HIGHER LEVELS OF FINITE FIELDS

Tesis
entregada a la
Universidad de Chile
en cumplimiento parcial de los requisitos
para optar al grado de
Doctor en Ciencias con mención en Matemáticas

Facultad de Ciencias
por
Mónica del Pilar Canales Chacón
Octubre, 1995

Director de Tesis: Prof. Dr. Eberhard Becker
Co-Director de Tesis: Dr. Ricardo Baeza

FACULTAD DE CIENCIAS
UNIVERSIDAD DE CHILE

INFORME DE APROBACION
TESIS DE DOCTORADO

Se informa a la Comisión de Postgrado de la Facultad de Ciencias que la Tesis de Doctorado Presentada por el candidato.

MONICA DEL PILAR CANALES CHACON

Ha sido aprobada por la Comisión de Evaluación de la Tesis como requisito de tesis para optar al grado de Doctor en Ciencias con mención en Matemáticas, en el Examen de Defensa de Tesis rendido el día 10 de Octubre de 1995.

Director de Tesis:
Prof. Dr. Eberhard Becker
Co-Director de Tesis:
Dr. Ricardo Baeza R.

Comisión de Evaluación de la Tesis:
Dr. Oscar Barriga
Dr. Eduardo Friedman
Dr. Jorge Soto-Andrade

A mis padres

AGRADECIMIENTOS

Muy especialmente al Prof. Eberhard Becker, por su increíble sencillez y humanidad. Me siento tremendamente honrada de haber sido su alumna.

Al Prof. Ricardo Baeza R., quien me ha enseñado más de lo que podré nunca agradecer (... incluyendo el amor a los árboles).

A Osvaldo y Erika, por su amistad.

Al Dr. Luis Vergara B. (Universidad Austral de Chile) por el apoyo y facilidades brindadas para realizar la redacción de esta Tesis.

A Helia, mi mamá, por todo.

Resumen

En este trabajo estudiamos los niveles superiores de los cuerpos finitos primos $\mathbf{F}_p$ ($p > 2$ un número primo), definido como

$$s_d(\mathbf{F}_p) = min\{s | -1 = a_1^d + \cdots + a_s^d, a_i \in \mathbf{F}_p^*\}$$

El resultado es la determinación de $s_d(\mathbf{F}_p)$, y más generalmente de $s_d(\mathbf{Z}/p^\ell\mathbf{Z})$, $\ell \geq 1$, en términos de los coeficientes de ciertas ecuaciones de período de grado $p^{r-j}k$ ($0 \leq j \leq r$) para $d = p^r k$ par, $r \geq 0, k|p-1$.

Abstract

In this work we study the higher levels of the prime finite fields $\mathbf{F}_p (p > 2$ a rational prime), defined as

$$s_d(\mathbf{F}_p) = min\{s | -1 = a_1^d + \cdots + a_s^d, a_i \in \mathbf{F}_p^*\}$$

We achieve to determine $s_d(\mathbf{F}_p)$, and more generally, $s_d(\mathbf{Z}/p^\ell\mathbf{Z})$ for $\ell \geq 1$, in terms of the coefficients of some period equations of degree $p^{r-j}k$ $(0 \leq j \leq r)$ for $d = p^r k$ even, $r \geq 0, k|p-1$.

Contents

§ 4. Known Results

Chapter II: $s_d(\mathbf{Z}/p^\ell\mathbf{Z})$ for $d \geq 2$

§ 1. Preliminaries

§ 2. $s_d(\mathbf{F}_p)$

§ 3. $s_d(\mathbf{Z}/p^\ell\mathbf{Z}), \ell \geq 1$

Chapter III: On the explicit determination of $s_d(\mathbf{F}_p)$

§ 1. Preliminaries

§ 2. Examples

§ 3. On the Coefficients of the Period Equation

Higher Levels of Finite Fields

Introduction

The problem of the representation of rational integers as sum of squares has been studied since the very first times in mathematics. From this arises the problem of the representation of -1 as sum of squares, this time in more general domains, say, commutative rings, and hence, the problem of determining the minimal number s of squares needed, if such representation of -1 is possible in the ring.

This arithmetical invariant $s = s(O)$ of a ring O, is known as the Stufe or level of the ring. Some of the most important results about it establish that, in case it is finite, then the level of a field is always a power of 2 **[Pf]**, and the level of a semi-local ring is always of the form 2^n or $2^n - 1$ **[Ba]**, and also, that any natural number n may be the level of a ring **[DLP]**. However the explicit computation of $s(O)$ is, in general, a difficult task.

These results are the motivation for this work, where we study the natural generalization of the quadratic level to higher even exponents $d > 2$, i.e., we study the d^{th} level of a ring O, defined as

$$s_d(O) = min\{\ s \mid -1 = \alpha_1^d + \cdots + \alpha_s^d\ ,\ \alpha_i \in O\}$$

if such representation of -1 is possible in O, or, $s_d(O) = \infty$ otherwise.

In the literature (**[PAR 1-2]**, **[PR]** and recently **[AK]**), the problem has been studied essentially for finite fields or algebraic number fields and its $\wp$-adic completions. The results achieved by these authors are:

In **[PAR1]**, $s_4(\mathbf{F}_q)$ is found for $\mathbf{F}_q$ the finite field with q elements. Also, some results on $s_4(k)$ for k a quadratic number field are stated, and more generally, for k an algebraic number fields it is proved, $s_4(k) \leq 16$. (Indeed, by using **[B1]** one can prove, $s_d(k) \leq 2^d$. See § **2.(2.2)**, Chapter I). In **[PR]**, $s_d(\mathbf{F}_q)$ is studied, finding its values for $d = 6$, 8 and 10. In these works, some ad-hoc proofs and computer calculations are used, as well as the theory of cyclotomic numbers to decide which fields $\mathbf{F}_q$ (i.e. how large) have $s_d(\mathbf{F}_q) \leq 2$. (Indeed, this can be done for any $d \geq 2$ by using a more general result, on the number of solutions of additive equations over finite fields **[W]**. See § **3.(3.1)**, Chapter I).

In **[AK]**, $s_d(\mathbf{F}_q)$ is studied for $d = 2^r$, a power of 2. The authors establish very interesting experimental and theoretical results. Experimentally, they find (and so did we, for at least $d \leq 20$) that $s_{2^r}(\mathbf{F}_q) \leq 2$ for much smaller fields than what predicted by § **3.(3.1)** , Chapter I. Theoretically, they obtain $s_{2^r}(\mathbf{F}_q) \leq 2$, for all $q \neq p$ or p^3, where $p =$ char $\mathbf{F}_q$. And $s_{2^r}(\mathbf{F}_{p^3}) \leq 3$, finding in fact $s_{2^r}(\mathbf{F}_{p^3}) \leq 2$ for all $p \leq 101.711.873$.

Thus, these results establish as main open problem the determination of the d^{th} level for the prime finite fields $\mathbf{F}_p$.

Also, by generalizing some ideas used in **[PAR2]** we could state $s_d(k_\wp)$, $k_\wp$ the $\wp$-adic completion of an algebraic number field k, with ring of integers O and $\wp \subseteq O$ a prime ideal, in terms of $s_d(O/\wp^\nu)$, for some $\nu \geq 1$. (§ **4.(2.1)**, Chapter I). In particular, for $k = \mathbf{Q}$ we obtain $s_d(\mathbf{Q}_p) = s_d(\mathbf{Z}/p^{2r+1}\mathbf{Z})$ for $d = p^r k, r \geq 0$ and $(p, k) = 1$. In this way the study of the levels of the rings of integers mod p^ℓ becomes as well very interesting.

Hence, we study in this thesis the higher levels $s_d(\mathbf{Z}/p^\ell\mathbf{Z})$ for $\ell \geq 1$ and $p \geq 2$ a rational prime.

Chapter I (excepting perhaps for § **2.(2.2)**, § **3.3(4*)**, § **3.(3.1)**, § **4.(1.3)**

and § **4.(2.1)**), and the preliminaries in Chapter II and III (excepting for § **1.(3.1)**, § **1.(3.2)**, § **1.(3.3)**, and § **1.(4.2)** in Chapter II) are well known results which we wanted to include for completeness.

Our main results are stablished in § **2.** and § **3.** in Chapter II.

Chapter III is devoted to study some explicit examples and the coefficients of the period equations.

The results achieved are:

In the case $\ell = 1$ of the prime finite field $\mathbf{F}_p$ ($p > 2, d|p-1$ without loss of generality) and thanks to important ideas due to Prof. E. Becker, we find that considering the formal series $f(T) = \frac{1}{1-T\sum_{u\in\mathcal{U}} X^u}$ over $(K[X]/(X^p-1))$ [[T]] where $\mathcal{U} = (\mathbf{F}_p^*)^d$, enable us to take all possible sums of d^{th} powers in $\mathbf{F}_p^*$ and with this, by choosing $K = Q(\zeta)$ the cyclotomic field of the p^{th} roots of unity (related to $\mathbf{F}_p^*$ by Galois Theory), we obtain $s_d(\mathbf{F}_p)$ in terms of the coefficients of the period equation of degree d. This is, let

$$P(X) = X^d + \alpha_1 X^{d-1} + \alpha_2 X^{d-2} + \cdots + \alpha_d \in \mathbf{Z}[X]$$

be the minimal polynomial of the gaussian periods of length $(p-1)/d$. Then

$$s_d(\mathbf{F}_p) = min\{n|(n+1)\alpha_{n+1} - (1+n(p-1)/d)\alpha_n \neq 0\}$$

(§ **2.(2.2)**, Chapter II). And actually we only need to consider the first coefficients $\alpha_1, \cdots, \alpha_{d/2+1}$ since by [T], $s_d(\mathbf{F}_p) \leq d/2+1$ if $d \neq p-1$ and clearly $s_{p-1}(\mathbf{F}_p) = p-1$.

We should make notice that this is the first theoretical result on $s_d(\mathbf{F}_p)$ for $d > 2$, and provides a striking relation between the higher levels problem and the old problem of cyclotomy.

In the case $\ell > 1$, by noticing relations among congruences mod $p^\ell, p \geq 2$ **[Sch2]**, we find $s_d(\mathbf{Z}/2^\ell\mathbf{Z})$ (and by the way $s_d(\mathbf{Q}_2)$), in an elementary way.

Also for $p \neq 2, s_d(\mathbf{Z}/p^\ell\mathbf{Z})$ is found in terms of $s_d((\mathbf{Z}/p^{r+1}\mathbf{Z})^*)$ where $d = p^r k$ with $r \geq 0$ and $k|p-1$ (§ **1.(3.3)**, Chapter II). (In particular we get $s_2(\mathbf{Z}/p^\ell\mathbf{Z}) = s_2(\mathbf{F}_p)$, for all $\ell \geq 1$).

Finally $s_d((\mathbf{Z}/p^{r+1}\mathbf{Z})^*)$ is found in terms of the coefficients of a product of $r+1$ period equations (§ **3.(1.1)**, Chapter II), generalizing the result obtained for $\mathbf{F}_p$.

About the effective determination of the coefficients of the period equations, we have recently known some works **[G1-2]** and **[GZ]**, where the authors show that at least the beginning coefficients may be computed in an elementary way.

These results turn out to be very important for our work. For example, they lead us to some converse results (§ **3.(1.5)**, Chapter III), and we believe they will permit us finding some explicit examples of $s_d(\mathbf{Z}/p^\ell\mathbf{Z})$ for $\ell > 1$.

Chapter I: Higher Levels

§ 1. The Level of a Field

1. Introduction

The level of a field is defined as the minimal number s of squares needed to represent -1 as sum of squares.

This invariant of the field, which has been called Stufe in German, will be called here the level, or quadratic level, of the field k and denoted by $s = s(k)$.

The first question to be considered is the set of possible values of s. For example, if k is an ordered field, no such representation of -1 as sum of a finite number of squares is possible, so we say $s(k) = \infty$. If $k = \mathbf{C}$ the complex numbers, then $-1 = (\sqrt{-1})^2$ and $s(\mathbf{C}) = 1$.

On the other hand it can be easily proved that no field has level 3, 5, 6, or 7, while 4 or 8 cannot be excluded by the same method. This suggests that perhaps only powers of 2 can be values of the quadratic levels.

This question has been asked as a problem in the Jahresbericht der MDV in 1932 by B.L. van der Waerden.

A partial answer was given soon by H. Kneser, who proved that the only possible levels are $1, 2, 4, 8$ and $16\mathrm{m}$ ($m \in \mathbf{Z}$). But it was A. Pfister who answered the question completely. Pfister proved this very striking result about the level of a field.

Theorem (1.1) [Pf] Let k be a field. Then $s(k)$ is a power of 2.

We will intend to show how the Theory of Quadratic Forms helps giving very simple proofs of this result. Both proofs we present here are based on the following result due to Pfister.

Theorem (1.2) Let $\phi = < 1, a_1 > \otimes \cdots \otimes < 1, a_n >$ be an n-fold Pfister form over a field k, and let $D_k(\phi)$ be the set of elements in $k - \{0\}$ represented by ϕ. Then

$D_k(\phi)$ is a group.

Consequences:

(1) Let k be a field and $n \in \mathbf{N}$. If $\alpha_1, \cdots, \alpha_{2^n}$ and $\beta_1, \cdots, \beta_{2^n}$ are any element in k. Then, there exist $\gamma_1, \cdots, \gamma_{2^n}$ in k such that

$$\left(\sum_{i=1}^{2^n} \alpha_i^2\right)\left(\sum_{i=1}^{2^n} \beta_i^2\right) = \sum_{i=1}^{2^n} \gamma_i^2.$$

(2) Let ϕ be a Pfister form over a field k. Then

$$\phi \text{ isotropic over } k \implies \phi \text{ hyperbolic over } k.$$

1^{st} Proof of Theorem (1.1): Let $s = s(k)$. Then there exist $a_1, \cdots, a_s \in k$ and $n \in \mathbf{N}$ such that

$$a_1^2 + \cdots + a_s^2 = -1 \quad \text{with} \quad 2^n \leq s < 2^{n+1},$$

hence

$$a_1^2 + \cdots a_{2^n}^2 = -(1 + a_{2^n+1}^2 + \cdots + a_s^2)$$

and then

$$\frac{(a_1^2 + \cdots + a_{2^n}^2)(1 + a_{2^n+1}^2 + \cdots + a_s^2)}{(1 + a_{2^n+1}^2 + \cdot + a_s^2)^2} = -1.$$

This gives a representation of -1 as product of 2^n by $s + 1 - 2^n \leq 2^n$ squares. Hence by (1), -1 has a representation as sum of 2^n squares in k. The minimality of s implies $s = 2^n$.

□

2^d Proof of Theorem (1.1): Let $s = s(k)$ and $n \in \mathbf{N}$ be such that $2^n \leq s < 2^{n+1}$. Lets consider the $(n+1)$-fold Pfister form $\phi = \otimes_1^{n+1} < 1, 1 >= 2^{n+1} \times < 1 >$. Hence

$\phi = s\times < 1 > \perp (2^{n+1} - s)\times < 1 >$ is isotopic over k since $s\times < 1 >$ represents -1. Then ϕ is hyperbolic over k by (2), so

$$\phi = 2^{n+1}\times < 1 > \cong 2^n\times < 1 > \perp 2^n\times < -1 > .$$

Now by Witt's cancellation theorem, $2^n\times < 1 > \cong 2^n\times < -1 >$ and -1 can be represented as a sum of 2^n squares in k. Then again $s = 2^n$.

□

In general the exact determination of the level of a field or ring is a difficult problem and it is solved only in particular cases. Some examples will be presented in what follows.

2. Examples

The following are well known examples of the quadratic level.

Theorem (2.1) Let k be a totally complex algebraic number field. Then $s(k) \leq 4$.

Proof: It follows from the Hasse-Minkowski Local-Global Principle and the fact that every quadratic form over $\mathbf{Q}_p$, of dimension greater than 4, is isotropic over $\mathbf{Q}_p$ for all $p = 2, 3, \cdots < \infty$ prime numbers.

□

Theorem (2.2) Let $k = \mathbf{Q}(\sqrt{-m})$ be a quadratic number field with $m > 0$ a square free rational integer. Then

$$s(k) = \begin{cases} 1 \text{ if } m = 1 \\ 2 \text{ if } m \not\equiv 7(8), m \neq 1 \\ 4 \text{ if } m \equiv 7(8) \end{cases}$$

Proof: If follows from the next three results:

(i) Theorem (Lagrange). Every sum of squares in $\mathbf{Q}$ is a sum of 4 squares.

(ii) Theorem (Legendre). Let $m > 0$ be a rational integer. Then $x^2 + y^2 + z^2 = m$ has an integral solution iff $m \neq 4^a(8b + 7)$ with $a, b \in \mathbf{Z}$.

(iii) Theorem (Pfister). Let k be a formally real field and $a \in \sum k^2$ with $\ell(a)$ being the length of the shortest representation of a as sum of squares in k. Let $n \in \mathbf{N}$ be such that $2^n \leq \ell(a) < 2^{n+1}$. Then $k(\sqrt{-a})$ is nonformally real with level 2^n.

Thus if $m > 0$ is a square free rational integer, then $\ell(m) = 1$ iff $m = 1$. Otherwise $2 \leq \ell(m) \leq 4$ by (i), being $\ell(m) = 4$ iff $m \equiv 7(8)$ by (ii). The result follows by (iii).

□

Theorem (2.3) Let k be a formally real field. Let $X_1, \cdots, X_m$ be m independent variables and let K be the field extention $k(X_1, \cdots, X_m)(\sqrt{-(X_1^2 + \cdots + X_m^2)})$. Then $s(K) = 2^n$ where $n \in \mathbf{N}$ such that $2^n \leq m < 2^{n+1}$.

Proof: It follows from (iii) and Cassels' result which states that in the rational function field $k(X_1, \cdots, X_m), \ell(X_1^2 + \cdots + X_m^2) = m$

□

Finally, a classic result on finite fields is perhaps the most complete one that we have about levels of fields.

Theorem (2.4) Let $\mathbf{F}_q$ be the finite field with q elements. Then

$$s(\mathbf{F}_q) = \begin{cases} 1 & \text{if } q \equiv 1(4) \text{ or } q = 2^n \\ 2 & \text{if } q \equiv 3(4) \end{cases}$$

Proof: Since char $\mathbf{F}_q = 2$ is the trivial case, let $\mathbf{F}_q^* =< \omega / \omega^{q-1} = 1 >$ with char $\mathbf{F}_q \neq 2$. Then $-1 = \omega^{\frac{q-1}{2}}$ is a square in $\mathbf{F}_q^*$ iff $4|q-1$. Otherwise, since for every $x \in \mathbf{F}_q^*, |\mathbf{F}_q^2| = |x - \mathbf{F}_q^2| = \frac{q-1}{2} + 1 = \frac{q+1}{2}$, then $\mathbf{F}_q^2 \cap (x - \mathbf{F}_q^2) \neq \Phi$ and every element in $\mathbf{F}_q^*$, in particular -1, is a sum of two squares.

□

Hence the problem of the quadratic level is solved for the class of finite fields.

§ 2. Higher Levels

1. Introduction

Let A be a commutative ring with unit and let $d > 1$ be a rational integer. Then the higher level of A of exponent d, or, d^{th} level of A, is defined as

$$s_d(A) = min\{\, s \in \mathbf{N} \mid -1 = a_1^d + \cdots + a_s^d\,,\ a_i \in A\,\}$$

if such representation of -1 is possible in A. Otherwise $s_d(A) = \infty$.

In this work we will only consider rings of characteristic different from 2 and $d > 1$ will always means an *even* rational integer. Otherwise $s_d(A)$ is trivially equal to 1 since either $-1 = 1^d$ or $-1 = (-1)^d$.

Some more or less evident remarks on the numbers $s_d(A)$ are the following:

(1) If $d'|d$, then $s_{d'}(A) \leq s_d(A)$. In particular $s(A) = s_2(A) \leq s_d(A)$.

(2) If $A \longrightarrow B$ is a ring homomorphism, then $s_d(B) \leq s_d(A)$. In particular if $A \subseteq B$ or $B = A/I$, $I \subseteq A$ an ideal.

(3) Let A be a ring such that:

i) A contains a primitive ℓ^{th} root of unity ζ, some $\ell > 2$ prime.

ii) $\zeta - 1$ is not a zero divisor in A.

iii) $\ell \nmid d$.

Then $s_d(A) \leq \ell - 1$.

This follows from considering the homomorphism $\varphi : <\zeta> \longrightarrow <\zeta>, \varphi(\zeta) = \zeta^d$. By iii) φ is inyective. Then epiyective, since $<\zeta>$ is finite. Hence ζ is a d^{th} power in A. Now by i) $1 + \zeta + \cdots + \zeta^{\ell-1} = 0$, then -1 is a sum of $\ell - 1$ d^{th} powers in A.

(4) Let char $A = p$. Then $s_d(A) \leq p - 1$.

2. Examples

As we have seen, the quadratic level of a field is always a power of 2, Then, it is natural to ask if such a nice behavior is still attained by the $4^{th}, 6^{th}, \cdots, d^{th}$ levels.

One finds soon, this is not the case, as the following examples in **[PAR 1]** show:

(1) Let $\eta = e^{\pi i/4}$ be a primitive 8^{th} root of unity. Then $s_4(\mathbf{Q}(\eta)) = 1$.
Clearly, since $\eta^4 = -1$.

(2) Let $\rho = e^{2\pi i/3}$ be a primitive cubic root of unity. Then $s_4(\mathbf{Q}(\rho)) = 2$.
Clearly $-1 = \rho + \rho^2 = \rho^4 + (\rho^2)^4$. Moreover $\sqrt{-1} \notin \mathbf{Q}(\rho)$ and the result follows.

(3) $s_4(\mathbf{F}_{29}) = 3$ and $s_4(\mathbf{F}_5) = 4$.
Straight forward with $-1 \equiv 1^4 + 6^4 + 8^4(29)$ and $-1 \equiv 1^4 + 1^4 + 1^4 + 1^4(5)$.

(4) For all $d \geq 2$, $s_d(\mathbf{F}_q) \leq 2$ if $q = 3^n$.
Clearly, since char $\mathbf{F}_q = 3$ and $s_d(\mathbf{F}_q) \leq$ char $\mathbf{F}_q - 1$.

(5) $s_4(\mathbf{Q}(\sqrt{-2})) = 6$.
Since $-1 = 1 + 3(\sqrt{-2})^4 + (1 + \sqrt{-2})^4 + (1 - \sqrt{-2})^4$ and it may be proved, no shorter representation is possible.

Also it holds.

Theorem (2.1)([PAR1]) Let $m > 0$ be an integer. Then

$$s_4(\mathbf{Q}(\sqrt{-m})) \leq 15.$$

Proof: If $m = 1$, we have $-1 = 4(\frac{1+i}{2})^4$, thus $s_4(\mathbf{Q}(i)) \leq 4$. If $m > 1$, consider

$$X = a^4(r + \sqrt{-m})^4 + a^4(r - \sqrt{-m})^4,$$

then

$$X = 2a^4((r^2 - m)^2 - 4r^2m) \in \mathbf{Z}.$$

Choosing $r = [\sqrt{m}]$ or $r = [\sqrt{m}] + 1$ such that $(r^2 - m)^2 \equiv 1(2)$ and $X < 0$, and taking $a >> 0$, $a \equiv 1(2)$, we get $X \equiv 2a^4 \equiv 2(16)$. Thus $-X >> 0$ and $-X \not\equiv 0, 15(16)$. Then a result due to Davenport **[Da]** says that $-X \in \sum_1^{14} \mathbf{Z}^4$. Hence $0 \in \sum_1^{16} \mathbf{Q}(\sqrt{-m})^4$ and the result follows.

□

Theorem (2.2) Let k be a totally complex algebraic number field and $d > 1$ an integer. Then

$$s_d(k) \leq 2^d.$$

Proof: Following a proof in **[PAR 1]** for $d = 4$, based on:

i) Birch's Theorem (**[B1]**) Let k be an algebraic number field and let $b_1, \cdots, b_n$ be algebraic integers in k. If $n \geq 2^d + 1$, then

$$b_1X_1^d + \cdots + b_nX_n^d = 0$$

is non-trivially solvable in k iff it is non-trivially solvable in every real and p-adic completion of k.

ii) Hensel's Lemma (**[BS]**) Let $F(X_1, \cdots, X_n) \in \mathbf{Z}_p[X_1, \cdots, X_n]$ and $\gamma_1, \cdots, \gamma_n \in \mathbf{Z}_p, p \geq 2$ prime. And let $\delta \geq 0$ and $1 \leq j \leq n$ such that

$$F(\gamma_1, \cdots, \gamma_n) \equiv 0(p^{2\delta+1})$$

$$\frac{\partial F}{\partial X_j}(\gamma_1, \cdots, \gamma_n) \equiv 0(p^\delta), \not\equiv 0(p^{\delta+1}).$$

Then, there exist $\theta_1, \cdots, \theta_n \in \mathbf{Z}_p$ with $F(\theta_1, \cdots, \theta_n) = 0$ and $\theta_i \equiv \gamma_i (p^{\delta+1})$ for all $i = 1, \cdots n$.

We find the equation

$$X_1^d + \cdots + X_n^d = 0 \text{ with } n \geq 2^d + 1$$

is solvable in $\mathbf{Z}_p$, for all $p = 2, 3, \cdots < \infty$. This follows by Hensel's Lemma:

Write $d = p_0^{r_0} \cdot p_1^{r_1} \cdots p_k^{p_k}$ where $p_0 = 2, p_i > 2$ different primes for $1 \leq i \leq k$, $k \geq 0$ and $r_i \geq 1$. We show

$$\left.\begin{aligned} X_1^d + \cdots + X_n^d &\equiv 0(p^{2r+1}) \\ dX_j^{d-1} &\equiv 0(p^r) \text{ , } \not\equiv 0(p^{r+1}) \end{aligned}\right\}$$

is solvable for all $p = 2, 3, \cdots < \infty$.

Case $p \neq 2, p_1, \cdots, p_k$: Then

$$\left.\begin{aligned} X_1^d + \cdots + X_n^d &\equiv 0(p) \\ dX_j^{d-1} &\not\equiv 0(p) \end{aligned}\right\}$$

is solvable since $n \geq 2^d + 1 \geq d + 1$ and $\mathbf{F}_p$ is a C_1- field.

Case $p = 2$: Then for all $r_0 \geq 3$.

$$\left.\begin{aligned} \textstyle\sum_{j=1}^{2^d} 1^d &\equiv 0(2^d) \equiv 0(2^{2^{r_0}}) \equiv 0(2^{2r_0+1}) \\ d &\equiv 0(2^{r_0}), \not\equiv 0(2^{r_0+1}) \end{aligned}\right\}$$

If $r_0 = 2$ and $d = 4$: Then $n \geq 17$ and

$$\left.\begin{aligned} \textstyle\sum_{j=1}^{16} 1^4 + 2^4 &\equiv 0(2^5) \\ 4 &\equiv 0(2^2), \not\equiv 0(2^3) \end{aligned}\right\}$$

If $r_0 = 2$ and $d \geq 12$: Then $n \geq 2^{12} + 1$ and

$$\left.\begin{array}{rcl} \sum_{j=1}^{32} 1^d & \equiv & 0(2^5) \\ d & \equiv & 0(2^2), \not\equiv 0(2^3) \end{array}\right\}$$

If $r_0 = 1$ and $d = 2$: Then $n \geq 5$ and

$$\left.\begin{array}{rcl} \sum_{j=1}^{4} 2^2 + 4^2 & \equiv & 0(2^5) \\ 2 \cdot 2 & \equiv & 0(2^2), \not\equiv 0(2^3) \end{array}\right\}$$

If $r_0 = 1$ and $d \geq 6$: Then $n \geq 2^6 + 1$ and

$$\left.\begin{array}{rcl} \sum_{j=1}^{8} 1^d & \equiv & 0(2^3) \\ d & \equiv & 0(2), \not\equiv 0(2^2) \end{array}\right\}$$

Case $p = p_i$ some $1 \leq i \leq k$: Then for $r = r_i$

$$\left.\begin{array}{rcl} \sum_{j=1}^{p^{2r+1}} 1^d & \equiv & 0(p^{2r+1}) \\ d & \equiv & 0(p^r), \not\equiv 0(p^{r+1}) \end{array}\right\}$$

One can easily prove that $n \geq 2^d + 1 \geq 4^{p^r} + 1 \geq p^{2r+1}$ for all $p \geq 3, r \geq 1$. (For $r = 1, 4^p + 1 \geq p^3$ for all $p \geq 3$. and $4^{p^r} + 1 \geq p^{2r+1}$ implies $4^{p(r+1)} \geq p^{2(r+1)+1}$ for all $r \geq 1$)

Thus $X_1^d + \cdots X_n^d = 0$ with $n \geq 2^d + 1$ is solvable in $\mathbf{Z}_p$. But then Birch's Theorem gives it is solvable in k and then $s_d(k) \leq 2^d$.

□

§ 3. Higher Levels of Finite Fields

The first class of rings we will be interested in for the study of higher levels will be the class of finite fields.

In the paragraphs 1. and 2. we will state the results from the theory we will need ([Sch1], [H]). In 3. we will deduce some results.

1. Preliminaries: Additive Equations

Here we will be devoted to estimate the number of solutions of additive equations of the form

$$a_1X_1^{d_1} + \cdots + a_nX_n^{d_n} = 0 \qquad (**)$$

over finite fields, with $a_1, \cdots, a_n$ nonzero elements in the field and $d_1, \cdots, d_n$ positive integers.

Our goal is to deduce a general result which bounds the level's values as a function of the size of the field.

1.1. Characters of Finite Abelian Groups

Given an abelian (multiplicative) finite group G, a (multiplicative) character on G is a map χ from G to the nonzero complex numbers, such that

$$\chi(xy) = \chi(x)\chi(y) \quad \text{for all} \quad x, y \in G.$$

Since $\chi(x) = \chi(1)\chi(x)$ and $x^{|G|} = 1$ (the identity element in G) for all $x \in G$, we have $\chi(1) = 1$ and $\chi(x)^{|G|} = 1$, i.e., $\chi(x)$ is a $|G|^{th}$ root of unity, for all $x \in G$.

If χ, χ' are characters on G, then so are the maps $\chi\chi'$ and χ^{-1} defined by $\chi\chi'(x) = \chi(x)\chi'(x)$ and $\chi^{-1}(x) = 1/\chi(x) = \overline{\chi(x)}$ (the complex conjugate of $\chi(x)$ since $|\chi(x)| = 1$). We will denote χ^{-1} by $\overline{\chi}$. Now it is clear that the characters on G form a group under multiplication, denoted by $\hat{G}$, with identity element χ_0, called the principal character defined by $\chi_0(x) = 1$ for all $x \in G$.

Let $\zeta_n = e^{2\pi i/n}$.

Lemma (1.1.1) Let C_n be the cyclic group of order n and let ω be a generator. Let a be a residue class modulo n. Then the map χ_a on C_n defined by $\chi_a(\omega) = \zeta_n^a$

is a character of C_n and every character of C_n is of this type. Thus $\hat{C}_n$ is cyclic of order n.

□

More generally

Lemma (1.1.2) Let G be a finite abelian group. Then $\hat{G} \cong G$.

□

This fact is the basis for the Duality Principle between G and $\hat{G}$.

For example, from obvious propositions like:

1) $\chi(x) = 1$ for all $x \in G \Longrightarrow \chi = \chi_0$.

2) $\chi_1(x) = \chi_2(x)$ for all $x \in G \Longrightarrow \chi_1 = \chi_2$.

one obtains the non-obvious ones:

1′) $\chi(x) = 1$ for all $\chi \in \hat{G} \Longrightarrow x = 1$.

2′) $\chi(x_1) = \chi(x_2)$ for all $\chi \in \hat{G} \Longrightarrow x_1 = x_2$.

Hence, the set of values $\{\chi(x)|\chi \in \hat{G}\}$ characterizes the element $x \in G$.

Similarly one can use characters to characterize subgroups of G. In particular, we will be interested in the subgroup of the d^{th} powers of G.

Lemma (1.1.3)

(i) $\mathcal{U} \leq G \Longrightarrow \tilde{\mathcal{U}} = \{\chi \in \hat{G}|\chi(u) = 1, \text{ for all } u \in \mathcal{U}\} \leq \hat{G}$.

(ii) $U \leq \hat{G} \Longrightarrow \tilde{U} = \{x \in G|\chi(x) = 1, \text{ for all } \chi \in U\} \leq G$.

(iii) $\tilde{(\tilde{\mathcal{U}})} = \mathcal{U}$

□

In particular for $\mathcal{U} = G^d = \{x^d | x \in G\}$

$$\chi(x^d) = \chi(x)^d = 1, \text{ for all } x \in G \Longleftrightarrow \chi^d = \chi_0.$$

Then

$$\tilde{G}^d = \{\chi \in \hat{G} | \chi(y) = 1, \text{ for all } y \in G^d\}$$

and

$$(\tilde{(G)})^d = \{x \in G | \chi(x) = 1, \text{ for all } \chi \in \tilde{G}^d\} = G^d.$$

Thus

Lemma (1.1.4) $G^d = \{x \in G | \chi(x) = 1, \text{ for all } \chi \text{ with } \chi^d = \chi_0\}$.

□

Finally it holds.

Lemma (1.1.5) Let G be a finite abelian group of order n. Then

(i) Given $\chi \in \hat{G}$,

$$\sum_{x \in G} \chi(x) = \begin{cases} n & \text{iff} \quad \chi = \chi_0 \\ 0 & \text{iff} \quad \chi \neq \chi_0 \end{cases}$$

(ii) Given $x \in G$,

$$\sum_{\chi \in \hat{G}} \chi(x) = \begin{cases} n & \text{iff} \quad x = 1 \\ 0 & \text{iff} \quad x \neq 1 \end{cases}$$

□

Lemma (1.1.6): Let G be a finite abelian group with $\mathcal{U} \leq G$ a subgroup of index d and cyclic quotient $G/\mathcal{U}$. Then every character on $\mathcal{U}$ has exactly d extensions to G.

□

1.2 Character Sums associated with Finite Fields

Let $\mathbf{F}_q$ be the finite field with q elements. Then the nonzero elements of $\mathbf{F}_q$ form a cyclic group $\mathbf{F}_q^*$ of order $q-1$. Hence the characters on $\mathbf{F}_q^*$ also form a cyclic group of order $q-1$, so that $\chi^{q-1} = \chi_0$, for all $\chi \in \hat{\mathbf{F}}_q^*$.

We say χ is of order d, if $\chi^d = \chi_0$ and if d is the smallest positive integer with this property. It is easily seen that $d|q-1$.

We say χ is of exponent e, if $\chi^e = \chi_0$. Clearly this is equivalent to $d|e$.

Let $d|q-1$. We have by §**3.(1.1.4)**:

$x \in (\mathbf{F}_q^*)^d \Longleftrightarrow \chi(x) = 1$, for all characters χ of exponent d.

Then every character of exponent d may be considered as a character on the factor group $\mathbf{F}_q^*/(\mathbf{F}_{q^\bullet})^d$. There are precisely d such characters.

Lets extend the definition of a character χ on $\mathbf{F}_q^*$ by setting

$$\chi(0) = \begin{cases} 1 \text{ if } \chi = \chi_0 \\ 0 \text{ if } \chi \neq \chi_0 \end{cases}$$

Thus we have

Lemma (1.2.1) Let $d|q-1$. Then

$$\sum_{\chi/\chi^d=\chi_0} \chi(a) = \begin{cases} d & \text{if} \quad a \in (\mathbf{F}_q^*)^d \\ 0 & \text{if} \quad a \notin (\mathbf{F}_q^*)^d \\ 1 & \text{if} \quad a = 0 \end{cases}$$

Proof: The characters of exponent d are precisely the characters of $\mathbf{F}_q^*/(\mathbf{F}_q^*)^d$. Hence the first two cases follow from §3.(1.1.5). If $a = 0$ then $\sum_{\chi/\chi^d=\chi_0} \chi(a) = \chi_0(a) + \sum_{\substack{\chi^d=\chi_0 \\ \chi\neq\chi_0}} \chi(a) = 1 + 0 = 1$.

□

Lemma (1.2.2) Let $N[X^d = a]$ be the number of solutions in $\mathbf{F}_q$ of the equation $X^d = a$. Then

$$N[X^d = a] = \sum_{\chi/\chi^d=\chi_0} \chi(a)$$

Proof: If $a \in (\mathbf{F}_q^*)^d$, let $x \in \mathbf{F}_q^*$ be such that $x^d = a$. Let $V = \{z \in \mathbf{F}_q^* | z^d = 1\}$ be the subgroup of elements of $\mathbf{F}_q^*$ of exponent d. Then the lateral class xV is the set of solutions of $X^d = a$ in $\mathbf{F}_q$, since $(xz)^d = x^d z^d = x^d = a$ for $z \in V$, and any two solutions x_1, x_2 satisfy $(x_1 x_2^{-1})^d = 1$, therefore $x_1 x_2^{-1} \in V$. Then $N[X^d = a] = |V|$. But the Duality Principle gives $|V| = |\{\chi \in \hat{\mathbf{F}}_q^* | \chi^d = \chi_0\}| = d$. If $a = 0$ then clearly $N[X^d = a] = 1$. Hence

$$N[X^d = a] = \left\{ \begin{array}{lll} d & \text{if} & a \in (\mathbf{F}_q^*)^d \\ 0 & \text{if} & a \notin (\mathbf{F}_q^*)^d \\ 1 & \text{if} & a = 0 \end{array} \right\} = \sum_{\chi/\chi^d=\chi_0} \chi(a)$$

by §3.(1.2.1)

□

1.3 Gaussian Sums on Finite Fields: An Introduction

We will now also consider additive characters on $\mathbf{F}_q$ by considering $\mathbf{F}_q$ as an additive group of order $q = p^n$, where $p = \text{char}\mathbf{F}_q$.

Let $\zeta_p = e^{2\pi i/p}$.

Lemma (1.3.1) Let $\mathbf{F}_q$ be the finite field with $q = p^n$ elements and $t : \mathbf{F}_q \to \mathbf{F}_p$ be the trace. Let $a \in \mathbf{F}_q$. Then the map ψ_a on $\mathbf{F}_q$ defined by $\psi_a(x) = \zeta_p^{t(ax)}$ is an additive character of $\mathbf{F}_q$ and every additive character of $\mathbf{F}_q$ is of this type.

The character ψ_0 defined by $\psi_0(x) = 1$ for all $x \in \mathbf{F}_q$ is the identity element in $\hat{\mathbf{F}}_q$.

Let χ and ψ be a multiplicative and an additive character on $\mathbf{F}_q$. Then the sum

$$\tau(\chi, \psi) = \sum_{x \in \mathbf{F}_q} \chi(x)\psi(x)$$

is called a Gaussian sum. In view of **§3.(1.1.5)** it holds

Proposition (1.3.2)

$$\tau(\chi_0, \psi) = 0 \quad \text{if} \quad \psi \neq \psi_0$$

$$\tau(\chi, \psi_0) = 0 \quad \text{if} \quad \chi \neq \chi_0$$

$$\tau(\chi_0, \psi_0) = q$$

Theorem (1.3.3) Let $\chi \neq \chi_0$ and $\psi \neq \psi_0$. Then $|\tau(\chi, \psi)| = q^{1/2}$.

Proof: $|\tau(\chi, \psi)|^2 = \sum_x \sum_y \chi(x)\psi(x)\bar{\chi}(y)\bar{\psi}(y)$

Without restriction take $y \neq 0$, since $\chi(0) = 0$, and put $x = ty$, then

$$\begin{aligned} |\tau(\chi, \psi)|^2 &= \sum_{y \neq 0} \sum_t \chi(ty)\psi(ty)\chi(y^{-1})\psi(-y) \\ &= \sum_t \chi(t) \sum_{y \neq 0} \psi((t-1)y) \\ &= \sum_t \chi(t) \sum_y \psi((t-1)y) - \sum_t \chi(t) \\ &= \sum_t \chi(t) \sum_y \psi((t-1)y) \end{aligned}$$

by **§3.(1.1.5)** since $\chi \neq \chi_0$. And again by **§3.(1.1.5)** the inner sum is q for $t = 1$, and 0 if $t \neq 1$. Thus

$$|\tau(\chi, \psi)|^2 = \chi(1)q = q.$$

□

2. Estimates on the Number of Solutions of Additive Equations

Lemma (2.1) ([Gr]) Let m be an integer with $0 \leq m < q-1$. Then

$$\sum_{x \in \mathbf{F}_q^*} x^m = \begin{cases} -1 & \text{if} \quad m = 0 \\ 0 & \text{if} \quad m \neq 0 \end{cases}$$

Proof: If $m = 0$, $\sum_{x \in \mathbf{F}_q^*} x^m = \sum_{x \in \mathbf{F}_q^*} 1 = q - 1 = -1$. If $m \neq 0, m < q-1$, let ω be a generator of $\mathbf{F}_q^*$, cyclic of order $q-1$. Then

$$\sum_{x \in \mathbf{F}_q^*} x^m = \sum_{i=0}^{q-2} (\omega^m)^i = \frac{(\omega^m)^{q-1} - 1}{\omega^m - 1} = 0.$$

□

Theorem (2.2) (Chevalley-Warning) Let $f(X_1, \cdots, X_n) \in \mathbf{F}_q[X_1, \cdots, X_n]$ be a form of degree $d < n$. Then f has a nontrivial zero in $\mathbf{F}_q^n$.

Proof: See **[Sch 1]**, p. 136 or **[IR]** p. 143.

□

Theorem (2.3) Set $C =< \omega | \omega^n = 1 >$ be a cyclic group of order n. For any integer $d > 0$ let $C^d =< \omega^d >$ be the subgroup of d^{th} powers. Let $d^* = (d, n)$. Then $C^d = C^{d*}$.

Proof: We have $d^* = (d, n)$, then d^* divides d and every d^{th} power in C is a d^{*th} power in C, thus $C^d \subseteq C^{d*}$. Also, there exist $\lambda, \mu \in \mathbf{Z}$ such that $d^* = \lambda d + \mu n$, then $\omega^{d^*} = \omega^{\lambda d + \mu n} = (\omega^\lambda)^d$ since $\omega^n = 1$, thus $C^{d^*} \subseteq C^d$.

□

This means that the number of solutions of $(**)$ in $\mathbf{F}_q^n$ does not change if we take $d_i^* = (d_i, q-1)$ instead of d_i for $i = 1, \cdots, n$. Then without loss of generality, we may assume $d_i | q-1, i = 1, \cdots, n$.

Lemma (2.4) Let $\psi \neq \psi_0$ be an additive character and $a \in \mathbf{F}_q^*$. Let $d | q-1$. Then

$$\sum_{y \in \mathbf{F}_q} \psi(ay^d) = \sum_{\chi/\chi^d = \chi_0} \overline{\chi}(a)\tau(\chi, \psi)$$

Proof: Given $x \in \mathbf{F}_q$, let $N = N[X^d = x]$ be the number of solutions in $\mathbf{F}_q$ of the equation $X^d = x$. Then by §**3.(1.2.2)**

$$N = \sum_{\chi/\chi^d = \chi_0} \chi(x).$$

Then

$$\sum_{y \in \mathbf{F}_q} \psi(ay^d) = \sum_{x \in \mathbf{F}_q} \psi(ax) \sum_{\chi/\chi^d = \chi_0} \chi(x).$$

Replacing x by $a^{-1}x$, and noticing $\chi(a^{-1}x) = \overline{\chi}(a)\chi(x)$, we get

$$\begin{aligned} \textstyle\sum_{y \in \mathbf{F}_q} \psi(ay^d) &= \textstyle\sum_{x \in \mathbf{F}_q} \psi(x) \sum_{\chi/\chi^d = \chi_0} \overline{\chi}(a)\chi(x) \\ &= \textstyle\sum_{\chi/\chi^d = \chi_0} \overline{\chi}(a) \sum_{x \in \mathbf{F}_q} \chi(x)\psi(x) \\ &= \textstyle\sum_{\chi/\chi^d = \chi_0} \overline{\chi}(a)\tau(\chi, \psi). \end{aligned}$$

□

Proposition (2.5) Let $f(X_1, \cdots, X_n) \in \mathbf{F}_q[X_1, \cdots, X_n]$ and let N be the number of solutions in $\mathbf{F}_q^n$ of $f = 0$. Then

$$N = \frac{1}{q} \sum_{\psi} \sum_{x_1 \in \mathbf{F}_q} \cdots \sum_{x_n \in \mathbf{F}_q} \psi(f(x_1, \cdots, x_n))$$

where ψ runs through all additive characters of $\mathbf{F}_q$. Moreover if $\psi \neq \psi_0$ is fixed, then $\psi_a(x) := \psi(ax)$ runs through all additive characters if a runs through $\mathbf{F}_q$. Then

$$N = \frac{1}{q} \sum_{a \in \mathbf{F}_q} \sum_{x_1 \in \mathbf{F}_q} \cdots \sum_{x_n \in \mathbf{F}_q} \psi(af(x_1, \cdots, x_n))$$

Proof: By §3.**(1.1.5)**

$$\sum_{\psi} \psi(f(x_1, \cdots, x_n)) = \begin{cases} q & \text{if } f(x_1, \cdots, x_n) = 0 \\ 0 & \text{otherwise} \end{cases}$$

Now considering the sum through all $x_1, \cdots, x_n \in \mathbf{F}_q$ the result follows.

□

Theorem (2.6) Let N be the number of solutions in $\mathbf{F}_q^n$ of the equation $a_1 X_1^{d_1} + \cdots + a_n X_n^{d_n} = 0$, where $a_1, \cdots, a_n \in \mathbf{F}_q^*$ and $d_i | q-1$ for all $i = 1, \cdots n$. Then

$$N = q^{n-1} + \left(1 - \frac{1}{q}\right) \sum_{\substack{\chi_1 \neq \chi_0 \\ \chi_1^{d_1} = \chi_0}} \cdots \sum_{\substack{\chi_n \neq \chi_0 \\ \chi_n^{d_n} = \chi_0}} \overline{\chi_1}(a_1) \cdots \overline{\chi_n}(a_n) \tau(\chi_1, \psi) \cdots \tau(\chi_n, \psi)$$

where $\psi \neq \psi_0$ is an additive character, χ_i are multiplicative character for $i = 1, \cdots n$ and $\chi_1 \cdot \ldots \cdot \chi_n = \chi_0$.

Proof: By §3.**(2.5)**

$$\begin{aligned} qN &= \textstyle\sum_{a \in \mathbf{F}_q} \sum_{x_1 \in \mathbf{F}_q} \cdots \sum_{x_n \in \mathbf{F}_q} \psi(a(a_1 x_1^{d_1} + \cdots + a_n x_n^{d_n})) \\ &= \textstyle\sum_{a \in \mathbf{F}_q} \sum_{x_1, \cdots, x_n \in \mathbf{F}_q} \psi(a a_1 x_1^{d_1}) \cdots \psi(a a_n x_n^{d_n}) \\ &= \textstyle\sum_{a \in \mathbf{F}_q} \prod_{i=1}^{n} \left(\sum_{x_i \in \mathbf{F}_q} \psi(a a_i x_i^{d_i}) \right) \end{aligned}$$

Now by §3.**(1.2.2)**

$$\sum_{x_i \in \mathbf{F}_q} \psi(aa_i x_i^{d_i}) = \sum_{y_i \in \mathbf{F}_q} \psi(aa_i y_i) \sum_{\chi_i / \chi_i^d = \chi_0} \chi_i(y_i)$$

Since $aa_i \neq 0$, replacing y_i by $(aa_i)^{-1} y_i$ we get

$$\begin{aligned} \textstyle\sum_{x_i \in \mathbf{F}_q} \psi(aa_i x_i^{d_i}) &= \textstyle\sum_{y_i \in \mathbf{F}_q} \psi(y_i) \sum_{\chi_i / \chi_i^{d_i} = \chi_0} \overline{\chi_i}(aa_i) \chi_i(y_i) \\ &= \textstyle\sum_{\chi_i / \chi_i^{d_i} = \chi_0} \overline{\chi_i}(aa_i) \sum_{y_i \in \mathbf{F}_q} \chi_i(y_i) \psi(y_i) \\ &= \textstyle\sum_{\chi_i / \chi_i^{d_i} = \chi_0} \overline{\chi_i}(aa_i) \tau(\chi_i, \psi). \end{aligned}$$

Thus

$$\begin{aligned} qN - q^n &= \textstyle\sum_{a \neq 0} \left(\sum_{\chi_1 / \chi_1^d = \chi_0} \overline{\chi_1}(aa_1) \tau(\chi_1, \psi) \right) \cdots \left(\sum_{\chi_n / \chi_n^{d_n} = \chi_0} \overline{\chi_n}(aa_n) \tau(\chi_n, \psi) \right) \\ &= \textstyle\sum_{a \neq 0} \sum_{\chi_1 / \chi_1^{d_1} = \chi_0} \cdots \sum_{\chi_n / \chi_n^{d_n} = \chi_0} \overline{\chi_1}(aa_1) \cdots \overline{\chi_n}(aa_n) \tau(\chi_1, \psi) \cdots \tau(\chi_n, \psi) \\ &= \textstyle\sum_{\substack{\chi_1, \cdots, \chi_n \\ \chi_i^{d_i} = \chi_0}} \overline{\chi_1}(a_1) \cdots \overline{\chi_n}(a_n) \left(\sum_{a \neq 0} \overline{\chi_1 \cdots \chi_n}(a) \right). \end{aligned}$$

By §**3.(1.1.5)** we see that the inner sum is $q-1$ or zero in case $\chi_1 \cdots \chi_n = \chi_0$ or not. And since $G(\chi_i, \psi) = 0$ if $\chi_i = \chi_0$, we obtain

$$qN - q^n = (q-1) \sum_{\substack{\chi_1 \neq \chi_0, \cdots, \chi_n \neq \chi_0 \\ \chi_1 \cdots \chi_n = \chi_0 \\ \chi_i^{d_i} = \chi_0}} \overline{\chi_1}(a_1) \cdots \overline{\chi_n}(a_n) \tau(\chi_1, \psi) \cdots \tau(\chi_n, \psi)$$

and the result follows.

□

As consequence of this result N satisfies

$$|N - q^{n-1}| \leq (1 - \frac{1}{q}) \sum |\overline{\chi}_1(a_1) \cdots \overline{\chi}_n(a_n) \tau(\chi_1, \psi) \cdots \tau(\chi_n, \psi)|$$

This will allow us to find the lower bound for N we are looking for.

Let $\mathbf{F}_q^* =< \omega | \omega^{q-1} = 1 >$. If χ_i are characters of exponent $d_i, i = 1, \cdots, n$, then $\chi_i(\omega) = e^{2\pi i m_i/d_i}$, some $0 \leq m_i < d_i$. Moreover if $\chi_i \neq \chi_0$ and $\chi_1 \cdots \chi_n = \chi_0$, then $0 < m_i < d_i$ and $\frac{m_i}{d_i} + \cdots + \frac{m_n}{d_n} \in \mathbf{Z}$.

Let us consider then $A(d_1, \cdots, d_n) := |\{(m_1, \cdots, m_n) \in \mathbf{Z}^n \mid 0 < m_i < d_i \text{ and } \frac{m_i}{d_i} + \cdots + \frac{m_n}{d_n} \in \mathbf{Z}\}|$, i.e., the number of sumands in the sum of characters that estimates N above.

Since $|\tau(\chi_i, \psi)| = q^{1/2}$ by §**3.(1.3.3)** and $|\chi_1(a_i)| = 1$, we obtain N satisfies

$$|N - q^{n-1}| \leq (1 - \frac{1}{q}) q^{n/2} A(d_1, \cdots, d_n).$$

Lemma (2.7) Let $A_n(d) = |\{(m_1, \cdots, m_n) \in \mathbf{Z}^n \mid 0 \leq m_i < d \text{ and } m_1 + \cdots + m_n \equiv 0(d)\}|$. Then

$$A_n(d) = \frac{(d-1)}{d}[(d-1)^{n-1} - (-1)^{n-1}]$$

Proof: We have $A_1(d) = 0, A_2(d) = d - 1$. For $n > 2$ we see $(m_1, \cdots, m_n) \in A_n(d)$ iff $0 < m_i < d$ and $-m_n \equiv m_1 + \cdots + m_{n-1}(d)$ with $m_1 + \cdots + m_{n-1} \not\equiv 0(d)$.

This is, there are $(d-1)^{n-1} - A_{n-1}(d)$ possibilities for $(m_1, \cdots, m_n)$, and these determine m_n. Hence $A_n(d) = (d-1)^{n-1} - A_{n-1}(d)$. Then

$$A_n(d) = \sum_{k=1}^{n-1} (-1)^{n+1-k}(d-1)^k = \frac{(d-1)}{d}[(d-1)^n - (-1)^{n-1}].$$

□

Corollary (2.8) Let $d|q-1$. Let N be the number of solutions in $\mathbf{F}_q^n$ of the equation $X_1^d + \cdots + X_n^d = 0$. Then

$$|N - q^{n-1}| \leq (1 - \frac{1}{d})[(d-1)^{n-1} - (-1)^{n-1}](1 - \frac{1}{q}) q^{n/2}.$$

□

3. Some Bounds for $s_d(\mathbf{F}_p)$

Now we are able to establish the first results on the higher level of $\mathbf{F}_q$ of degree $d \geq 2$ ($q = p^n, p > 2$ prime), as well as the bound announced in §**3.1.**

Let $s_d(q) = s_d(\mathbf{F}_q)$.

(1*) It suffices to consider $d|q-1$:

By §**3.(2.3)** we have $(\mathbf{F}_q^*)^d = (\mathbf{F}_q^*)^{d^*}$ for $d^* = (d, q-1)$, thus $s_d(q) = s_{d^*}(q)$.

(2*) $s_d(q) \leq min\{\, p-1\,,\, d\,\}$:

This results from writing $-1 = \sum_{i=1}^{p-1} 1^d$ and from Chevalley-Warning's theorem §**3.(2.2)** for $X_1^d + \cdots + X_{d+1}^d = 0$.

(3*) $s_d(q) \leq \frac{d}{2} + 1$ if $(q,d) \neq (p, p-1)$:

See [**T**].

(4*) Let $d|p-1$. Then $s_d(p) = p-1$ iff $d = p-1$:

Assume $s_d(p) = p-1$ and $d < p-1$. Then §**3.(2.1)** gives $\sum_{x \in \mathbf{F}_p^*} x^d = 0$, thus $s_d(p) \leq p-2$ which contradicts our assumption. On the other hand $s_{p-1}(p) = p-1$ clearly.

In particular, if $2^r|p-1$

$$s_{2^r}(p) = p-1 \text{ iff } p = 2^r + 1 \text{ is a Fermat prime}$$

(5*) (**[PAR 2]**) Let $d = 2^r k$ with $r \geq 1$ and $(2,k) = 1$. Then

i) $s_d(q) = 1$ iff $s_{2^r}(q) = 1$:

If $-1 = a^d, a \in \mathbf{F}_q^*$, then $-1 = (a^k)^{2^r}$. On the other hand if $-1 = a^{2^r}, a \in \mathbf{F}_q^*$, then $-1 = (-1)^k = a^d$.

ii) $s_{2^r}(q) = 1$ iff $q \equiv 1(2^{r+1})$:

If $-1 = a^{2^r}, a \in \mathbf{F}_q^*$ Then $1 = a^{2^{r+1}}$. Thus $2^{r+1}|q-1$. On the other hand, let $q-1 \equiv 0(2^{r+1})$ and $\mathbf{F}_q^* =< \omega|\omega^{q-1} = 1 >$, then $-1 = \omega^{(q-1)/2} = \omega^{2^r \cdot \ell}$, some $\ell \in \mathbf{Z}$. The result follows by i).

The study of higher levels is embedded in the theory of Homogeneous Forms of degree $d > 2$, however, here it does not seem to exist the adecuate tools to attack the problem like in the quadratic case. The only general result one could establish, is consequence of well known theorems on the estimates of the number of solutions of additive equations over finite fields, which we have already settled in §**3.2.** and seems to be long ignored.

Theorem (3.1) Let $d > 2, d|q-1$. Then

$$q \geq d^{2s/(s-1)} \implies s_d(q) \leq s.$$

Proof: By §**3.(2.8)** we have the number N of solutions in $\mathbf{F}_q^{s+1}$ of the equation $X_0^d + X_1^d + \cdots + X_s^d = 0$ satisfies

$$|N - q^s| \leq A(d)(1 - \frac{1}{q})q^{(s+1)/2}$$

where

$$A(d) = (1 - \frac{1}{d})[(d-1)^s - (-1)^s].$$

Hence, there exists a nontrivial solution if we have

$$N \geq q^s - A(d)(q-1)q^{(s-1)/2} > 1$$

i.e.

$$\left(\frac{q^s - 1}{q-1}\right) q^{-(s-1)/2} > A(d).$$

But noticing that

$$\frac{1+q+\cdots+q^{s-1}}{q^{(s-1)/2}} > q^{(s-1)/2} \text{ and } d^s > A(d)$$

then

$$q^{(s-1)/2} \geq d^s \implies N > 1.$$

Thus

$$q \geq d^{2s/(s-1)} \implies s_d(q) \leq s.$$

□

We have obtained, as expected, bounding $s_d(q)$ by a function of the size of the field $\mathbf{F}_q$. For example: $s_d(q) \leq 2$ if $q \geq d^4$.

However, computer results ([**AK**] and ourselves) have shown this bound far from being optimal, since $s_d(q)$ seems to be already 2 for much smaller fields then those predicted.

This and other results will be given next.

Remark (3.2) $N[X_0^d + X_1^d + X_2^d] > 1$ if $q^2 - A(d)(q-1)q^{1/2} > 1$, where $A(d) = \frac{(d-1)}{d}[(d-1)^2 - (-1)^2] = (d-1)(d-2)$, *i.e.*, $q^{1/2} + q^{-1/2} > (d-1)(d-2) \implies N > 1$. Thus $q \geq (d-1)^2(d-2)^2 - 1 \implies s_d(q) \leq 2$.

□

§ 4. Known Results

Parnami, Agrawal, Rajwade and Pall have published several works on higher levels, with the ones we started our work.

1. <u>On $s_d(\mathbf{F}_q)$</u>

Here we just want to present some examples, calculated by these authors and ourselves, using § **3.(3.2)** and ad-hoc proofs or computer calculations for the missing cases.

Proposition (1.1) ([PAR1])

$$s_4(q) = \begin{cases} 1 & \text{if } q \equiv 1(8) \text{ or } q = 2^n \\ 4 & \text{if } q = 5 \\ 3 & \text{if } q = 29 \\ 2 & \text{otherwise} \end{cases}$$

Proof: Let $q = p^n, n \geq 1$. We have $s_4(q) = 1$ for $p = 2$ or $q \equiv 1(8)$ by §**3.3.**(**5***). If $q \equiv 3(8), s_4(q) = 2$ since then $p \equiv 3(4)$ and $n \equiv 1(2)$, thus $-1 = x_1^2 + x_2^2$ is solvable in $\mathbf{F}_p$, but $x^2 = x^{2+q-1}$ in $\mathbf{F}_q$ and $2 + q - 1 \equiv 0(4)$, so actually $-1 \in \sum_1^2 \mathbf{F}_q^4$. If $q \equiv 5(8), q \equiv 5, 13, 21(24)$ and we have: **i)** $q \equiv 21(24) \Longrightarrow 3|q \Longrightarrow p = 3$, hence $s_4(q) \leq p - 1 = 2$. **ii)** $q \equiv 13(24) \Longrightarrow 3|q - 1$, then $s_4(q) = 2$ by §**2.1.**(**3**). **iii)** $q \equiv 5(24) \Longrightarrow s_4(q) \leq 2$ if $q \geq (4-1)^2(4-2)^2 - 1 = 35$ by § **3.(3.2)**, thus the only chances for $s_4(q)$ to be greater that 2 are $q = 5, 29$. One finds $s_4(5) = 4(-1 \equiv 4 \cdot 1^4(5))$ and $s_4(29) = 3(-1 \equiv 1^4 + 6^4 + 8^4(29))$.

□

Proposition (1.2) ([PAR2])

$$s_6(q) = \begin{cases} 1 & \text{if } q \equiv 1(4) \text{ or } q = 2^n \\ 6 & \text{if } q = 7 \\ 3 & \text{if } q = 31, 67, 79, 139, 223 \\ 2 & \text{otherwise} \end{cases}$$

$$s_8(q) = \begin{cases} 1 & \text{if } q \equiv 1(16) \text{ or } q = 2^n \\ 4 & \text{if } q = 5, 41 \\ 3 & \text{if } q = 29, 89, 137, 233, 761 \\ 2 & \text{otherwise} \end{cases}$$

$$s_{10}(q) = \begin{cases} 1 & \text{if } q \equiv 1(4) \text{ or } q = 2^n \\ 10 & \text{if } q = 11 \\ 3 & \text{if } q = 71, 131, 311, 431, 491, 911 \\ 2 & \text{otherwise} \end{cases}$$

Proposition (1.3)

$$s_{12}(\mathbf{F}_q) = \begin{cases} 1 & \text{if } q \equiv 1(8) \text{ or } q = 2^n \\ 12 & \text{if } q = 13 \\ 6 & \text{if } q = 7 \\ 4 & \text{if } q = 5, 229 \\ 3 & \text{if } q = 29, 31, 61, 67, 79, 139, 157, \\ & \qquad 223, 277, 349, 421, 661, 733, \\ & \qquad 877, 1069, 1453, 1669, 1741 \\ 2 & \text{otherwise} \end{cases}$$

2. On $s(k_\wp), k_\wp$ the $\wp$-adic completion of an Algebraic Number Field

Let k be an algebraic number field, O the ring of integers in $k, \wp \subseteq O$ a prime ideal over p and $k_\wp$ the $\wp$-adic completion of k at $\wp$. Let $\nu = \nu_\wp$ be the $\wp$-adic valuation on $k_\wp, A = \{x \in k_\wp | \nu(x) \geq 0\}$ the complete discrete valuation ring and $m = \{x \in A | \nu(x) > 0\}$ the maximal ideal in A.

(1) $O \subseteq k \subseteq k_\wp \Longrightarrow s_d(O) \geq s_d(k) \geq s_d(k_\wp)$.

(2) $k_\wp =$ Quot $(A), A \supseteq m$ principal $\Longrightarrow s_d(k_\wp) = s_d(A)$: Clearly $s_d(k_\wp) \leq s_d(A)$. Now if $-1 = c_1^d + \cdots + c_s^d, c_i \in k_\wp$, then multiplying by the denominators, there exist $\alpha_0, \alpha_1, \cdots, \alpha_n \in A$ such that $0 = \alpha_0^d + \alpha_1^d + \cdots + \alpha_s^d$. Then, simplifying if necessary, we may assume $m \dagger (\alpha_j)$ some $0 \leq j \leq s$, hence $\alpha_j \in A^*$, the subgroup of units in A, and $s_d(A) \leq s$. Thus $s_d(k_\wp) \geq s_d(A)$.

(3) $O \longrightarrow O/\wp^i \Longrightarrow s_d(O) \geq s_d(O/\wp^i) \geq s_d(O/\wp^{i-1}) \geq \cdots$ for all $i \geq 1$.

(4) $A/m^i \cong O/\wp^i$ for all $i \geq 1$:

It follows since $A/m \cong O/\wp$.

(5) Hensel's Lemma: Let $f(X_1, \cdots, X_n) \in A[X_1, \cdots, X_n]$ where A is a complete discrete valuation ring, with maximal ideal m. Let $\gamma_1, \cdots, \gamma_n$ in A , $\delta \geq 0$ and some $1 \leq j \leq n$ such that

$$f(\gamma_1, \cdots, \gamma_n) \equiv 0(m^{2\delta+1})$$

$$\frac{\partial f}{\partial X_j}(\gamma_1, \cdots, \gamma_n) \equiv 0(m^{\delta}); \not\equiv 0(m^{\delta+1}).$$

Then, there exist $\theta_1, \cdots, \theta_n \in A$ with $f(\theta_1, \cdots, \theta_n) = 0$ and $\theta_i \equiv \gamma_i(m^{\delta})$ for all $1 \leq i \leq n$.

(6) $s_d(k_\wp) \geq s_d(O/\wp^i)$ for all $i \geq 1$:

By $A \longrightarrow A/m^i, s_d(A) \geq s_d(A/m^i)$ Now **(2)** and **(4)** give $s_d(k_\wp) = s_d(A) \geq s_d(O/\wp^i)$ for all $i \geq 1$.

This last remark shows that the increasing sequence in $\mathbf{N}, \{s_d(O/\wp^i)\}_{i\geq 1}$, is bounded by $s_d(k_\wp)$. Indeed we proved

Theorem (2.1) Let $d = p^r k$ with $r \geq 0$ and $(p, k) = 1$.

Let $\wp^e || p$. Then $s_d(k_\wp)$ is finite, moreover

$$s_d(k_\wp) = s_d(O/\wp^{2re+1})$$

Proof: We have $A \subseteq k_\wp$ is a complete discret valuation ring with $m \subseteq A$ maximal ideal, $m \bigcap O = \wp$, $\wp \bigcap \mathbf{Z} = (p)$ and $(p) = \wp^e \mathcal{A}$, $\mathcal{A} \subseteq O$ an ideal with $\wp \nmid \mathcal{A}$.

By **(6)**, it suffices to prove $s_d(k_\wp) \leq s_d(O/\wp^{2re+1})$ Let $\beta_0, \beta_1, \cdots, \beta_s$ in O be such that

$$\beta_0^d + \cdots + \beta_s^d \equiv 0(\wp^{2re+1}), \wp \nmid (\beta_i) \text{ some } 0 \leq i \leq s.$$

Thus $d\beta_i^{d-1} \equiv 0(\wp^{re}), \not\equiv 0(\wp^{re+1})$ since $\wp^{re} || (p^r)$. Hence by Hensel's Lemma there exist $\alpha_0, \alpha_1, \cdots, \alpha_s$ in A such that $\alpha_0^d + \cdots + \alpha_s^d = 0$ in A. Then $s_d(k_\wp) \leq s_d(O/\wp^{2re+1})$ and the result follows.

□

In particular, in the case $k = \mathbf{Q}$ we obtain

$$s_d(\mathbf{Q}_p) = s_d(\mathbf{Z}/p^{2r+1}\mathbf{Z}) \quad \text{if} \quad d = p^r k, r \geq 1$$

$$s_d(\mathbf{Q}_p) = s_d(\mathbf{F}_p) \qquad \text{if} \quad p \dagger d.$$

The only results from the literature on higher levels of $\mathbf{Q}_p$, as far as we know, state:

(i) Ramanujam's Theorem ([**Ra**]) Let $d = p^r k, (p,k) = 1$. Let

$$\nu = \begin{cases} r+1 & \text{if} \quad p \neq 2 \\ r+2 & \text{if} \quad p = 2 \end{cases}, \quad \delta = \begin{cases} 1 & \text{if } k = p-1 \\ 0 & \text{otherwise} \end{cases}$$

Then

$$s_d(\mathbf{Q}_p) \leq \begin{cases} d & \text{if } p \dagger d \\ \left(\frac{p^\nu - 1}{p-1}\right) k + \delta - 1 & \text{if } p | d \end{cases}$$

(ii) Revoy's Theorem ([**R**]) $s_{2^r}(\mathbf{Q}_2) = 2^{r+2} - 1$.

Hence, the study of higher levels of the rings of integers modulo p^ℓ would give us the higher levels of the class of the p-adic fields.

We will give an elementary proof for (ii) in § **1.(3.4)**, Chapter II.

3. On $s_d(\mathbf{F}_q)$ for d a Power of 2

Let $d = 2^r, r \geq 1$ and let $h = h(q)$ the dyadic valuation of $q-1$, i.e., $q - 1 = 2^h \ell\,, (2, \ell) = 1$. Then by §**3.3.**(**1***) and §**3.3.**(**5***)

$$s_{2^r}(\mathbf{F}_q) = \begin{cases} 1 & \text{iff} \quad r < h \\ 1 < s_{2^h}(\mathbf{F}_q) \leq 2^h & \text{if} \quad r \geq h \end{cases}$$

this is, the increasing sequence of higher levels $\{s_{2^r}(\mathbf{F}_q)\}_{r \geq 1}$ takes only two values and it stabilizes from $r = h(q)$ on.

Recently, Amice and Kahn have found very interesting theoretical and experimental results on $s(q) = s_{2^h}(\mathbf{F}_q)$:

Theorem (3.1) ([AK]) Let $s(q) = s_{2^h}(\mathbf{F}_q) > 1$. Then

1) $\frac{\sqrt{q^s}-\sqrt{q^{-s}}}{\sqrt{q}-\sqrt{q^{-1}}} > \left(1 - \frac{1}{2^n}\right)\left[(2^h-1)^s - (-1)^s\right] \implies s(q) \leq s.$

In particular,

$$q \geq 2^{2hs/(s-1)} \implies s(q) \leq s.$$

2) $q \geq (2^h-1)^2(2^h-2)^2 \implies s(q) = 2.$

3) $q \geq (2^h-1)(2^{2h} - 3\cdot 2^h + 3) \implies s(q) \leq 3.$

4) $q = p^3 \implies s(q) \leq 3.$

5) $q \neq p, p^3 \implies s(q) = 2.$

Proof: The first four statements are direct consequences of § **3.(2.8)**. Now for 5), let $q = p^n$. If $n \equiv 0(2)$, then it may be proved by induction, that 3 divides $q-1$, if $p \neq 3$. Then there exist a cubic root of unity in the field and thus $s(q) = 2$ by § **2.1.(3)** and clearly $s(q) = 2$ if $p = 3 =$ char $\mathbf{F}_q$. If $n \equiv 1(2)$, then 2^h divides $q - 1 = (p-1)(1 + p + \cdots + p^{n-1})$ iff 2^h divides $p-1$. Thus for $n \geq 5$ we have $q \geq p^5 \geq 2^{5h} > 2^{4h}$, then $s(q) = 2$ by 1).

□

Also, experimental results from **[AK]** show that $s(p^3) = 2$, for all primes p up to 101.711.873 and $s(p) \leq 12$, for all $p < 10^9$ (excluding Fermat primes). Actually they find $s(p) = 2$ as soon as $p \geq 2^{2,72h(p)}$ for $p < 10^9, h(p) \leq 7$ (instead of $p \geq 2^{4h(p)}$ by § **3.(3.1)**, Chapter I).

4. Open Problems

The preceding results leave as main open problems, the determination of $s_d(p)$, the d^{th} level of the prime finite fields for $p > 2$ and more generally, the determination of $s_d(\mathbf{Z}/p^\ell\mathbf{Z}), \ell \geq 1$, since these would also provide the d^{th} levels of the p-adic fields $\mathbf{Q}_p$.

Chapter II: $s_d(\mathbf{Z}/p^\ell\,\mathbf{Z})$ for $d \geq 2$

In this Chapter we will establish the main result on the d^{th} level of the prime finite fields $\mathbf{F}_p, p > 2$, and its generalization to the rings of integers modulo p^ℓ, $\ell > 1$.

It will be seen that $s_d(\mathbf{F}_p)$ can be completely determined by the coefficients $\alpha_2, \alpha_3, \cdots, \alpha_{d/2+1}$ of the *period equation* $T^d + T^{d-1} + \alpha_2 T^{d-2} + \cdots + \alpha_d \in \mathbf{Z}[T]$ associated to the factorization $p - 1 = de$.

In this way, a striking relation has been found between the higher levels problem and the old problem of cyclotomy.

The generalization of this result has been also achieved for $s_d(\mathbf{Z}/p^\ell\mathbf{Z}), \ell > 1$ when $p > 2$, while $s_d(\mathbf{Z}/2^\ell\mathbf{Z})$ is found directly.

§ 1. Preliminaries

We start studying the congruences modulo p^ℓ, $\ell \geq 1$, $p \geq 2$ a prime :

$$X_1^d + \cdots + X_n^d \equiv c \pmod{p^\ell} \quad \text{where } c \in \mathbf{Z} \text{ and } d \geq 2 \text{ even}.$$

Moreover, all through this chapter it will be considered the following factorization of d respect to p :

$$d = p^r k \quad \text{with } p \nmid k \text{ and } \begin{cases} r \geq 0,\ k \text{ even} & \text{if } p \neq 2 \\ r \geq 1,\ k \geq 1 & \text{if } p = 2 \end{cases}$$

We will write for short just $d = p^r k$.

We say a solution $(x_1, \cdots, x_n)$ of a congruence is *primitive* if $p \nmid x_i$ for some $1 \leq i \leq n$.

For $c = -1$ it may be easily seen, it is enough to consider solutions $(x_1, \cdots, x_n)$ with x_i in the group of units of integers modulo p^ℓ, for all $i = 1, \cdots, n$. Thus we will state first the structure of these groups ([IR], [H]).

1. The Structure of the Group of Units mod p^ℓ

Let $\mathcal{U}_\ell = (\mathbf{Z}/p^\ell\,\mathbf{Z})^*$ be the group of units mod p^ℓ, $\ell \geq 1$, $p \geq 2$ a prime.

$\ell = 1$:

In this case $\mathcal{U}_\ell$ is the multiplicative group $\mathbf{F}_p^*$ of the nonzero elements of the finite field with p elements and has order $\varphi(p) = p-1$. Thus if $a \in \mathbf{F}_p^*$, the order of a divides $p-1$. Actually for any $d|p-1$, there exists $a \in \mathbf{F}_p^*$ with order d. In particular for $d = p-1$. Hence

Theorem (1.1) $\mathbf{F}_p^*$ is a cyclic group.

□

We will call an element $\omega \in \mathbf{F}_p^*$ a *primitive root mod p* if ω generates $\mathbf{F}_p^*$. Then one has $\omega^{p-1} \equiv 1(\text{ mod } p)$.

$\ell > 1$:

In this case $\mathcal{U}_\ell$ has order $\varphi(p^\ell) = p^{\ell-1}(p-1)$. One finds descompositions of $\mathcal{U}_\ell$ as direct product of cyclic groups.

Structure of $\mathcal{U}_\ell$ for $p \neq 2$:

Theorem (1.2) $\mathcal{U}_\ell \cong \mathcal{U}_\ell' \times \mathcal{U}_\ell''$ direct product of cyclic groups given by

$$\mathcal{U}_\ell' = \left\langle \omega(\text{mod } p^\ell) |\, \omega \equiv \omega_o^{p^{\ell-1}} (\text{mod } p^\ell),\ \omega_o \text{ a primitive root mod } p \right\rangle$$

with $|\mathcal{U}_\ell'| = p-1$.

$$\mathcal{U}_\ell'' = \left\langle 1 + ap(\text{mod } p^\ell) | a \neq 0(\text{mod } p) \right\rangle$$

with $|\mathcal{U}_\ell''| = p^{\ell-1}$.

Moreover $\mathcal{U}_\ell$ is cyclic given by

$$\mathcal{U}_\ell = \left\langle \tilde{\omega}(\text{mod } p^\ell) | \tilde{\omega}^{p-1} \equiv 1(\text{mod } p),\ \tilde{\omega}^{p-1} \not\equiv 1(\text{mod } p^2) \right\rangle.$$

□

Remark (1.3) The generator of $\mathcal{U}_\ell'$ is completely determined by the properties $\omega \equiv \omega_o(\bmod p)$, ω_o a primitive root mod p and $\omega^{p-1} \equiv 1(\bmod p^\ell)$. In this case we say ω is a *normalized primitive root mod p*. Thus, a generator of $\mathcal{U}_\ell$ is $\tilde{\omega} \equiv \omega(1+p)^\alpha(\bmod p^\ell)$ where ω is a normalized primitive root mod p and $\alpha \not\equiv 0(\bmod p)$.

Structure of $\mathcal{U}_\ell$ for $p = 2$:

Theorem (1.4) $\mathcal{U}_\ell \cong \mathcal{U}_\ell' \times \mathcal{U}_\ell''$ direct product of cyclic groups given by

$$\mathcal{U}_\ell' = < -1 > \text{ with } |\mathcal{U}_\ell'| = 2,$$

$$\mathcal{U}_\ell'' = < 1 + a \cdot 2^2 (\bmod 2^\ell) | a \not\equiv 0(\bmod 2) > \text{ with } |\mathcal{U}_\ell''| = 2^{\ell-2}.$$

□

Remark (1.5) For $\ell \geq 3$,

$$(\mathbf{Z}/2^\ell\,\mathbf{Z})^* \cap \{a(\bmod 2^\ell) | a \equiv 1(\bmod 4)\} = \mathcal{U}_\ell'$$

is cyclic of order $2^{\ell-2}$, generated by $5 \pmod{2^\ell}$. For $\ell = 1, 2$ the group of units mod 2^ℓ are cyclic, generated by $1 \pmod 2$ and $3 \pmod 4$, and these are the only cases since $\pm 5 \pmod{2^\ell}$ has order $2^{\ell-2}$.

These theorems follow mainly from the following useful properties on congruences modulo p^ℓ ([**IR**], p. 40-45, or, [**H**] p. 77-84):

Lemma (1.6)

(i) If $\ell \geq 1$, then

$$a \equiv b \pmod{p^\ell} \Rightarrow a^p \equiv b^p (\bmod p^{\ell+1})$$

(ii) If $\nu \geq 1$, then

$$a \equiv 1 (\mathrm{mod}\, p^{\nu}) \;\Rightarrow\; a^{p^{\ell-\nu}} \equiv 1 (\mathrm{mod}\, p^{\ell}), \quad \forall \ell \geq \nu$$

(iii) If $p \neq 2$, then

$$a \equiv 1 + bp \pmod{p^2} \;\Rightarrow\; a^{p^{\ell-1}} \equiv 1 + bp^{\ell} (\mathrm{mod}\, p^{\ell+1}), \quad \forall \ell \geq 1$$

(iv) If $p = 2$, then

$$a \equiv 1 + b \cdot 2^2 (2^3) \;\Rightarrow\; a^{2^{\ell-2}} \equiv 1 + b \cdot 2^{\ell} (2^{\ell+1}), \quad \forall \ell \geq 2$$

□

2. Congruences mod p^{ℓ}

Let

$$G_{\ell} = \begin{cases} (\mathbf{Z}/p^{\ell}\,\mathbf{Z})^*, \ \ell \geq 1 & \text{if} \quad p \neq 2 \\ (\mathbf{Z}/2^{\ell}\,\mathbf{Z})^* \cap \{a \equiv 1 (\mathrm{mod}\, 4)\}, \ \ell \geq 2 & \text{if} \quad p = 2 \end{cases}$$

Then G_{ℓ} is a cyclic group of order

$$|G_{\ell}| = \begin{cases} p^{\ell-1}(p-1) & \text{if} \quad p \neq 2 \\ 2^{\ell-2} & \text{if} \quad p = 2 \end{cases}$$

Let $d \geq 2$. Recall

$$d = p^r k \ , \ p \nmid k \text{ and } \begin{cases} r \geq 0, \ k \text{ even} & \text{if} \quad p \neq 2 \\ r \geq 1, \ k \geq 1 & \text{if} \quad p = 2 \end{cases}$$

And define

$$\nu = \begin{cases} r+1 & \text{if} \quad p \neq 2 \\ r+2 & \text{if} \quad p = 2 \end{cases}$$

Then $|G_{\ell}| = p^{\ell+r-\nu}(p-1)$, and the following relations between congruences mod p^{ν} and congruences mod p^{ℓ}, $\ell \geq \nu$ may be proved (**[Sch2]**).

Lemma (2.1) Let $a \not\equiv 0(\text{mod } p)$ be such that $X^d \equiv a(\text{mod } p^\nu)$ is solvable. Then so is $X^d \equiv a(\text{mod } p^\ell)$ for all $\ell \geq 1$.

Proof. Notice that $a \not\equiv 0(\text{mod } p)$ and $X^d \equiv a(\text{mod } p)$ solvable, gives $a \in G_\ell$, (i.e. $a \equiv 1(\text{mod } 4)$ if $p = 2$). Thus, let ω be a generator of G_ℓ, of order $p^{\ell+r-\nu}(p-1)$ and $a \equiv \omega^\alpha(\text{mod } p^\ell)$. One has

$$x \equiv \begin{cases} \omega^\eta(\text{mod } p^\ell), & p \neq 2 \\ (-1)^\sigma\omega^\eta(\text{mod } 2^\ell), & p = 2 \end{cases}$$

$$y \equiv \begin{cases} \omega^\varepsilon(\text{mod } p^\ell), & p \neq 2 \\ (-1)^\rho\omega^\varepsilon(\text{mod } 2^\ell), & p = 2 \end{cases}$$

are solutions of $x^d \equiv a(\text{mod } p^\nu)$ and $y^d \equiv a(\text{mod } p^\ell)$ iff $d\eta \equiv \alpha(\text{mod } |G_\nu|)$ and $d\varepsilon \equiv \alpha(\text{mod } |G_\ell|)$, and this holds iff $(d, |G_\nu|)|\alpha$ and $(d, |G_\ell|)|\alpha$. Since it is enough to show the result for $\ell \geq \nu$ and thus $(d, |G_\ell|) = (p^r k, p^{\ell+r-\nu}(p-1)) = p^r(k, p-1) = (d, |G_\nu|)$, then the result follows.

□

Lemma (2.2) If $X_1^d + \cdots + X_n^d \equiv c \ (\text{mod } p^\nu)$ has a primitive solution, then the number N of primitive solutions of $X_1^d + \cdots + X_n^d \equiv c(\text{mod } p^\ell)$ satisfies $N \geq p^{(\ell-\nu)(n-1)}$, for all $\ell \geq \nu$. In particular $N \geq 1$, for all $\ell \geq \nu$.

Proof: Let $x_1^d + \cdots + x_n^d \equiv c \ (\text{mod } p^\nu)$ with $x_1 \not\equiv 0(\text{mod } p)$ be a primitive solution. Then $c - (x_2^d + \cdots + x_n^d) \not\equiv 0(\text{mod } p)$. Choose $y_i \equiv x_i(\text{mod } p^\nu)$ for $i = 2, \cdots, n$. It can be easily seen that there are $p^{(\ell-\nu)(n-1)}$ possible choices for the $y_i's$ modulo p^ℓ, $\ell \geq \nu$, and for each choice the congruence

$$X^d \equiv c - (y_2^d + \cdots + y_n^d)(\text{mod } p^\nu)$$

has $X = x_1$ as a solution. Thus by §1.(2.1) above this congruence is solvable mod p^ℓ, for all $\ell \geq 1$. In particular the number N of primitive solutions mod p^ℓ satisfies $N \geq p^{(\ell-\nu)(\nu-1)} \geq 1$, for all $\ell \geq \nu$.

□

3. On the Higher Levels of $\mathbf{Z}/p^\ell\,\mathbf{Z}$

Let $d = p^r k$ as above and

$$s_d(\mathbf{Z}/p^\ell\,\mathbf{Z}) = min\{\, s \in \mathbf{N} \mid a_1^d + \cdots + a_s^d \equiv -1 (\mathrm{mod}\ p^\ell)\,\}.$$

If the congruence $X_1^d + \cdots + X_s^d \equiv -1 (\mathrm{mod}\ p^\nu)$ has a (necessarily) primitive solution, then by §1.(2.2) above it has a primitive solution mod p^ℓ, for all $\ell \geq \nu$. Thus

$$s_d(\mathbf{Z}/p^\ell\,\mathbf{Z}) \leq s_d(\mathbf{Z}/p^\nu\,\mathbf{Z}) \quad \text{for all} \quad \ell \geq \nu.$$

Since trivially a solution mod p^ℓ is a solution mod p^ν for $\nu \leq \ell$, we obtain

Proposition (3.1) Let $d = p^r k$ and let $\nu = r+1$ if $p \neq 2$, $\nu = r+2$ if $p = 2$. Then

$$s_d(\mathbf{Z}/p^\ell\,\mathbf{Z}) = s_d(\mathbf{Z}/p^\nu\,\mathbf{Z}) \quad \text{for all} \quad \ell \geq \nu.$$

□

Thus, it suffices to find $s_d(\mathbf{Z}/p^\ell\,\mathbf{Z})$ for $\ell \leq \nu$.

On the other hand, if $d > 2$ for $p = 2$,

$$d = p^r k \geq \nu = \begin{cases} r+1 & \text{if } p \neq 2 \\ \\ r+2 & \text{if } p = 2 \end{cases}$$

then

$$x \equiv 0 (\mathrm{mod}\ p) \Longrightarrow x^d \equiv 0 (\mathrm{mod}\ p^\nu) \equiv 0 (\mathrm{mod}\ p^\ell) \text{ for all } \ell \leq \nu.$$

Hence it suffices to consider solutions of $X_1^d + \cdots + X_s^d \equiv -1 (\mathrm{mod}\ p^\ell)$ with $x_i \not\equiv 0 (\mathrm{mod}\ p)$, i.e., x_i in the group of units mod p^ℓ, for all $\ell \leq \nu$. Thus we have proved

Proposition (3.2) Let $d = p^r k$ $(d > 2$ if $p = 2)$. And let ν as above. Then

$$s_d(\mathbf{Z}/p^\ell\,\mathbf{Z}) = s_d((\mathbf{Z}/p^\ell\,\mathbf{Z})^*) \quad \text{for all} \quad \ell \leq \nu.$$

□

Now in case $p \neq 2$ we find:

Then $G_\ell = (\mathbf{Z}/p^\ell\mathbf{Z})^*$ is cyclic and thus by § **3.(2.3)**, Chapter I

$$s_d(G_\ell) = s_{d^*}(G_\ell) \text{ if } d^* = (d, |G_\ell|).$$

Hence it suffices to study the d^{th} level of G_ℓ for $d|\,|G_\ell|$, i.e., for

$$d = p^r k \text{ with } k|p-1 \text{ and } 0 \leq r \leq \ell + r - \nu = \ell - 1$$

since $\nu = r+1$. But then $\ell \geq \nu$. This together with propositions §**1.(3.1)** and §**1.(3.2)** give it suffices to find the d^{th} level of G_ℓ for $\ell = \nu = r + 1$.

Thus, we have found a relation among the higher levels of the ring of integers mod p^ℓ for $p \neq 2$.

Theorem (3.3) Let $p \neq 2$ and $G_\ell = (\mathbf{Z}/p^\ell\,\mathbf{Z})^*$. Let $d = p^r k$, with $k|p-1$ without loss of generality and $\nu = r + 1 \geq 1$. Then

$$s_d(\mathbf{Z}/p^\ell\,\mathbf{Z}) = \begin{cases} s_d(G_\nu) & \text{if} \quad \ell \geq \nu \\ \\ s_{p^{\ell-1}k}(G_\ell) & \text{if} \quad \ell < \nu \end{cases}$$

In particular

$$s_2(\mathbf{Z}/p^\ell\,\mathbf{Z}) = s_2(\mathbf{F}_p) \text{ for all } \ell \geq 1.$$

□

Thus for $p \neq 2$ we see the problem is solved if we may find

$$s_d(G_{r+1}) \text{ for } d = p^r k, \quad k | p-1.$$

In case $p = 2$:

The d^{th} level of the ring of integers mod 2^ℓ may be determined in an elementary way.

Theorem (3.4) Let $d = 2^r k > 2$, $\nu = r + 2$. Then

$$s_d(\mathbf{Z}/2^\ell\,\mathbf{Z}) = \begin{cases} 2^\nu - 1 & \text{if } \ell \geq \nu \\ \\ 2^\ell - 1 & \text{if } \ell < \nu \end{cases}$$

and

$$s_2(\mathbf{Z}/2^\ell\,\mathbf{Z}) = \begin{cases} 4 & \text{if } \ell \geq 3 \\ \\ 2^\ell - 1 & \text{if } \ell = 1, 2 \end{cases}$$

Proof: Let $a_1^d + \cdots + a_s^d \equiv -1 (\text{mod } 2^\nu)$ with s minimal. Then $a_i \equiv 1 (\text{mod } 2)$ for all $i = 1, \cdots, s$ since $d > 2$ gives $d > \nu$ and then $a \equiv 0 (\text{mod } 2)$ gives $a^d \equiv 0 (\text{mod } 2^\nu)$.

Hence by §1.(1.4)(iv), $a_i^{2^r} \equiv 1 (\text{mod } 2^{r+2})$ for all $i = 1, \cdots s$.

Thus $a_i^d \equiv 1 (\text{mod } 2^\ell)$ for all $\ell \leq \nu$. It follows that $s \equiv -1 (\text{mod } 2^\ell)$ for all $\ell \leq \nu$. The minimality of s gives $s = 2^\ell - 1$ for all $\ell \leq \nu$. Now §1.(3.1) gives $s = 2^\nu - 1$ for all $\ell \geq \nu$.

If $d = 2$ one finds

$$s_2(\mathbf{Z}/2\,\mathbf{Z}) = 1\ ,\ s_2(\mathbf{Z}/4\,\mathbf{Z}) = 3\ ,\ s_2(\mathbf{Z}/8\,\mathbf{Z}) = 4,$$

and by §1.(3.1) with $d = p = 2$ and $\nu = r + 2 = 3$

$$s_2(\mathbf{Z}/2^\ell\mathbf{Z}) = s_2(\mathbf{Z}/8\,\mathbf{Z}) = 4 \quad \text{for all } \ell \geq 3.$$

Hence the result follows.

□

4. On the Period Equation for $d|p-1$

The method of Gauss to solve the cyclotomic equation $X^p - 1 = 0$ (related to the constructibility of a regular polygon of p sides, "... principles upon which the division of a circle into p parts depends ...", [Gauss diary, March 30, 1796]), leads to the concept of the cyclotomic periods and its properties which we would like to include here for completeness ([B]):

Let p be an odd prime. Then the roots of the irreducible cyclotomic polynomial

$$1 + X + X^2 + \cdots + X^{p-1} = 0 \tag{1}$$

are given by the powers of a primitive p^{th} root of unity

$$\zeta, \zeta^2 \cdots \zeta^{p-1}. \tag{2}$$

Now, if ω is a primitive root modulo p, then $1, \omega, \cdots, \omega^{p-2}$ represents, in some order, the numbers $1, 2, \cdots, p-1 (\text{mod } p)$. Then the set (2) may also be written as

$$\zeta, \zeta^{\omega} \cdots \zeta^{\omega^{p-2}}. \tag{3}$$

In this way, the roots of (1) are arranged in such a way that each one is the ω^{th} power of the previous one, as the first is the ω^{th} power of the last.

If $p-1$ is factored, say, $p-1 = de$, then the $p-1$ roots in (3) may be distributed in d groups of e members.

$$\zeta, \zeta^{\omega^{2d}}, \cdots, \zeta^{\omega^{(e-1)d}}$$

$$\zeta^{\omega}, \zeta^{\omega^{d+1}}, \zeta^{\omega^{2d+1}}, \cdots, \zeta^{\omega^{(e-1)d+1}}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\zeta^{\omega^{d-1}}, \zeta^{\omega^{2d-1}}, \zeta^{3d-1}, \cdots, \zeta^{de-1}$$

satisfying each group, that each of their roots is the ω^{dth} power of the previous one, as the first is the ω^{dth} power of the last.

These groups define sums called *periods*:

$$\begin{aligned}
\eta_0 &= \zeta + \zeta^{\omega^d} + \zeta^{\omega^{2d}} + \cdots + \zeta^{\omega^{(e-1)d}} \\
\eta_1 &= \zeta^{\omega} + \zeta^{\omega^{d+1}} + \zeta^{\omega^{2d+1}} + \cdots + \zeta^{\omega^{(e-1)d+1}} \\
\cdots &\quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
\eta_{d-1} &= \zeta^{\omega^{d-1}} + \zeta^{\omega^{2d-1}} + \zeta^{\omega^{3d-1}} + \cdots + \zeta^{\omega^{de-1}}
\end{aligned}$$

which satisfy the following properties:

(i) If we replace the root ζ by $\zeta^{\omega^{nd}}$, then the periods do not change. More generally, if we replace ζ by ζ^{ω^h}, then the periods $\eta_0, \eta_1, \cdots, , \eta_{d-1}$ become $\eta_h, \eta_{h+1}, \cdots, \eta_{h+d-1}$, i.e., $\eta_h, \cdots, \eta_{d-1}, \eta_0, \eta_1, \cdots, \eta_{h-1}$.

(ii) The distribution of all roots of (1) into periods does not depend on the choice of ω, the primitive root modulo p.

(iii) All periods are numerically different: Otherwise, assume $\eta_h = \eta_k$, some $0 \leq h \neq k \leq d-1$. Then

$$\zeta^{\omega^h} + \zeta^{\omega^{d+h}} + \cdots + \zeta^{\omega^{(e-1)d+h}} - \zeta^{\omega^k} - \zeta^{\omega^{d+k}} - \cdots - \zeta^{\omega^{(e-1)d+k}} = 0$$

is a nontrivial equation for ζ, since in different periods, different roots of (1) occur. Now dividing by ζ, since no power of ω is zero, we obtain an equation $f(\zeta) = 0$, with $\deg f$ at most $p-2$. This contradicts the fact that (1) , the irreducible polynomial of ζ, has degree $p-1$.

(iv) Any integral polynomial function of the roots of (1), invariant by substitution of ζ by ζ^{ω^d}, is an integral linear function of the periods: Let

$$f(\zeta) = a + a_0\zeta + a_1\zeta^{\omega} + \cdots + a_{p-2}\zeta^{\omega^{p-2}} \text{ with } a, a_0, \cdots, a_{p-2} \in \mathbf{Z},$$

be such that $f(\zeta) = f(\zeta^{\omega^d})$. Hence

$$f(\zeta^{\omega^d}) = f(\zeta^{\omega^{2d}}) = \cdots = f(\zeta^{\omega^{(e-1)d}})$$

and then

$$ef(\zeta) = ea + a_0\eta_0 + a_1\eta_1 + \cdots + a_{p-2}\eta_{p-2}.$$

An important consequence of this fact is that the product of any two periods, being an integral function invariant by substitution of ζ by ζ^{ω^d}, is a linear function of the periods, i.e.,

$$\eta_0\eta_k = (k,0)\eta_0 + (k,1)\eta_1 + \cdots + (k,d-1)\eta_{d-1} + \delta_k e, \quad 0 \leq k \leq d-1$$

where

$$(k,h) = |\{(t,z), 0 \leq t,z \leq e-1 | 1 + \omega^{dt+k} \equiv \omega^{dz+h}(p)\}|, \ 0 \leq k,h \leq d-1$$

and

$$\delta_k = \begin{cases} 1 \text{ if } e \equiv 0(2) \text{ and } k = 0, \text{ or }, e \equiv 1(2) \text{ and } k = d/2 \\ 0 \text{ otherwise} \end{cases}$$

Moreover replacing ζ by ζ^{ω^m}, we obtain

$$\eta_m\eta_{m+k} = (k,0)\eta_m + (k,1)\eta_{m+1} + \cdots + (k,d-1)\eta_{m+d-1} + \delta_k e$$

so that every product may be obtained in this way.

The cyclotomic problem is solved if we have the coefficients of the period equation or the d^2 cyclotomic constants $(k,h), 0 \leq k,h \leq d-1$.

(v) Every integral function of the roots of (1), invariant by substitution of ζ by ζ^{ω}, has an integral value: Just consider $d = 1$, then the only period is $\eta_0 = \zeta + \zeta^{\omega} + \cdots + \zeta^{\omega^{p-1}} = -1$. Now let F be an integral function of the roots of (1), then $F(\zeta) = F(\zeta^{\omega}) = F(\zeta^{\omega^d})$, hence, an integral linear function of η_0, thus $F(\zeta) \in \mathbf{Z}$.

Hence by (i), the symetric functions of the periods are integers, i.e.,

$$P(X) = (X - \eta_0)(X - \eta_1)\cdots(X - \eta_{d-1}) \in \mathbf{Z}[X]$$

(vi) The *period equation*

$$P(X) = \Pi_{i=0}^{d-1}(X - \eta_i) \in \mathbf{Z}[X]$$

is irreducible: Let $\tilde{P}(X)|P(X), \tilde{P}(X)$ nonconstant. Then $\tilde{P}(\eta_k) = 0$ for some $0 \leq k \leq d-1$. But then $\tilde{P}(\eta_k) = P(\zeta^{\omega^k} + \cdots) = f(\zeta) = 0$, some $f(X) \in \mathbf{Z}[X]$. Thus the irreducible polynomial of ζ divides f. Hence $f(\zeta^{\omega^h}) = 0$ for all roots of (1). Then $\tilde{P}(\eta_{k+h}) = \tilde{P}(\zeta^{\omega^{k+h}} + \cdots) = f(\zeta^{\omega^h}) = 0$, i.e., $\tilde{P}$ has all periods as roots, i.e., $\tilde{P}(X) = P(X)$ is irreducible.

Now we can settle the following lemma which we will need in §**2**.

Lemma (4.1) Let $d|p-1$. Let $\mathbf{Q}(\zeta)$ be the cyclotomic field of the p^{th} roots of unity, and $\mathcal{U} = (\mathbf{F}_p^*)^d$ the subgroup of the d^{th} powers in $\mathbf{F}_p^*$. Let $\eta_0, \eta_1, \cdots, \eta_{d-1} \in \mathbf{Q}(\zeta)$ be the periods for $d|p-1$. Then

$$\text{Fix } \mathcal{U} = \mathbf{Q}(\eta_0).$$

Proof: It is well known that Gal $(\mathbf{Q}(\zeta)/\mathbf{Q}) \cong \mathbf{F}_p^*; \sigma_a : \zeta \longrightarrow \zeta^a$. Now let $L =$ Fix $\mathcal{U}$, the elements of $\mathbf{Q}(\zeta)$ fixed by $\mathcal{U}$. Then by construction $\eta_0 \in L$. Moreover, by Galois correspondence $\text{Gal}(L/\mathbf{Q}) \cong \mathbf{F}_p^*/\mathcal{U}$, thus $[L : \mathbf{Q}] = [\mathbf{F}_p^* : \mathcal{U}] = d$. But η_0 is one of the d periods for $d|p-1$. Then by (vi) above, $[\mathbf{Q}(\eta_0) : \mathbf{Q}] = d$. Hence $L = \mathbf{Q}(\eta_0)$.

□

Thus, we see that the subfield of $\mathbf{Q}(\zeta)$ of degree d over $\mathbf{Q}$, is associated to $\mathcal{U}$ in the Galois correspondence and hence to the d^{th} level problem.

Moreover we could prove the following generalization, which we will need in §3.

Lemma (4.2) Let ζ be a primitive root of the cyclotomic equation $X^{p^{r+1}}-1=0$. Then their $\varphi(p^{r+1})=p^r(p-1)$ primitive roots may be ordered in $d=p^rk$, $k|p-1$, different periods of $e=\frac{(p-1)}{k}$ terms

$$\eta_i=\zeta^{\omega^i}+\zeta^{\omega^{d+i}}+\cdots+\zeta^{\omega^{(e-1)d+i}}\ ,\ 0\leq i\leq d-1$$

which are all the roots of an irreducible polynomial over $\mathbf{Z}$. Moreover let $\mathcal{U}_{r+1}=G_{r+1}^d$ and $L=\text{Fix }\mathcal{U}_{r+1}$. Then

$$L=\mathbf{Q}(\eta_0).$$

Proof: We have the minimal polynomial of ζ over $\mathbf{Q}$ is

$$\text{Irr }(\zeta,\mathbf{Q})(X)=X^{(p-1)p^r}+X^{(p-2)p^r}+\cdots+X^{p^r}+1$$

and

$$\text{Gal }(\mathbf{Q}(\zeta)/\mathbf{Q})\cong(\mathbf{Z}/p^{r+1}\,\mathbf{Z})^*=G_{r+1};\sigma_a:\zeta\longrightarrow\zeta^a(a\text{ modulo }p^{r+1},(a,p)=1).$$

If $L=\text{Fix }\mathcal{U}_{r+1}$, where $\mathcal{U}_{r+1}$ is the subgroup of d^{th} powers in G_{r+1}, then $\text{Gal}(L/\mathbf{Q})\cong G_{r+1}/\mathcal{U}_{r+1}$. Thus $[L:\mathbf{Q}]=[G_{r+1}:\mathcal{U}_{r+1}]=d$. Moreover by construction, $\eta_0=\zeta+\zeta^{\omega^d}+\cdots+\zeta^{\omega^{(e-1)d}}\in L$.

We want to show $\eta_i\neq\eta_j$ for all $0\leq i\neq j\leq d-1$. Assume $\eta_i=\eta_j$ for some $0\leq i\neq j\leq d-1$. Then

$$X^{\omega^i}+X^{\omega^{d+i}}+\cdots+X^{\omega^{(e-1)d+i}}-X^{\omega^j}-\cdots-X^{\omega^{(e-1)d+j}}=0$$

is a nontrivial equation satisfied by ζ. Dividing by ζ we have, there exist $f(X) \in \mathbf{Z}[X]$ such that $f(\zeta) = 0$, with $\deg f \leq p^{r+1} - 2$ and all $2e$ powers of X in f being different. Then $\mathrm{Irr}(\zeta, \mathbf{Q})(X) | f(X)$.

If $r = 0$, then $p - 1 \leq p - 2$, which is a contradiction.

If $r > 0$, let $g(X) \in \mathbf{Z}[X]$ be such that

$$f(X) = (1 + X^{p^r} + \cdots + X^{(p-1)p^r}) g(X)$$

Since $\deg g + (p-1)p^r \leq p^{r+1} - 2$, then $\deg g \leq p^r - 2$. Let $g(X) = \sum_{k=0}^{\ell} g_k X^k$ with $\ell \leq p^r - 2$.

Thus

$$f(X) = \mathrm{Irr}(\zeta, \mathbf{Q})(X) g(X) = \sum_{k=0}^{\ell} g_k X^k + \sum_{k=0}^{\ell} g_k X^{p^r+k} + \cdots + \sum_{k=0}^{\ell} g_k X^{(p-1)p^r+k}$$

is a sum of $p\ell_0$ some $\ell_0 \leq \ell$, different powers of X, since $\ell \leq p^r - 2$.

Then

$$2e = p\ell_0 \implies p | e = (p-1)/k$$

which is a contradiction too. Therefore all d periods are different. Now since $\eta_0 \in L$ and $\eta_i = \sigma_{\omega^i}(\eta_0)$, then $\mathrm{Irr}\,(\eta_0, \mathbf{Q}) = \Pi_{i=0}^{d-1}(X - \eta_i) \in \mathbf{Z}[X]$ and $L = \mathbf{Q}(\eta_0)$.

□

§2. $s_d(\mathbf{F}_p)$

1. Preliminaries

Let $\mathbf{F}_p$ be the prime finite field with p elements, $p \neq 2$ a prime. To find the d^{th} level of $\mathbf{F}_p$, $s_d(p) = s_d(\mathbf{F}_p)$, we must study the congruence mod p

$$X_1^d + \cdots + X_n^d \equiv -1 (\mathrm{mod}\ p),$$

where we know it is enough to consider $d | p - 1$.

Let $\mathcal{U} = (\mathbf{F}_p^*)^d$ be the subgroup of the d^{th} powers of elements in $\mathbf{F}_p^*$, of order $e = (p-1)/d$. We want to consider all possible sums of elements in $\mathcal{U}$, in order to find the minimal length s of the sums which represent -1.

One way to do this is considering the formal series

$$f(T) = \frac{1}{1 - T\sum_{u\in\mathcal{U}} X^u} \in k[[T]] \ , \ k \text{ some field},$$

since then

$$f(T) = \sum_{k=0}^{\infty} \left(T \sum_{u\in\mathcal{U}} X^u \right)^k = \sum_{k=0}^{\infty} \left(\sum_{u_1,\cdots,u_k\in\mathcal{U}} X^{u_1+\cdots+u_k} \right) T^k,$$

and thus, with X such that $X^i = X^j$ iff $i \equiv j(\text{mod } p)$, i.e., $X \neq 1$ such that $X^p = 1$, we obtain

$$f(T) = \sum_{j=0}^{p-1} \left(\sum_{k=0}^{\infty} N(k,j)T^k \right) X^j \in k[[T]] \ , \ k = K[X]/(X^p - 1) \text{ for some field } K,$$

where

$$N(k,j) = |\{(u_1,\cdots,u_k) \in \mathcal{U}^k | u_1 + \cdots + u_k \equiv j(\text{mod } p)\}|.$$

In this way a first expression for $s_d(p)$ is attained:

$$s_d(p) = min\{\ k \mid u_1 + \cdots + u_k \equiv -1(\text{mod } p),\ u_i \in \mathcal{U}\} = min\{\ k \mid N(k,p-1) \neq 0\},$$

i.e.

$$s_d(p) = \text{ord}_T(F(T)) \quad \text{where} \quad F(T) = \sum_{k=0}^{\infty} N(k,p-1)T^k$$

and ord_T being the usual valuation on the ring of formal series ($\text{ord}_T(\sum_{k=0}^{\infty} a_k T^k) = \min\{k | a_k \neq 0\}$).

On the other hand, considering the following well known result, an election for K may be done, which enables us to calculate $N(k,p-1)$ otherwise.

Proposition (1.1) Let K be a field containing a cyclic group of order n and let C be a cyclic group of the same order. Then the group ring $K[C]$ is isomorphic to the direct product of n copies of K.

Proof: Let $<\zeta|\zeta^n = 1> \subseteq K$ and let $C =< X|X^n = 1 >$. It suffices to find an orthogonal system of idempotents in $K[C]$. For $\rho \in <\zeta>$ let us define

$$e_\rho = \frac{1}{n}\sum_{i=0}^{n-1} \rho^{-i} X^i \in K[C].$$

It is easy to see that $e_\rho^2 = e_\rho$, $e_\rho \cdot e_{\rho'} = 0$ if $\rho \neq \rho'$, and $\sum_{\rho \in <\zeta>} e_\rho = 1$. Thus, this is such a system and we may write

$$\begin{aligned} X = 1 \cdot X = \left(\sum_\rho e_\rho\right) X &= \sum_\rho \left(\tfrac{1}{n}\sum_{i=0}^{n-1} \rho^{-i} X^i\right) X \\ &= \sum_\rho \rho \cdot \tfrac{1}{n}\sum_{i=0}^{n-1} \rho^{-(i+1)} X^{i+1} \\ &= \sum_\rho \rho e_\rho \end{aligned}$$

and more generally

$$\begin{aligned} h(X) = \sum_{i=0}^{n-1} h_i X^i &= \sum_{i=0}^{n-1} h_i \left(\sum_\rho \rho e_\rho\right)^i \\ &= \sum_{i=0}^{n-1} h_i \left(\sum_\rho \rho^i e_\rho\right) \\ &= \sum_\rho \left(\sum_{i=0}^{n-1} h_i \rho^i\right) e_\rho \\ &= \sum_\rho h(\rho) e_\rho \end{aligned}$$

Thus, $\varphi : K[C] \longrightarrow \Pi_o^{n-1} K$, $h(x) \longrightarrow (h(\rho))_{\rho \in <\zeta>}$, is an isomorphism.

□

Notice that $\mathbf{Q}(\zeta)$, where ζ is a primitive p^{th} root of unity, contains a cyclic group of order p. Hence

$$\mathbf{Q}(\zeta)[X]/(X^p-1) \cong \mathbf{Q}(\zeta)[< X/X^p = 1 >] \cong \Pi_0^{p-1}\mathbf{Q}(\zeta).$$

Then, let $K = \mathbf{Q}(\zeta)$ be the cyclotomic field generated by ζ a fixed primitive p^{th} root of unity, i.e., $\zeta \neq 1$ such that $\zeta^p = 1$, and $k = \mathbf{Q}(\zeta)[X]/(X^p-1)$. Constructing an orthogonal system of idempotents in k

$$e_\rho = \frac{1}{p}\sum_{i=0}^{p-1} \rho^{-i}X^i, \text{ where } \rho \in < \zeta >$$

one obtains by §2.(1.1)

$$h(X) = \sum_{\rho \in <\zeta>} h(\rho)e_\rho \text{ for all } h(x) \in k.$$

Applying this to

$$f(T) = \frac{1}{1-TS(X)} \in k[[T]] \text{, where } S(X) = \sum_{u \in \mathcal{U}} X^u \in k$$

we obtain

Lemma (1.2) Let $N(k,j) = |\{(u_1, \cdots, u_k) \in \mathcal{U}^k | u_1 + \cdots + u_k \equiv j (\text{ mod } p)\}|$ where $\mathcal{U} = (\mathbf{F}_p^*)^d$, and $d|p-1$. Let ζ is a fixed primitive p^{th} root of unity. Then

$$N(k,j) = \frac{1}{p}\sum_{\rho \in <\zeta>} S(\rho)^k \bar{\rho}^j \text{ where } S(\rho) = \sum_{u \in \mathcal{U}} \rho^u$$

Proof: We have

$$f(T) = \frac{1}{1-TS(X)} = \sum_{k=0}^{\infty} S(X)^k T^k \text{, where } S(X) = \sum_{u \in \mathcal{U}} X^u$$

thus by §2.(1.1)

$$S(X) = \sum_{\rho \in <\zeta>} S(\rho)e_\rho \text{, with } e_\rho = \frac{1}{p}\sum_{i=0}^{p-1} \bar{\rho}^i X^i$$

and then

$$\begin{aligned} f(T) &= \sum_{k=0}^{\infty} \left(\sum_{\rho \in <\zeta>} S(\rho) e_\rho\right)^k T^k \\ &= \sum_{k=0}^{\infty} \left(\sum_{\rho \in <\zeta>} S(\rho)^k e_\rho\right) T^k \\ &= \sum_{k=0}^{\infty} \frac{1}{p} \left(\sum_{i=0}^{p-1} \left(\sum_{\rho \in <\zeta>} S(\rho)^k \bar{\rho}^i\right) X^i\right) T^k \\ &= \sum_{i=0}^{p-1} \left(\sum_{k=0}^{\infty} \frac{1}{p} \left(\sum_{\rho \in <\zeta>} S(\rho)^k \bar{\rho}^i\right) T^k\right) X^i \end{aligned}$$

Hence

$$N(k,j) = \frac{1}{p} \sum_{\rho \in <\zeta>} S(\rho)^k \bar{\rho}^j.$$

□

In this way, an expression for $N(k,j) \in \mathbf{Q}(\zeta)$ has been found, that relates the higher levels problem of $\mathbf{F}_p$ with the cyclotomic field $\mathbf{Q}(\zeta)$, which has a isomorphic to $\mathbf{F}_p^*$ Galois group.

2. The Main Result

The main role in the expressions of $N(k,j)$ is played by $S(\zeta)$ where ζ is a (primitive) p^{th} root of unity.

Lemma (2.1) Let $K = \mathbf{Q}(\zeta)$ be the cyclotomic field generated by ζ a primitive p^{th} root of unity. Let $G = \mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q}) \cong \mathbf{F}_p^*$, $\mathcal{U} = (\mathbf{F}_p^*)^d \leq G$, and $d|p-1$. Then

$$\mathrm{Fix}\,\mathcal{U} = \mathbf{Q}(S(\zeta)) \quad \text{where} \quad S(\zeta) = \sum_{u \in \mathcal{U}} \zeta^u$$

Proof: We have

$$S(\zeta) = \sum_{u \in \mathcal{U}} \zeta^u = \eta_0$$

is one of the d roots of the period equation for $d|p-1$. Thus the result follows by §1.(4.1).

□

Now we are able to prove the following striking result on the d^{th} levels of prime finite fields.

Theorem (2.2) Let $\mathbf{F}_p$ be the prime finite field with $p > 2$ elements and let $d > 1$ be such that $d|p-1$. Let

$$P(T) = T^d + \alpha_1 T^{d-1} + \alpha_2 T^2 + \cdots + \alpha_d \in \mathbf{Z}[T]$$

be the gaussian period equation of degree d. Then

$$s_d(p) = min\{\ n \mid (n+1)\alpha_{n+1} - (1 + n\frac{(p-1)}{d})\alpha_n \neq\ 0\}$$

Proof: We have $s_d(p) = \mathrm{ord}_T(F(T))$ where

$$F(T) = \sum_{k=0}^{\infty} N(k, p-1)T^k$$

and

$$N(k, p-1) = \frac{1}{p}\sum_{\rho} S(\rho)^k \rho \quad \text{with} \quad S(\rho) = \sum_{u \in \mathcal{U}} \rho^u$$

and ρ running through the p^{th} roots of unity in $\mathbf{Q}(\zeta)$. Then

$$\begin{aligned} pN(k, p-1) &= S(1)^k + \textstyle\sum_{\rho \neq 0} S(\rho)^k \rho \\ &= |\mathcal{U}|^k + \textstyle\sum_{i=1}^{p-1} S(\zeta^i)^k \zeta^i \\ &= |\mathcal{U}|^k + \textstyle\sum_{x \in \mathbf{F}_p^*/\mathcal{U}} \sum_{u \in \mathcal{U}} S(\zeta^{ux})^k \zeta^{ux} \\ &= |\mathcal{U}|^k + \textstyle\sum_{x \in \mathbf{F}_p^*/\mathcal{U}} S(\zeta^x)^k \sum_{u \in \mathcal{U}} \zeta^{ux} \\ &= |\mathcal{U}|^k + \textstyle\sum_{x \in \mathbf{F}_p^*/\mathcal{U}} S(\zeta^x)^{k+1} \end{aligned}$$

Now since $\mathbf{F}_p^*/\mathcal{U} \cong \mathrm{Gal}(L/\mathbf{Q})$; $\sigma_x : \zeta \longrightarrow \zeta^x$, where $L = \mathbf{Q}(S(\zeta))$ by §2.(2.1), then

$$N(k,p-1) = \frac{1}{p}\left(|\mathcal{U}|^k + t_{L/\mathbf{Q}}(S(\zeta)^{k+1}\right),$$

$t_{L/\mathbf{Q}}$ the usual trace on $L/\mathbf{Q}$. Thus

$$\begin{aligned} F(T) &= \textstyle\sum_{k=0}^{\infty} \frac{1}{p}\left(|\mathcal{U}|^k + \sum_{x\in\mathbf{F}_p^*/\mathcal{U}} \sigma_x(S(\zeta))^{k+1}\right) T^k \\ &= \textstyle\sum_{k=0}^{\infty} \frac{1}{p}\left(|\mathcal{U}|^k T^k + \sum_{x\in\mathbf{F}_p^*/\mathcal{U}} \sigma_x(S(\zeta))\sigma_x(S(\zeta))^k T^k\right) \\ &= \frac{1}{p}\left(\frac{1}{1+|\mathcal{U}|T} + \sum_{x\in\mathbf{F}_p^*/\mathcal{U}} \frac{\sigma_x(S(\zeta))}{1-\sigma_x(S(\zeta))T}\right). \end{aligned}$$

Now let

$$P(T) = \mathrm{irr}(S(\zeta),\mathbf{Q})(T) = \Pi_{x\in\mathbf{F}_p^*/\mathcal{U}}\left(T - \sigma_x(S(\zeta))\right).$$

Then its reciprocal polynomial is

$$H(T) = T^d P(T^{-1}) = \Pi_{x\in\mathbf{F}_p^*/\mathcal{U}}\left(1 - \sigma_x(S(\zeta))T\right)$$

and satisfies

$$H'(T) = \sum_{x\in\mathbf{F}_p^*/\mathcal{U}} -\sigma_x(S(\zeta))\Pi_{\substack{y\in\mathbf{F}_p^*/\mathcal{U}\\ y\neq x}}\left(1-\sigma_y(S(\zeta))T\right),$$

thus

$$\frac{H'(T)}{H(T)} = -\sum_{x\in\mathbf{F}_p^*/\mathcal{U}} \frac{\sigma_x(S(\zeta))}{1-\sigma_x(S(\zeta))T}\ .$$

Then

$$F(T) = \frac{1}{p}\left(\frac{1}{1-|\mathcal{U}|T} - \frac{H'(T)}{H(T}\right) = \frac{1}{p}\left(\frac{H(T)-(1-|\mathcal{U}|T)H'(T)}{(1-|\mathcal{U}|T)H(T)}\right).$$

Moreover if

$$P(T) = T^d + \alpha_1 T^{d-1} + \alpha_2 T^{d-2} + \cdots + \alpha_d \in \mathbf{Z}[X]$$

where

$$\alpha_1 = -\sum_{x \in \mathbf{F}_p^*/\mathcal{U}} \sigma_x(S(\zeta)) = -\sum_{z \in \mathbf{F}_p^*} \zeta^z = -(-1) = 1$$

then

$$H(T) = \alpha_d T^d + \cdots + T + 1 \ \in \mathbf{Z}[X]$$

and

$$\begin{aligned} H(T) - (1 - |\mathcal{U}|T)H'(t) \ &= \ \alpha_d(1 + d|\mathcal{U}|)T^d + \cdots + \\ &+ (\alpha_k(1 + k|\mathcal{U}|) - (k+1)\alpha_{k+1})T^k + \\ &+ \cdots + (1 + |\mathcal{U}| - 2\alpha_2)T, \end{aligned}$$

and it holds

$$\mathrm{ord}_T(H(T)) = \mathrm{ord}_T(1 - |U|T) = 0.$$

With this we have finally obtained

$$s_d(p) = \mathrm{ord}_T(F(T)) = \mathrm{ord}_T(H(T) - (1 - |\mathcal{U}|T)H'(T))$$

i.e.

$$s_d(p) = min\{\ k \mid (k+1)\alpha_{k+1} - (1 + k\frac{(p-1)}{d})\alpha_k \neq 0\ \}$$

□

This seems to be the first general result on the higher levels of prime finite fields and provides a very striking relation to the problem of cyclotomy.

Although finding the coefficients of the period equation is an old problem, for $s_d(p)$ we only need to know $\alpha_2, \cdots, \alpha_{d/2+1}$ since by [**T**], $s_d(p) \leq d/2 + 1$, if $d \neq p - 1$.

Moreover, experimental results have shown that the main part of the problem is solved if we can decide which primes p have $s_d(p) > 2$, i.e., if we can decide when $3\alpha_3 \neq (1 + 2\frac{(p-1)}{d})\alpha_2$. Thus the first coefficients α_2 and α_3 give already a great deal of information.

By using gaussian sums one may find expressions for the coefficients of the period equation. This will be done in the next chapter.

Now we will establish a generalization of §2.(2.2) to the rings of integers mod p^ℓ, for $\ell > 1$ and $p \neq 2$, which is the case still missing.

§3. $s_d(\mathbf{Z}/p^\ell\mathbf{Z})$, $\ell \geq 1$

1. Generalization of the Main Result to $\mathbf{Z}/p^\ell\,\mathbf{Z}$, $\ell \geq 1$ for $p \neq 2$

In § 1.(3.3) we established the levels of the rings of integers mod $p^\ell (\ell > 1, p \neq 2)$ in terms of

$$s_d((\mathbf{Z}/p^{r+1}\mathbf{Z})^*) \quad \text{for} \quad d = p^r k \quad (d \text{ even}, \ r \geq 0, k|p-1).$$

And in this case, a generalization of the main result can be achieved as follows.

For all $0 \leq j \leq r$, let

$$G_{r+1-j} = (\mathbf{Z}/p^{r+1-j}\mathbf{Z})^*$$

and

$$\mathcal{U}_{r+1-j} = G_{r+1-j}^{d_j} \quad \text{where} \quad d_j = p^{r-j}k, k|p-1.$$

Thus, $G_1 = \mathbf{F}_p^*$ and $\mathcal{U}_1 = \mathcal{U} = (\mathbf{F}_p^*)^k$.

Recall that $\mathcal{U}_i \equiv \mathcal{U}(\bmod p^i)$, hence $|\mathcal{U}_i| = |\mathcal{U}| = (p-1)/k$.

Let ζ be a primitive $p^{(r+1)th}$ root of unity. Thus ζ^{p^j} is a primitive $p^{(r+1-j)th}$ root and it holds

$$\text{Gal}\,(\mathbf{Q}(\zeta^{p^j})/\mathbf{Q}) \cong G_{r+1-j}; x : \zeta^{p^j} \to \zeta^{p^j x} (x \bmod p^{r+1-j}, (x,p) = 1)$$

and

$$\mathbf{Q}(s(\zeta^{p^j})) = \text{ Fix } \mathcal{U}_{r+1-j}, \text{ where } s(\zeta^{p^j}) = \sum_{u \in \mathcal{U}_{r+1-j}} \zeta^{p^j u}$$

as we proved in § **1.(4.2).** This defines $r+1$ period equations

$$P_j(T) = \Pi_{x \in G_{r+1-j}/\mathcal{U}_{r+1-j}}(T - s(\zeta^{p^j})^x)$$

of degree $d_j = p^{r-j}k$.

Then we have found

Theorem (1.1) Let $G_{r+1} = (\mathbf{Z}/p^{r+1})^*$ and $d = p^r k$ even where $p > 2$ prime, $r \geq 0$ and $k|p-1$. Let

$$H(T) = \alpha_{d_*} T^{d_*} + \alpha_{d_*-1} T^{d_*-1} + \cdots + \alpha_1 T + 1 \in \mathbf{Z}[X]$$

be the product of the $r+1$ reciprocal polynomials of the period equations $P_j(T)$ of degree $p^{r-j}k, 0 \leq j \leq r$, where $d_* = \left(\frac{p^{r+1}-1}{p-1}\right) k$. Then

$$s_d(G_{r+1}) = min\{n | (n+1)\alpha_{n+1} - (1 + n\frac{(p-1)}{k})\alpha_n \neq 0\}$$

Proof: As we want to study the congruence

$$X_1^d + \cdots + X_s^d \equiv -1 (\text{mod } p^{r+1}),$$

we will consider this time the formal series

$$f(T) = \frac{1}{1 - T\sum_{u \in \mathcal{U}_{r+1}} X^u}$$

since then

$$f(T) = \sum_{k=0}^{\infty} (T \sum_{u \in \mathcal{U}_{r+1}} X^u)^k = \sum_{k=0}^{\infty} \left(\sum_{u_1, \cdots, u_k \in \mathcal{U}_{r+1}} X^{u_1 + \cdots + u_k} \right) T^k$$

and thus, with X such that $X^i = X^j$ iff $i \equiv j (\text{mod} p^{r+1})$, we obtain

$$f(T) = \sum_{j=0}^{p^{r+1}-1} \left(\sum_{k=0}^{\infty} N(k,j) T^k \right) X^j \in \left(K[X]/(X^{p^{r+1}} - 1) \right) [[T]], K \text{ some field,}$$

where

$$N(k,j) = |\{(u_1, \cdots, u_k) \in \mathcal{U}_{r+1}^k | u_1 + \cdots + u_k \equiv j (\text{mod } p^{r+1})\}|.$$

Hence

$$s_d(G_{r+1}) = \text{ord}_T \left(\sum_{k=0}^{\infty} N(k, p^{r+1} - 1) T^k \right).$$

Now, let $K = \mathbf{Q}(\zeta)$, where ζ is a primitive $p^{(r+1)th}$ root of unity. Hence by §2.(1.1)

$$\mathbf{Q}(\zeta)[X]/(X^{p^{r+1}} - 1) \cong \Pi_0^{p^{r+1}-1} \mathbf{Q}(\zeta),$$

via an orthogonal system of idempotents given by

$$e_\rho = \frac{1}{p^{r+1}} \sum_{i=0}^{p^{r+1}-1} \rho^{-1} X^i ,$$

where $\rho \in < \zeta >$ runs through *all* $p^{(r+1)\,th}$ roots of unity. Then one may easily see that

$$S(X) = \sum_{u \in \mathcal{U}_{r+1}} X^u = \sum_{\rho \in <\zeta>} S(\rho) e_\rho \text{ , where } S(\rho) = \sum_{u \in \mathcal{U}_{r+1}} \rho^u$$

and hence

$$\begin{aligned} f(T) &= \textstyle\sum_{k=0}^{\infty} S(X)^k T^k \\ &= \textstyle\sum_{k=0}^{\infty} \left(\sum_{\rho \in <\zeta>} S(\rho)^k e_\rho \right) T^k \\ &= \textstyle\sum_{j=0}^{p^{r+1}} \frac{1}{p^{r+1}} \left(\sum_{k=0}^{\infty} \left(\sum_{\rho \in <\zeta>} S(\rho)^k \rho^{-j} \right) T^k \right) X^j. \end{aligned}$$

Then

$$N(k,j) = \frac{1}{p^{r+1}} \sum_{\rho \in <\zeta>} S(\rho)^k \rho^{-j}.$$

Just like in the case $r = 0$, the cyclotomic field $\mathbf{Q}(\zeta)$ and G_{r+1}, and more generally, $\mathbf{Q}(\zeta^{p^j})$ and G_{r+1-j} for $0 \leq j \leq r$, are related by Galois Theory and as seen in § **1.(4.2)**

$$\text{Gal } (\mathbf{Q}(S(\zeta^{p^j}))/\mathbf{Q}) \cong G_{r+1-j}/\mathcal{U}_{r+1-j}, \text{ where } S(\zeta^{p^j}) = \sum_{u \in \mathcal{U}_{r+1-j}} \zeta^{p^j u}.$$

These remarks lead us to find the sum $\sum = p^{r+1} N(k, p^{r+1} - 1)$:

$$\begin{aligned}
\sum &= \textstyle\sum_{i=0}^{p^{r+1}-1} S(\zeta^i)^k \zeta^i \\
&= S(1)^k + \sum_{\substack{i=0 \\ (i,p)=1}}^{p^{r+1}-1} S(\zeta^i)^k \zeta^i + \sum_{j=1}^{p^r-1} S(\zeta^{pj})^k \zeta^{pj} \\
&= |\mathcal{U}_{r+1}|^k + \textstyle\sum_{i \in G_{r+1}} S(\zeta^i)^k \zeta^i + \sum_{j=1}^{p^r-1} S(\zeta^{pj})^k \zeta^{pj} \\
&= |\mathcal{U}|^k + \textstyle\sum_{x \in G_{r+1}/\mathcal{U}_{r+1}} \sum_{u \in \mathcal{U}_{r+1}} S(\zeta^{xu})^k \zeta^{xu} + \sum_{j=1}^{p^r-1} S(\zeta^{pj})^k \zeta^{pj} \\
&= |\mathcal{U}|^k + \textstyle\sum_{x \in G_{r+1}/\mathcal{U}_{r+1}} S(\zeta^x)^{k+1} + \sum_{j=1}^{p^r-1} S(\eta^j)^k \eta^j
\end{aligned}$$

where $\eta = \zeta^p$ is a primitive $p^{r\,th}$ root of unity. Then by the remarks above we have

$$\text{Gal}(\mathbf{Q}(\eta)/(\mathbf{Q}) \cong G_r,$$

and

$$\text{Gal}(\mathbf{Q}(S(\eta))/\mathbf{Q}) \cong G_r/\mathcal{U}_r$$

where

$$\mathcal{U}_r = G_r^{d_r}, \;\; d_1 = p^{r-1}k.$$

Therefore, the second sum may be found by repeating the process used for the first. Thus repeating this process we obtain

$$\begin{aligned}\Sigma &= |\mathcal{U}|^k + \textstyle\sum_{x\in G_{r+1}/\mathcal{U}_{r+1}} S(\zeta^x)^{k+1} + \sum_{x\in G_r/\mathcal{U}_r} S(\zeta^{px})^{k+1} \\ &\quad + \textstyle\sum_{x\in G_{r-1}/\mathcal{U}_{r-1}} S(\zeta^{p^2x})^{k+1} + \cdots \\ &\quad \cdots + \textstyle\sum_{x\in G_1/\mathcal{U}_1} S(\zeta^{p^rx})^{k+1}.\end{aligned}$$

Hence

$$\begin{aligned}F(T) &= \textstyle\sum_{k=0}^{\infty} N(k, p^{r+1}-1)T^k \\ &= \textstyle\sum_{k=0}^{\infty} \frac{1}{p^{r+1}} \left(|\mathcal{U}|^k + \sum_{j=0}^{r} \sum_{x\in G_{r+1-j}/\mathcal{U}_{r+1-j}} S(\zeta^{p^jx})^{k+1}\right) T^k \\ &= \textstyle\frac{1}{p^{r+1}} \left(\frac{1}{1-|\mathcal{U}|T} + \sum_{j=0}^{r} \sum_{x\in G_{r+1-j}/\mathcal{U}_{r+1-j}} \frac{S(\zeta^{p^jx})}{1-S(\zeta^{p^jx})T}\right)\end{aligned}$$

Again, considering the reciprocal of

$$P_j(T) = \Pi_{x\in G_{r+1-j}/\mathcal{U}_{r+1-j}}(T - S(\zeta^{p^j})^x) \text{ of degree } p^{r-j}k$$

i.e.

$$H_{r+1-j}(T) = \Pi_{x\in G_{r+1-j}/\mathcal{U}_{r+1-j}}(1 - S(\zeta^{p^j})^x T).$$

which satisfies

$$\frac{H'_{r+1-j}(T)}{H_{r+1-j}(T)} = -\sum_{x\in G_{r+1-j}/\mathcal{U}_{r+1-j}} \frac{S(\zeta^{p^jx})}{1-S(\zeta^{p^jx})T}$$

we finally obtain

$$s_d(G_{r+1}) = \text{ ord }_T \left(\frac{1}{1-|\mathcal{U}|T} - \sum_{j=0}^{r} \frac{H'_{r+1-j}(T)}{H_{r+1-j}(T)}\right) = \text{ ord }_T \left(\frac{H(T) - (1-|\mathcal{U}|T)H'(T)}{(1-|\mathcal{U}|T)H(T)}\right).$$

where

$$H(T) = H_1(T)H_2(T)\cdots H_{r+1}(T).$$

Now since

$$\mathrm{ord}_T(1-|\mathcal{U}|T) = \mathrm{ord}_T(H_1(T)\cdots H_{r+1}(T)) = 0$$

then

$$s_d(G_{r+1}) = \mathrm{ord}_T(H-(1-\frac{(p-1)}{k}T)H'(T)).$$

Now let

$$H(T) = \alpha_{d_*}T^{d_*} + \alpha_{d_*-1}T^{d_*-1} + \cdots + \alpha_1(T) + 1 \in \mathbf{Z}[T]$$

where $d_* = \sum_{j=0}^{r} p^{r-j}k = (\frac{p^{r+1}-1}{p-1})k$. Then we obtain

$$s_d(G_{r+1}) = min\{n|(n+1)\alpha_{n+1} - (1+n\frac{(p-1)}{k})\alpha_n \neq 0\}.$$

□

Remark (1.2) Clearly for $r=0$ i.e. $G_{r+1} = \mathbf{F}_p^*$ we recover §**2(2.2)**.

2. Application to $\mathbf{Q}_p$

In § **4.2.**, Chapter I, we established that if $p^r||d$, then

$$s_d(\mathbf{Q}_p) = s_d(\mathbf{Z}/p^{2r+1}\mathbf{Z})$$

Now, by § **1.(3.3)** and § **1.(3.4)** we obtain

Theorem (2.1) Let $d = p^r k$ even, $r \geq 0, k|p-1$. Then

$$s_d(\mathbf{Q}_p) = \begin{cases} s_d(\mathbf{Z}/p^{r+1}\mathbf{Z}) & \text{if} \quad p \neq 2 \\ 2^{r+2}-1 & \text{if} \quad p=2, d>2 \\ 4 & \text{if} \quad p=2, d=2 \end{cases}$$

□

With this, an improvement of Ramanujam's result settled in §**4.2.** , Chapter I, is achieved.

Corollary (2.2) Let $d = p^r k$ even, $r \geq 0, k|p-1$ for $p > 2$ prime. Then

$$s_d(\mathbf{Q}_p) \leq \left(\frac{p^{r+1}-1}{p-1}\right) k - 1.$$

Proof: We have

$$s_d(\mathbf{Z}/p^{r+1}\mathbf{Z}) = \min \{1 \leq n \leq d_* | (n+1)\alpha_{n+1} - (1 + n\frac{(p-1)}{k})\alpha_n \neq 0\}$$

where $d_* = \left(\frac{p^{r+1}-1}{p-1}\right) k$. Thus the result follows.

□

This results enable us to give a list of examples of the values of $s_d(\mathbf{Q}_p)$, obtaining by the way, the quadratic level for the class of the p-adic fields:

Corollary (2.3)

$$s_2(\mathbf{Q}_p) = \left\{ \begin{array}{lll} 4 & \text{if} & p = 2 \\ s_2(\mathbf{F}_p) & \text{if} & p \neq 2 \end{array} \right\} = \left\{ \begin{array}{lll} 1 & \text{if} & p \equiv 1(4) \\ 2 & \text{if} & p \equiv 3(4) \\ 4 & \text{if} & p = 2 \end{array} \right.$$

$$s_4(\mathbf{Q}_p) = \left\{ \begin{array}{lll} 15 & \text{if} & p = 2 \\ s_4(\mathbf{F}_p) & \text{if} & p \neq 2 \end{array} \right\} = \left\{ \begin{array}{lll} 1 & \text{if} & p \equiv 1(8) \\ 3 & \text{if} & p = 29 \\ 4 & \text{if} & p = 5 \\ 15 & \text{if} & p = 2 \\ 2 & \text{otherwise} & \end{array} \right.$$

$$s_6(\mathbf{Q}_p) = \begin{cases} 7 & \text{if} \quad p = 2 \\ 2 & \text{if} \quad p = 3 \\ s_6(\mathbf{F}_p) & \text{otherwise} \end{cases}$$

$$s_8(\mathbf{Q}_p) = \begin{cases} 31 & \text{if} \quad p = 2 \\ s_8(\mathbf{F}_p) & \text{if} \quad p \neq 2 \end{cases}$$

$$s_{10}(\mathbf{Q}_p) = \begin{cases} 7 & \text{if} \quad p = 2 \\ 1 & \text{if} \quad p = 5 \\ s_{10}(\mathbf{F}_p) & \text{otherwise} \end{cases}$$

$$s_{12}(\mathbf{Q}_p) = \begin{cases} 15 & \text{if} \quad p = 2 \\ 8 & \text{if} \quad p = 3 \\ s_{12}(\mathbf{F}_p) & \text{otherwise} \end{cases}$$

□

Chapter III: On the explicit determination of $s_d(\mathbf{F}_p)$

In the preceding Chapter, the d^{th} level of the rings $\mathbf{Z}/p^\ell\mathbf{Z}, \ell \geq 1$ was found in terms of the coefficients of some period equations.

As examples, we would like to find here $s_d(\mathbf{F}_p)$ explicitly for $d \leq 8$. This will be done by obtaining the coefficients of the period equations in terms of character sums on $\mathbf{F}_p^*$.

This will also lead us to find beautiful formulae for the primes p with d^{th} level $s > 2$, in terms of parameters that appear in the representation of p, or multiples of p, by binary quadratic forms.

Further, since the main problem is now the determination of coefficients of the period equations, we will present an inductive method to express them in terms of some sums of Jacobi sums.

Even though it does not seem to be easy to calculate in general these last sums (we have found them only for $d \leq 8$), this provides a criteria to decide when $s_d(\mathbf{F}_p) > 2$.

In the case $\ell > 1$, the same theory may be applied, but now the character sums mod p^ℓ cannot be found explicitly, at least for $\ell \geq 3$. We believe that the recently known results **[G1 -2]** and **[GZ]** will permit us finding some explicit examples of $s_d(\mathbf{Z}/p^\ell\mathbf{Z})$ for $\ell > 1$.

§ 1. Preliminaries

Let

$$P_j(X) = \Pi_{a \in G_{r+1-j}/\mathcal{U}_{r+1-j}}(X - S(\zeta^{p^j})^a) \text{ and } \begin{cases} d = p^r k \text{ even }, k|p-1 \\ 0 \leq j \leq r \end{cases}$$

be the period equations of degree $p^{r-j}k$ defined in Chapter II, where ζ is a primitive

$p^{(r+1)th}$ root of unity , $G_{r+1-j} = (\mathbf{Z}/p^{r+1-j}\mathbf{Z})^*, \mathcal{U}_{r+1-j} = G_{r+1-j}^{d_j}$ and $S(\zeta^{p^j}) = \sum_{u \in \mathcal{U}_{r+1-j}} \zeta^{p^j u}$.

Since $S(\zeta^{p^j}), 0 \leq j \leq r$ and its conjugates turn out to be a character sum on G_{r+1-j}, we will present here the results from the theory of characters and character sums we will use to calculate the coefficients of these polynomials ([H], [BE]).

1. Characters mod p^ℓ

Let $(\mathbf{Z}/m\mathbf{Z})^*$ be the group of units mod m, $m \geq 1$ a rational integer.

A character on $(\mathbf{Z}/m\mathbf{Z})^*$ will be called a character mod m and all results seen in §**3.1.1.**, Chapter I on characters of finite abelian groups hold.

In particular, we will be interested in $m = p^\ell$ where $\ell \geq 1$ and $p > 2$ prime. We will denote as before $(\mathbf{Z}/p^\ell\mathbf{Z})^*$ by G_ℓ.

2. Gaussian Sums and Character Sums mod p^ℓ

Let χ_m be a character mod m and let ζ_m be a primitive m^{th} root of unity. Then

$$\tau(\chi_m, \zeta_m^a) = \sum_{\substack{x \bmod m \\ (x,m)=1}} \chi_m(x)\zeta_m^{ax}$$

is the Gaussian sum associated to the character χ_m, where a is a rational integer mod m.

The following properties hold for these sums ([H] p. 444-450):

(1) $\tau(\chi_m, \zeta_m^{ca}) = \bar{\chi}_m(c)\tau(\chi_m, \zeta_m^a)$ for c mod $m, (c, m) = 1$.

(2) Let $m_0 = \frac{m}{(a,m)}$ and $a_0 = \frac{a}{(a,m)}$. Then

$$f | m_0 \Longrightarrow \tau(\chi_m, \zeta_m^a) = \frac{\varphi(m)}{\varphi(m_0)} \mu\left(\frac{m_0}{f}\right) \chi\left(\frac{m_0}{f}\right) \bar{\chi}(a_0)\tau(\chi)$$

where φ and μ are the Euler and Möbius functions, $\chi = \chi_f, \tau(\chi) = \tau(\chi, \zeta_f)$ and f is the conductor of χ_m.

Via this reduction formula one only needs to find the Gaussian sums $\tau(\chi)$ for primitive characters χ mod p^ℓ, i.e., characters with conductor $f = p^\ell$.

(3) $\tau(\chi_m, \zeta_m^a) \neq 0 \Longleftrightarrow \frac{m_0}{f} \in \mathbf{Z}$ is square free and prime to f.

In our case $m = p^\ell$, this conditions say: If χ is a character mod p^ℓ with conductor $f = p^\nu (\nu \leq \ell)$, then

$$\tau(\chi, \zeta_{p^\ell}^a) \neq 0 \Longleftrightarrow a = p^{\ell-\nu} a_0, (a_0, p) = 1.$$

(4) Let $G_\ell =< \omega(1+p)(\text{ mod } p^\ell) | \omega \equiv \omega_0 (\text{mod} p)$ for some ω_0 primitive root mod $p, \omega^{p-1} \equiv 1(\text{ mod } p^\ell)$ and $(1+p)^{p^{\ell-1}} \equiv 1(\text{ mod } p^\ell) >$. Then every character mod $p^\ell (p > 2)$ is of the form

$\chi = \chi_p^{\alpha'} \chi_{p^\ell}^{\alpha''}$

where χ_p and χ_{p^ℓ} are characters mod p^ℓ with conductors p and p^ℓ defined by

$$\chi_p(\omega) = \zeta_{p-1} \ , \ \chi_p(1+p) = 1.$$
$$\chi_{p^\ell}(\omega) = 1, \chi_{p^\ell}(1+p) = \zeta_{p^{\ell-1}}.$$

Moreover, $\chi \neq \chi_0$ is primitive iff $\alpha' \not\equiv 0(p-1)$ if $\ell = 1$ or $\alpha'' \not\equiv 0(p)$ if $\ell > 1$.

(5) χ a character mod p^ℓ is primitive if and only if the order of χ is $d = p^{\ell-1}k$ with $k|p-1$.

Now, let χ be a primitive character mod $p^\ell, \ell > 1$. Then:

(6) $\tau(\chi)\overline{\tau(\chi)} = |\tau(\chi)|^2 = p^\ell$.

(7) $\tau(\chi)\tau(\bar{\chi}) = \chi(-1)p^{\ell-1}(p-1)$.

Finally, lets consider in particular characters mod p :

Let χ, λ be characters mod$p$ of orders $k, \ell | p-1$ (i.e. χ, λ are primitive characters on $\mathbf{F}_p^*$ with $\chi^k = \lambda^\ell = \chi_0$, the principal character).

Let $\zeta = \zeta_p$ be a primitive p^{th} root of unity.

Then we will consider the character sums:

$$\tau(\chi) = \tau(\chi, \zeta) = \sum_{x \in \mathbf{F}_p^*} \chi(x)\zeta^x$$

which is the Gaussian sum associated to the character χ. And

$$\pi(\chi, \lambda) = \sum_{\substack{x,y \in \mathbf{F}_p^* \\ x+y=1}} \chi(x)\lambda(y)$$

called the Jacobi sum associated to the characters χ and λ.

These sums are in fact related. We will state their main properties ([**H**] p. 453-465):

(1′) $\tau(\chi_0) = \sum_{x \in \mathbf{F}_p^*} \zeta^x = -1$.

(2′) $\tau(\chi)\overline{\tau(\chi)} = |\tau(\chi)|^2 = p$.

(3′) $\tau(\chi)\tau(\overline{\chi}) = \chi(-1)p$.

(4′) In particular for $\psi = \left(\frac{\cdot}{p}\right)$ the quadratic character mod$p$ defined by

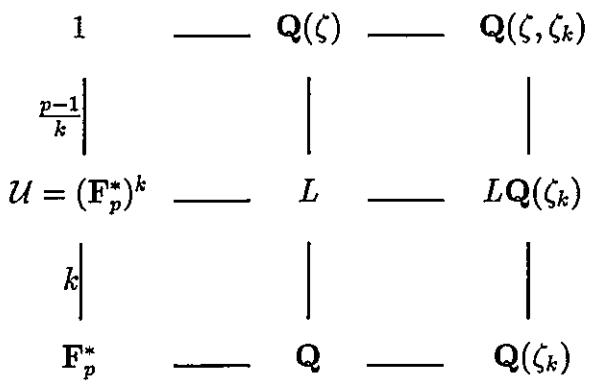
$$\left(\frac{a}{p}\right) = \begin{cases} 1 \text{ if } a \text{ is a square mod} p. \\ \\ -1 \text{ if otherwise} \end{cases}$$

it holds $\psi \neq \chi_0, \psi^2 = \chi_0$ and

$$\tau(\psi) = \begin{cases} \sqrt{p} & \text{if} \quad p \equiv 1(4) \\ \\ i\sqrt{p} & \text{if} \quad p \equiv 3(4). \end{cases}$$

(5′) $\tau(\chi, \zeta) \in \mathbf{Q}(\zeta, \zeta_k)$, where ζ_k is a primitive k^{th} root of unity.

Moreover by Galois correspondence we have:



with

$$\text{Gal}\,(L\mathbf{Q}(\zeta_k)/\mathbf{Q}(\zeta_k)) \cong \text{Gal}\,(L/\mathbf{Q}) \cong \mathbf{F}_q^*/\mathcal{U}$$

and since

$$\tau(\chi)^a = \bar{\chi}(a)\tau(\chi)$$

hence $\tau(\chi)$ is invariant by exactly the automorphisms corresponding to $a : \zeta \to \zeta^a$, $a \in \mathcal{U}$ subgroup of $\mathbf{F}_p^*$ of index k with cyclic quotient. Thus $\tau(\chi)$ has exactly k conjugates in $L\mathbf{Q}(\zeta_k)$. Then

$$L\mathbf{Q}(\zeta_k) = \mathbf{Q}(\zeta_k)(\tau(\chi)).$$

Now, since $\chi^k = \chi_0$, then $\tau(\chi)^k$ is invariant by the entire Galois group. Hence

$$\tau(\chi)^k \in \mathbf{Q}(\zeta_k).$$

(6′) $\pi(\chi_0, \chi_0) = p$.

(7′) Let $\chi \neq \chi_0$. Then

$$\pi(\chi, \chi_0) = \pi(\chi_0, \chi) = 0.$$

(8′) Let χ, λ and $\chi\lambda \neq \chi_0$. Then

$$\pi(\chi,\lambda) = \frac{\tau(\chi)\tau(\lambda)}{\tau(\chi\lambda)} \text{ and } |\pi(\chi,\lambda)| = \sqrt{p}.$$

and

(9′) Let $\chi \neq \chi_0$ with order $k \geq 3$. Then

$$\tau(\chi)^k = \chi(-1)p\pi(\chi,\chi)\pi(\chi,\chi^2)\cdots\pi(\chi,\chi^{k-2}).$$

(10′) Let $\ell | p-1$ and let χ be a character mod$p$ with $\chi^\ell \neq \chi_0$. Then

$$\tau(\chi)^\ell = \tau(\chi^\ell,\zeta^\ell)\Pi_{\substack{\varphi^\ell=\chi_0 \\ \varphi\neq\chi_0}}\pi(\chi,\varphi) = \bar{\chi}^\ell(\ell)\tau(\chi^\ell)\Pi_{\substack{\varphi^\ell=\chi_0 \\ \varphi\neq\chi_0}}\Pi(\chi,\varphi)$$

In particular if $\chi^2 \neq \chi_0$, we obtain

$$\tau(\chi)^2 = \bar{\chi}^2(2)\tau(\chi^2)\pi(\chi,\psi) \text{ where } \psi = \left(\frac{-}{p}\right) \text{ is the quadratic character.}$$

Finally, lets introduce a new character sum defined by

$$k(\chi) = \chi(4)\pi(\chi,\chi).$$

Then ([**BE**]):

(11′) Let $\chi \neq \chi_0, \psi = \left(\frac{-}{p}\right)$. Then

$$k(\chi) = \pi(\chi,\psi)$$

(12′) Let χ be a character with order > 2 and $\psi = \left(\frac{-}{p}\right)$. Then

$$k(\chi) = \left(\frac{-1}{p}\right)k(\bar{\chi}\psi) = \chi(-1)\pi(\chi,\bar{\chi}\psi)$$

(13′) Let χ be a character with order $= 2k$. Then

$$k(\chi) = \left(\frac{-1}{p}\right)k(\chi^{k-1}) = \chi(-1)\pi(\chi,\chi^{k-1}).$$

Now we are in conditions to express the coefficients of the polynomials $P_j(X), 0 \leq j \leq r$, in terms of character sums mod p^{r+1-j}. We have:

$S(\zeta^{p^j}) = \sum_{u \in \mathcal{U}_{r+1-j}} \zeta^{p^j u} = \tau(\chi_0)$
is the Gaussian sum associated to χ_0 the principal character on $\mathcal{U}_{r+1-j}$, since ζ^{p^j} is a primitive $p^{(r+1-j)th}$ root of unity.

Now since $G_{r+1-j}/\mathcal{U}_{r+1-j}$ is cyclic of order $d_{r+1-j} = p^{r-j}k$, we have by § **3.(1.1.6)**, Chapter I, χ_0 has exactly d_{r+1-j} extensions to G_{r+1-j} and hence we find:

$S(\zeta^{p^j}) = \tau_{\mathcal{U}_{r+1-j}}(\chi_0) = \frac{1}{d_{r+1-j}} \sum_{\chi^{d_{r+1-j}} = \chi_0} \tau(\chi)$

and

$S(\zeta^{p^j})^a = \frac{1}{d_{r+1-j}} \sum_{\chi^{d_{r+1-j}} = \chi_0} \bar{\chi}(a)\tau(\chi)$

for all $a \in G_{r+1-j}/\mathcal{U}_{r+1-j}; a : \zeta^{p^j} \to \zeta^{p^j a}$.

Then, the coefficients of $P_j(X)$ will be obtained as the symmetric functions of $S(\zeta^{p^j})^a, a \in G_{r+1-j}/\mathcal{U}_{r+1-j}$.

§2. Examples

Next we will find the period equations for d = 4, 6 and 8 in terms of character sums mod$p$, to obtain these levels for $\mathbf{F}_p$.

It will be seen that finding (or at least bounding) the solutions of certain diophantine quadratic equations, provides the primes p for which $s_d(p) > 2$.

Besides, a determination of these primes is found related to their representation, or the representation of multiples of them, by certain binary quadratic forms.

1. $s_4(\mathbf{F}_p)$

Let p be a prime such that $p \equiv 1(4)$, $p \not\equiv 1(8)$. Let $\mathcal{U} = (\mathbf{F}_p^*)^4$, $\mathbf{F}_p^* = <\omega>$, ζ a primitive p^{th} root of unity and $s(\zeta) = \sum_{u \in \mathcal{U}} \zeta^u$.

Let χ be a biquadratic character mod p, given by $\chi(\omega) = i$, a primitive 4^{th} root of unity. Thus $\chi^2 = \psi = \left(\frac{\cdot}{p}\right)$ the quadratic character, $\chi^3 = \bar{\chi} = \chi^{-1}$ and

$\chi^4 = \chi_0$ the principal character. Then we have

$$s(\zeta) = \tau_u(\chi_0) = \frac{1}{4}[\tau(\chi_0) + \tau(\psi) + \tau(\chi) + \tau(\bar{\chi})]$$

Now since

$$\begin{aligned} \tau(\chi_0) &= -1 \\ \tau(\chi) &= \sqrt{p} \quad \text{since } p \equiv 1(4) \\ \tau(\chi)\tau(\bar{\chi}) &= \chi(-1)p = -p \quad \text{since } p \not\equiv 1(8) \end{aligned}$$

and by (10′)

$$\tau(\chi) = \psi(2)\tau(\psi)\pi(\chi, \psi)$$

where $\pi(\chi, \psi) = \sum_{x+y=1} \chi(x)\psi(y)$ the Jacobi sum associated to χ and ψ.

Then we find

$$\begin{aligned} \tau(\chi)^2 &= -\sqrt{p}\pi \\ \tau(\bar{\chi})^2 &= -\sqrt{p}\bar{\pi} \end{aligned}$$

where

$$\pi := \psi(2)\pi(\chi, \psi) = a + bi \in \mathbf{Z}[i].$$

This provides a representation of p as sum of two squares, such that

$$p = \pi\bar{\pi} = a^2 + b^2 \text{ with } a \equiv 1(\text{mod } 4), \ b \equiv 0(\text{mod } 2).$$

With all this, finding the conjugates of $s(\zeta)$ we obtain the period equation of degree 4:

$$
\begin{aligned}
P(X) &= \Pi_{a\in\mathbf{F}_p^*/\mathcal{U}}(X - s(\zeta)) \\
&= \left(\tfrac{1}{4}\right)^4 (4X - \tau(\chi_0) - \tau(\psi) - \tau(\chi) - \tau(\bar{\chi}))\cdot \\
&\quad (4X - \tau(\chi_0) - \tau(\psi) - i\tau(\chi) - i\tau(\bar{\chi}))\cdot \\
&\quad (4X - \tau(\chi_0) + \tau(\psi) + i\tau(\chi) - i\tau(\bar{\chi}))\cdot \\
&\quad (4X - \tau(\chi_0) + \tau(\psi) - i\tau(\chi) + i\tau(\bar{\chi})) \\
&= X^4 + X^3 + \alpha_2 X^2 + \alpha_3 X + \alpha_4
\end{aligned}
$$

where

$$
\begin{aligned}
\alpha_2 &= \tfrac{3+p}{8} \\
\alpha_3 &= \tfrac{1+(1+2a)p}{16} \\
\alpha_4 &= \tfrac{1+2(1+2a(2-a))p+9p^2}{256}.
\end{aligned}
$$

Now, by the result on the d^{th} level of $\mathbf{F}_p$ obtained in §2.(2.2), Chapter II, it holds

$$s_4(p) > n \Longleftrightarrow (n+1)\alpha_{n+1} = (1 + n\frac{(p-1)}{4})\alpha_n.$$

Thus, as we know since $p \not\equiv 1(8)$

$$s_4(p) > 1 \text{ and } 2\alpha_2 = (1 + \frac{(p-1)}{4}) = \frac{3+p}{4}.$$

Following, we get

$$
\begin{aligned}
s_4(p) > 2 &\iff 3\alpha_3 = (1 + \tfrac{(p-1)}{2})\alpha_2 \\
&\iff 3(1 + (1+2a)p) = 3 + 4p + p^2
\end{aligned}
$$

i.e.

$$s_4(p) > 2 \Longleftrightarrow p = 6a - 1.$$

Since $p = a^2 + b^2$, then

$$6a - 1 = a^2 + b^2 \geq a^2 + 4 \Longrightarrow 1 \leq a \leq 5$$

and hence $p \leq 29$. Actually only $p = 5, 29$ satisfy $p \not\equiv 1(8)$.

And finally

$$\begin{aligned} s_4(p) > 3 &\iff 4\alpha_4 = (1 + 3\tfrac{(p-1)}{4})\alpha_3 \quad \text{with } p = 6a - 1 \\ &\iff 5a^2 - 6a + 1 = 0, \quad a \in \mathbf{Z} \\ &\iff a = 1 \\ &\iff p = 5 \end{aligned}$$

for which clearly we have $s_4(5) = 4$ since then $d = p - 1$. Thus

$$s_4(p) = \begin{cases} 1 & \text{iff } p \equiv 1(8) \text{ or } p = 2 \\ 4 & \text{if } p = 5 \\ 3 & \text{if } p = 29 \\ 2 & \text{otherwise} \end{cases}$$

□

Remark (1.1) Actually, these are the values of the 4^{th} level for $\mathbf{F}_q$, $q = p^n$, i.e. $s_4(q) \leq 2$ for all $q \neq p$.

2. $s_6(\mathbf{F}_p)$

Let $p > 2$ be a prime such that $p \equiv 1(3)$, $p \not\equiv 1(4)$. Let $\mathcal{U} = (\mathbf{F}_p^*)^6, \mathbf{F}_p^* = <\omega>$, ζ a primitive p^{th} root of unity and $s(\zeta) = \sum_{u \in \mathcal{U}} \zeta^u$.

Let χ be a cubic character mod p, given by $\chi(\omega) = \rho = e^{2\pi i/3}$, and $\psi = (\frac{\cdot}{p})$ the quadratic character. Hence $\varphi = \chi\psi$ has order 6. Then

$$s(\zeta) = \tau_{\mathcal{U}}(\chi_0) = \frac{1}{6}\sum_{i=0}^{5}\tau(\varphi^i)$$

By Galois correspondence we have:

$$\begin{array}{ccc}
1 & \text{——} & \mathbf{Q}(\zeta) \\
\frac{p-1}{6}\Big| & & \Big| \\
\mathcal{U} = (\mathbf{F}_p^*)^6 & \text{——} & \mathbf{Q}(S(\zeta)) \\
3\Big| & & \Big| \\
(\mathbf{F}_p^*)^2 & \text{——} & \mathbf{Q}(\sqrt{p}) \\
2\Big| & & \Big| \\
\mathbf{F}_p^* & \text{——} & \mathbf{Q}
\end{array}$$

Now recalling

$$\psi(-1) = -1 \text{ since } p \equiv 3(4)$$

and by $(9')$ and $(10')$,

$$\tau(\chi)\tau(\bar{\chi}) = \chi(-1)p = p \text{ since } p \equiv 1(6)$$

and

$$\tau(\chi)^3 = p\pi$$

$$\tau(\bar{\chi})^3 = p\bar{\pi}$$

where

$$\pi = \chi(2)\pi(\chi,\psi) = \frac{a + 3b\sqrt{-3}}{2}$$

This provides a representation of $4p$ as sum of squares such that

$$4p = a^2 + 27b^2 \quad \text{with} \quad a \equiv 1(3).$$

Remark (2.1) $\chi(2) = 1 \Longleftrightarrow b \equiv 0(2)$.

With this, finding the minimal polynomial of $s(\zeta)$ over $\mathbf{Q}(i\sqrt{p})$, and then squaring, we obtain the period equation of degree 6:

$$p(X) = X^6 + X^5 + \alpha_2 X^4 + \alpha_3 X^3 + \alpha_4 X^2 + \alpha_5 X + \alpha_6$$

where

$$\alpha_2 = \tfrac{5+p}{12}$$

$$\alpha_3 = \tfrac{1}{3(6^2)}[10 + \{6(R+1) + 3R' - a\}p]$$

$$\alpha_4 = \tfrac{1}{2(6^3)}[5 + \{3(R+2)^2 + 2(3R' - a) - 2a^2 - 6\}p + \{6t+5\}p^2]$$

$$\alpha_5 = \tfrac{1}{6^4}[1 + \{(R+2)(3(R+1) - a^2) - (3(R+1-R') + a + 1)\}p + \{(R+2)(3t+1) + 3(R+1-R') + a\}p^2]$$

$$\alpha_6 = \tfrac{1}{6^6}[\{3(R+1-R')p + ap - 1\}^2 + \{(3t+1)p + 3(R+1) - a^2\}^2 p]$$

with

$$a = 2\mathrm{Re}\,\pi$$

$$R = 2\mathrm{Re}\bar{\chi}(2)\pi = \begin{cases} a & \text{if } \chi(2) = 1 \\ \frac{(-a+9b)}{2} & \text{if } \chi(2) = \rho \\ \frac{(-a-9b)}{2} & \text{if } \chi(2) = \bar{\rho} \end{cases}$$

$$R' = 2\mathrm{Re}\,\chi(2)\pi = \begin{cases} a & \text{if } \chi(2) = 1 \\ \frac{(-a-9b)}{2} & \text{if } \chi(2) = \rho \\ \frac{(-a+9b)}{2} & \text{if } \chi(2) = \bar{\rho} \end{cases}$$

and

$$t = 2\mathrm{Re}\,\chi(2) = \begin{cases} 2 & \text{if } \chi(2) = 1 \\ -1 & \text{if } \chi(2) \neq 1 \end{cases}$$

where $\rho = (-1 + i\sqrt{3})/2$ and χ is the cubic character as defined above.

Thus, we obtain

$$\begin{aligned} s_6(p) > 2 &\iff 3\alpha_3 = (1 + \tfrac{(p-1)}{3})\alpha_2 \\ &\iff 3(2(R+1) + R')p - ap + 10 = p^2 + 7p + 10 \\ &\iff p = 6(R+1) + 3R' - a - 7 \end{aligned}$$

i.e.

$$s_6(p) > 2 \iff p = \begin{cases} 8a - 1 & \text{if } \chi(2) = 1 \\ \frac{-11+27b}{2} - 1 & \text{if } \chi(2) = \rho \\ \frac{-11-27b}{2} - 1 & \text{if } \chi(2) = \bar{\rho}. \end{cases}$$

Here, we should distinguish two cases.

Case $\chi(2) = 1$: $4p = a^2 + 27b^2$, then

$$8a - 1 = \frac{a^2 + 27b^2}{4}, \qquad b \equiv 0(2)$$

gives $4 \leq a \leq 28$, and hence $p \leq 223$.

Since

$$p = 8a - 1, \quad t = 2, \text{ and } \quad R = R' = a,$$

then

$$\begin{aligned} s_6(p) > 3 &\iff 31a^2 - 128a + 16 = 0, \quad a \in \mathbf{Z} \\ &\iff a = 4 \\ &\iff p = 31 \end{aligned}$$

But then, $s_6(31) = 4$ (since $s_d(p) \leq \frac{d}{2} + 1$ if $d \neq p - 1$, by [T]). Then, this is the only prime with $\chi(2) = 1$ and level $s > 3$, the other $p = 233$ has level $s = 3$.

Case $\chi(2) \neq 1$: $4p = a^2 + 27b^2 = -22a \pm 2(27)b - 4$, then we obtain the diophantine equation

$$(a+11)^2 + 27(b \mp 1)^2 = 144$$

with solutions

$$b = \pm 1 \text{ and } a = 1 \text{ or } -23(\equiv 1(3)),$$

or

$$a = 3(2\varepsilon) - 11 \text{ and } b = 2\varepsilon \pm 1, \text{ where } \varepsilon = 1 \text{ or } -1,$$

i.e.

$$p = 79, 133, 13, 67, 139 \text{ or } 7.$$

Actually only

$$p = 7, 67, 79, 139 \not\equiv 1(4).$$

Following, we get

$$s_6(p) > 3 \Longleftrightarrow 4\alpha_4 = (1 + \frac{(p-1)}{2})\alpha_3$$

with p determined by $s_6(p) > 2$ and $\alpha_3 = \frac{1}{3(6^2)}[10 + 7p + p^2]$.

Since

$$p = \frac{-11a' \pm 27b}{2} - 1, \quad t = -1 \text{ and } \begin{cases} R &= \frac{(-a \pm 9b)}{2} \\ R' &= \frac{(-a \mp 9b)}{2} \end{cases}$$

where the sing $+$ or $-$ depends on whether $\chi(2) = \rho$ or $\bar{\rho}$, then

$$s_6(p) > 3 \Longleftrightarrow p^2 + 8p + 17 = -2p + \frac{3}{2}(-a \pm 9b + 4)^2 + 6(-a \mp 9b - 2) - 4a(a+1)$$

We find out for $p = 67 = \frac{(-5)^2+27(3^2)}{2}$, that $p = \frac{-11(-5)\pm 27(\pm 3)}{2} - 1$ does not satisfy the equation above, then $s_6(67) = 3$.

Similarly, $s_6(79) = s_6(139) = 3$.

On the other hand, $p = 7 = \frac{-11(1)-27(-1)}{2} - 1$ (since $\chi(2) = \bar{\rho}$), satisfies the equation above.

Actually, one can verify that $p = 7$ satisfies the equation for

$$s_6(p) > 4, \quad \text{i.e.,} \quad 5\alpha_5 = (1 + 2\frac{(p-1)}{3})\alpha_4$$

and

$$s_6(p) > 5, \quad \text{i.e.,} \quad 6\alpha_6 = (1 + 5\frac{(p-1)}{6})\alpha_5$$

or, we can immediately state $s_6(7) = 6$, as it is clear.

Thus

$$s_6(p) = \begin{cases} 1 & \text{if } p \equiv 1(4) \text{ or } p = 2 \\ 6 & \text{if } p = 7 \\ 4 & \text{if } p = 31 \\ 3 & \text{if } p = 67, 79, 139, 233 \\ 2 & \text{otherwise} \end{cases}$$

□

Remarks. (2.2) Actually these are the values of the 6^{th} level for $\mathbf{F}_q$, $q = p^n$,. i.e. , $s_d(q) \leq 2$ for all $q \neq p$.

3. $s_8(\mathbf{F}_p)$

Let $p > 2$ be a prime such that $p \equiv 1(8)$, $p \not\equiv 1(16)$. Similarly to the preceding examples, and using this time the representations of p

$$p = a_*^2 + 2b_*^2 \quad \text{with} \quad a_* \equiv -1(4)$$

and

$$p = a^2 + b^2 \quad \text{with} \quad a \equiv 1(4), \quad b \equiv 0(2)$$

given by

$$|k(\varphi)| = |\pi(\varphi, \psi)| \text{ and } |\pi| = |\varphi(2)\pi(\chi, \psi)|$$

where $\psi = \left(\frac{-}{p}\right), \varphi$ a character of order 8, and χ a character of order 4, since by (13'), $k(\varphi) = \left(\frac{-1}{p}\right) k(\varphi^3) = k(\varphi^3)$, thus $k(\varphi) \in Fix < \pm 3 >= \mathbf{Q}(\sqrt{-2})$, and $\pi(\chi, \varphi) \in \mathbf{Q}(\sqrt{-1})$. Then we come to obtain, after rather long calculations, the period equation of degree 8 :

$$P(X) = X^8 + X^7 + \alpha_2 X^6 + \cdots + \alpha_8$$

where

$$\alpha_2 = \tfrac{1}{8^2}[28 + C_6] = \tfrac{7+p}{16}$$

$$\alpha_3 = \tfrac{1}{8^3}[56 + 6C_6 + C_5] = \tfrac{1}{8^2}[7 + 3p + 2(1+2\varepsilon)ap + 4(1-\chi(2))a_*p]$$

$$\begin{aligned}\alpha_4 = \tfrac{1}{8^4}[&70 + 15C_6 + 5C_5 + C_4] = \tfrac{1}{8^4}[70 + 60p + 8(1+2\varepsilon)ap + 160(1-\chi(2))a_*p \\ &+(70 - 96\varepsilon)p^2 - 8a^2p - 48a_*^2p \\ &+32((3+\varepsilon)\chi(2) - 3)aa_*p]\end{aligned}$$

$$\begin{aligned}\alpha_5 = \tfrac{1}{8^5}[&56 + 20C_6 + 10C_5 + 4C_4 + C_3] = \tfrac{1}{8^4}[7 + \{10 + 20(1+2\varepsilon)a + 4(1-\chi(2))a_* \\ &-4a^2 - 24a_*^2 \\ &+16((3+\varepsilon)\chi(2) - 3)aa_* \\ &-16\chi(2)a^2a_* + 8(1 - 4\chi(2))aa_*^2\}p \\ &+\{(35 - 48\varepsilon) + 20(2\varepsilon - 1)a \\ &+8(5 + 4\varepsilon - \chi(2)(3+2\varepsilon))a_*)\}p^2]\end{aligned}$$

$$\alpha_6 = \tfrac{1}{8^6}[28 + 15C_6 + 10C_5 + 6C_4 + 3C_3 + C_2]$$

$$\alpha_7 = \tfrac{1}{8^7}[8 + 6C_6 + 5C_5 + 4C_4 + 3C_3 + 2C_2 + C_1]$$

$$\alpha_8 = \tfrac{1}{8^8}[1 + C_6 + C_5 + C_4 + C_3 + C_2 + C_1 + C_0]$$

where ε results to be equal to $\chi(2) = \pm 1$, χ the biquadratic character defined before, and the constants C_k $(0 \le k \le 6)$ are determined in terms of the coefficients of the minimal polynomial of $\theta(\zeta) = 8S(\zeta) + 1 - \sqrt{p}$ over $\mathbf{Q}(\sqrt{p})$:

$$
\begin{aligned}
C_6 &= 4p \\
C_5 &= 16[\beta_2 p - 2\gamma_1] \\
C_4 &= 100p^2 + 2[5p^2 + 16\gamma_2 p + 4\delta_1] - 16\beta_2^2 p - 32[3p + 4\gamma_2]p \\
C_3 &= -160p[\beta_2 p + 2\gamma_1] + 8[4\beta_2 p + 16\gamma_1 + 4\delta_2]p \\
&\quad +32\beta_2[3p + 4\gamma_2]p \\
C_2 &= 64[\beta_2 p + 2\gamma_1]^2 + 20p[5p^2 + 16\gamma_2 p + 4\delta_1] \\
&\quad -16[3p + 4\gamma_2]^2 p - 8\beta_2[4\beta_2 p + 16\gamma_1 + 4\delta_2]p \\
C_1 &= -16[\beta_2 p + 2\gamma_1][5p^2 + 16\gamma_2 p + 4\delta_1] \\
&\quad +8[3p + 4\gamma_2][4\beta_2 p + 16\gamma_1 + 4\delta_2]p \\
C_0 &= [5p^2 + 16\gamma_2 p + 4\delta_1]^2 - [4\beta_2 p + 16\gamma_1 + 4\delta_2]^2 p
\end{aligned}
$$

since

$$
\text{irr } (\theta(\zeta), \mathbf{Q}(\sqrt{p}))(X) = X^4 + \beta X^2 - \gamma X + \delta
$$

where

$$
\beta = 4(\beta_1 + \beta_2\sqrt{p}) \, , \quad \begin{cases} \beta_1 &= p \\ \beta_2 &= a + 2a_* \end{cases}
$$

$$
\gamma = 16(\gamma_1 + \gamma_2\sqrt{p}) \, , \quad \begin{cases} \gamma_1 &= \chi(2)a_* - \varepsilon a \\ \gamma_2 &= \varepsilon p - \chi(2)aa_* \end{cases}
$$

and

$$
\delta = 4(x + y\sqrt{p}) \, , \quad \begin{cases} x &= \{2a_*^2 + a^2 + 4(\varepsilon\chi(2) - 1)aa_*\}p + 7p^2 \\ y &= \{4(3 - \varepsilon\chi(2))a_* - 4a\}p + 2aa_*^2 \end{cases}
$$

Then, we obtain

$$s_8(p) > 2 \Longleftrightarrow p = \begin{cases} 18a - 1 & \text{if } \chi(2) = 1 \\ 24a_* - 6a - 1 & \text{if } \chi(2) = -1 \end{cases}$$

Studying the diophantine equations defined by this and the representations of p as sum of squares, we get

Case $\chi(2) = 1$:

$$s_8(p) > 2 \Longrightarrow p \leq 305$$

Case $\chi(2) = -1$:

$$s_8(p) > 2 \Longrightarrow p \leq 869$$

Now, like before, we find:

$$s_8(p) = \begin{cases} 1 & \text{if } p \equiv 1(16) \text{ or } p = 2 \\ 4 & \text{if } p = 41 \\ 3 & \text{if } p = 89, 137, 233, 761 \\ 2 & \text{otherwise} \end{cases}$$

□

Remark (3.1) Actually these are the values of the 8^{th} level of $\mathbf{F}_q, q = p^n, i.e., s_8(q) \leq 2$ for all $q \neq p$.

Remark (3.2) We should mention that the cyclotomic numbers of even order $d = 6, 8, 10, 12, 14, 16, 20, 24$ and 30 have been found (see **[LW]**). Thus, the corresponding period equations may be computed (in terms of the symmetric powers sums $S_n = \sum_{i=0}^{d-1} \eta_i^n$, by Newton's identities $S_n + \alpha_1 S_{n-1} + \alpha_2 S_{n-2} + \cdots + \alpha_{n-1} S_1 + n\alpha_n = 0, 0 \leq n \leq d$), then $s_d(\mathbf{F})$ may be considered as known for these exponents too.

§ 3. On the Coefficients of the Period Equation

1. On the Coefficients of the Period Equation for $s_d(\mathbf{F}_p)$

In §2. we calculated $s(\zeta)$ and its conjugates in terms of Gaussian sums, i.e.,

$$s(\zeta) = \tau_{\mathcal{U}}(\chi_0) = \frac{1}{d}\sum_{\chi^d=\chi_0}\tau(\chi)$$

and

$$s(\zeta)^a = \frac{1}{d}\sum_{\chi^d=\chi_0}\bar{\chi}(a)\tau(\chi)$$

where $a \in G = \mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q}) \cong \mathbf{F}_p^*/\mathcal{U}$; $a : \zeta \to \zeta^a$.

Here we will also write $a < b$ for $a, b \in G$ if $a \equiv \omega^i \pmod{\mathcal{U}}$, $b \equiv \omega^j \pmod{\mathcal{U}}$ with $0 \le i < j \le d-1$.

Thus we obtain the following expressions for the coeficients of the period equation $P(X) = X^d + \alpha_1 X^{d-1} + \alpha_2 X^{d-2} + \cdots + \alpha_d$ for $d|p-1$:

$$\begin{aligned}
\alpha_1 &= -\textstyle\sum_a s(\zeta)^a = -\sum_{x\in\mathbf{F}_p^*}\zeta^x = -(-1) = 1.\\
\alpha_2 &= \textstyle\sum_{a_1<a_2}\left(\frac{1}{d}\sum_{\chi_1^d=\chi_0}\bar{\chi}_1(a_1)\tau(\chi_1)\right)\left(\frac{1}{d}\sum_{\chi_2^d=\chi_0}\bar{\chi}_2(a_2)\tau(\chi_2)\right)\\
&= \textstyle\frac{1}{d^2}\sum_{\chi_1^d=\chi_2^d=\chi_0}\left(\sum_{a_1<a_2}\bar{\chi}_1(a_1)\bar{\chi}_2(a_2)\right)\tau(\chi_1)\tau(\chi_2)
\end{aligned}$$

and, in general

$$\alpha_n = \frac{(-1)^n}{d^n}\sum_{\chi_1^d=\cdots=\chi_n^d=\chi_0}\left(\sum_{a_1<\cdots<a_n}\bar{\chi}_1(a_1)\cdots\bar{\chi}_n(a_n)\right)\tau(\chi_1)\cdots\tau(\chi_n) \qquad (**)$$

for all $1 \le n \le d$.

($|\mathbf{F}_p^*/\mathcal{U}| = d \Longrightarrow \{(a_1,\cdots,a_n) \in G^n | a_1 < \cdots < a_n\} \neq \Phi$, for all $1 \le n \le d$).

Now, notice that the products $\tau(\chi_1)\cdots\tau(\chi_n)$ commute, so we may find these sums as follows.

Since

$$\sum_{\chi_1,\chi_2}\sum_{a_1<a_2}\bar{\chi}_1(a_1)\bar{\chi}_2(a_2)=\sum_{\chi_1,\chi_2}\sum_{a_1>a_2}\bar{\chi}_1(a_1)\chi_2(a_2)$$

then

$$\sum_{\chi_1,\chi_2}\sum_{a_1,a_2}\bar{\chi}_1(a_1)\bar{\chi}_2(a_2)=2\sum_{\chi_1,\chi_2}\sum_{a_1<a_2}\bar{\chi}_1(a_1)\bar{\chi}_2(a_2)+\sum_{\chi_1,\chi_2}\sum_{a_1=a_2}\bar{\chi}_1(a_1)\bar{\chi}_2(a_2)$$

Hence, we obtain

$$\alpha_2=\frac{1}{d^2}\sum_{\chi_1^d=\chi_2^d=\chi_0}\left[\frac{1}{2}\sum_{a_1}\bar{\chi}_1(a_1)\sum_{a_2}\bar{\chi}_2(a_2)-\frac{1}{2}\sum_{a}\overline{\chi_1\chi_2}(a)\right]\tau(\chi_1)\tau(\chi_2)$$

Let χ be a character of order d. Then

$$\sum_{i=1}^{d-1}\chi^i(-1)=\begin{cases} d-1 & \text{if } 2d|p-1 \\ \\ -1 & \text{if } 2d\nmid p-1 \end{cases}$$

and

$$\sum_{x\in\mathbf{F}_p^*/\mathcal{U}}\chi(x)=\begin{cases} d & \text{if } \chi=\chi_0 \\ \\ 0 & \text{if } \chi\neq\chi_0. \end{cases}$$

Thus

$$\begin{aligned}\alpha_2 &= \tfrac{1}{d^2}\textstyle\sum_{i,j=0}^{d-1}\left(\sum_{a_1<a_2}\bar{\chi}^i(a_1)\bar{\chi}^j(a_2)\right)\tau(\chi^i)\tau(\chi^j)\\ &= \tfrac{1}{d^2}\left[\tfrac{(d^2-d)}{2}\tau(\chi_0)^2-\tfrac{d}{2}\textstyle\sum_{i=1}^{d-1}\tau(\chi^i)\tau(\bar{\chi}^i)\right].\end{aligned}$$

Since $\tau(\chi^i)\tau(\bar{\chi}^i)=\chi^i(-1)p$ and $\tau(\chi_0)=-1$, we find

$$\alpha_2=\frac{d-1}{2d}-\frac{p}{2d}\sum_{i=1}^{d-1}\chi^i(-1)$$

i.e.

$$\alpha_2=\begin{cases} \frac{(1-p)(d-1)}{2d} & \text{if } 2d|p-1 \\ \\ \frac{p+(d-1)}{2d} & \text{if } 2d\nmid p-1. \end{cases}$$

Similarly, we obtain a formula for the inner sums $\sum_{a_1<\cdots<a_n} \bar{\chi}_1(a_1)\cdots\bar{\chi}_n(a_n)$ in terms of the free sums $\sum_{a_1}, \sum_{a_1,a_2}, \cdots, \sum_{a_1,\cdots,a_n}$, which may be found by properties of character sums.

To simplify the writing, we will introduce the following notation: Let

$$\begin{aligned}
\sum_{a_1,\cdots,a_k} &= \sum_{\chi_1,\cdots,\chi_n} \sum_{a_1,\cdots,a_k=\cdots=a_n} \bar{\chi}_1(a_1)\cdots\bar{\chi}_n(a_n) \\
\sum_{a_1<\cdots<a_k} &= \sum_{\chi_1,\cdots,\chi_n} \sum_{a_1<\cdots<a_k=\cdots=a_n} \bar{\chi}_1(a_1)\cdots\bar{\chi}_n(a_n) \\
\sigma_i^{(n-k)} &= i+(i+1)+\cdots+(n-k) \\
\sigma_i^{(n-k)^2} &= i\sigma_i^{(n-k)} + (i+1)\sigma_{i+1}^{(n-k)} + \cdots + (n-k)^2 \\
&= i^2 + i(i+1) + \cdots + i(n-k) \\
&\quad +(i+1)^2 + \cdots + (i+1)(n-k) \\
&\quad \vdots \\
&\quad +(n-k)^2 \\
\sigma_i^{(n-k)^3} &= i\sigma_i^{(n-k)^2} + (i+1)\sigma_{i+1}^{(n-k)^2} + \cdots + (n-k)^3 \\
&\vdots
\end{aligned}$$

for $n \geq 2,\ 2 \leq i \leq n-k, 0 \leq k \leq n-2$

Then we find

Lemma (1.1)

$$
\begin{aligned}
n!\sum_{a_1<\cdots<a_n} &= \sum_{a_1,\cdots,a_n} -(n-1)![1+\sigma_2^{(n-1)}]\sum_{a_1<\cdots<a_{n-1}} \\
&\quad -\cdots \\
&\quad -(n-k)![1+\sigma_2^{(n-k)}+\sigma_2^{(n-k)^2}+\cdots+\sigma_2^{(n-k)^k}]\sum_{a_1<\cdots<a_{n-k}} \\
&\quad \vdots \\
&\quad -2![1+2+2^2+\cdots+2^{n-2}]\sum_{a_1<a_2} \\
&\quad -\sum_{a_1}
\end{aligned}
$$

Proof: We had found

$$\sum_{a_1,a_2} = 2\sum_{a_1<a_2} + \sum_{a_1}$$

and then

$$2!\sum_{a_1<a_2} = \sum_{a_1,a_2} - \sum_{a_1}$$

Now considering

$$\sum_{a_1,a_2,a_3} = \sum_{a_3}\left(\sum_{a_1,a_2}\right)$$

we obtain

$$
\begin{aligned}
\sum_{a_1,a_2,a_3} &= \sum_{a_3}\left(2\sum_{a_1<a_2}+\sum_{a_1}\right) \\
&= 2\sum_{a_1<a_2,a_3}+\sum_{a_1,a_3} \\
&= 2\left(3\sum_{a_1<a_2<a_3}+2\sum_{a_1<a_2=a_3}\right)+\left(2\sum_{a_1<a_2}+\sum_{a_1}\right) \\
&= 3!\sum_{a_1<a_2<a_3}+2(1+2)\sum_{a_1<a_2}+\sum_{a_1}
\end{aligned}
$$

Thus, recurrently we prove by induction that

$$\begin{aligned}
\sum_{a_1,\cdots,a_n} &= n!\sum_{a_1<\cdots<a_n} + (n-1)![1+\sigma_2^{(n-1)}]\sum_{a_1<\cdots<a_{n-1}} \\
&+\cdots \\
&+(n-k)![1+\sigma_2^{(n-k)}+\sigma_2^{(n-k)^2}+\cdots+\sigma_2^{(n-k)^k}]\sum_{a_1<\cdots<a_{n-k}} \\
&+\cdots \\
&+2![1+2+2^2+\cdots+2^{n-2}]\sum_{a_1<a_2} \\
&+\sum_{a_1}
\end{aligned}$$

and the result follows.

□

This leads to a general expression of the coefficients of the period equation in terms of Gaussian sums.

Following we find

$$\begin{aligned}
\alpha_3 &= \tfrac{(-1)}{d^3}\big[\tfrac{(d^3-3d^2+2d)}{6}\tau(\chi_0)^3 \\
&+\tfrac{(3d^2-6d)}{6}p\textstyle\sum_{j=1}^{d-1}\chi^j(-1) \\
&+\tfrac{2d}{6}\displaystyle\sum_{\substack{i,j,k=1\\ i+j+k\equiv 0(d)}}^{d-1}\tau(\chi^i)\tau(\chi^j)\tau(\chi^k)\big]
\end{aligned}$$

this is

$$\alpha_3 = \frac{1}{6d^2}[d^2-3d+2+(3d-6)p-2\alpha_3^* p]$$

where

$$\alpha_3^* = \sum_{\substack{i,j=1\\ i+j\not\equiv 0(d)}}^{d-1}\chi^{i+j}(-1)\pi(\chi^i,\chi^j).$$

Thus in general α_n is completely determined up to the determination of

$$\alpha_n^* = \sum_{\substack{i_1,\cdots,i_{n-1}=1 \\ i_1+\cdots+i_{n-1}\not\equiv 0(d)}}^{d-1} \tau(\chi^{i_1})\cdots\tau(\chi^{i_{n-1}})\tau(\bar{\chi}^{i_1+\cdots+i_{n-1}}),$$

where χ is a character of order d.

Corollary (1.2) Let $d|p-1$, $2d \nmid p-1$. Then

$$s_d(p) > 2 \iff p = -1 - \sum_{\substack{i,j=1 \\ i+j\not\equiv 0(d)}} \chi^{i+j}(-1)\pi(\chi^i,\chi^j).$$

□

This result provides a general criteria to decide when $s_d(p) > 2$, for any $d > 2$.

Certainly, the sums $\alpha_3^*, \cdots, \alpha_n^*$ are not easy to calculate. We have done it only for $d \leq 8$. And we believe that a much deeper study on the arithmetic of the fields were they live is needed to procede.

Remark (1.3) Just recently we be came acquainted with the works of Gurak **[G1-2]** and Gupta-Zagier **[GZ]**, where they study the coefficients of the period equations for $e = (p-1)/d$ fixed. They show that at least the beginning coefficients may be computed in an elementary way.

They prove that: If $p \equiv 1(e), e > 1$ with minimal prime factor ℓ, then the coefficient α_n of the period equation of degree $d = (p-1)/e$ is a polynomial in p of degree $[n/\ell]$, if $p > n^{\varphi(e)}$ (where φ is the Euler function and [ ] is the greatest integer function). In particular if $1 < n < \ell$, then

$$\alpha_n = (1+(n-1)e)(1+(n-2)e)\cdots(1+2e)(1+e)/n!.$$

This result actually gives

$$k\alpha_k = (1+(k-1)e)\alpha_{k-1} \text{ for all } 1 < k \leq n,$$

which is exactly the relation that determines $s_d(\mathbf{F}_p)$.

Hence we find as inmediate consequences

Corollary (1.4) Let $d|p-1$ and let $1 < e = (p-1)/d$ with minimal prime factor ℓ. If $1 < n < \ell$ and $p > n^{\varphi(e)}$, then

$$s_d(\mathbf{F}_p) \geq n.$$

□

Moreover, recalling that $s_d(\mathbf{F}_p) \leq 2$ if $3d|p-1$, we obtain the following converse result.

Corollary (1.5) Let $d|p-1, 2d \nmid p-1$ and let $\varphi(p,d)$ be the Euler function of $(p-1)/d > 1$.

If $p > 3^{\varphi(p,d)}$, then it holds

$$s_d(\mathbf{F}_p) = 2 \iff 3d|p-1.$$

Proof: $s_d(\mathbf{F}_p) > 1$ since $2d \nmid p-1$. Hence clearly $3d|p-1 \Longrightarrow s_d(\mathbf{F}_p) = 2$.

Conversely, assume $3d \nmid p-1$. Then the minimal prime factor in $(p-1)/d$ is $\ell \geq 5$. Thus for $n = 3$, if $p > 3^{\varphi(p,d)}$, then $3\alpha_3 = (1 + 2(p-1)/d)\alpha_2$ by (1.4) above. Hence $s_d(\mathbf{F}_p) > 2$ and the result follows.

□

2. On the Coefficients of the Period Equations for $s_d(\mathbf{Z}/p^\ell\mathbf{Z})$

The same method developed in **1.** may be applied to find expresions for the coefficients of the period equations

$$P_j(X) = \Pi_{a \in G_{r+1-j}/\mathcal{U}_{r+1-j}}(X - S(\zeta^{p^j})^a) \text{ of degree } \begin{cases} d_j = p^{r-j}k, k|p-1 \\ 0 \leq j \leq r \end{cases}$$

involved in the calculation of $s_d(\mathbf{F}/p^\ell\mathbf{Z})$.

The easiest example of $s_d(\mathbf{Z}/p^{r+1}\mathbf{Z})$ we may try to find is that for $r = 1$ with $k = 2$:

Let

$$G_2 = (\mathbf{Z}/p^2\mathbf{Z})^*, \mathcal{U}_2 = G_2^{d_0}, d_0 = 2p = d$$

$$G_1 = (\mathbf{Z}/p\mathbf{Z})^*, \mathcal{U}_1 = G_1^{d_1}, d_1 = 2$$

and

$$H_0(T) = \beta_d T^d + \beta_{d-1} T^{d-1} + \cdots + \beta_1 T + 1$$

$$H_1(T) = \alpha_2 T^2 + \alpha_1 T + 1$$

reciprocal polynomials of

$$P_0(T) = \Pi_{a \in G_2/\mathcal{U}_2}(T - S(\zeta^{p^2})^a)$$

$$P_1(T) = \Pi_{a \in G_1/\mathcal{U}_1}(T - S(\zeta^p)^a).$$

Then

$$H(T) = H_1(T)H_2(T) = \gamma_{d+k} T^{d+k} + \gamma_{d+k-1} T^{d+k-1} + \cdots + \gamma_1 T + 1$$

where

$$\gamma_\ell = \sum_{i+j=\ell} \alpha_i \beta_i \quad \text{with} \quad \alpha_0 = \alpha_1 = \beta_0 = 1.$$

Then

$$H(T) - (1 - \frac{(p-1)}{k} T)H'(T) = \sum_{n=0}^{d+k} [(1 + n\frac{(p-1)}{k}\gamma_n - (n+1))\gamma_{n+1}]T^n$$

and

$$s_{2p}(\mathbf{Z}/p^2\mathbf{Z}) = min\{n | (1 + n\frac{(p-1)}{k})\gamma_n \neq (n+1)\gamma_{n+1}\}.$$

Let $s = s_{2p}(\mathbf{Z}/p^2\mathbf{Z})$

For $H_1(T)$ we know:

$$\begin{aligned} \alpha_1 &= 1 \\ \alpha_2 &= \begin{cases} -(p-1)/4 \text{ if } p \equiv 1(4) \\ (p+1)/4 \text{ if } p \equiv 3(4) \end{cases} \end{aligned}$$

For $H_0(T)$ we find:

$$\begin{aligned} \beta_1 &= -\textstyle\sum_{x \in G_2/\mathcal{U}_2} S(\zeta_{p^2})^x \\ &= \textstyle\sum_{x \in G_2/\mathcal{U}_2} \sum_{u \in \mathcal{U}_2} \zeta_{p^2}^{ux} \\ &= -\textstyle\sum_{x \in G_2} \zeta_{p^2}^{x} \\ &= -\left[\textstyle\sum_{i=1}^{p^2-1} \zeta_{p^2}^{i} - \sum_{i=1}^{p-1} \zeta_{p^2}^{pi}\right] \\ &= -[(-1)-(-1)] \\ &= 0 \end{aligned}$$

Following by the method developed in **1.**, applying lemma **(3.1)** to characters mod p^2, we obtain

$$\beta_2 = \frac{(-1)^2}{(2p)^2} \sum_{i,j=1}^{2p-1} \left(\frac{1}{2} \sum_a \bar{\chi}^i(a) \sum_b \bar{\chi}^j(b) - \frac{1}{2} \sum_a \bar{\chi}^{i+j}(a) \right) \tau(\chi^i)\tau(\chi^j)$$

where χ is a primitive character mod p^2, of order $d = 2p$, and $a, b \in G_2/\mathcal{U}_2$.

Notice that then χ^i is primitive for all $1 \leq i \neq p \leq 2p-1$. Hence

$$\begin{aligned} \tau(\chi^i) &\neq 0 \text{ for all } 1 \leq i \neq p \leq 2p-1 \\ \tau(\chi_0) &= 0 \end{aligned}$$

and

$$\tau(\chi^p) = 0 \text{ where } \chi^p \text{ is the quadratic character mod } p^2.$$

Moreover, for all $i \leq i \neq p \leq 2p-1$

$$\tau(\chi^i)\tau(\bar{\chi}^i) = \chi^i(-1)p(p-1)$$

and

$$\sum_{i=0}^{2p-1} \chi^i(-1) = \begin{cases} 2p & \text{if} \quad -1 \in \mathcal{U}_2 \\ 0 & \text{if} \quad -1 \notin \mathcal{U}_2 \end{cases}$$

Thus we obtain

$$\beta_2 = \begin{cases} -\frac{(p-1)^2}{2} & \text{if} \quad p \equiv 1(4) \\ 0 & \text{if} \quad p \equiv 3(4) \end{cases}$$

since χ^p is the quadratic character and $s = 1$ iff $p \equiv 1(4)$, otherwise $s > 1 \Longrightarrow 2\gamma_2 = (1 + \frac{(p-1)}{2}) \Longrightarrow \beta_2 = \frac{p}{2}$. (Actually this fact may be elementary proved).

Similarly we find

$$\beta_3 = -\frac{1}{12p^2} \sum_{\substack{i,j=1 \\ i,j,i+j \equiv 0(p)}}^{2p-1} \tau(\chi^i)\tau(\chi^j)\tau(\bar{\chi}^{i+j})$$

where the sum may be expressed in a simpler way since if χ is a primitive character mod p^2 (i.e. if χ has order $d = pk$, some $k|p-1$), then $\tau(\chi) = p\zeta_{p^2}$, where ζ_{p^2} is a primitive $p^{2\,th}$ root of unity. Then, by the reduction formula (2) in §**1.1**, the Gaussian sums mod p^2 may be computed.

Since the case $p \equiv 1(4)$ is solved, let us take $p \equiv 3(4)$.

Then the following conditions may be obtained:

$$s > 1 \;\text{ since }\; 2\gamma_2 = (1 + \frac{(p-1)}{2})\gamma_1 \;\text{ i.e. }\; \beta_2 = 0$$

$$
\begin{aligned}
s > 2 &\iff 3\gamma_3 = (1 + 2\tfrac{(p-1)}{2})\gamma_2 \\
&\iff \beta_3 = \tfrac{p(p+1)}{12} \\
s > 3 &\iff 4\gamma_4 = (1 + 3\tfrac{(p-1)}{2})\gamma_3 \\
&\iff \beta_4 = \tfrac{p(p+1)(p-3)}{32} \\
&\vdots
\end{aligned}
$$

Remark (2.1) We believe that the results in **[G1-2]** and **[GZ]** will let us compute explicit examples of $s_d(\mathbf{Z}/p^\ell\mathbf{Z})$ even if $\ell > 2$.

REFERENCES

[**AK**] Y. Amice, B. Kahn: Sommes de puissances dans les corps finis. Universite Paris 7, Unité de Recherche Associeé 212 - Theories Géométriques Nr.28 April (1992).

[**B**] P. Bachmann: Die Lehre von der Kreistheilung. Leipzig (1872).

[**Ba**] R. Baeza: Über die Stufe eines semi-lokalen Ringes. Math. Ann. 215 (1975), 13-21.

[**B1**] B.J. Birch: Waring's problem in algebraic number fields. Proc. Camb. Phil. Soc. 57 (1961), 449-459.

[**B2**] B.J. Birch: Waring's problem for p-adic number fields. Acta Arith. 9 (1964), 169-176.

[**BE**] B. Berndt, R. Evans: Sums of Gauss, Jacobi, and Jacobsthal. Journal of Number Theory 11 (1979) 349-398.

[**BS**] S.I. Borewicz, I.R. Safarevic: Zahlentheorie. Birkhäuser (1966).

[**Da**] H. Davenport: On Waring's problem for 4^{th} powers. Annals of Math. 40 (1939) 731-747.

[**D1**] L. E. Dickson: Cyclotomy, higher congruences and Waring's problem. Amer. J. Math. 57 (1935), 391-424.

[**D2**] L. E. Dickson: Cyclotomy, higher congruences and Waring's problem. Amer. J. Math. 57 (1935), 463-474.

[**D3**] L. E. Dickson: Cyclotomy and trinomial congruences. Trans. Amer. Math. Soc. 37 (1935), 363-380.

[**DLP**] Z.D. Dai, T.Y. Lam, C.K. Peng: Levels in algebra and topology. Bull. Amer. Math. Soc. 3 (1980), 845-848.

[**G1**] S. Gurak: Minimal Polynomials for Gauss Circulants and Cyclotomic Units. Pac. J. Math. vol.102, N°2 (1982) 347-353.

[**G2**] S. Gurak: Minimal Polynomials for Circular Numbers. Pac. J. Math. vol. 112, N°2 (1984) 313-331.

[**GZ**] S. Gupta, D. Zagier: On the coefficients of the minimal polynomials of gaussian periods. Math. of Comp. vol.60, N°201 January (1993) 385-398.

[**Gr**] M. Greenberg: Lecture on forms in many variables. Benjamin (1969).

[**H**] H. Hasse: Vorlesungen über Zahlentheorie. Springer (1964).

[**IR**] K. Ireland, M. Rosen: A clasical introduction to modern number theory. Springer (1990).

[**LW**] P. A. Leonard, K. S. Williams: The cyclotomic numbers of order eleven. Acta Arith. 26 (1975) 365-383.

[**Pf**] A. Pfister: Darstellung von -1 als Summe von Quadraten in einem Körper. J. London Math. Soc. 40 (1965), 159-165.

[**PAR1**] J.C. Parnami, M.K. Agrawal, A.R. Rajwade: On the 4-power Stufe of a field. Rendiconti del Circolo Mat. di Palermo 30 (1981), 245-254.

[**PAR2**] J.C. Parnami, M.K. Agrawal, A.R. Rajwade: On the fourth power Stufe of p-adic completions of algebraic number fields. Rend. Sem. Mat. Univers. Politecn. Torino vol. 44°, 1 (1986), 141-153.

[**PR**] S. Pall, A.R. Rajwade: Power Stufe of Galois fields. Bulletin de la Société Mathématique de Belgique 35 (1983), 123-130.

[**R**] C.P. Ramanujam: Sums of m^{th} powers in p-adic rings, Mathematika 10 (1963), 137-146.

[**Re**] Ph. Revoy: Niveaux supérieurs des corps et des anneaux. C. R. Acad. Sci. Paris 307 (1988), 203-204.

[**S**] Ch. Small: Sums of powers in large finite fields. Proc. Am. Math. Soc. vol. 65, Nr. 1 July (1977).

[**Sch1**] W. Schmidt: Equations over finite fields. Lecture Notes in Mathematics 536. Springer (1974).

[**Sch2**] W. Schmidt: Analytische Methoden für diophantische Gleichungen. Birkhäuser (1984).

[**T**] A. Tietäväinen: On diagonal forms over finite fields. Ann. Univ. Turku. Ser. AI 118 (1968), 10 pp.

[**W**] A. Weil: Number of solutions of equations in finite fields. Bull. Amer. Math. Soc. 55 (1949), 497-508.