.3337  35.9289   89.467789  0 0 -1 0
1291  -5 121 -78 118   1 0 0 1 2   0.3338  -35.9289   -89.467743  0 -1 0 0
1291  11 3 5 12   1 0 0 2 1   -6.8007  35.2810   100.910423  0 0 -1 0

v=  -6,-4,-2,3
1301  46 13 20 42   1 0 0 2 3   0.2905  -36.0682   -89.538460  1 1 1 1
1301  35 31 2 53   1 0 0 1 4   -32.8079  -14.9881   -155.447037  -1 0 0 0
1301  53 2 31 35   1 0 0 4 1   -32.8079  14.9881   155.447037  0 0 0 -1
1301  42 20 13 46   1 0 0 3 2   0.2905  36.0682   89.538521  1 1 1 1

v=  -6,1,-5,1
1321  78 -53 81 -5   1 0 0 4 0   -23.4438  -27.7739   -130.167496  0 0 -1 0
1321  -4 -12 5 -13   1 0 0 2 2   -1.7424  -36.3038   -92.747849  0 0 -1 0
1321  -13 5 -12 -4   1 0 0 3 1   -1.7425  36.3038   92.747910  0 -1 0 0
1321  -5 81 -53 78   1 0 0 1 3   -23.4438  27.7739   130.167480  0 -1 0 0

v=  -5,-1,-1,3
1361  -24 -7 -10 -23   1 0 0 2 0   -16.9155  32.7852   117.291397  0 0 0 -1
1361  -45 -64 12 -92   1 0 0 1 1   3.2801  -36.7456   -84.899002  0 0 0 -1
1361  -92 12 -64 -45   1 0 0 4 3   3.2801  36.7456   84.898979  -1 0 0 0
1361  -23 -10 -7 -24   1 0 0 3 4   -16.9154  -32.7852   -117.291367  -1 0 0 0

v=  -6,-2,5,4
1381  -12 -23 6 -30   1 0 0 4 2   -15.9193  -33.5794   -115.364731  -1 0 0 0
1381  71 23 30 67   1 0 0 2 4   37.1073  -2.0109   -3.101919  0 0 0 -1
1381  67 30 23 71   1 0 0 3 3   37.1074  2.0109   3.101919  -1 0 0 0
1381  -30 6 -23 -12   1 0 0 1 0   -15.9194  33.5794   115.364769  0 0 0 -1

v=  -6,-1,-3,1
1451  -2 2 1 -5   1 0 0 4 1   -37.1918  -8.2321   -167.519318  1 1 1 1
1451  1 -2 -5 2   1 0 0 2 3   13.7472  35.5248   68.844788  0 -1 0 0
1451  2 -5 -2 1   1 0 0 3 2   13.7472  -35.5248   -68.844757  0 0 -1 0
1451  -5 1 2 -2   1 0 0 1 4   -37.1918  8.2321   167.519318  1 1 1 1
```

```
v=  -6,-5,0,-3
1471  107 -100 128 -34   1 0 0 3 1   -37.8894  5.9491   171.076645  1 1 1 1
1471  -7 -8 1 -10   1 0 0 4 0   -21.1073  32.0231   123.389900  0 0 0 -1
1471  -10 1 -8 -7   1 0 0 1 3   -21.1072  -32.0232   -123.389801  -1 0 0 0
1471  -34 128 -100 107   1 0 0 2 2   -37.8895  -5.9492   -171.076630  1 1 1 1

v=  -2,-1,5,-1
1481  -70 16 -53 -27   1 0 0 1 0   4.4027  -38.2311   -83.430779  1 1 1 1
1481  -13 15 -17 6   1 0 0 3 3   21.2611  32.0775   56.463352  0 0 -1 0
1481  6 -17 15 -13   1 0 0 2 4   21.2612  -32.0775   -56.463257  0 -1 0 0
1481  -27 -53 16 -70   1 0 0 4 2   4.4026  38.2311   83.430878  1 1 1 1

v=  -6,0,-4,1
1511  -16 -1 -11 -11   1 0 0 0 2   38.6964  -3.6871   -5.442837  0 0 -1 0
1511  154 -6 99 89   1 0 0 0 2   -3.5274  38.7112   95.206512  -1 0 0 0
1511  89 99 -6 154   1 0 0 0 2   -3.5274  -38.7112   -95.206467  0 0 0 -1
1511  -11 -11 -1 -16   1 0 0 0 2   38.6964  3.6871   5.442873  0 -1 0 0

v=  -6,-1,3,5
1531  16 3 10 12   1 0 0 2 4   -38.4314  -7.3506   -169.171982  0 -1 0 0
1531  -175 -49 -78 -157   1 0 0 1 0   -38.0324  9.1943   166.409546  1 1 1 1
1531  -157 -78 -49 -175   1 0 0 4 2   -38.0325  -9.1944   -166.409470  1 1 1 1
1531  12 10 3 16   1 0 0 3 3   -38.4314  7.3506   169.172028  0 0 -1 0

v=  -6,-1,2,1
1571  3 2 1 -5   1 0 0 4 0   23.8864  -31.6297   -52.940212  -1 0 0 0
1571  1 3 -5 2   1 0 0 2 2   37.3432  13.2847   19.582882  0 0 0 -1
1571  2 -5 3 1   1 0 0 3 1   37.3432  -13.2847   -19.582821  -1 0 0 0
1571  -5 1 2 3   1 0 0 1 3   23.8865  31.6297   52.940189  0 0 0 -1

v=  -5,-4,5,5
1601  9 9 4 -1   1 0 0 0 0   -29.4354  -27.1027   -137.362549  0 0 0 -1
1601  4 9 -1 9   1 0 0 0 0   18.6800  -35.3844   -62.169746  0 0 -1 0
1601  9 -1 9 4   1 0 0 0 0   18.6799  35.3845   62.169857  0 -1 0 0
1601  -1 4 9 9   1 0 0 0 0   -29.4354  27.1027   137.362610  -1 0 0 0

v=  -6,4,-3,1
1621  -7 -3 -4 -10   1 0 0 4 0   39.2102  9.1411   13.122961  1 1 1 1
1621  -4 -7 -10 -3   1 0 0 2 2   -24.2565  32.1345   127.046997  0 -1 0 0
1621  -3 -10 -7 -4   1 0 0 3 1   -24.2564  -32.1345   -127.046951  0 0 -1 0
1621  -10 -4 -3 -7   1 0 0 1 3   39.2102  -9.1410   -13.122855  1 1 1 1

v=  -6,3,-2,-4
1721  -2 2 -4 5   1 0 0 4 0   -6.4260  40.9842   98.910988  0 0 -1 0
1721  -4 -2 5 2   1 0 0 2 2   32.4600  -25.8330   -38.514194  0 0 -1 0
1721  2 5 -2 -4   1 0 0 3 1   32.4600  25.8330   38.514210  0 -1 0 0
```

```
1721  5 -4 2 -2   1 0 0 1 3   -6.4260  -40.9842   -98.910904  0 -1 0 0

v=  -3,-3,4,-2
1741  31 63 -20 82   1 0 0 2 1   36.7811  19.7015   28.175434  0 -1 0 0
1741  20 -9 17 3   1 0 0 1 2   29.1820  29.8230   45.622395  1 1 1 1
1741  3 17 -9 20   1 0 0 4 4   29.1820  -29.8230   -45.622360  1 1 1 1
1741  82 -20 63 31   1 0 0 3 0   36.7811  -19.7016   -28.175470  0 0 -1 0

v=  -4,3,6,6
1801  6 -67 45 -63   1 0 0 2 3   -30.4465  29.5637   135.842880  0 -1 0 0
1801  10 16 -3 23   1 0 0 1 4   -34.6339  -24.5254   -144.696411  1 1 1 1
1801  23 -3 16 10   1 0 0 4 1   -34.6339  24.5253   144.696533  1 1 1 1
1801  -63 45 -67 6   1 0 0 3 2   -30.4465  -29.5637   -135.842819  0 0 -1 0

v=  -5,4,-1,-2
1811  -34 -27 -5 -48   1 0 0 2 0   -41.0091  -11.3692   -164.504715  0 0 0 -1
1811  60 1 37 38   1 0 0 1 1   -39.0637  -16.8829   -156.626465  0 0 0 -1
1811  38 37 1 60   1 0 0 4 3   -39.0636  16.8829   156.626480  -1 0 0 0
1811  -48 -5 -27 -34   1 0 0 3 4   -41.0091  11.3692   164.504745  -1 0 0 0

v=  -3,0,-1,5
1831  -128 -125 -2 -204   1 0 0 3 3   -20.7070  -37.4463   -118.941643  -1 0 0 0
1831  13 7 6 15   1 0 0 4 2   41.0921  -11.9350   -16.195637  -1 0 0 0
1831  15 6 7 13   1 0 0 1 0   41.0920  11.9350   16.195709  0 0 0 -1
1831  -204 -2 -125 -128   1 0 0 2 4   -20.7070  37.4462   118.941666  0 0 0 -1

v=  -4,3,3,-1
1861  0 -4 -3 -7   1 0 0 1 1   42.3390  -8.2708   -11.053321  0 -1 0 0
1861  -3 0 -7 -4   1 0 0 3 4   -38.5126  19.4366   153.220779  0 -1 0 0
1861  -4 -7 0 -3   1 0 0 2 0   -38.5126  -19.4366   -153.220734  0 0 -1 0
1861  -7 -3 -4 0   1 0 0 4 3   42.3390  8.2708   11.053410  0 0 -1 0

v=  -5,2,2,2
1871  -16 -46 19 -56   1 0 0 0 4   14.2627  -40.8359   -70.747231  0 0 -1 0
1871  -41 -6 -21 -31   1 0 0 0 4   -10.3154  -42.0071   -103.796707  -1 0 0 0
1871  -31 -21 -6 -41   1 0 0 0 4   -10.3154  42.0071   103.796745  0 0 0 -1
1871  -56 19 -46 -16   1 0 0 0 4   14.2627  40.8360   70.747337  0 -1 0 0

v=  -6,-4,-5,1
1901  38 -28 41 -5   1 0 0 4 1   28.7346  -32.7921   -48.773026  0 -1 0 0
1901  -19 -27 5 -38   1 0 0 2 3   26.1893  34.8586   53.082413  -1 0 0 0
1901  -38 5 -27 -19   1 0 0 3 2   26.1893  -34.8586   -53.082375  0 0 0 -1
1901  -5 41 -28 38   1 0 0 1 4   28.7346  32.7921   48.773052  0 0 -1 0

v=  -5,-1,5,2
1931  31 88 -35 107   1 0 0 2 4   27.9880  -33.8773   -50.437984  0 -1 0 0
1931  -20 -9 -8 -22   1 0 0 1 0   -35.0233  26.5399   142.845901  1 1 1 1
```

```
1931  -22 -8 -9 -20   1 0 0 4 2   -35.0233  -26.5400   -142.845840  1 1 1 1
1931  107 -35 88 31   1 0 0 3 3   27.9879  33.8774   50.438053  0 0 -1 0

v=  -6,-1,0,3
1951  24 -96 74 -81   1 0 0 0 0   19.8828  -39.4421   -63.247295  0 -1 0 0
1951  14 9 4 19   1 0 0 0 0   -39.0949  20.5571   152.263428  0 0 0 -1
1951  19 4 9 14   1 0 0 0 0   -39.0948  -20.5571   -152.263351  -1 0 0 0
1951  -81 74 -96 24   1 0 0 0 0   19.8828  39.4421   63.247314  0 0 -1 0

v=  -6,-3,0,5
2011  -7 -3 1 -5   1 0 0 4 3   36.7020  25.7676   35.071812  0 0 0 -1
2011  -309 128 -270 -63   1 0 0 2 0   41.4477  17.1199   22.442982  1 1 1 1
2011  -63 -270 128 -309   1 0 0 3 4   41.4477  -17.1198   -22.442909  1 1 1 1
2011  -5 1 -3 -7   1 0 0 1 1   36.7020  -25.7675   -35.071747  -1 0 0 0

v=  -4,3,3,4
2081  0 1 -3 -7   1 0 0 1 0   -1.0936  45.6048   91.373726  0 -1 0 0
2081  -3 0 -7 1   1 0 0 3 3   2.2317  -45.5633   -87.195923  0 -1 0 0
2081  1 -7 0 -3   1 0 0 2 4   2.2316  45.5634   87.195961  0 0 -1 0
2081  -7 -3 1 0   1 0 0 4 2   -1.0936  -45.6049   -91.373680  0 0 -1 0

v=  -6,-3,2,-2
2111  60 146 -53 183   1 0 0 1 1   -45.3831  7.1676   171.025146  1 1 1 1
2111  -13 -5 -7 -14   1 0 0 3 4   -37.5372  -26.4944   -144.784897  0 0 -1 0
2111  -14 -7 -5 -13   1 0 0 2 0   -37.5373  26.4944   144.784988  0 -1 0 0
2111  183 -53 146 60   1 0 0 4 3   -45.3831  -7.1676   -171.025040  1 1 1 1

v=  -6,0,3,4
2131  -20 26 -28 13   1 0 0 1 0   12.1930  -44.5233   -74.684639  0 -1 0 0
2131  -38 -35 -2 -59   1 0 0 3 3   -42.7481  17.4242   157.824127  0 -1 0 0
2131  -59 -2 -35 -38   1 0 0 2 4   -42.7481  -17.4242   -157.824081  0 0 -1 0
2131  13 -28 26 -20   1 0 0 4 2   12.1930  44.5234   74.684723  0 0 -1 0

v=  -5,-5,2,-1
2141  -10 1 -8 -2   1 0 0 1 2   -27.0956  -37.5077   -125.844360  0 0 0 -1
2141  107 175 -42 241   1 0 0 3 0   6.2876  -45.8417   -82.190094  -1 0 0 0
2141  241 -42 175 107   1 0 0 2 1   6.2876  45.8418   82.190140  0 0 0 -1
2141  -2 -8 1 -10   1 0 0 4 4   -27.0956  37.5077   125.844406  -1 0 0 0

v=  -6,3,-3,2
2161  -2 -8 1 -5   1 0 0 4 3   15.0096  -43.9967   -71.162773  0 0 -1 0
2161  1 -2 -5 -8   1 0 0 2 0   -37.5094  27.4599   143.792831  0 0 -1 0
2161  -8 -5 -2 1   1 0 0 3 4   -37.5093  -27.4599   -143.792755  0 -1 0 0
2161  -5 1 -8 -2   1 0 0 1 1   15.0095  43.9967   71.162880  0 -1 0 0

v=  -6,-1,5,3
2221  129 9 74 89   1 0 0 0 4   26.5579  38.9317   55.699532  0 -1 0 0
```

```
2221  14 14 -1 24   1 0 0 0 4   -22.7677  41.2629   118.888664  0 0 0 -1
2221  24 -1 14 14   1 0 0 0 4   -22.7677  -41.2630   -118.888596  -1 0 0 0
2221  89 74 9 129   1 0 0 0 4   26.5579  -38.9317   -55.699451  0 0 -1 0

v=  -6,2,1,-1
2251  -20 -24 2 -37   1 0 0 1 4   47.3938  2.1957   2.652546  0 0 -1 0
2251  42 -35 48 -9   1 0 0 3 -3   -40.4602  24.7783   148.516190  0 0 0 -1
2251  -9 48 -35 42   1 0 0 2 3   -40.4602  -24.7784   -148.516068  -1 0 0 0
2251  -37 2 -24 -20   1 0 0 4 1   47.3939  -2.1956   -2.652472  0 -1 0 0

v=  -6,-4,2,-1
2281  -27 2 -19 -15   1 0 0 4 2   16.9532  -44.6497   -69.208580  0 -1 0 0
2281  96 -17 70 42   1 0 0 2 4   29.4661  -37.5866   -51.905251  -1 0 0 0
2281  42 70 -17 96   1 0 0 3 3   29.4660  37.5866   51.905319  0 0 0 -1
2281  -15 -19 2 -27   1 0 0 1 0   16.9531  44.6497   69.208618  0 0 -1 0

v=  -6,-1,3,0
2311  16 18 0 27   1 0 0 2 0   43.5574  20.3408   25.031992  0 0 -1 0
2311  -110 -49 -38 -117   1 0 0 1 1   3.5873  -47.9388   -85.720474  0 -1 0 0
2311  -117 -38 -49 -110   1 0 0 4 3   3.5872  47.9389   85.720551  0 0 -1 0
2311  27 0 18 16   1 0 0 3 4   43.5574  -20.3408   -25.032017  0 -1 0 0

v=  -4,-1,-3,4
2341  -9 3 -10 -3   1 0 0 2 1   11.9156  46.8937   75.743034  0 0 -1 0
2341  230 -24 157 118   1 0 0 1 2   -35.8541  -32.4883   -137.819427  0 -1 0 0
2341  118 157 -24 230   1 0 0 4 4   -35.8541  32.4882   137.819534  0 0 -1 0
2341  -3 -10 3 -9   1 0 0 3 0   11.9157  -46.8937   -75.742874  0 -1 0 0

v=  -6,1,2,-1
2351  -12 17 -19 10   1 0 0 4 1   47.7145  -8.6215   -10.242173  0 -1 0 0
2351  96 23 45 82   1 0 0 2 3   26.1265  40.8461   57.395626  -1 0 0 0
2351  82 45 23 96   1 0 0 3 2   26.1266  -40.8461   -57.395607  0 0 0 -1
2351  10 -19 17 -12   1 0 0 1 4   47.7145  8.6215   10.242230  0 0 -1 0

v=  -6,1,1,-5
2371  46 -2 30 27   1 0 0 2 2   45.2901  17.8831   21.546919  0 0 0 -1
2371  -30 31 -38 13   1 0 0 1 3   -9.1461  47.8262   100.826302  0 0 0 -1
2371  13 -38 31 -30   1 0 0 4 0   -9.1460  -47.8262   -100.826210  -1 0 0 0
2371  27 30 -2 46   1 0 0 3 1   45.2901  -17.8831   -21.546919  -1 0 0 0

v=  -3,6,-1,4
2381  -385 -89 -183 -327   1 0 0 1 0   7.6648  48.1897   80.962555  0 0 -1 0
2381  7 0 8 1   1 0 0 3 3   -10.4835  -47.6560   -102.406425  0 0 0 -1
2381  1 8 0 7   1 0 0 2 4   -10.4835  47.6560   102.406471  -1 0 0 0
2381  -327 -183 -89 -385   1 0 0 4 2   7.6648  -48.1898   -80.962509  0 -1 0 0

v=  -5,-3,-4,3
```

```
2411  31 48 -10 67   1 0 0 2 0   39.2546  29.4970   36.922241  1 1 1 1
2411  -45 -9 -23 -37   1 0 0 1 1   12.4068  -47.5086   -75.364143  -1 0 0 0
2411  -37 -23 -9 -45   1 0 0 4 3   12.4068  47.5086   75.364182  0 0 0 -1
2411  67 -10 48 31   1 0 0 3 4   39.2547  -29.4970   -36.922108  1 1 1 1

v=  -6,-5,2,0
2441  -99 -107 5 -168   1 0 0 2 1   -48.2741  -10.5174   -167.709106  0 0 -1 0
2441  -5 11 -8 8   1 0 0 1 2   42.7029  -24.8487   -30.194969  0 -1 0 0
2441  8 -8 11 -5   1 0 0 4 4   42.7029  24.8486   30.194901  0 0 -1 0
2441  -168 5 -107 -99   1 0 0 3 0   -48.2741  10.5173   167.709213  0 -1 0 0

v=  -7,-3,6,5
2521  -7 -3 6 5   1 0 0 4 0   43.3408  -25.3490   -30.322361  0 0 -1 0
2521  6 -7 5 -3   1 0 0 2 2   -16.9230  -47.2717   -109.697136  0 0 -1 0
2521  -3 5 -7 6   1 0 0 3 1   -16.9231  47.2717   109.697189  0 -1 0 0
2521  5 6 -3 -7   1 0 0 1 3   43.3408  25.3491   30.322380  0 -1 0 0

v=  -7,-1,4,5
2531  2 10 -7 11   1 0 0 3 3   5.2336  50.0361   84.028725  0 -1 0 0
2531  183 -13 121 100   1 0 0 4 2   -49.2178  -10.4216   -168.044495  0 0 -1 0
2531  100 121 -13 183   1 0 0 1 0   -49.2178  10.4215   168.044586  0 -1 0 0
2531  11 -7 10 2   1 0 0 2 4   5.2337  -50.0361   -84.028648  0 0 -1 0

v=  -7,-6,-4,3
2551  1 3 10 7   1 0 0 2 3   19.5605  -46.5660   -67.214622  0 0 -1 0
2551  10 1 7 3   1 0 0 1 4   27.5055  -42.3610   -57.003838  0 -1 0 0
2551  3 7 1 10   1 0 0 4 1   27.5055  42.3609   57.003784  0 0 -1 0
2551  7 10 3 1   1 0 0 3 2   19.5605  46.5660   67.214706  0 -1 0 0

v=  -5,5,-2,-2
2591  -146 -31 -71 -121   1 0 0 0 3   26.3901  43.5265   58.771561  0 0 0 -1
2591  -6 14 -11 9   1 0 0 0 3   50.2813  7.9235   8.955237  0 0 -1 0
2591  9 -11 14 -6   1 0 0 0 3   50.2814  -7.9235   -8.955237  0 -1 0 0
2591  -121 -71 -31 -146   1 0 0 0 3   26.3902  -43.5266   -58.771542  -1 0 0 0

v=  -7,-2,1,4
2621  -23 -35 8 -49   1 0 0 3 1   33.1751  -38.9925   -49.608662  1 1 1 1
2621  -52 12 -39 -20   1 0 0 4 0   -12.6284  -49.6138   -104.280472  0 0 0 -1
2621  -20 -39 12 -52   1 0 0 1 3   -12.6284  49.6138   104.280518  -1 0 0 0
2621  -49 8 -35 -23   1 0 0 2 2   33.1751  38.9925   49.608639  1 1 1 1

v=  -6,-5,2,-5
2671  -204 -212 5 -338   1 0 0 2 2   -19.3812  47.9100   112.024994  -1 0 0 0
2671  -5 6 -3 3   1 0 0 1 3   -51.6437  -1.9818   -177.802322  0 0 -1 0
2671  3 -3 6 -5   1 0 0 4 0   -51.6437  1.9818   177.802322  0 -1 0 0
2671  -338 5 -212 -204   1 0 0 3 1   -19.3812  -47.9100   -112.024956  0 0 0 -1
```

```
v=  -5,-2,4,-1
2711  32 10 13 31   1 0 0 3 4   47.1471  -22.0943   -25.108921  0 0 -1 0
2711  53 67 -9 100   1 0 0 4 3   51.0471  -10.2560   -11.360162  1 1 1 1
2711  100 -9 67 53   1 0 0 1 1   51.0471  10.2561   11.360266  1 1 1 1
2711  31 13 10 32   1 0 0 2 0   47.1470  22.0943   25.108994  0 -1 0 0

v=  -7,-2,-2,2
2731  -12 -3 -9 -10   1 0 0 4 2   -34.0860  39.6125   130.711517  0 0 0 -1
2731  306 23 175 212   1 0 0 2 4   46.8834  23.0857   26.215971  1 1 1 1
2731  212 175 23 306   1 0 0 3 3   46.8834  -23.0857   -26.215956  1 1 1 1
2731  -10 -9 -3 -12   1 0 0 1 0   -34.0859  -39.6125   -130.711456  -1 0 0 0

v=  -7,-4,4,3
2741  -3 -10 -7 1   1 0 0 3 0   5.2820  -52.0874   -84.209641  0 0 -1 0
2741  -7 -3 1 -10   1 0 0 4 4   -46.7768  -23.5143   -153.311707  1 1 1 1
2741  -10 1 -3 -7   1 0 0 1 2   -46.7769  23.5143   153.311798  1 1 1 1
2741  1 -7 -10 -3   1 0 0 2 1   5.2819  52.0874   84.209724  0 -1 0 0

v=  -7,-1,2,2
2791  67 5 38 46   1 0 0 3 0   -29.6484  43.7262   124.139084  0 0 -1 0
2791  28 -23 31 -5   1 0 0 4 4   -41.5679  32.6053   141.889832  1 1 1 1
2791  -5 31 -23 28   1 0 0 1 2   -41.5679  -32.6054   -141.889801  1 1 1 1
2791  46 38 5 67   1 0 0 2 1   -29.6483  -43.7262   -124.139030  0 -1 0 0

v=  -1,0,0,7
2801  -168 70 -147 -34   1 0 0 3 2   51.8802  -10.4615   -11.400678  0 -1 0 0
2801  -7 -8 1 -15   1 0 0 4 1   36.4930  -38.3308   -46.407009  0 0 -1 0
2801  -15 1 -8 -7   1 0 0 1 4   36.4930  38.3309   46.407047  0 -1 0 0
2801  -34 -147 70 -168   1 0 0 2 3   51.8803  10.4616   11.400712  0 0 -1 0

v=  -7,-7,-1,-4
2851  -175 -154 -13 -262   1 0 0 1 4   52.7555  -8.2375   -8.874780  0 0 -1 0
2851  2 10 -2 11   1 0 0 3 2   -11.0456  -52.2397   -101.938843  0 0 0 -1
2851  11 -2 10 2   1 0 0 2 3   -11.0458  52.2397   101.939018  -1 0 0 0
2851  -262 -13 -154 -175   1 0 0 4 1   52.7554  8.2376   8.874912  0 -1 0 0

v=  -7,-7,4,6
2861  35 -49 52 -27   1 0 0 1 1   45.0470  -28.8403   -32.628498  0 0 -1 0
2861  -8 20 -17 16   1 0 0 3 4   18.9255  -50.0282   -69.278534  0 0 0 -1
2861  16 -17 20 -8   1 0 0 2 0   18.9255  50.0283   69.278603  -1 0 0 0
2861  -27 52 -49 35   1 0 0 4 3   45.0470  28.8404   32.628544  0 -1 0 0

v=  -3,-1,-1,6
2971  -34 38 -45 17   1 0 0 2 2   18.2133  -51.3738   -70.479286  -1 0 0 0
2971  45 1 27 28   1 0 0 1 3   9.9859  -53.5843   -79.443542  0 0 -1 0
2971  28 27 1 45   1 0 0 4 0   9.9858  53.5844   79.443619  0 -1 0 0
2971  17 -45 38 -34   1 0 0 3 1   18.2133  51.3738   70.479309  0 0 0 -1
```

```
v=  -3,-3,-3,5
3001  64 -16 49 24   1 0 0 0 0   16.8584  -52.1228   -72.076920  0 -1 0 0
3001  39 24 9 49   1 0 0 0 0   -54.7805  0.3062   179.679794  0 0 0 -1
3001  49 9 24 39   1 0 0 0 0   -54.7805  -0.3063   -179.679794  -1 0 0 0
3001  24 49 -16 64   1 0 0 0 0   16.8583  52.1230   72.077087  0 0 -1 0

v=  -7,0,6,7
3011  1 8 0 2   1 0 0 2 0   54.8199  -2.4030   -2.509908  -1 0 0 0
3011  -385 -364 -13 -602   1 0 0 1 1   26.9151  -47.8182   -60.626411  0 0 -1 0
3011  -602 -13 -364 -385   1 0 0 4 3   26.9149  47.8183   60.626644  0 -1 0 0
3011  2 0 8 1   1 0 0 3 4   54.8199  2.4030   2.509908  0 0 0 -1

v=  -7,-1,1,3
3041  6 8 10 7   1 0 0 2 1   -54.3386  -9.3980   -170.187668  -1 0 0 0
3041  10 6 7 8   1 0 0 1 2   -54.7762  6.3700   173.366760  0 0 -1 0
3041  8 7 6 10   1 0 0 4 4   -54.7761  -6.3700   -173.366730  0 -1 0 0
3041  7 10 8 6   1 0 0 3 0   -54.3385  9.3979   170.187698  0 0 0 -1

v=  -7,-3,2,-1
3061  223 27 121 165   1 0 0 4 3   -36.7411  41.3654   131.611755  0 0 0 -1
3061  11 8 0 17   1 0 0 2 0   -2.5229  -55.2687   -92.613579  1 1 1 1
3061  17 0 8 11   1 0 0 3 4   -2.5229  55.2687   92.613640  1 1 1 1
3061  165 121 27 223   1 0 0 1 1   -36.7411  -41.3654   -131.611694  -1 0 0 0

v=  -7,1,1,-4
3121  3 12 -4 15   1 0 0 4 0   8.8114  -55.1666   -80.925148  1 1 1 1
3121  -139 63 -125 -23   1 0 0 2 2   54.2001  13.5408   14.027120  0 -1 0 0
3121  -23 -125 63 -139   1 0 0 3 1   54.2001  -13.5408   -14.027049  0 0 -1 0
3121  15 -4 12 3   1 0 0 1 3   8.8114  55.1666   80.925179  1 1 1 1

v=  -7,3,-4,-6
3181  2 -100 63 -99   1 0 0 3 3   8.7116  55.7235   81.114487  1 1 1 1
3181  3 -13 11 -10   1 0 0 4 2   40.2010  -39.5585   -44.538410  0 0 0 -1
3181  -10 11 -13 3   1 0 0 1 0   40.2010  39.5585   44.538475  -1 0 0 0
3181  -99 63 -100 2   1 0 0 2 4   8.7118  -55.7235   -81.114349  1 1 1 1

v=  -7,-4,-2,4
3191  6 -2 5 -3   1 0 0 2 1   26.3083  -49.9888   -62.242908  0 0 0 -1
3191  -5 -259 157 -262   1 0 0 1 2   40.6189  39.2569   44.023132  0 0 0 -1
3191  -262 157 -259 -5   1 0 0 4 4   40.6189  -39.2569   -44.023106  -1 0 0 0
3191  -3 5 -2 6   1 0 0 3 0   26.3083  49.9887   62.242825  -1 0 0 0

v=  -7,-2,3,7
3221  -7 -3 -9 -5   1 0 0 4 0   -53.7024  -18.3588   -161.126373  0 0 -1 0
3221  581 128 280 487   1 0 0 2 2   -50.8704  25.1635   153.680283  0 0 -1 0
3221  487 280 128 581   1 0 0 3 1   -50.8703  -25.1636   -153.680206  0 -1 0 0
```

```
3221  -5 -9 -3 -7   1 0 0 1 3   -53.7025  18.3588   161.126434  0 -1 0 0

v=  -6,-1,-1,4
3251  -6 -1 -1 4   1 0 0 0 0   56.9933  1.6620   1.670467  -1 0 0 0
3251  -1 -6 4 -1   1 0 0 0 0   -56.5934  -6.9424   -173.006332  0 -1 0 0
3251  -1 4 -6 -1   1 0 0 0 0   -56.5933  6.9424   173.006378  0 0 -1 0
3251  4 -1 -1 -6   1 0 0 0 0   56.9932  -1.6620   -1.670349  0 0 0 -1

v=  -7,-1,2,-3
3271  107 45 38 111   1 0 0 3 1   48.3359  30.5719   32.312889  1 1 1 1
3271  28 -8 21 10   1 0 0 4 0   55.7153  12.9156   13.051412  0 0 0 -1
3271  10 21 -8 28   1 0 0 1 3   55.7153  -12.9154   -13.051275  -1 0 0 0
3271  111 38 45 107   1 0 0 2 2   48.3359  -30.5719   -32.312843  1 1 1 1

v=  -7,5,-4,-3
3301  -9 13 -15 7   1 0 0 2 3   5.6404  57.1767   84.366089  0 0 0 -1
3301  125 -24 92 53   1 0 0 1 4   -50.1621  -28.0137   -150.818192  0 0 0 -1
3301  53 92 -24 125   1 0 0 4 1   -50.1621  28.0137   150.818237  -1 0 0 0
3301  7 -15 13 -9   1 0 0 3 2   5.6405  -57.1768   -84.365967  -1 0 0 0

v=  -6,-2,2,7
3331  -7 -13 -9 -5   1 0 0 4 2   33.5177  -46.9847   -54.496895  0 0 0 -1
3331  -9 -7 -5 -13   1 0 0 2 4   -37.0187  44.2788   129.896851  1 1 1 1
3331  -13 -5 -7 -9   1 0 0 3 3   -37.0187  -44.2789   -129.896820  1 1 1 1
3331  -5 -9 -13 -7   1 0 0 1 0   33.5177  46.9847   54.496956  -1 0 0 0

v=  -5,0,-3,4
3361  15 1 7 13   1 0 0 1 1   55.0587  -18.1536   -18.248074  0 0 -1 0
3361  147 150 -2 241   1 0 0 3 4   54.9343  -18.5262   -18.636276  0 0 0 -1
3361  241 -2 150 147   1 0 0 2 0   54.9343  18.5263   18.636372  -1 0 0 0
3361  13 7 1 15   1 0 0 4 3   55.0586  18.1536   18.248106  0 -1 0 0

v=  -7,0,1,2
3371  -4 8 -5 2   1 0 0 2 2   -44.9426  36.7579   140.720764  0 -1 0 0
3371  -215 -194 -13 -327   1 0 0 1 3   -34.9632  -46.3528   -127.026703  1 1 1 1
3371  -327 -13 -194 -215   1 0 0 4 0   -34.9632  46.3527   127.026779  1 1 1 1
3371  2 -5 8 -4   1 0 0 3 1   -44.9428  -36.7580   -140.720779  0 0 -1 0

v=  -3,-1,6,-1
3391  1 -2 0 7   1 0 0 2 1   -15.9079  56.0173   105.853569  1 1 1 1
3391  0 1 7 -2   1 0 0 1 2   13.9775  -56.5299   -76.111694  -1 0 0 0
3391  -2 7 1 0   1 0 0 4 4   13.9775  56.5299   76.111679  0 0 0 -1
3391  7 0 -2 1   1 0 0 3 0   -15.9079  -56.0173   -105.853607  1 1 1 1

v=  -7,-3,4,2
3461  7 5 3 -4   1 0 0 3 -1   2.6689  58.7696   87.399796  0 0 0 -1
3461  3 7 -4 5   1 0 0 4 3   50.2979  -30.5144   -31.244068  0 -1 0 0
```

```
3461  5 -4 7 3   1 0 0 1 1   50.2978  30.5144   31.244122  0 0 -1 0
3461  -4 3 5 7   1 0 0 2 0   2.6690  -58.7696   -87.399727  -1 0 0 0

v=  -7,-4,2,-5
3491  -23 -85 38 -99   1 0 0 3 0   54.9101  21.8148   21.667038  0 0 -1 0
3491  28 12 11 30   1 0 0 4 4   19.1232  -55.9044   -71.115707  1 1 1 1
3491  30 11 12 28   1 0 0 1 2   19.1231  55.9045   71.115822  1 1 1 1
3491  -99 38 -85 -23   1 0 0 2 1   54.9101  -21.8147   -21.666927  0 -1 0 0

v=  -6,-5,0,7
3511  -103 30 -82 -34   1 0 0 3 4   6.7802  -58.8645   -83.429428  -1 0 0 0
3511  -17 -18 1 -30   1 0 0 4 3   -58.9349  6.1384   174.053696  -1 0 0 0
3511  -30 1 -18 -17   1 0 0 1 1   -58.9349  -6.1385   -174.053665  0 0 0 -1
3511  -34 -82 30 -103   1 0 0 2 0   6.7803  58.8644   83.429382  0 0 0 -1

v=  -3,-2,6,0
3541  -92 117 -129 60   1 0 0 4 4   -40.8090  -43.3085   -133.297989  0 -1 0 0
3541  -14 -7 -5 -18   1 0 0 2 1   56.5345  18.5699   18.183792  -1 0 0 0
3541  -18 -5 -7 -14   1 0 0 3 0   56.5346  -18.5697   -18.183628  0 0 0 -1
3541  60 -129 117 -92   1 0 0 1 2   -40.8091  43.3085   133.298050  0 0 -1 0

v=  -7,-5,-2,5
3571  -21 -1 -11 -16   1 0 0 0 4   -55.6948  -21.6584   -158.750061  0 0 -1 0
3571  -121 -111 -6 -186   1 0 0 0 4   38.2885  45.8802   50.153877  -1 0 0 0
3571  -186 -6 -111 -121   1 0 0 0 4   38.2885  -45.8801   -50.153816  0 0 0 -1
3571  -16 -11 -1 -21   1 0 0 0 4   -55.6949  21.6584   158.750137  0 -1 0 0

v=  -7,7,-5,1
3581  85 1 52 53   1 0 0 1 0   59.5858  5.5255   5.298016  1 1 1 1
3581  -8 -30 13 -34   1 0 0 3 3   -46.9816  -37.0638   -141.730072  0 0 -1 0
3581  -34 13 -30 -8   1 0 0 2 4   -46.9816  37.0638   141.730072  0 -1 0 0
3581  53 52 1 85   1 0 0 4 2   59.5858  -5.5255   -5.297978  1 1 1 1

v=  -7,1,-5,2
3631  7 5 -2 6   1 0 0 3 3   48.0751  36.3289   37.077290  0 0 0 -1
3631  -2 7 6 5   1 0 0 4 2   50.0076  33.6192   33.912189  0 -1 0 0
3631  5 6 7 -2   1 0 0 1 0   50.0075  -33.6191   -33.912197  0 0 -1 0
3631  6 -2 5 7   1 0 0 2 4   48.0752  -36.3289   -37.077164  -1 0 0 0

v=  -4,-2,-3,5
3671  230 81 92 223   1 0 0 1 3   38.8492  46.4945   50.119053  1 1 1 1
3671  7 -10 8 -4   1 0 0 3 1   58.5437  15.6090   14.928982  0 0 -1 0
3671  -4 8 -10 7   1 0 0 2 2   58.5437  -15.6089   -14.928889  0 -1 0 0
3671  223 92 81 230   1 0 0 4 0   38.8493  -46.4946   -50.119026  1 1 1 1

v=  -7,-1,3,6
3691  0 -14 7 -12   1 0 0 1 2   12.7940  59.3913   77.843163  -1 0 0 0
```

```
3691  147 110 23 201   1 0 0 3 0   15.1617  58.8314   75.548515  1 1 1 1
3691  201 23 110 147   1 0 0 2 1   15.1617  -58.8313   -75.548523  1 1 1 1
3691  -12 7 -14 0   1 0 0 4 4   12.7940  -59.3912   -77.843147  0 0 0 -1

v=  -6,-4,3,-2
3701  -59 38 -60 2   1 0 0 2 3   29.5818  -53.1593   -60.905151  0 0 -1 0
3701  5 26 -13 28   1 0 0 1 4   38.2908  47.2739   50.993305  0 -1 0 0
3701  28 -13 26 5   1 0 0 4 1   38.2908  -47.2739   -50.993294  0 0 -1 0
3701  2 -60 38 -59   1 0 0 3 2   29.5818  53.1593   60.905117  0 -1 0 0

v=  -5,5,-1,-3
3761  18 -3 11 10   1 0 0 4 3   -48.8616  37.0615   142.819687  1 1 1 1
3761  176 103 45 212   1 0 0 2 0   -10.8943  -60.3517   -100.232460  0 -1 0 0
3761  212 45 103 176   1 0 0 3 4   -10.8943  60.3515   100.232536  0 0 -1 0
3761  10 11 -3 18   1 0 0 1 1   -48.8614  -37.0615   -142.819595  1 1 1 1

v=  -7,-2,-6,1
3821  -175 121 -183 13   1 0 0 1 3   -33.0770  -52.2198   -122.350929  0 0 0 -1
3821  7 10 -2 11   1 0 0 3 1   -0.3829  -61.8130   -90.354935  -1 0 0 0
3821  11 -2 10 7   1 0 0 2 2   -0.3829  61.8131   90.354889  0 0 0 -1
3821  13 -183 121 -175   1 0 0 4 0   -33.0771  52.2198   122.350998  -1 0 0 0

v=  -6,-2,-1,5
3851  9 -1 4 9   1 0 0 0 0   39.9256  47.5073   49.955994  0 0 -1 0
3851  194 244 -31 364   1 0 0 0 0   -34.5530  51.5472   123.834648  -1 0 0 0
3851  364 -31 244 194   1 0 0 0 0   -34.5528  -51.5472   -123.834511  0 0 0 -1
3851  9 4 -1 9   1 0 0 0 0   39.9257  -47.5073   -49.955929  0 -1 0 0

v=  -5,3,4,-1
3881  32 -5 23 16   1 0 0 3 3   -20.4524  -58.8447   -109.165649  0 0 -1 0
3881  -12 67 -49 60   1 0 0 4 2   -61.7048  8.5742   172.089096  1 1 1 1
3881  60 -49 67 -12   1 0 0 1 0   -61.7048  -8.5744   -172.088959  1 1 1 1
3881  16 23 -5 32   1 0 0 2 4   -20.4524  58.8447   109.165703  0 -1 0 0

v=  -7,-4,-5,2
3911  7 5 -2 1   1 0 0 3 4   57.1101  -25.4839   -24.047541  0 0 0 -1
3911  -2 7 1 5   1 0 0 4 3   -19.7229  -59.3464   -108.383484  0 -1 0 0
3911  5 1 7 -2   1 0 0 1 1   -19.7230  59.3465   108.383545  0 0 -1 0
3911  1 -2 5 7   1 0 0 2 0   57.1102  25.4839   24.047533  -1 0 0 0

v=  -7,1,2,0
3931  -88 -45 -27 -99   1 0 0 3 3   -61.6105  11.6250   169.314697  -1 0 0 0
3931  38 22 11 45   1 0 0 4 2   -62.5910  -3.6566   -176.656540  -1 0 0 0
3931  45 11 22 38   1 0 0 1 0   -62.5909  3.6566   176.656540  0 0 0 -1
3931  -99 -27 -45 -88   1 0 0 2 4   -61.6106  -11.6251   -169.314651  0 0 0 -1

v=  -7,1,0,2
```

```
4001  2 0 -7 1   1 0 0 3 2   61.8830  13.0954   11.948439  0 -1 0 0
4001  -7 2 1 0   1 0 0 4 1   48.9827  40.0212   39.250446  0 0 -1 0
4001  0 1 2 -7   1 0 0 1 4   48.9827  -40.0212   -39.250420  0 -1 0 0
4001  1 -7 0 2   1 0 0 2 3   61.8832  -13.0954   -11.948323  0 0 -1 0

v=  -5,4,3,-1
4021  4 -6 9 -6   1 0 0 0 4   42.6445  46.9302   47.739231  -1 0 0 0
4021  -251 -136 -71 -291   1 0 0 0 4   -62.2224  -12.2216   -168.887543  0 -1 0 0
4021  -291 -71 -136 -251   1 0 0 0 4   -62.2225  12.2216   168.887589  0 0 -1 0
4021  -6 9 -6 4   1 0 0 0 4   42.6446  -46.9302   -47.739151  0 0 0 -1

v=  -6,2,5,5
4051  -2 -3 6 -5   1 0 0 4 1   -54.7212  32.5052   149.289032  1 1 1 1
4051  -479 -42 -270 -338   1 0 0 2 3   54.0115  -33.6714   -31.939867  0 -1 0 0
4051  -338 -270 -42 -479   1 0 0 3 2   54.0114  33.6715   31.939976  0 0 -1 0
4051  -5 6 -3 -2   1 0 0 1 4   -54.7212  -32.5053   -149.288956  1 1 1 1

v=  -7,4,-3,2
4091  107 -60 103 6   1 0 0 3 0   -3.0668  -63.8874   -92.748260  1 1 1 1
4091  18 -8 16 5   1 0 0 4 4   47.2074  43.1562   42.433002  0 0 0 -1
4091  5 16 -8 18   1 0 0 1 2   47.2074  -43.1562   -42.432983  -1 0 0 0
4091  6 103 -60 107   1 0 0 2 1   -3.0668  63.8873   92.748314  1 1 1 1

v=  -4,0,-1,6
4111  93 2 56 60   1 0 0 4 3   -35.6715  53.2781   123.803680  1 1 1 1
4111  21 28 -5 42   1 0 0 2 0   -12.4952  -62.8878   -101.237762  0 -1 0 0
4111  42 -5 28 21   1 0 0 3 4   -12.4953  62.8877   101.237823  0 0 -1 0
4111  60 56 2 93   1 0 0 1 1   -35.6714  -53.2781   -123.803574  1 1 1 1

v=  -8,1,-3,1
4201  -27 77 -64 60   1 0 0 4 1   25.9337  -59.4007   -66.414436  -1 0 0 0
4201  -24 -17 -5 -33   1 0 0 2 3   -57.8572  29.2154   153.208145  0 0 0 -1
4201  -33 -5 -17 -24   1 0 0 3 2   -57.8572  -29.2155   -153.208130  -1 0 0 0
4201  60 -64 77 -27   1 0 0 1 -1   25.9336  59.4008   66.414536  0 0 0 -1

v=  -8,3,-1,-3
4211  1 -12 10 -13   1 0 0 2 0   -35.5565  54.2837   123.225288  0 -1 0 0
4211  -175 -89 -53 -197   1 0 0 1 1   55.9300  -32.9064   -30.470444  1 1 1 1
4211  -197 -53 -89 -175   1 0 0 4 3   55.9299  32.9065   30.470531  1 1 1 1
4211  -13 10 -12 1   1 0 0 3 4   -35.5565  -54.2838   -123.225250  0 0 -1 0

v=  -8,0,-2,1
4231  -8 0 -2 1   1 0 0 3 3   -58.2337  -28.9799   -153.542816  0 0 -1 0
4231  -2 -8 1 0   1 0 0 4 2   2.4795  -64.9988   -87.815376  1 1 1 1
4231  0 1 -8 -2   1 0 0 1 0   2.4796  64.9989   87.815323  1 1 1 1
4231  1 -2 0 -8   1 0 0 2 4   -58.2337  28.9798   153.542923  0 -1 0 0
```

```
v=  -6,-5,3,-1
4241  -85 -39 -28 -92   1 0 0 1 2   63.1509  -15.9050   -14.136335  1 1 1 1
4241  -38 -25 -7 -49   1 0 0 3 0   65.1225  -0.2137   -0.187672  0 0 -1 0
4241  -49 -7 -25 -38   1 0 0 2 1   65.1227  0.2138   0.187672  0 -1 0 0
4241  -92 -28 -39 -85   1 0 0 4 4   63.1509  15.9051   14.136448  1 1 1 1

v=  -7,-1,0,4
4261  75 31 27 78   1 0 0 1 1   -17.3008  -62.9418   -105.369331  0 0 0 -1
4261  17 35 -12 46   1 0 0 3 4   -58.2215  -29.5172   -153.115860  -1 0 0 0
4261  46 -12 35 17   1 0 0 2 0   -58.2214  29.5171   153.115891  0 0 0 -1
4261  78 27 31 75   1 0 0 4 3   -17.3009  62.9418   105.369400  -1 0 0 0

v=  -5,4,7,5
4271  -2 7 -4 0   1 0 0 4 0   62.0696  -20.4542   -18.238964  0 0 -1 0
4271  -139 -317 110 -403   1 0 0 2 2   34.7715  -55.3347   -57.855316  0 0 -1 0
4271  -403 110 -317 -139   1 0 0 3 1   34.7716  55.3349   57.855373  0 -1 0 0
4271  0 -4 7 -2   1 0 0 1 3   62.0695  20.4543   18.239096  0 -1 0 0

v=  -8,-5,2,-8
4391  9 44 -21 49   1 0 0 0 3   64.0283  17.0702   14.928041  1 1 1 1
4391  -56 -31 -16 -66   1 0 0 0 3   20.8066  -62.9133   -71.699966  1 1 1 1
4391  -66 -16 -31 -56   1 0 0 0 3   20.8065  62.9133   71.700058  1 1 1 1
4391  49 -21 44 9   1 0 0 0 3   64.0283  -17.0700   -14.927948  1 1 1 1

v=  -8,-7,-6,2
4421  -9 -7 0 -8   1 0 0 2 2   41.6205  51.8529   51.247185  -1 0 0 0
4421  -110 251 -223 183   1 0 0 1 3   54.1248  38.6202   35.509388  0 0 -1 0
4421  183 -223 251 -110   1 0 0 4 0   54.1247  -38.6201   -35.509350  0 -1 0 0
4421  -8 0 -7 -9   1 0 0 3 1   41.6207  -51.8530   -51.247135  0 0 0 -1

v=  -5,-1,8,4
4441  9 4 9 9   1 0 0 0 3   64.9999  -14.6975   -12.741235  0 0 -1 0
4441  -526 -31 -306 -356   1 0 0 0 3   -11.0804  65.7132   99.571045  -1 0 0 0
4441  -356 -306 -31 -526   1 0 0 0 3   -11.0803  -65.7132   -99.570915  0 0 0 -1
4441  9 9 4 9   1 0 0 0 3   64.9999  14.6976   12.741328  0 -1 0 0

v=  -7,-6,-2,6
4451  -15 -14 -3 -22   1 0 0 1 4   56.1281  36.0644   32.722282  0 -1 0 0
4451  212 70 88 201   1 0 0 3 2   1.4958  -66.6991   -88.715294  0 -1 0 0
4451  201 88 70 212   1 0 0 2 3   1.4957  66.6991   88.715347  0 0 -1 0
4451  -22 -3 -14 -15   1 0 0 4 1   56.1283  -36.0643   -32.722137  0 0 -1 0

v=  -6,-1,-5,3
4481  -81 -201 74 -251   1 0 0 0 1   56.0975  36.5250   33.068104  -1 0 0 0
4481  14 4 9 14   1 0 0 0 1   22.2636  -63.1295   -70.574013  0 -1 0 0
4481  14 9 4 14   1 0 0 0 1   22.2635  63.1295   70.574081  0 0 -1 0
4481  -251 74 -201 -81   1 0 0 0 1   56.0975  -36.5248   -33.067974  0 0 0 -1
```

```
v=  -8,-6,1,-6
4561  6 -2 0 7   1 0 0 2 0   8.1615  -67.0401   -83.058891  -1 0 0 0
4561  0 6 7 -2   1 0 0 1 1   -59.7260  -31.5245   -152.174118  0 0 -1 0
4561  -2 7 6 0   1 0 0 4 3   -59.7262  31.5245   152.174149  0 -1 0 0
4561  7 0 -2 6   1 0 0 3 4   8.1614  67.0403   83.059021  0 0 0 -1

v=  -8,-4,7,6
4591  -42 -18 -14 -45   1 0 0 4 4   -40.6803  54.1861   126.897408  -1 0 0 0
4591  -74 -57 -10 -103   1 0 0 2 1   18.4542  -65.1955   -74.195343  0 0 0 -1
4591  -103 -10 -57 -74   1 0 0 3 0   18.4541  65.1954   74.195404  -1 0 0 0
4591  -45 -14 -18 -42   1 0 0 1 2   -40.6800  -54.1861   -126.897255  0 0 0 -1

v=  -4,5,0,5
4621  9 4 9 4   1 0 0 0 4   55.4069  -39.3838   -35.405613  -1 0 0 0
4621  9 9 4 4   1 0 0 0 4   17.6031  65.6591   74.992012  0 -1 0 0
4621  4 4 9 9   1 0 0 0 4   17.6032  -65.6593   -74.991997  0 0 -1 0
4621  4 9 4 9   1 0 0 0 4   55.4069  39.3839   35.405678  0 0 0 -1

v=  -7,5,-6,4
4651  534 -71 374 259   1 0 0 0 0   65.2731  -19.7588   -16.841541  0 0 -1 0
4651  -11 -6 -6 -6   1 0 0 0 0   8.1448  67.7101   83.140884  -1 0 0 0
4651  -6 -6 -6 -11   1 0 0 0 0   8.1449  -67.7103   -83.140854  0 0 0 -1
4651  259 374 -71 534   1 0 0 0 0   65.2733  19.7589   16.841612  0 -1 0 0

v=  -5,-2,5,-2
4691  -41 -1 -26 -26   1 0 0 0 3   38.8384  56.4144   55.454628  0 0 0 -1
4691  114 19 59 89   1 0 0 0 3   -39.3983  -56.0247   -125.116066  0 0 -1 0
4691  89 59 19 114   1 0 0 0 3   -39.3985  56.0248   125.116150  0 -1 0 0
4691  -26 -26 -1 -41   1 0 0 0 3   38.8385  -56.4143   -55.454445  -1 0 0 0

v=  -8,-2,2,-1
4721  -37 -13 -14 -35   1 0 0 4 0   -11.7022  -67.7057   -99.806038  -1 0 0 0
4721  -74 48 -75 2   1 0 0 2 2   5.8634  68.4589   85.104645  0 0 0 -1
4721  2 -75 48 -74   1 0 0 3 1   5.8635  -68.4590   -85.104599  -1 0 0 0
4721  -35 -14 -13 -37   1 0 0 1 3   -11.7022  67.7058   99.806053  0 0 0 -1

v=  -7,-5,-5,3
4751  -11 14 -16 9   1 0 0 0 0   64.2699  24.9073   21.183428  1 1 1 1
4751  49 99 -31 129   1 0 0 0 0   -68.2552  -9.6037   -171.990921  1 1 1 1
4751  129 -31 99 49   1 0 0 0 0   -68.2552  9.6036   171.990967  1 1 1 1
4751  9 -16 14 -11   1 0 0 0 0   64.2700  -24.9072   -21.183380  1 1 1 1

v=  -6,3,8,6
4801  -2 -8 -14 -5   1 0 0 4 1   19.7152  -66.4253   -73.468971  0 -1 0 0
4801  -14 -2 -5 -8   1 0 0 2 3   -6.2771  -69.0043   -95.197670  -1 0 0 0
4801  -8 -5 -2 -14   1 0 0 3 2   -6.2771  69.0043   95.197739  0 0 0 -1
```

```
4801  -5 -14 -8 -2   1 0 0 1 4   19.7151  66.4253   73.469086  0 0 -1 0

v=  -8,-8,-6,3
4831  16 -32 30 -23   1 0 0 2 4   -8.1497  69.0260   96.733559  -1 0 0 0
4831  -30 -49 12 -67   1 0 0 1 0   60.1292  -34.8640   -30.105925  0 0 -1 0
4831  -67 12 -49 -30   1 0 0 4 2   60.1291  34.8639   30.105871  0 -1 0 0
4831  -23 30 -32 16   1 0 0 3 3   -8.1496  -69.0260   -96.733490  0 0 0 -1

v=  -5,-3,5,-1
4861  -128 -165 23 -244   1 0 0 3 4   -16.7572  67.6772   103.906990  0 0 0 -1
4861  -12 7 -9 0   1 0 0 4 3   -69.5619  -4.7069   -176.128998  0 -1 0 0
4861  0 -9 7 -12   1 0 0 1 1   -69.5618  4.7069   176.128937  0 0 -1 0
4861  -244 23 -165 -128   1 0 0 2 0   -16.7572  -67.6773   -103.906990  -1 0 0 0

v=  -7,-5,3,0
4871  19 -11 19 -1   1 0 0 0 4   66.8800  19.9515   16.610813  0 -1 0 0
4871  -41 -96 34 -121   1 0 0 0 4   -66.8583  -20.0244   -163.326782  0 0 0 -1
4871  -121 34 -96 -41   1 0 0 0 4   -66.8583  20.0243   163.326813  -1 0 0 0
4871  -1 19 -11 19   1 0 0 0 4   66.8800  -19.9514   -16.610682  0 0 -1 0

v=  -6,-3,-4,4
4931  -35 -4 -18 -27   1 0 0 1 0   33.1793  61.8882   61.803501  -1 0 0 0
4931  -103 -75 -17 -139   1 0 0 3 3   -40.8362  57.1263   125.558746  1 1 1 1
4931  -139 -17 -75 -103   1 0 0 2 4   -40.8362  -57.1262   -125.558739  1 1 1 1
4931  -27 -18 -4 -35   1 0 0 4 2   33.1794  -61.8881   -61.803387  0 0 0 -1

v=  -7,-1,3,-4
4951  50 6 27 38   1 0 0 1 4   -70.2239  -4.4286   -176.391464  0 0 -1 0
4951  17 60 -27 71   1 0 0 3 2   49.5180  49.9896   45.271568  0 0 0 -1
4951  71 -27 60 17   1 0 0 2 3   49.5180  -49.9897   -45.271580  -1 0 0 0
4951  38 27 6 50   1 0 0 4 1   -70.2239  4.4286   176.391464  0 -1 0 0

v=  -7,-3,3,-7
5011  -403 45 -277 -204   1 0 0 3 4   64.1374  -29.9567   -25.035891  0 0 0 -1
5011  13 7 6 10   1 0 0 4 3   10.4863  70.0073   81.481102  0 -1 0 0
5011  10 6 7 13   1 0 0 1 1   10.4864  -70.0075   -81.481041  0 0 -1 0
5011  -204 -277 45 -403   1 0 0 2 0   64.1372  29.9567   25.035963  -1 0 0 0

v=  -8,-7,0,-4
5021  23 -18 26 -5   1 0 0 4 0   -31.5314  -63.4569   -116.422508  1 1 1 1
5021  -59 -67 5 -103   1 0 0 2 2   -1.2336  -70.8483   -90.997543  0 -1 0 0
5021  -103 5 -67 -59   1 0 0 3 1   -1.2337  70.8483   90.997574  0 0 -1 0
5021  -5 26 -18 23   1 0 0 1 3   -31.5314  63.4569   116.422523  1 1 1 1

v=  -8,2,-1,-7
5051  176 38 85 147   1 0 0 2 3   -58.9203  -39.7418   -146.000275  0 -1 0 0
5051  25 11 7 28   1 0 0 1 4   34.4243  62.1768   61.028847  1 1 1 1
```

```
5051  28 7 11 25   1 0 0 4 1   34.4243  -62.1769   -61.028820  1 1 1 1
5051  147 85 38 176   1 0 0 3 2   -58.9203  39.7418   146.000320  0 0 -1 0

v=  -8,2,-5,2
5081  -1 -41 24 -41   1 0 0 0 1   38.3597  -60.0793   -57.442410  0 -1 0 0
5081  64 34 19 74   1 0 0 0 1   -60.7441  37.2984   148.449036  0 0 0 -1
5081  74 19 34 64   1 0 0 0 1   -60.7440  -37.2984   -148.448990  -1 0 0 0
5081  -41 24 -41 -1   1 0 0 0 1   38.3597  60.0794   57.442444  0 0 -1 0

v=  -7,5,-3,-4
5101  -3 -15 8 -19   1 0 0 3 2   -70.2419  12.9261   169.572937  -1 0 0 0
5101  -52 -118 41 -150   1 0 0 4 1   -10.9490  70.5770   98.818321  -1 0 0 0
5101  -150 41 -118 -52   1 0 0 1 4   -10.9490  -70.5770   -98.818275  0 0 0 -1
5101  -19 8 -15 -3   1 0 0 2 3   -70.2420  -12.9263   -169.572800  0 0 0 -1

v=  -6,-3,4,-4
5171  -18 -5 -7 -19   1 0 0 3 1   -29.2554  65.6896   114.006218  1 1 1 1
5171  -92 -158 41 -215   1 0 0 4 0   7.6281  -71.5039   -83.910637  0 0 0 -1
5171  -215 41 -158 -92   1 0 0 1 3   7.6281  71.5039   83.910706  -1 0 0 0
5171  -19 -7 -5 -18   1 0 0 2 2   -29.2553  -65.6895   -114.006149  1 1 1 1

v=  -8,-1,3,2
5231  2 5 -2 11   1 0 0 3 3   68.1513  24.2158   19.561361  1 1 1 1
5231  13 262 -154 270   1 0 0 4 2   -68.2547  23.9231   160.684586  0 0 0 -1
5231  270 -154 262 13   1 0 0 1 0   -68.2546  -23.9230   -160.684555  -1 0 0 0
5231  11 -2 5 2   1 0 0 2 4   68.1512  -24.2157   -19.561331  1 1 1 1

v=  -7,-3,-3,4
5261  -52 -143 56 -175   1 0 0 4 3   50.1411  -52.4106   -46.267773  0 -1 0 0
5261  21 8 10 22   1 0 0 2 0   -58.6455  42.6814   143.953384  -1 0 0 0
5261  22 10 8 21   1 0 0 3 4   -58.6456  -42.6816   -143.953339  0 0 0 -1
5261  -175 56 -143 -52   1 0 0 1 1   50.1411  52.4108   46.267860  0 0 -1 0

v=  -7,0,5,8
5281  -11 9 -11 4   1 0 0 0 1   33.4491  64.5147   62.594479  0 0 0 -1
5281  -121 99 -136 24   1 0 0 0 1   61.4345  -38.8176   -32.286903  0 0 -1 0
5281  24 -136 99 -121   1 0 0 0 1   61.4344  38.8178   32.287064  0 -1 0 0
5281  4 -11 9 -11   1 0 0 0 1   33.4492  -64.5149   -62.594517  -1 0 0 0

v=  -6,3,5,4
5351  -77 -23 -34 -70   1 0 0 4 1   -13.0784  71.9720   100.299103  0 0 0 -1
5351  56 33 15 67   1 0 0 2 3   64.6031  34.3138   27.974903  1 1 1 1
5351  67 15 33 56   1 0 0 3 2   64.6032  -34.3138   -27.974867  1 1 1 1
5351  -70 -34 -23 -77   1 0 0 1 4   -13.0783  -71.9718   -100.299034  -1 0 0 0

v=  -5,-4,5,0
5381  9 4 4 -1   1 0 0 0 1   30.8147  -66.5692   -65.160690  0 -1 0 0
```

```
5381  4 9 -1 4   1 0 0 0 1   35.4470  64.2223   61.103809  0 0 0 -1
5381  4 -1 9 4   1 0 0 0 1   35.4470  -64.2224   -61.103840  -1 0 0 0
5381  -1 4 4 9   1 0 0 0 1   30.8147  66.5692   65.160751  0 0 -1 0

v=  -8,-5,3,1
5431  -8 -5 3 1   1 0 0 3 3   -36.4592  64.0448   119.651817  0 0 -1 0
5431  3 -8 1 -5   1 0 0 4 2   -73.5449  4.7076   176.337494  1 1 1 1
5431  -5 1 -8 3   1 0 0 1 0   -73.5448  -4.7077   -176.337387  1 1 1 1
5431  1 3 -5 -8   1 0 0 2 4   -36.4591  -64.0449   -119.651733  0 -1 0 0

v=  -4,7,-1,-1
5441  0 1 -3 8   1 0 0 1 2   -29.1863  -67.7432   -113.308159  0 -1 0 0
5441  -3 0 8 1   1 0 0 3 0   -41.5782  -60.9283   -124.310135  0 -1 0 0
5441  1 8 0 -3   1 0 0 2 1   -41.5784  60.9282   124.310226  0 0 -1 0
5441  8 -3 1 0   1 0 0 4 4   -29.1862  67.7434   113.308067  0 0 -1 0

v=  -8,-2,1,5
5471  183 12 106 125   1 0 0 4 0   44.9866  58.7130   52.540237  -1 0 0 0
5471  -29 -7 -15 -23   1 0 0 2 2   -39.8270  -62.3282   -122.578133  0 0 0 -1
5471  -23 -15 -7 -29   1 0 0 3 1   -39.8271  62.3281   122.578232  -1 0 0 0
5471  125 106 12 183   1 0 0 1 3   44.9866  -58.7129   -52.540188  0 0 0 -1

v=  -8,-5,1,8
5501  6 13 5 -3   1 0 0 2 -2   44.8696  59.0570   52.773571  0 -1 0 0
5501  5 6 -3 13   1 0 0 1 4   -29.3018  68.1352   113.270340  1 1 1 1
5501  13 -3 6 5   1 0 0 4 1   -29.3018  -68.1353   -113.270233  1 1 1 1
5501  -3 5 13 6   1 0 0 3 2   44.8696  -59.0569   -52.773552  0 0 -1 0

v=  -6,3,7,7
5521  -7 -13 -4 0   1 0 0 4 0   -65.8889  -34.3460   -152.468246  0 -1 0 0
5521  -4 -7 0 -13   1 0 0 2 2   73.9406  7.3352   5.665450  -1 0 0 0
5521  -13 0 -7 -4   1 0 0 3 1   73.9404  -7.3351   -5.665346  0 0 0 -1
5521  0 -4 -13 -7   1 0 0 1 3   -65.8890  34.3460   152.468292  0 0 -1 0

v=  -8,0,-3,2
5531  49 4 29 34   1 0 0 0 1   42.3438  61.1392   55.294338  0 0 -1 0
5531  -106 -16 -56 -81   1 0 0 0 1   -38.7741  -63.4631   -121.423668  -1 0 0 0
5531  -81 -56 -16 -106   1 0 0 0 1   -38.7741  63.4631   121.423683  0 0 0 -1
5531  34 29 4 49   1 0 0 0 1   42.3438  -61.1392   -55.294254  0 -1 0 0

v=  -8,-2,-2,3
5581  0 11 -3 8   1 0 0 1 0   -46.7985  -58.2315   -128.787552  1 1 1 1
5581  -338 -165 -107 -374   1 0 0 3 3   73.8414  11.3336   8.725981  0 0 -1 0
5581  -374 -107 -165 -338   1 0 0 2 4   73.8414  -11.3334   -8.725868  0 -1 0 0
5581  8 -3 11 0   1 0 0 4 2   -46.7984  58.2314   128.787537  1 1 1 1

v=  -8,1,-4,2
```

```
5591  -251 139 -241 -16   1 0 0 0 3   24.4231  70.6719   70.935616  0 0 0 -1
5591  -1 9 -6 4   1 0 0 0 3   68.9096  -29.0253   -22.841253  0 0 -1 0
5591  4 -6 9 -1   1 0 0 0 3   68.9096  29.0253   22.841263  0 -1 0 0
5591  -16 -241 139 -251   1 0 0 0 3   24.4233  -70.6719   -70.935547  -1 0 0 0

v=  -7,-5,5,3
5641  -11 -16 4 -21   1 0 0 0 3   56.1788  49.8490   41.583515  -1 0 0 0
5641  -81 99 -111 49   1 0 0 0 3   52.1126  54.0859   46.064484  0 -1 0 0
5641  49 -111 99 -81   1 0 0 0 3   52.1125  -54.0857   -46.064445  0 0 -1 0
5641  -21 4 -16 -11   1 0 0 0 3   56.1788  -49.8489   -41.583473  0 0 0 -1

v=  -6,-4,4,-3
5651  2 10 3 6   1 0 0 3 2   70.7630  25.3696   19.723537  0 0 0 -1
5651  3 2 6 10   1 0 0 4 1   33.4389  -67.3265   -63.587906  0 -1 0 0
5651  10 6 2 3   1 0 0 1 4   33.4389  67.3262   63.587784  0 0 -1 0
5651  6 3 10 2   1 0 0 2 3   70.7630  -25.3695   -19.723476  -1 0 0 0

v=  -8,-6,2,-7
5701  -9 -2 -10 -8   1 0 0 2 3   18.1407  -73.2933   -76.098183  0 0 0 -1
5701  -10 -9 -8 -2   1 0 0 1 4   46.9950  -59.0971   -51.507694  0 0 0 -1
5701  -2 -8 -9 -10   1 0 0 4 1   46.9948  59.0970   51.507732  -1 0 0 0
5701  -8 -10 -2 -9   1 0 0 3 2   18.1406  73.2933   76.098274  -1 0 0 0

v=  -6,-2,5,-1
5711  -12 -63 31 -70   1 0 0 4 3   0.9283  75.5655   89.296158  1 1 1 1
5711  46 23 15 52   1 0 0 2 0   21.6052  72.4170   73.387848  0 -1 0 0
5711  52 15 23 46   1 0 0 3 4   21.6053  -72.4169   -73.387741  0 0 -1 0
5711  -70 31 -63 -12   1 0 0 1 1   0.9284  -75.5654   -89.296120  1 1 1 1

v=  -7,4,-1,-5
5741  -8 35 -27 31   1 0 0 3 0   55.3005  -51.7962   -43.125866  -1 0 0 0
5741  38 52 -9 75   1 0 0 4 4   59.5491  46.8498   38.193626  -1 0 0 0
5741  75 -9 52 38   1 0 0 1 2   59.5491  -46.8497   -38.193546  0 0 0 -1
5741  31 -27 35 -8   1 0 0 2 1   55.3006  51.7963   43.125900  0 0 0 -1

v=  -8,3,-7,-7
5791  -15 11 -18 3   1 0 0 1 2   -73.6827  -19.0224   -165.524231  0 0 0 -1
5791  172 70 63 176   1 0 0 3 0   -51.1971  56.3015   132.281433  -1 0 0 0
5791  176 63 70 172   1 0 0 2 1   -51.1970  -56.3016   -132.281326  0 0 0 -1
5791  3 -18 11 -15   1 0 0 4 4   -73.6829  19.0224   165.524307  -1 0 0 0

v=  -7,0,-1,4
5801  259 -6 164 154   1 0 0 0 0   -72.4360  -23.5380   -161.998520  0 -1 0 0
5801  -21 -6 -11 -16   1 0 0 0 0   -71.8514  25.2663   160.625931  0 0 0 -1
5801  -16 -11 -6 -21   1 0 0 0 0   -71.8512  -25.2664   -160.625809  -1 0 0 0
5801  154 164 -6 259   1 0 0 0 0   -72.4358  23.5377   161.998611  0 0 -1 0
```

```
v=  -7,-6,-5,4
5821  75 6 42 53   1 0 0 1 3   30.1957  70.0658   66.685822  0 0 0 -1
5821  57 35 13 71   1 0 0 3 1   -42.1808  63.5750   123.563522  -1 0 0 0
5821  71 13 35 57   1 0 0 2 2   -42.1807  -63.5750   -123.563454  0 0 0 -1
5821  53 42 6 75   1 0 0 4 0   30.1958  -70.0658   -66.685730  -1 0 0 0

v=  -7,-4,5,2
5851  -3 -5 -12 -9   1 0 0 3 2   20.6106  -73.6628   -74.368561  -1 0 0 0
5851  -12 -3 -9 -5   1 0 0 4 1   50.9962  -57.0120   -48.187950  -1 0 0 0
5851  -5 -9 -3 -12   1 0 0 1 4   50.9963  57.0122   48.187969  0 0 0 -1
5851  -9 -12 -5 -3   1 0 0 2 3   20.6106  73.6626   74.368492  0 0 0 -1

v=  -8,-4,3,0
5861  71 -17 55 27   1 0 0 2 0   76.4881  3.2528   2.435180  1 1 1 1
5861  -55 6 -38 -27   1 0 0 1 1   7.2773  76.2105   84.545395  -1 0 0 0
5861  -27 -38 6 -55   1 0 0 4 3   7.2774  -76.2106   -84.545311  0 0 0 -1
5861  27 55 -17 71   1 0 0 3 4   76.4880  -3.2527   -2.435099  1 1 1 1

v=  -5,0,-4,5
5881  9 4 -1 4   1 0 0 0 1   68.2371  -34.9956   -27.151138  0 -1 0 0
5881  -1 9 4 4   1 0 0 0 1   -40.5253  -65.1052   -121.900566  0 0 0 -1
5881  4 4 9 -1   1 0 0 0 1   -40.5254  65.1052   121.900650  -1 0 0 0
5881  4 -1 4 9   1 0 0 0 1   68.2373  34.9956   27.151102  0 0 -1 0

v=  -5,-1,0,7
5981  136 -82 135 2   1 0 0 2 4   14.9871  -75.8708   -78.825943  0 -1 0 0
5981  -25 -4 -13 -17   1 0 0 1 0   21.3702  -74.3257   -73.958961  1 1 1 1
5981  -17 -13 -4 -25   1 0 0 4 2   21.3701  74.3257   73.959007  1 1 1 1
5981  2 135 -82 136   1 0 0 3 3   14.9871  75.8708   78.825974  0 0 -1 0

v=  -8,-3,-5,2
6011  -1 -26 14 -26   1 0 0 0 2   -13.9809  76.2599   100.388771  0 0 -1 0
6011  129 34 59 114   1 0 0 0 2   12.3803  76.5358   80.811539  -1 0 0 0
6011  114 59 34 129   1 0 0 0 2   12.3803  -76.5357   -80.811508  0 0 0 -1
6011  -26 14 -26 -1   1 0 0 0 2   -13.9807  -76.2596   -100.388687  0 -1 0 0

v=  -8,-3,-2,4
6091  5 6 12 8   1 0 0 1 2   36.1493  69.1680   62.407036  0 0 -1 0
6091  12 5 8 6   1 0 0 3 0   -44.6220  -64.0303   -124.872208  0 0 0 -1
6091  6 8 5 12   1 0 0 2 1   -44.6221  64.0303   124.872261  -1 0 0 0
6091  8 12 6 5   1 0 0 4 4   36.1496  -69.1683   -62.406963  0 -1 0 0

v=  -8,-8,5,7
6101  4 9 -6 14   1 0 0 0 0   -74.5622  -23.2695   -162.667816  -1 0 0 0
6101  259 139 74 299   1 0 0 0 0   -17.6345  76.0922   103.048027  0 -1 0 0
6101  299 74 139 259   1 0 0 0 0   -17.6345  -76.0921   -103.048035  0 0 -1 0
6101  14 -6 9 4   1 0 0 0 0   -74.5623  23.2695   162.667816  0 0 0 -1
```

```
v=  -8,7,-6,-2
6121  176 -67 150 42   1 0 0 2 2   -65.9158  -42.1437   -147.406906  1 1 1 1
6121  15 11 2 23   1 0 0 1 3   68.1359  38.4512   29.437380  -1 0 0 0
6121  23 2 11 15   1 0 0 4 0   68.1360  -38.4512   -29.437359  0 0 0 -1
6121  42 150 -67 176   1 0 0 3 1   -65.9159  42.1436   147.406982  1 1 1 1

v=  -3,-1,7,-2
6131  -9 -7 -10 -8   1 0 0 2 4   56.6246  54.0799   43.683208  0 0 -1 0
6131  -10 -9 -8 -7   1 0 0 1 0   -39.3060  -67.7203   -120.131577  0 -1 0 0
6131  -7 -8 -9 -10   1 0 0 4 2   -39.3061  67.7202   120.131668  0 0 -1 0
6131  -8 -10 -7 -9   1 0 0 3 3   56.6249  -54.0799   -43.683071  0 -1 0 0

v=  -7,2,3,-2
6151  -128 150 -172 71   1 0 0 3 2   74.6610  -24.0153   -17.830824  0 0 -1 0
6151  18 7 6 15   1 0 0 4 1   42.0301  66.2154   57.594765  1 1 1 1
6151  15 6 7 18   1 0 0 1 4   42.0302  -66.2153   -57.594624  1 1 1 1
6151  71 -172 150 -128   1 0 0 2 3   74.6610  24.0153   17.830790  0 -1 0 0

v=  -5,-4,5,-5
6211  9 -1 4 -1   1 0 0 0 2   31.7330  72.1388   66.255867  1 1 1 1
6211  4 9 -1 -1   1 0 0 0 2   74.2649  -26.3768   -19.553598  1 1 1 1
6211  -1 -1 9 4   1 0 0 0 2   74.2649  26.3769   19.553680  1 1 1 1
6211  -1 4 -1 9   1 0 0 0 2   31.7331  -72.1388   -66.255821  1 1 1 1

v=  -6,-4,-1,7
6221  2 5 13 6   1 0 0 3 1   -62.8963  -47.5927   -142.885742  0 -1 0 0
6221  13 2 6 5   1 0 0 4 0   -59.4514  51.8318   138.916977  0 0 -1 0
6221  5 6 2 13   1 0 0 1 3   -59.4513  -51.8318   -138.916901  0 -1 0 0
6221  6 13 5 2   1 0 0 2 2   -62.8963  47.5925   142.885849  0 0 -1 0

v=  -6,4,-1,4
6271  -6 4 -1 4   1 0 0 0 4   0.5403  -79.1878   -89.609039  1 1 1 1
6271  -1 -6 4 4   1 0 0 0 4   61.4511  49.9475   39.104229  1 1 1 1
6271  4 4 -6 -1   1 0 0 0 4   61.4513  -49.9474   -39.104073  1 1 1 1
6271  4 -1 4 -6   1 0 0 0 4   0.5402  79.1879   89.609184  1 1 1 1

v=  -8,0,1,3
6301  1 3 0 -8   1 0 0 2 3   -34.3921  -71.5416   -115.674942  1 1 1 1
6301  0 1 -8 3   1 0 0 1 4   -65.0466  -45.4963   -145.029419  -1 0 0 0
6301  3 -8 1 0   1 0 0 4 1   -65.0467  45.4964   145.029449  0 0 0 -1
6301  -8 0 3 1   1 0 0 3 2   -34.3922  71.5415   115.675003  1 1 1 1

v=  -8,-7,1,-5
6311  13 222 -129 230   1 0 0 4 3   -23.7685  -75.8028   -107.409195  0 0 -1 0
6311  -14 -2 -10 -13   1 0 0 2 0   78.0165  14.9798   10.868955  0 0 -1 0
6311  -13 -10 -2 -14   1 0 0 3 4   78.0169  -14.9797   -10.868828  0 -1 0 0
```

```
6311  230 -129 222 13   1 0 0 1 1   -23.7686  75.8030   107.409203  0 -1 0 0

v=  -7,-4,-3,5
6361  -63 20 -52 -19   1 0 0 3 4   -64.2756  -47.2190   -143.697769  1 1 1 1
6361  63 -3 41 35   1 0 0 4 3   -70.8711  36.5826   152.697906  0 0 0 -1
6361  35 41 -3 63   1 0 0 1 1   -70.8710  -36.5826   -152.697861  -1 0 0 0
6361  -19 -52 20 -63   1 0 0 2 0   -64.2757  47.2190   143.697815  1 1 1 1

v=  -4,-3,6,-3
6421  35 -74 67 -52   1 0 0 1 3   14.3056  78.8438   79.716003  1 1 1 1
6421  32 20 8 41   1 0 0 3 1   8.1184  79.7188   84.185135  0 0 -1 0
6421  41 8 20 32   1 0 0 2 2   8.1185  -79.7190   -84.185104  0 -1 0 0
6421  -52 67 -74 35   1 0 0 4 0   14.3056  -78.8437   -79.715965  1 1 1 1

v=  -7,-3,7,4
6451  158 67 56 165   1 0 0 4 1   75.4151  -27.6330   -20.123421  0 -1 0 0
6451  21 18 0 32   1 0 0 2 3   80.1006  -5.9075   -4.217979  -1 0 0 0
6451  32 0 18 21   1 0 0 3 2   80.1005  5.9076   4.218119  0 0 0 -1
6451  165 56 67 158   1 0 0 1 4   75.4151  27.6330   20.123421  0 0 -1 0

v=  -8,-2,3,-2
6481  -15 1 -8 -12   1 0 0 1 0   49.3754  63.5853   52.169868  -1 0 0 0
6481  -168 -205 23 -309   1 0 0 3 3   -38.9530  70.4532   118.937820  1 1 1 1
6481  -309 23 -205 -168   1 0 0 2 4   -38.9529  -70.4532   -118.937759  1 1 1 1
6481  -12 -8 1 -15   1 0 0 4 2   49.3754  -63.5851   -52.169788  0 0 0 -1

v=  -8,6,-4,-3
6491  -461 99 -346 -186   1 0 0 0 3   80.4598  4.1513   2.953599  0 -1 0 0
6491  -6 -1 -1 -11   1 0 0 0 3   66.7265  -45.1505   -34.084255  0 0 0 -1
6491  -11 -1 -1 -6   1 0 0 0 3   66.7264  45.1507   34.084377  -1 0 0 0
6491  -186 -346 99 -461   1 0 0 0 3   80.4597  -4.1513   -2.953467  0 0 -1 0

v=  -8,-8,-1,8
6521  -24 -32 5 -48   1 0 0 2 2   -43.4433  -68.0711   -122.546219  1 1 1 1
6521  -5 -64 37 -67   1 0 0 1 3   -53.0673  -60.8675   -131.083542  -1 0 0 0
6521  -67 37 -64 -5   1 0 0 4 0   -53.0674  60.8675   131.083618  0 0 0 -1
```

Bibliography

[Ba] H. Bass: *Generators and relations for cyclotomic units.* Nagoya Math. J. Vol**27**(1966) 401-407.

[A. Bear] Alan F. Beardon: *The geometry of Discrete groups* Graduate Texts in Mathematics, Vol**91**(1983)ed. Springer-Verlag New York Inc.

[B1] B. C. Berndt, R. J. Evans, K. S. Williams: *Gauss and Jacobi Sums*Can. Math. Soc. Vol**21**(1998)ed. John Wiley and sons.

[C-F] J. W. S. Cassels, A. Fröhlich: *Algebraic number theory*,Proc Inter.Conf. Lond.Math. Soc (1967)351-353.

[J.W.S] J.W.S Cassels:*On the determination of generalized Gauss sums*,Arch. Math.**t.5**,(1969)79-84.

[J.W.S1] J.W.S Cassels:*On Kummer sums*,Proc. London Math. Soc. (3)**21**,(1970)19-27.

[C] A. Cauchy: *Methode simple et nouvelle pour la determination complete des sommes alternees formees avec les racines primitives des equations binomes* J. de Math. pures et appl., ser 1**5**(1840)154-168

[E] G. Eisenstein:*Beweis der allgemeinsten Reziprozitästgesetze zwischen reellen und complexen Zahlen*,Monastber. d. preuss. Akad. d. Wiss. zu Berlin (1850)189-190.

[Da] H. Davenport:*Multiplicative Number Theory*,2nd ed., Springer-Verlag, New York(1980) .

[E.T] T. Estermann: *On the sign of Gaussian sum*,J.London Math. Soc. **20**(1945)66-67.

[I.M. Gel] I. M. Gel'fand, M. I. Graev, I. I. Pyatetskii-Shapiro: *The Representation Theory and Automorphic functions* Translated from the Russian by K. A. Hirsch,(1969)ed. W.B. Saunders Company .

[G.VN] H. Goldstine and J. Von Neumann: *A numerical study of a conjecture of Kummer*,Math of comp. **7**(1953)133-134

[HP] D. R. Heath-Brown and S.J. Patterson : *The distribution of Kummer sums at prime arguments*,J. reine und angew. Math. **310**,(1979)111-130.

[H] D. Hilbert:*Theorie des corps de nombres algébriques*,edition Jacques Gabay,Sceaux(1991).

[Ha] Habicht:*Ein elementarer Beweis des kubischen Reziprozitästgesetzes*, Math. Annalen **139**(1959-1960)343-345.

[H] D. Hilbert:*Theorie des nombres algebriques*,Ann.Fac.Sc.Toulouse**3. serie**No.3(1911)

[R-H] R. Hill:*Ein geometrischer Beweis eines Reziprozitätsgesetzes*Diss Goettingen(1992).

[I.R] K. Ireland, M. Rosen*A Classical Introduction to Moderne Number Theory*,Graduate Texts in Mathematics,vol. 84 (1982)by Springer Verlag, New York.

[K.L] L. Kronecker: *Sur une formule de Gauss*,J. de Math. Pures et Appl.**(ser. 2)**1(1856)392-395.

[KB1] T. Kubota: *On a special kind of Dirichlet series*,J. Math. Soc. Japan, **20**(1968) 193-207

[KB2] T. Kubota: *Some results concerning reciprocity laws and real automorphic functions*,"1969 Number Theory Institute". p 382-395. -Providence, American Mathematical Society,1971(Proceedings of Symposia in pure Mathematics, 20).

[KuNi] L. Kuipers and Niederreiter: *Uniform distribution of sequences.* Wiley, New York, (1974).

[K] E.E Kummer: *Über die Zerlegung der aus Würzeln der Einheit gebildeten komplexen Zahlen in ihre Primfaktoren*,J.R.A.M **35**(1847)327-367 or CW vol I(1975)211-251.

[K1] E.E Kummer: *Eine Aufgabe, betrefend die Theorie der kubischen Reste*,,J.Reine Angew. Math **32**(1842)285-286 or CW vol I(1975)143-144.

[K2] E.E Kummer: *De residuis cubicis disquitiones nonnullae analyticae*,J.Reine Angew. Math **32**(1846)341-349 or CW vol I(1975)145-164.

[S.L] S. Lang:*Cyclotomic fields*,Graduate Texts in Mathematics, vol. 59(1978) by Springer Verlag, New York

[S.L1] S. Lang:*Algebraic Number Theory*,(1970)by Adison-Wesley Pubblishing Company

[EL] E. Lehmer: *On the location of Gauss sums*,Math. of Comp.**10**(1956) 194-202

[F-Lem] F. Lemmermeyer:*Reciprocity Laws from Euler to Eisenstein*,(2000) Springer Monograph in Mathematics.

[F-L] F. Lemmermeyer: *The Euclidean algorithm in algebraic number fields*,Expos.Math.**13**,No.5(1995)385-416.

[H.W.L] H. W. Lenstra:*Lectures on Euclidean ring*,Bielefeld 1974.

[Lox] J. H. Loxton :*Product related to Gauss* ,J. Reine Angew. Math. **268**(1974)53-67.

[Lox1] J. H. Loxton :*Some conjectures concerning Gauss sums.* J. Reine Angew. Math. 297, 153-158 (1978).

[Mat] C. R. Matthews:*Gauss sums and elliptic functions,I. The Kummer sum,*Invent Math. **52**,(1979)163-185; The quartic sum, Invent. Math. **52**(1979),23-52.

[Mc.G] A. D. McGettrick :*A result in the theory of Weierstrass elliptic functions*,Proc. London Math. Soc **3**,No.25(1972)41-54.

[Mc.G1] A. D. McGettrick*On the biquadratic Gauss sum.* Proc. Camb. Philos. Soc.**71**, 79-83 (1972).

[G.M] G. Meyerson: *period polynomial and Gauss sums for finite fields*,Acta Arith.**39**No. 3(1981)251-264.

[Min] H. Minkowski: *Zur Theorie der Einheiten in den algebraischen Zahlkoerpern.* Nach. Ges. Wiss. Goettingen, (1900),90-93.

[MON] H. L. Montgomery: *Ten lectures on the interface between analytic number theory and harmonic analysis* CBMS Regional Conference series, vol. 84, Amer. math. soc., 1994.

[MO] C. Moreno :*Sur le problème de Kummer* Enseignement Math. **20**(1974), 45-51

[Na] Melvyn B. Nathason :*Elementary Methods in Number Theory.* Graduate Texts in Mathematics. **195**,(2000) Springer

[O] J. Ouspensky:*Note sur les nombres entiers dependant d'une racine cinquieme de l unite*,Mathematische Annalen **LXVI**1908.

[SJP1] S.J. Patterson : *The distribution of general Gauss sums at prime arguments*,Advances in analytic number theory, Durham(1979) (ed. H. Halberstam and C. Hooley, Academic Press, London,(1981),Vol. 2, pp 171-182.

[SJP2] S.J. Patterson : *The distribution of general Gauss sums and similar arithmetic functions at prime arguments*,Proc. London Math. Soc **3**,No.54(1987)193-215.

[SJP3] S.J. Patterson : *The cubic analogue of the theta series I*,J. reine und angew. Math. **296**,(1977)125-161.

[SJP4] S.J. Patterson : *The cubic analogue of the theta series II*,J. reine und angew. Math. **296**,(1977)217-220.

[SJP5] S.J. Patterson : *On the distribution of Kummer sums*,J. reine und angew. Math. **303/304**,(1978)126-143.

[SJP6] S.J. Patterson : *Gaußs'sche Summe: ein Thema mit variationen* Antrittsvorlesung, Goettingen (1981)

[Ram] Ramachandra : *On the units of cyclotomic fields*, Acta artith. **12**,(1966)165-173.

[P] L. S. Pontriagin:*Topological Groups*,Princeton(1946)

[P.S] P. Samuel:*Algebraic theory of numbers*,Hermann,Houghton Mifflin,Boston,1970.

[S.I] I. Schur:*Über die Gaussschen Summen*,Gött. Nachrichten,(1920-210)147-153.

[G-S] C-G.Schmidt:*Über die Führer von Gaussschen Summen als Grössencharaktere*,J. Number Theorie**12**,No.3(1980)283-309.

[G-S1] C-G.Schmidt:*Grössencharaktere und Relativklassenzahl abelscher Zahlkörper*,J. Number Theorie**11**,No.1(1979)128-159.

[SL] L. Stickelberger:*Über eine Verallgemeinerung der Kreisteilung*,Math.Ann.**37**(1890)321-367.

[F.T1] F. Thaine: *Families of irreducible polynomials of Gaussian periods and matrice of cyclotomic number*,Math.Comp.**69**No 232(2000)1653-1666.

[F.T2] F. Thaine: *Gaussian periods that are rational integers* ,Preprint, CICMA, Concordia University.

[V] H. Vandivier:*Some properties of of a certain system of fundamental units in cyclotomic field* Ann.Math. **31** (1930)123-125.

[WR] R. Webster:*Convexity*,Oxford Science Publication,1994.

[w1] A. Weil: *La cyclotomic jadis et naguère*,Enseign.Math.**20**(1974)247-263.

[w2] A. Weil: *Jacobi sums as Grössencharaktere*,Trans.Amer.Math.Soc. **73**(1952)487-495.

[w3] A. Weil: *Sommes de Jacobi et caracteres de Hecke*,Gött. Nach.**1**(1974)1-14.

[w4] A.Weil: *Basic Number Theory*,Springer,1967.

[V] H. Vandivier:*Some properties of of a certain system of fundamental units in cyclotomic field* Ann.Math. **31** (1930)123-125.

Lebenslauf von FOSSI TALOM Léopold

Ich wurde am 05.01.1968 in Bandjoun-yom V, Kamerun, geboren.
Schulausbildung:
1973-1979: Katholische Schule zu Yom mit dem Abschluss Certificat d'Etudes Primaires et Elémentaires (C.E.P.E.).
1979-1984: College d'Enseignement Secondaire Géneral(C.E.S) de Bandjoun mit dem Abschluss Brevet d'Etudes du Premier Cycle (B. E. P. C.).
1979-1988: Lycée Classique et moderne de Bafoussam mit den Abschlussen, Probatoire Serie C (1987) und Baccalauréat Serie C.(1988)
Studium:
1988-1995: Studium der Mathematik, Informatik und Physik and der Université de Yaoundé, Abschluss: Licence, Maitrise, D.E.A(Diplôme d'Etudes Approfondies)
1994-1996: Teilzeit wissenschalicher Mitarbeiter an der mathematischen Fakultät der universität Yaoundé.
1996-1997: Assistent an der Fakültät für Wirtschaft- und Socialwissenschaft der Université Catholique d'Afrique Centrale.
April-sept 1997: Sprachkurs am Goethe Institut Mannheim mit dem Abschluss P.N.D.S
1997- : Zulassung zur Promotion, Fakültät für Mathematik der Georg August Universität Göttingen.