A cyclotomic approach to the solution of Waring’s problem mod $p$

Mónica del Pilar Canales Ch.

Instituto de Matemáticas
Universidad Austral de Chile
Casilla 567, Valdivia
monicadelpilar@gmail.com

Abstract
Let $s_d(p, a) = \min\{k \mid a = \sum_{i=1}^{k} a_i^d, a_i \in \mathbb{F}_p^*\}$ be the smallest number of $d$–th powers in the finite field $\mathbb{F}_p$, sufficient to represent the number $a \in \mathbb{F}_p^*$. Then

$$g_d(p) = \max_{a \in \mathbb{F}_p^*} s_d(p, a)$$

gives an answer to Waring’s Problem mod $p$.

We first introduce cyclotomic integers $n(k, \nu)$, which then allow to state and solve Waring’s problem mod $p$ in terms of only the cyclotomic numbers $(i, j)$ of order $d$.

We generalize the reciprocal of the Gaussian period equation $G(T)$ to a $\mathbb{C}$–differentiable function $I(T) \in \mathbb{Q}[[T]]$, which also satisfies $I'(T)/I(T) \in \mathbb{Z}[[T]]$. We show that and why $a \equiv -1 \mod \mathbb{F}_p^*$ (the classical Stufe, if $d = 2$) behaves special: Here (and only here) $I(T)$ is in fact a polynomial from $\mathbb{Z}[T]$, the reciprocal of the period polynomial.

We finish with explicit calculations of $g_d(p)$ for the cases $d = 3$ and $d = 4$, all primes $p$, using the known cyclotomic numbers compiled by Dickson.

1. Introduction

Let $p > 2$ be a prime number, $d \geq 2$ a rational integer, and let $s_d(p, a)$ be the least positive integer $s$ such that $a \in \mathbb{F}_p^*$ is the sum of $s$ $d$–th powers in

\[1\] Supported by DID–UACh, Grant S–03–06
\( \mathbb{F}_p \), i.e.

\[
\text{s}_d(p, a) = \min\{k \mid a = \sum_{i=1}^{k} a_i^d, \ a_i \in \mathbb{F}_p^* \}.
\]

Since \( \mathbb{F}_p^* = \mathbb{F}_p^{gcd(d, p-1)} \), it suffices to consider \( d \mid p - 1 \).

Let \( f = (p - 1)/d \) and let \( \omega \) be a generator of \( \mathbb{F}_p^* \), fixed from now on. Clearly, it is enough to consider \( s_d(p, a) \) only for the \( d \) classes mod \( \mathbb{F}_p^* \).

Let \( a \in \mathbb{F}_p^* \) with \( \alpha \equiv \text{ind}_\omega(a) \mod d \) and let \( \theta \equiv \text{ind}_\omega(-1) \mod d \), i.e. \( \theta = 0 \) if \( f \) is even, and \( \theta = d/2 \) if \( f \) is odd.

In [2][3] we established, by considering the generating function

\[
g(T) = \frac{1}{1 - (\sum_{u \in \mathbb{F}_p^*} X_u)^T} \in (K[X]/(X^p - 1)) [[T]]
\]

with \( K = \mathbb{Q}(\zeta) \) the cyclotomic field given by \( \zeta \) a primitive \( p \)-th root of unity in \( \mathbb{C} \) that if

\[
N(k, a) := \#\{(u_1, \ldots, u_k) \in \mathbb{F}_p^* \times \cdots \times \mathbb{F}_p^* \mid a = u_1 + \cdots + u_k\}
\]

then

\[
N(k, a) = \frac{1}{p} \sum_{x=0}^{p-1} S(\zeta^x)^k \zeta^{-ax} = \frac{1}{p} \left[ f^k + \sum_{x \in \mathbb{F}_p^*/\mathbb{F}_p^*} S(\zeta^x)^k \cdot S(\zeta^{-ax}) \right],
\]

where \( S(\rho) := \sum_{u \in \mathbb{F}_p^*} \rho^u \).

Setting \( i \equiv \text{ind}_\omega(x) \mod d \) and \( \alpha + \theta \equiv \text{ind}_\omega(-a) \mod d \), we may write now

\[
N(k, a) = \frac{1}{p} \left[ f^k + \sum_{i=0}^{d-1} \eta_i^k \cdot \eta_{i+\alpha+\theta} \right]
\]

where

\[
\eta_i := S(\zeta^{d+i}) = \zeta^{d+i} + \zeta^{2d+i} + \cdots + \zeta^{(f-1)d+i}; 0 \leq i \leq d - 1
\]

are the classical Gauss periods, with minimal polynomial over \( \mathbb{Q} \) the so-called period polynomial of degree \( d \)

\[
G(T) = \prod_{i=0}^{d-1} (T - \eta_i) = \alpha_d + \alpha_{d-1}T + \cdots + \alpha_2T^{d-2} + T^{d-1} + T^d \in \mathbb{Z}[T],
\]
resolvent of the cyclotomic equation $X^p - 1 = 0$.

Hence, since $s_d(p, a) = \min\{k \mid N(k, a) \neq 0\}$ we obtain:

$$s_d(p, a) = \min\{k \mid f^k + \sum_{i=0}^{d-1} \eta_i^k \cdot \eta_{i+a+6} \neq 0\}.$$

Our goal now is to determine $s_d(p, a)$, and thus $g_d(p)$, only using the cyclotomic numbers of order $d$,

$$(i, j) := \#\{(u, v); 0 \leq u, v \leq f-1 \mid 1+\omega^{du+i} \equiv \omega^{dv+j} \mod p\}, 0 \leq i, j \leq d-1,$$

which have been extensively studied in the literature.

2. Cyclotomic Integers

We call a polynomial expression on the periods, with integer coefficients a cyclotomic integer if it has an integer value.

Examples of this are the coefficients of the period polynomial,

$$\alpha_k = s_k(\eta_0, \ldots, \eta_{d-1}) = (-1)^k \sum_{0 \leq i_1 < \cdots < i_k \leq d-1} \eta_{i_1} \cdots \eta_{i_k} \in \mathbb{Z},$$

and its discriminant

$$D_d = \prod_{0 \leq i < j \leq d-1} (\eta_i - \eta_j)^2 \in \mathbb{Z}.$$ 

We study now, for all $k \in \mathbb{N}$ and $0 \leq \nu \leq d - 1$, the non trivial cyclotomic integers

$$n(k, \nu) = \sum_{i=0}^{d-1} \eta_i^k \cdot \eta_{i+\nu} \in \mathbb{Z}; 0 \leq \nu \leq d - 1.$$ 

The theory of cyclotomy states the following formulae for the periods and the cyclotomic numbers (see [1][3][5]). For all $0 \leq k, l \leq d - 1$ it holds:

(i) $\eta_l \eta_{l+k} = \sum_{h=0}^{d-1} (k, h) \eta_{l+h} + f \delta_{\theta k}$

(ii) $\sum_{l=0}^{d-1} \eta_l \eta_{l+k} = p \delta_{\theta k} - f$

(iii) $\sum_{h=0}^{d-1} (k, h) = f - \delta_{\theta k}$

3
with Kronecker’s $\delta_{ij}$.

The cyclotomic integers $n(k, \nu)$ assume values in $\mathbb{Z}$ despite not being symmetric on the periods, since they satisfy the following recurrence formula:

**Lemma 1.** Let $0 \leq \nu \leq d - 1$ and $k \geq 1$. Then

$$n(k + 1, \nu) = \sum_{l=0}^{d-1} (\nu, l) n(k, l) + f \delta_{\nu \nu} n(k - 1, 0)$$

where $n(0, \nu) = -1$ and $n(1, \nu) = p \delta_{\nu \nu} - f$.

**Proof.** Clearly,

$$n(0, \nu) = \sum_{i=0}^{d-1} \eta_{i+\nu} = \zeta + \zeta^2 + \cdots + \zeta^{p-1} = -1$$

and

$$n(1, \nu) = \sum_{i=0}^{d-1} \eta_{i+\nu} \eta_i = p \delta_{\nu \nu} - f$$

by (ii).

Now by (i), multiplying $\eta_l \eta_{\nu+l}$ by $\eta_l^k$ and adding over $l$ we get

$$n(k + 1, \nu) = \sum_{l=0}^{d-1} \eta_{i+\nu+l}^k + f \delta_{\nu \nu} n(k - 1, 0).$$

This turns out to be the key to determine $N(k, a)$ in terms of only the cyclotomic numbers in a remarkably simple way, since we find

**Lemma 2.** Let $0 \leq \nu \leq d - 1$. Then

$$n(1, \nu) + f = p \delta_{\nu \nu}$$

$$n(2, \nu) + f^2 = p (\nu, \theta)$$

$$n(3, \nu) + f^3 = p \sum_{i=0}^{d-1} (\nu, i) (i, \theta) + f \delta_{\nu \nu} [n(1, \nu) + f]$$

$$n(4, \nu) + f^4 = p \sum_{i,j=0}^{d-1} (\nu, i) (i, j) (j, \theta) + f \delta_{\nu \nu} [n(2, \nu) + f^2] + f(0, \theta) [n(1, \nu) + f].$$

and for $k \geq 5$
\[ n(k, \nu) + f^k = \sum_{i_2, \ldots, i_{k-1} = 0}^{d-1} p(l, i_2)(i_2, i_3) \ldots (i_{k-1}, \theta) + f\delta_0[n(k-2, \nu) + f^{k-2}] + f(0, \theta)[n(k-3, \nu) + f^{k-3}] + \sum_{j=4}^{k-1} f \sum_{i_2, \ldots, i_{j-2} = 0}^{d-1} (0, i_2) \ldots (i_{j-2}, \theta) \right] n(k-j, \nu) + f^{k-j} \]

**Proof.** The formulae for \( k = 1, 2, 3, 4 \) result by straightforward computation. For higher \( k \), we use induction on \( k \). For all \( 0 \leq l \leq d-1 \), assume the formula for up to \( k \geq 4 \). This is (the empty sum for \( k = 4 \) is assumed null by convention)

\[ n(k, l) = \sum_{i_2, \ldots, i_{k-1} = 0}^{d-1} p(l, i_2)(i_2, i_3) \ldots (i_{k-1}, \theta) - f^k + f\delta_0[n(k-2, l) + f^{k-2}] + f(0, \theta)[n(k-3, l) + f^{k-3}] + \sum_{j=4}^{k-1} f \sum_{i_2, \ldots, i_{j-2} = 0}^{d-1} (0, i_2) \ldots (i_{j-2}, \theta) \right] n(k-j, l) + f^{k-j}. \]

Hence, by our previous lemma and the induction hypothesis, we have

\[ n(k+1, \nu) = \sum_{l=0}^{d-1} (\nu, l) n(k, l) + f\delta_0 n(k-1, 0) + f\delta_0 \sum_{l=0}^{d-1} (\nu, l) - f^k + f\delta_0[n(k-2, l) + f^{k-2}] + f(0, \theta)[n(k-3, l) + f^{k-3}] + \sum_{j=4}^{k-1} f \sum_{i_2, \ldots, i_{j-2} = 0}^{d-1} (0, i_2) \ldots (i_{j-2}, \theta) \right] n(k-j, l) + f^{k-j} \]

Now, since \( p\delta_0 = n(1, \nu) + f \) and \( \sum_{l=0}^{d-1} (\nu, l) = f - \delta_0 \nu \), and using that

\[ \sum_{l=0}^{d-1} (\nu, l) n(k-j, l) = n(k+1) - j, \nu - f\delta_0 \nu n((k-1) - j, 0), \]

the result follows as we may write \( \sum_{l=0}^{d-1} (\nu, l) n(k-j, l) + (f - \delta_0 \nu) f^{k-j} \) as \( n((k+1) - j, \nu) + f^{(k+1)-j} - f\delta_0 \nu [n((k-1) - j, 0) + f^{(k-1)-j}] \). \( \square \)
3. The Cyclotomic Solution of Waring’s Problem mod \( p \)

We now may state the result that completes our study on higher levels and Waring’s problem in \( \mathbb{F}_p \) in terms of cyclotomy.

**Theorem 1.** Let \( p > 2 \) be a prime number and \( d \geq 2 \) an integer with \( p - 1 = df \). Let \( \omega \) be a fixed generator of \( \mathbb{F}_p^* \), let \((i, j); 0 \leq i, j \leq d - 1\) be the cyclotomic numbers of order \( d \). Also let \( \theta = 0 \) if \( f \) even, and \( \theta = d/2 \) if \( f \) odd. Then, given \( a \in \mathbb{F}_p^* \setminus \mathbb{F}_d^* \) with \( \alpha \equiv \text{ind}_\omega(a) \mod d \), we get

\[
s_d(p, a) = 2 \quad \text{if} \quad (\alpha + \theta, \theta) \neq 0
\]

and otherwise

\[
s_d(p, a) = \min\{s \mid \exists 0 \leq i_2, \ldots, i_{s-1} \leq d - 1: (\alpha + \theta, i_2)(i_3) \ldots (i_{s-1}, \theta) \neq 0\}. \]

**Proof.** Since \( a \in \mathbb{F}_p^* \setminus \mathbb{F}_d^* \) and \( \alpha + \theta \equiv \text{ind}_\omega(-a) \mod d \), we have

\[
s_d(p, a) = \min\{k \geq 2 \mid n(k, \alpha + \theta) + f^k \neq 0\},
\]

and hence \( n(l, \alpha + \theta) + f^l = 0 \), for all \( l < s_d(p, a) = s \). Then by Lemma 2

\[
n(s, \alpha + \theta) + f^s = p \sum_{i_2, \ldots, i_{s-1} = 0}^{d-1} (\alpha + \theta, i_2)(i_3) \ldots (i_{s-1}, \theta).
\]

Thus clearly

\[
s_d(p, a) = 2, \quad \text{for} \quad (\alpha + \theta, \theta) \neq 0
\]

and otherwise \( s_d(p, a) \) is the least integer \( s \) with \( 3 \leq s \leq d \), such that for some \( 0 \leq i_2, \ldots, i_{s-1} \leq d - 1 \), we have a nonvanishing consecutive product of \( s - 1 \) cyclotomic numbers of the form \( (\alpha + \theta, i_2)(i_3) \ldots (i_{s-1}, \theta) \neq 0 \). □

Hence we obtain a solution of Waring’s problem in \( \mathbb{F}_p \) via cyclotomy as:

**Theorem 2.** Let \( p, d, f, \omega, \theta, a, \alpha = \text{ind}_\omega(a) \) and the cyclotomic numbers \((i, j)\) be as in Theorem 2. We define a matrix \( M = (m_{ij})_{0 \leq i, j \leq d - 1} \) by

\[
m_{ij} = \begin{cases} 0, & \text{if } (i, j) = 0, \\ 1, & \text{otherwise,} \end{cases}
\]

and we denote its \( n \)-th power as \( (m_{ij}^{(n)}) := M^n \).

Then

\[
g_d(p) = \max_{0 \leq \alpha \leq d - 1} \min\{s \mid m_{(\alpha + \theta)\theta}^{(s-1)} \neq 0\}.
\]
Proof. By Theorem 1, $s_d(p,a)$ is the least integer $s$ with $2 \leq s \leq d$ such that $(\alpha + \theta, \theta) \neq 0$ or for some $0 \leq i_2, \ldots, i_{s-1} \leq d-1$ we have $(\alpha + \theta, i_2)(i_2, i_3) \ldots (i_{s-1}, \theta) \neq 0$. Also, $g_d(p) = \max_{0 \leq \alpha \leq d-1} \{s_d(p,a)\}$.

Thus, since

$$m_{(\alpha+\theta)\theta}^{(n)} = \sum_{i_2, i_3, \ldots, \eta = 0}^{d-1} m_{(\alpha+\theta)i_2} \cdot m_{i_3 i_3} \cdot \ldots \cdot m_{i_n \theta}$$

is the entry at $(\alpha + \theta, \theta)$ of the $n$–th power of the matrix $M$, where $m_{ij} \neq 0$ iff $(i, j) \neq 0$, the result follows. □

4. On the Generalization of Theorem 1 in [2]

In [2], we only consider the case $a \equiv -1 \mod \mathbb{F}_p^\times$, i.e. $\alpha + \theta \equiv 0 \mod d$, finding $s_d(p,-1)$ in terms of the coefficients $\alpha_k; 2 \leq k \leq d$ of the period polynomial.

Now if $\alpha + \theta \neq 0 \mod d$, we can generalize Theorem 1 in [2] as follows:

**Theorem 3.** Let $p > 2$ be a prime number and $d \geq 2$ an integer with $d \mid p-1$. Let $\omega$ be a fixed generator of $\mathbb{F}_p^\times$ and let $\eta_i; 0 \leq i \leq d-1$ be the Gaussian periods. Then if $a \in \mathbb{F}_p^\times \setminus \mathbb{F}_p^\times d$ with ind$_\omega(-a) \equiv \alpha + \theta \mod d$, we have

$$s_d(p, a) = \text{ord}_T \left( \frac{1}{1-fT} - \frac{I_{\alpha+\theta}(T)^{d}}{I_{\alpha+\theta}(T)} \right)$$

where

$$I_{\alpha+\theta}(T) = \prod_{i=0}^{d-1} (1 - \eta_i T)^{\frac{\eta_i (\alpha+\theta)}{n_i}} \in \mathbb{Q}[[T]]$$

is a complex differentiable function of $T$ and ord$_T$ is the usual valuation in $\mathbb{Z}[[T]]$.

**Proof:** We have

$$s_d(p, a) = \min \{ k \mid N(k, a) \neq 0 \} = \text{ord}_T \left( \sum_{k=0}^{\infty} N(k, a) T^k \right)$$
where 
\[ N(k, a) = \frac{1}{p} [f^k + n(k, \alpha + \theta)] = \frac{1}{p} [f^k + \sum_{i=0}^{d-1} \eta_i^k \cdot \eta_i + \alpha + \theta]. \]

Thus formally
\[
\sum_{k=0}^{\infty} N(k, a) T^k = \frac{1}{p} \left[ \sum_{k=0}^{\infty} f^k T^k + \sum_{k=0}^{\infty} n(k, \alpha + \theta) T^k \right]
= \frac{1}{p} \left[ \sum_{k=0}^{\infty} f^k T^k + \sum_{k=0}^{\infty} \left( \sum_{i=0}^{d-1} \eta_i^k \cdot \eta_i + \alpha + \theta \right) T^k \right]
= \frac{1}{p} \left[ \sum_{k=0}^{\infty} f^k T^k + \sum_{i=0}^{d-1} \left( \sum_{k=0}^{\infty} \eta_i^k \cdot \eta_i + \alpha + \theta \right) T^k \right]
= \frac{1}{p} \left[ \sum_{i=0}^{d-1} \frac{1}{1-f T} + \sum_{i=0}^{d-1} \frac{\eta_i + \alpha + \theta}{1-\eta_i T} \right].
\]

Now, considering \( \frac{\eta_i + j}{1-\eta_i T} \) as a complex differentiable function of \( T \) for all \( 0 \leq i, j \leq d-1 \), and recalling that \( \frac{\eta_i + j}{\eta_i} \in \mathbb{C}\{0\} \), we have
\[
\sum_{i=0}^{d-1} \frac{\eta_i + j}{1-\eta_i T} = -\sum_{i=0}^{d-1} \frac{\eta_i + j}{\eta_i} \cdot \frac{(1-\eta_i T)'}{(1-\eta_i T)}
= -\sum_{i=0}^{d-1} \frac{\eta_i + j}{\eta_i} \log(1-\eta_i T)'
= -\left[ \sum_{i=0}^{d-1} \log((1-\eta_i T)^{\frac{\eta_i + j}{\eta_i}}) \right]'
= -\log \left( \prod_{i=0}^{d-1} (1-\eta_i T)^{\frac{\eta_i + j}{\eta_i}} \right)'
= -\log I_j(T)'
= -\frac{I_j(T)'}{I_j(T)} \in \mathbb{Z}[[T]],
\]
where \( I_j(T) = \prod_{i=0}^{d-1} (1-\eta_i T)^{\frac{\eta_i + j}{\eta_i}} \) has a power series expansion \( I_j(T) = \sum_{k=0}^{\infty} c_k T^k \in \mathbb{C}[[T]] \), where \( c_k = -\frac{1}{k} \sum_{i=0}^{k-1} c_i \cdot n(k-1-l, j) \) and \( c_0 = 1 \). Thus, we recursively obtain \( k!c_k \in \mathbb{Z}, \forall k \geq 0 \), and hence \( I_j(T), I_j(T)' \in \mathbb{Q}[[T]] \). \( \square \)
Remark: This finally shows the class of $-1$ to be special since

$$I_{\alpha+\theta}(T) \in \mathbb{Q}[T] \Leftrightarrow \frac{\eta_{i+\alpha+\theta}}{\eta_i} \in \mathbb{N}, \ \forall \ 0 \leq i \leq d-1.$$  

This is, iff $\alpha + \theta = 0$ and hence $a \equiv -1 \mod \mathbb{F}_p^{*}$. In this case,

$$I_0(T) = \prod_{i=0}^{d-1} (1 - \eta_iT) = T^dG(T^{-1})$$

is the reciprocal of the Gauss period polynomial and we recover Theorem 1 of [2].

5. Explicit Numerical Results

We state the complete results for $d = 3$ and $d = 4$, for all primes $p$, following [4][5]:

**Theorem 4.** Let $p = 3f + 1$ be a prime number with $4p = L^2 + 27M^2$ and $L \equiv 1 \mod 3$. Then

$$g_3(p) = \begin{cases} 3, & \text{if } p = 7, \\ 2, & \text{otherwise.} \end{cases}$$

**Proof.** Since $f$ is even, we have $(h,k) = (k,h)$, and it is known by [4] that

$$18(0,1) = 2p - 4 - L + 9M$$

and $18(0,2) = 2p - 4 - L - 9M$.

Then by Theorem 1, with $\theta = 0$ and the sign of $M$ depending on the choice of the generator $\omega$, we have

$$s_3(p, \omega) = \begin{cases} 2, & \text{if } (1,0) \neq 0 \ i.e. \ 2p \neq 4 + L - 9M \\ 3, & \text{otherwise} \end{cases}$$

and

$$s_3(p, \omega^2) = \begin{cases} 2, & \text{if } (2,0) \neq 0 \ i.e. \ 2p \neq 4 + L + 9M \\ 3, & \text{otherwise.} \end{cases}$$
Thus
\[ g_3(p) = \begin{cases} 
2, & \text{if } 2p \neq 4 + L \pm 9M, \\
3, & \text{otherwise}.
\end{cases} \]

Now, \( g_3(p) = 3 \iff \exists \alpha \in \{1, 2\} \) with \( (\alpha, 0) = 0 \iff 4p = L^2 + 27M^2 = 8 + 2L \pm 18M \iff L = M = 1 \iff p = 7. \quad \square \)

**Theorem 5.** Let \( p = 4f + 1 \) be a prime number with \( p = x^2 + 4y^2 \) and \( x \equiv 1 \mod 4 \). Then
\[ g_4(p) = \begin{cases} 
4, & \text{if } p = 5, \\
3, & \text{if } p = 13, 17, 29, \\
2, & \text{otherwise}.
\end{cases} \]

**Proof.** By Theorem 1, with \( \theta = \begin{cases} 
0, & \text{if } f \text{ even}, \\
d/2, & \text{if } f \text{ odd},
\end{cases} \) and the sign of \( y \) depending on the choice of the generator \( \omega \), we have
\[ s_4(p, \omega^\alpha) = \begin{cases} 
1, & \text{if } \alpha = 0 \\
2, & \text{if } \alpha \neq 0, (\alpha + \theta, \theta) \neq 0 \\
3, & \text{if } \alpha \neq 0, (\alpha + \theta, \theta) = 0 \\
 & \text{and } (\alpha + \theta, i)(i, \theta) \neq 0 \text{ for some } 0 \leq i \leq 3 \\
4, & \text{otherwise}
\end{cases} \]
where by [4] we may find the cyclotomic numbers in terms of the representation of \( p \).

If \( f \) is even:
\begin{align*}
16(0, 0) &= p - 11 - 6x \\
16(0, 1) &= p - 3 + 2x + 8y \\
16(0, 2) &= p - 3 + 2x \\
16(0, 3) &= p - 3 + 2x - 8y \\
16(1, 2) &= p + 1 - 2x
\end{align*}
and
\begin{align*}
(1, 1) &= (0, 3), \quad (1, 3) = (2, 3) = (1, 2), \quad (2, 2) = (0, 2), \quad (3, 3) = (0, 1), \quad \text{with} \\
(i, j) &= (j, i).
\end{align*}
If $f$ is odd:

\[ 16(0, 0) = p - 7 + 2x \]
\[ 16(0, 1) = p + 1 + 2x - 8y \]
\[ 16(0, 2) = p + 1 - 6x \]
\[ 16(0, 3) = p + 1 + 2x + 8y \]
\[ 16(1, 0) = p - 3 - 2x \]

and

\[ (1, 1) = (2, 1) = (2, 3) = (3, 0) = (3, 3) = (1, 0), \]
\[ (1, 3) = (3, 2) = (0, 1), (2, 0) = (2, 2) = (0, 0). \]

Thus, we find $g_4(p) > 2$ if $p = x^2 + 4y^2$, with $x \equiv 1 \mod 4$, satisfies one of the following diophantine equations:

\[ f \text{ even:} \]
\[ (\alpha = 1) \quad x^2 + 4y^2 + 2x + 8y = 3 \]
\[ (\alpha = 2) \quad x^2 + 4y^2 + 2x = 3 \]
\[ (\alpha = 3) \quad x^2 + 4y^2 + 2x - 8y = 3 \]

\[ f \text{ odd:} \]
\[ (\alpha = 1) \quad x^2 + 4y^2 + 2x - 8y = -1 \]
\[ (\alpha = 2) \quad x^2 + 4y^2 - 6x = -1 \]
\[ (\alpha = 3) \quad x^2 + 4y^2 + 2x + 8y = -1 \]

All these are equations of the form $(x + a)^2 + 4(y + b)^2 = c$ and one easily finds that the only solutions give $p = 5, 13, 17, 29$.

Now, checking for these primes the equations for $g_4(p) = 4$ we find only $g_4(5) = 4$, and thus $g_4(13) = g_4(17) = g_4(29) = 3$. \hfill \square

We may obtain complete solutions for Waring’s problem mod $p$ and thus Waring’s problem mod $n$ (see [6][7]), for all $d \geq 3$ for which the cyclotomic numbers are known or may be found in terms of the representations of multiples of $p$ by binary quadratic forms. Clearly, for $d > 4$ much effort is needed to obtain the $d^2$ cyclotomic constants, and other representations of multiples of $p$ by quadratic forms and the study of different cases is necessary (see [2][3][4][5]), but since $s_d(p, -1)$ and $g_d(p)$ are still open problems for $3d + 1 \leq p < (d - 1)^4$, our work seems to give the only complete theoretical result on the subject.
Conclusion

We introduced the concept of cyclotomic integers and gave some non-trivial examples, the \( n(k, \nu) \), which allowed us to solve the modular Waring’s Problem using only the classical cyclotomic numbers.

We saw that the analytic function \( I_{\alpha+\theta}(T) \) is a formal power series with coefficients in \( \mathbb{Q} \), and that for \( a \equiv -1 \mod \mathbb{F}_p^* \), i.e. \( \alpha = \theta \), in fact \( I_{\alpha+\theta}(T) = I_0(T) \) is a polynomial in \( \mathbb{Z}[T] \), the reciprocal of the Gauss period equation.

We finished with two examples of explicit calculations of \( g_d(p) \) for \( d = 3 \) and \( d = 4 \), all primes \( p \).

References

[1] P. Bachmann, Die Lehre von der Kreisteilung und ihre Beziehungen zur Zahlentheorie, Leipzig, Teubner 1872.

[2] E. Becker, M. del P. Canales, Higher levels of \( \mathbb{Z}/p^d \mathbb{Z} \) and period equations, manuscripta math. 99 (1999), 425–441.

[3] M. del P. Canales, Higher levels of finite fields, Dissertation. Universidad de Chile, 1995.

[4] L. E. Dickson, Cyclotomy, higher congruences and Waring’s problem. Amer. J. Math 57 (1935), 391–424.

[5] L. E. Dickson, Cyclotomy, higher congruences and Waring’s problem. Amer. J. Math 57 (1935), 463–474.

[6] Ch. Small, Waring’s problem mod \( n \), Amer. Math. Monthly 84 (1977), 12–25.

[7] Ch. Small, Solution of Waring’s problem mod \( n \) (Addendum to [4]).

[8] Waring, Meditationes algebraicae, 1770/1782.