Equations in Fp. Elementary Methods

Rafael Jakimczuk

División Matemática, Universidad Nacional de Luján
Buenos Aires, Argentina
jakimczu@mail.unlu.edu.ar

Abstract

Consider the general equation in Fp, $A_1x_1^d + \ldots + A_kx_k^d = A$. Where $p$ is a prime of the form $p = dn + 1$. In this article we obtain elementary recursive formulas (in function of the cyclotomic numbers of order $d$) which give us the number $N$ of solutions $(x_1, \ldots, x_k)$ to this equation. Cyclotomic numbers of order 3 and 4 were determined in an elementary way by Gauss (see [1], pages 71-78). These numbers are given by polynomials in three variables. From our recursive formulas follow in once that $N$ ($d = 3$ and $d = 4$) is also given by a polynomial in three variables. In this article we determine using also an elementary method the cyclotomic numbers of order 3 and 4. The number $N$ of solutions to these equations ($d = 3$ and $d = 4$) is studied in [1] (see pages 307-318 and page 337) using more sophisticated methods as generalized Jacobi sums. A general formula for $N$ in terms of generalized Jacobi sums was given by A. Weil (see [1], page 337). Cyclotomic numbers of order 5 can also be determined in an elementary way (see [1], pages 93-94 and page 99). These numbers are given by polynomials in five variables. From our recursive formulas follow in once that $N$ ($d = 5$) is also given by a polynomial in five variables. This equation ($d = 5$) has been studied by H. S. Hayashi [4] (see also [1], page 337) using more sophisticated methods as Gauss sums, Jacobi sums, etc. H. S. Hayashi takes as starting point a well known not elementary general formula for $N$ in terms of Gauss sums and obtain a general not elementary formula in terms of cyclotomic numbers. Our elementary recursive formulas in terms of the cyclotomic numbers can be used whenever explicit formulas for cyclotomic numbers of order $d$ exist. There are explicit formulas for cyclotomic numbers of other orders, these formulas are determined in a not elementary way, using Jacobi sums (see [1], page 152, for an account).

Mathematics Subject Classification: 11A07, 11T22, 11T99

Keywords: Equations in Fp, number of solutions, explicit formulas, elementary methods
1 Introduction

Let us consider a positive odd prime $p$ of the form $p = dn + 1$, where $d$ is a positive integer. Let $g$ be a primitive root modulo $p$, then the set $\{1, \ldots, p-1\}$ can be written in the form $\{g^0 = 1, g^1 = g, g^2, \ldots, g^{p-2}\}$.

Let $C_0$ be a residue of the form $g^{dk}$ ($k = 0, \ldots, n - 1$), that is a $d$-th potential residue. The set of these $n$ residues we denote $C'_0$.

Let $C_i$ be ($i = 1, \ldots, d - 1$) a residue of the form $g^{dk+i}$ ($k = 0, \ldots, n - 1$). The set of these $n$ residues we denote $C'_i$.

Consequently the $d$ sets $C'_i$ ($i = 0, \ldots, d - 1$) are a partition of the set $\{1, \ldots, p-1\}$.

It is well known these $d$ sets do not depend of the primitive root $g$, only their denotation can change if we change the primitive root $g$.

**Example 1.** If $p = 3.6 + 1 = 19$ then $d = 3$ and $n = 6$. If $g = 2$ we obtain

$$C'_0 = \{1, 7, 8, 11, 12, 18\}$$

$$C'_1 = \{2, 3, 5, 14, 16, 17\}$$

$$C'_2 = \{4, 6, 9, 10, 13, 15\}$$

On the other hand, if $g = 10$ we obtain

$$C'_0 = \{1, 7, 8, 11, 12, 18\}$$

$$C'_1 = \{4, 6, 9, 10, 13, 15\}$$

$$C'_2 = \{2, 3, 5, 14, 16, 17\}$$

We have the following table of multiplication

$$C_i \ C_j = C_k \quad (k \equiv i + j \ (mod \ d))$$

**Example 2.** If $d = 3$ we have the following table of multiplication

$$C_0 \ C_0 = C_0, \quad C_0 \ C_1 = C_1, \quad C_0 \ C_2 = C_2$$

$$C_1 \ C_0 = C_1, \quad C_1 \ C_1 = C_2, \quad C_1 \ C_2 = C_0$$

$$C_2 \ C_0 = C_2, \quad C_2 \ C_1 = C_0, \quad C_2 \ C_2 = C_1$$

We indicate $C_i + C_j = C_k$ the set of all sums whose first summand is a $C_i$, whose second summand is a $C_j$ and whose result is a fixed $C_k$. The number
of sums in this set of sums we denote \( X_{i,j,k} \). Clearly \( X_{i,j,k} \) does not depend of the fixed \( Ck \).

We indicate \( Ci + Cj = 0 \) the set of all sums whose first summand is a \( Ci \), whose second summand is a \( Cj \) and whose result is zero. The number of sums in this set of sums we denote \( B_{i,j} \).

Clearly we have (commutative property) \( X_{i,j,k} = X_{j,i,k} \) and \( B_{i,j} = B_{j,i} \).

Note that if \( d \) is odd then \( n \) is even. On the other hand, if \( d \) is even then \( n \) is even or odd.

If \( n \) is even, it is well known that the additive inverse of each element in \( C'i \) also is in \( C'i \) (see example 1). Consequently, if \( n \) is even

\[
B_{i,i} = n \quad (i = 0, \ldots, d - 1)
\]

\[
B_{i,j} = 0 \quad (i \neq j)
\]

If \( n \) is odd, it is well known that the additive inverse of each element in \( C'i \) \( (i = 0, 1, \ldots, \frac{d}{2} - 1) \) is in \( C'(i + d/2) \). We shall say that \( C'i \) and \( C'(i + d/2) \) are inverse sets. Consequently, if \( n \) is odd

\[
B_{i,i+d/2} = B_{i+d/2,i} = n \quad (i = 0, 1, \ldots, \frac{d}{2} - 1)
\]

And in any other case \( B_{i,j} = 0 \).

Therefore the numbers \( B_{i,j} \) have been determined.

**Example 3.** If \( p = 4.7 + 1 = 29 \) then \( d = 4 \) and \( n = 7 \). If \( g = 2 \) we obtain

\[
C'0 = \{1, 7, 16, 20, 23, 24, 25\}
\]

\[
C'1 = \{2, 3, 11, 14, 17, 19, 21\}
\]

\[
C''2 = \{4, 5, 6, 9, 13, 22, 28\}
\]

\[
C'3 = \{8, 10, 12, 15, 18, 26, 27\}
\]

Consequently \( C'0 \) and \( C''2 \) are inverse sets and also \( C'1 \) and \( C'3 \) are inverse sets.

**Example 4.** In example 1 (with \( g=2 \)) we have \( X_{0,0,0} = 2 \). Since there are two sums with the same result in the set \( C0 + C0 = C0 \), for example \( 8+12 = 1 \) and \( 12+8 = 1 \). We have \( X_{0,0,1} = 1 \). Since there is one sum with the same result in the set \( C0 + C0 = C1 \), for example \( 8+8 = 16 \). We have \( X_{0,0,2} = 2 \). Since there are two sums with the same result in the set \( C0 + C0 = C2 \), for example \( 8+7 = 15 \) and \( 7+8 = 15 \).

**Remark.** In this article there are some long calculations. Use for example the software Maple 9.5 of Maplesoft (a division of Waterloo Maple Inc.) to obtain quickly these calculations.
2 A Recursive Elementary Method

Theorem 2.1 Let \( p \) be a prime of the form \( dn + 1 \). Let us consider the equation in \( F_p \),
\[
A_1 x_1^d + \ldots + A_k x_k^d = A
\]
Where the number of coefficients in each set \( C'_i \) (\( i = 0, 1, \ldots, d - 1 \)) is fixed and \( A \) is a fixed \( C_i \) (\( i = 0, 1, \ldots, d - 1 \)) or 0.

The number \( N \) of solutions \( (x_1, \ldots, x_k) \) to this equation is given by a polynomial of rational coefficients whose variables are the cyclotomic numbers \((s, t)_d \) and \( p \).

This polynomial can be determined from the cyclotomic numbers \((s, t)_d \) using certain polynomial recursive formulas.

These recursive formulas appear below, in the proof of this theorem.

Proof. Let us consider the following \( d + 1 \) equations (\( k \geq 3 \)). The number of solutions to these equations is indicated in the right hand. For example the first equation has \( A_0^{k-1} \) solutions.
\[
\begin{align*}
x_1^d + \ldots + x_{k-1}^d &= C0 & A_0^{k-1} \\
x_1^d + \ldots + x_{k-1}^d &= C1 & A_1^{k-1} \\
&\vdots \\
x_1^d + \ldots + x_{k-1}^d &= C(d-1) & A_{d-1}^{k-1} \\
x_1^d + \ldots + x_{k-1}^d &= 0 & B_0^{k-1}
\end{align*}
\]
Consider the case \( k = 3 \).

If \( n \) is even, let us consider the following sets of sums. The number of sums in these sets is indicated in the right hand.
\[
\begin{align*}
C0 + C0 &= C0 & X_{0,0}\,0 \\
C0 + C0 &= C1 & X_{0,0}\,1 \\
&\vdots \\
C0 + C0 &= C(d-1) & X_{0,0}\,d-1 \\
C0 + C0 &= 0 & B_{0,0} = n
\end{align*}
\]
If \( n \) is odd, let us consider the following sets of sums.
\[
\begin{align*}
C0 + C0 &= C0 & X_{0,0}\,0 \\
C0 + C0 &= C1 & X_{0,0}\,1
\end{align*}
\]
Now, consider the equations.

\[ x_1^d + x_2^d = C_i \quad (i = 0, 1, \ldots, d - 1) \quad A_i^2 \]

\[ x_1^d + x_2^d = 0 \quad B^2 \]

If \( n \) is even, from (2) we obtain

\[ A_0^2 = X_{0,0,0} \ d^2 + 2d \quad (4) \]

\[ A_j^2 = X_{0,0,j} \ d^2 \quad (j = 1, \ldots, d - 1) \]

\[ B^2 = nd^2 + 1 \]

If \( n \) is odd, from (3) we obtain

\[ A_0^2 = X_{0,0,0} \ d^2 + 2d \quad (5) \]

\[ A_j^2 = X_{0,0,j} \ d^2 \quad (j = 1, \ldots, d - 1) \]

\[ B^2 = 1 \]

Now, consider the following \( d + 1 \) equations \((k \geq 3)\).

\[ x_1^d + \ldots + x_k^d = C0 \quad A_0^k \]

\[ x_1^d + \ldots + x_k^d = C1 \quad A_1^k \]

\[ \vdots \]

\[ x_1^d + \ldots + x_k^d = C(d - 1) \quad A_{d-1}^k \]

\[ x_1^d + \ldots + x_k^d = 0 \quad B^k \]

Consider the first equation in (6). Note that is equation can be written in the form

\[ (x_1^d + \ldots + x_{k-1}^d) + x_k^d = C0 \quad A_0^k \quad (7) \]

We have the following sets of sums whose result is a fixed \( C0 \).

\[ C0 + 0 = C0 \quad 1 \]

\[ C0 + C0 = C0 \quad X_{0,0,0} \]

\[ C1 + C0 = C0 \quad X_{1,0,0} \]
\[ C(d - 1) + C0 = C0 \quad X_{d-1,0,0} \]
\[ 0 + C0 = C0 \quad 1 \]

These sets of sums, (7) and (1) give,

\[ A_k^0 = A_0^{k-1} + d \sum_{i=0}^{d-1} A_i^{k-1} X_{i,0,0} + dB^{k-1} \quad (8) \]

Now, consider the following \( d - 1 \) equations in (6). Note that are equations can be written in the form

\[ (x_1^d + \ldots + x_{k-1}^d) + x_k^d = Ci \quad (i = 1, \ldots, d - 1) \quad A_i^k \quad (9) \]

We have the following sets of sums whose result is a fixed \( Ci \).

\[ Ci + 0 = Ci \quad 1 \]
\[ C0 + C0 = Ci \quad X_{0,0,i} \]
\[ C1 + C0 = Ci \quad X_{1,0,i} \]
\[ \vdots \]
\[ C(d - 1) + C0 = Ci \quad X_{d-1,0,i} \]

These sets of sums, (9) and (1) give,

\[ A_i^k = A_i^{k-1} + d \sum_{j=0}^{d-1} A_j^{k-1} X_{j,0,i} \quad (i = 1, \ldots, d - 1) \quad (10) \]

Finally, consider the last equation in (6). Note that this equation can be written in the form

\[ (x_1^d + \ldots + x_{k-1}^d) + x_k^d = 0 \quad B^k \quad (11) \]

If \( n \) is even, we have the following sets of sums whose result is 0.

\[ 0 + 0 = 0 \quad 1 \]
\[ C0 + C0 = 0 \quad B_{0,0} = n \]

These sets of sums, (11) and (1) give

\[ B^k = B^{k-1} + A_0^{k-1} nd \quad (12) \]
If $n$ is odd, we have the following sets of sums whose result is 0.

\[
0 + 0 = 0 \quad 1 \\
C(d/2) + C0 = 0 \quad B_{d/2,0} = n
\]

These sets of sums, (11) and (1) give

\[
B^k = B^{k-1} + A_{d/2}^{k-1} nd
\]  

(13)

Equations (8), (10), (12) and (13) together with equations (4) and (5) are recursive formulas which give us the numbers of solutions to the equations (6).

Now, consider the following $d + 1$ equations ($k \geq 2$). The number of solutions to these equations is indicated in the right hand. For example the first equation has $A_{j,0}^k$ solutions.

\[
A_{j,1}x_1^d + \ldots + A_{j,k}x_k^d = C0 \quad A_{j,0}^k \\
A_{j,1}x_1^d + \ldots + A_{j,k}x_k^d = C1 \quad A_{j,1}^k \\
\vdots \\
A_{j,1}x_1^d + \ldots + A_{j,k}x_k^d = C(d-1) \quad A_{j,d-1}^k \\
A_{j,1}x_1^d + \ldots + A_{j,k}x_k^d = 0 \quad B_{j,k}
\]

Where the coefficients $A_{j,i}$ ($i = 1, \ldots, k$) belong to $C'j$ ($j = 0, \ldots, d - 1$).

In this case the number of solutions to these equations is obtained without difficulty from the number of solutions to the equations (6).

Thus, if the coefficients belong to $C'0$ (that is, $j = 0$) clearly we have

\[
A_{0,1}x_1^d + \ldots + A_{0,k}x_k^d = C0 \quad A_{0,0}^k = A_0^k \\
A_{0,1}x_1^d + \ldots + A_{0,k}x_k^d = C1 \quad A_{0,1}^k = A_1^k \\
\vdots \\
A_{0,1}x_1^d + \ldots + A_{0,k}x_k^d = C(d-1) \quad A_{0,d-1}^k = A_{d-1}^k \\
A_{0,1}x_1^d + \ldots + A_{0,k}x_k^d = 0 \quad B_{0,k} = B_k
\]

(14)

That is, the number of solutions of these equations is equal to the number of solutions of the corresponding equations (6).

Consequently if the coefficients belong to $C'j$ ($j = 1, \ldots, d - 1$) we obtain

\[
A_{j,1}x_1^d + \ldots + A_{j,k}x_k^d = Ch1 \quad A_{j,h1}^k = A_0^k \quad (h1 \equiv j \pmod d) \\
A_{j,1}x_1^d + \ldots + A_{j,k}x_k^d = Ch2 \quad A_{j,h2}^k = A_1^k \quad (h2 \equiv j + 1 \pmod d)
\]  

(15)
Now, let us consider the more general equations. Below of each we indicate its number.

Note that if $k = 1$, it is well known we have

\[
A_{j,1}x_1^d = C_i \quad A_{j,1}^1 = 0 \quad (i \neq j)
\]

\[
A_{j,1}x_1^d = Cj \quad A_{j,1}^1 = d
\]

\[
A_{j,1}x_1^d = 0 \quad Bj^1 = 1
\]

Now, let us consider the more general equations. Below of each we indicate its number of solutions.

For example the first equation has $Aj1,\ldots, j$s, $j(s+1)^{k1,\ldots,ks,k(s+1)}$ solutions.

\[
A_{j,1}x_1^d + \ldots + A_{j,k}x_k^d = Ch(d-1) \quad A_{j,1}^{k(d-1)} = A_{d-1}^k \quad (h(d-1) \equiv j+(d-1) \ (mod \ d))
\]

\[
A_{j,1}x_1^d + \ldots + A_{j,k}x_k^d = 0 \quad Bj^k = B^k
\]

In these equations, $k1$ coefficients belong to $C'j1,\ldots, ks$ coefficients belong to $C'js$ and $k(s+1)$ coefficients belong to $C'j(s+1)$. Where $j1,\ldots, js$ and $j(s+1)$ are $s+1 \ (s \geq 1)$ different numbers which belong to the set $\{0,1,\ldots, d-1\}$.
Let us consider the following equations (we obtain these equations by elimination of the last \(k(s + 1)\) coefficients in the equations (17)). Below of each we indicate its number of solutions.

\[
A_{j_1,1}x_1^d + \ldots + A_{j_1,k_1}x_{k_1}^d + \ldots + A_{j_s,1}x_{k_1+\ldots+k(s-1)+1}^d + \ldots + A_{j_s,k_s}x_{k_1+\ldots+k_s}^d = C0
\]

\(\text{A}j_1,\ldots j^{s_{k_1},\ldots k_s}
\]

\[
A_{j_1,1}x_1^d + \ldots + A_{j_1,k_1}x_{k_1}^d + \ldots + A_{j_s,1}x_{k_1+\ldots+k(s-1)+1}^d + \ldots + A_{j_s,k_s}x_{k_1+\ldots+k_s}^d = C1
\]

\(\text{A}j_1,\ldots j^{s_{k_1},\ldots k_s}
\]

\vdots

\[
A_{j_1,1}x_1^d + \ldots + A_{j_1,k_1}x_{k_1}^d + \ldots + A_{j_s,1}x_{k_1+\ldots+k(s-1)+1}^d + \ldots + A_{j_s,k_s}x_{k_1+\ldots+k_s}^d = C(d-1)
\]

\(\text{A}j_1,\ldots j^{s_{k_1},\ldots k_s}
\]

\[
A_{j_1,1}x_1^d + \ldots + A_{j_1,k_1}x_{k_1}^d + \ldots + A_{j_s,1}x_{k_1+\ldots+k(s-1)+1}^d + \ldots + A_{j_s,k_s}x_{k_1+\ldots+k_s}^d = 0
\]

\(\text{B}j_1,\ldots j^{s_{k_1},\ldots k_s}
\]

Let us consider the following equations (we obtain these equations from the last \(k(s + 1)\) coefficients in the equations (17))

\[
A_{j(s+1),1}x_1^d + \ldots + A_{j(s+1),k(s+1)}x_{k(s+1)}^d = C0
\]

\(\text{A}j(s+1)^{k(s+1)}_0
\]

\[
A_{j(s+1),1}x_1^d + \ldots + A_{j(s+1),k(s+1)}x_{k(s+1)}^d = C1
\]

\(\text{A}j(s+1)^{k(s+1)}_1
\]

\vdots

\[
A_{j(s+1),1}x_1^d + \ldots + A_{j(s+1),k(s+1)}x_{k(s+1)}^d = C(d-1)
\]

\(\text{A}j(s+1)^{k(s+1)}_{d-1}
\]

\[
A_{j(s+1),1}x_1^d + \ldots + A_{j(s+1),k(s+1)}x_{k(s+1)}^d = 0
\]

\(\text{B}j(s+1)^{k(s+1)}
\]

We have the following sets of sums whose result is a fixed \(Ch\).

\[
Ch + 0 = Ch \quad 1
\]

\[
0 + Ch = Ch \quad 1
\]

\[
Ci + Ck = Ch \quad i \in \{0, \ldots, d-1\} \quad k \in \{0, \ldots, d-1\} \quad X_{i,k,h}
\]

From these sets of sums, (18) and (19) we obtain (\(h = 0, \ldots, d-1\))

\[
A_{j_1,\ldots, j_s,k(s+1)}^{h_{k_1,\ldots, k_s}} + B_{j_1,\ldots, j_s,k(s+1)}^{h_{k_1,\ldots, k_s}} + \sum (A_{j_1,\ldots, j_s,k(s+1)}^{h_{k_1,\ldots, k_s}} X_{i,k,h})
\]
Where the sum runs on all pairs \((i,k)\) such that \(i \in \{0, \ldots, d-1\}\) and \(k \in \{0, \ldots, d-1\}\).

If \(n\) is even we have the following sets of sums whose result is 0.

\[
0 + 0 = 0 \quad 1
\]

\[
Ci + Ci = 0 \quad i \in \{0, \ldots, d-1\} \quad B_{i,i} = n
\]

From these sets of sums, (18) and (19) we obtain

\[
Bj1, \ldots, js, j(s+1)^{k1, \ldots, ks,k(s+1)} = Bj1, \ldots, js^{k1, \ldots, ks}Bj(s+1)^{k(s+1)}
\]

\[+
\sum_{i=0}^{d-1} \left( Aj1, \ldots, js_i^{k1, \ldots, ks}Aj(s+1)_i^{k(s+1)} \right)
\]

(21)

If \(n\) is odd we have the following sets of sums whose result is 0.

\[
0 + 0 = 0 \quad 1
\]

\[
Ci + Ck = 0 \quad (C'i and C'k are inverse sets) \quad B_{i,k} = n
\]

From these sets of sums, (18) and (19) we obtain

\[
Bj1, \ldots, js, j(s+1)^{k1, \ldots, ks,k(s+1)} = Bj1, \ldots, js^{k1, \ldots, ks}Bj(s+1)^{k(s+1)}
\]

\[+
\sum_{i=0}^{d-1} \left( Aj1, \ldots, js_i^{k1, \ldots, ks}Aj(s+1)_i^{k(s+1)} \right)
\]

(22)

Where the sum runs on all pairs \((i,k)\) such that \(C'i\) and \(C'k\) are inverse sets.

Equations (20), (21) and (22) together with equations (14), (15) and (16) are recursive formulas which give us the numbers of solutions to the equations (17).

Therefore, the number \(N\) of solutions to the general equation

\[
A_1x_1^d + \ldots + A_kx_k^d = A
\]

where the number of coefficients in each set \(C'i\) \((i = 0, 1, \ldots, d-1)\) is fixed and \(A\) is a fixed \(Ci\) \((i = 0, 1, \ldots, d-1)\) or 0, is given by a polynomial of rational coefficients in the \(d^3\) variables \(X_{i,j,k}\) and \(p\) since \(n = (p-1)/d\).

This polynomial can be determined by recurrence using the formulas proved in this theorem.

Let us consider two integers \(j\) and \(k\) such that \(j \in \{0, 1, \ldots, d-1\}\) and \(k \in \{0, 1, \ldots, d-1\}\).

The cyclotomic number \((j,k)_d\) of order \(d\) is defined (see [1], page 68) as the number of pairs \((u_1,u_2)\) of integers satisfying

\[
1 + g^{du_1+j} = g^{du_2+k} \quad 0 \leq u_1, u_2 \leq n - 1
\]

(23)
Where $g$ is a primitive root ($mod$ $p$). Consequently there are $d^2$ cyclotomic numbers.

Now we show that the numbers $X_{i,j,k}$ are cyclotomic numbers.

Let us choose a residue $a$ in $C'k$. If we multiply both sides of the $(j,k)_d$ equations (23) by an certain residue in the set $C'0$ such that the right side becomes $a$ clearly we obtain all $X_{0,j,k}$ sums in the set $C0 + Cj = Ck$ whose result is $a$. Consequently we have

$$X_{0,j,k} = (j,k)_d$$

Now, consider the set of sums $Ci + Cj = Ck$ where $i \neq 0$. If we multiply both sides of each sum in this set of sums by a same residue in $C'(d - i)$ clearly we obtain all the sums in the set $C0 + Ct = Cs$ where $t \equiv j + d - i (mod d)$ and $s \equiv k + d - i (mod d)$. Consequently we have

$$X_{i,j,k} = X_{0,t,s} = (t,s)_d$$

For example if $d=4$ we have $X_{1,3,2} = X_{0,2,1} = (2,1)_4$.

Therefore, from equations (24) and (25) the theorem follows. The theorem is proved.

3 The Cubic Equation

Theorem 3.1 If $d = 3$, the 9 cyclotomic numbers $X_{0,j,k}$ can be determined in an elementary way. We have

$$X_{0,0,0}$$
$$X_{0,0,1} = X_{0,1,0} = X_{0,2,2}$$
$$X_{0,0,2} = X_{0,1,1} = X_{0,2,0}$$
$$X_{0,1,2} = X_{0,2,1}$$

They are given by the following polynomials of rational coefficients in the three variables $F$, $G$ and $p$. Namely,

$$9X_{0,0,0} = p + F - 8$$
$$18X_{0,0,1} = 2p - F + 3G - 4$$
$$18X_{0,0,2} = 2p - F - 3G - 4$$
$$9X_{0,1,2} = p + F + 1$$

Where the integers $F$ and $G$ are given by

$$4p = F^2 + 3G^2, \quad F \equiv 1 (mod 3) \quad G \equiv 0 (mod 3)$$

(28)
The sign of $G$ depend of the primitive root $g$ used.

Consequently the cubic equation

$$A_1 x_1^3 + \ldots + A_k x_k^3 = A$$

where the number of coefficients in each set $C^i (i = 0, 1, 2)$ is fixed and $A$ is a fixed $C^i (i = 0, 1, 2)$ or 0, can be solved using elementary methods by application of theorem 2.1. The number $N$ of solutions to this equation is given by a polynomial of rational coefficients in the three variables $F$, $G$ and $p$.

Proof. The 9 unknowns $X_{0,j,k}$ can be reduced to 6. Since (conmutative property and (25))

$$X_{0,1,1} = X_{0,2,0} \quad X_{0,2,1} = X_{0,1,2} \quad X_{0,2,2} = X_{0,1,0}$$

On the other hand, clearly we have

$$X_{0,1,0} = X_{0,0,1} \quad X_{0,2,0} = X_{0,0,2}$$

Therefore now we have 4 unknowns, $X_{0,0,0}$, $X_{0,0,1}$, $X_{0,0,2}$ and $X_{0,1,2}$. Consequently (26) is proved.

The following sets of sums

$$C0 + C0 = C0 \quad X_{0,0,0}$$

(29)

$$C0 + C0 = C1 \quad X_{0,0,1}$$

(30)

$$C0 + C0 = C2 \quad X_{0,0,2}$$

(31)

give us the equation

$$nX_{0,0,0} + nX_{0,0,1} + nX_{0,0,2} = n^2 - n$$

That is

$$X_{0,0,0} + X_{0,0,1} + X_{0,0,2} + 1 = n$$

(32)

Now consider the following set of sums which has $D$ sums.

$$C0 + C1 + C2 = 0 \quad D$$

Consequently we have

$$C0 + C1 = C2 \quad X_{0,1,2} = D/n$$

On the other hand, the following sets of sums (use (26))

$$C0 + C2 = C0 \quad X_{0,0,2}$$
Equations in $\mathbb{F}_p$

\begin{align*}
C_0 + C_2 &= C_1 & D/n \\
C_0 + C_2 &= C_2 & X_{0,0,1}
\end{align*}

give us the equation

$$(X_{0,0,2} + D/n + X_{0,0,1})n = n^2$$

That is

$$X_{0,0,2} + D/n + X_{0,0,1} = n \quad (33)$$

The following sets of sums have the same number $E$ of sums

\begin{align*}
C_0 + C_1 + C_2 &= C_0 & E \\
C_0 + C_1 + C_2 &= C_1 & E \\
C_0 + C_1 + C_2 &= C_2 & E
\end{align*}

From the following sets of sums (use (26) and (25))

\begin{align*}
C_0 + 0 &= C_0 & 1 \\
C_0 + C_0 &= C_0 & X_{0,0,0} \\
C_0 + C_1 &= C_0 & X_{0,0,1} \\
C_0 + C_2 &= C_0 & X_{0,0,2}
\end{align*}

and

\begin{align*}
C_1 + C_2 &= 0 & 0 \\
C_1 + C_2 &= C_0 & D/n \\
C_1 + C_2 &= C_1 & X_{0,0,1} \\
C_1 + C_2 &= C_2 & X_{0,0,2}
\end{align*}

We obtain (multiply in order)

$$E = X_{0,0,0} D/n + X_{0,0,1}^2 + X_{0,0,2}^2 \quad (34)$$

The following 4 sets of sums

\begin{align*}
C_0 + C_1 + C_2 &= 0 & D \\
C_0 + C_1 + C_2 &= C_0 & E \\
C_0 + C_1 + C_2 &= C_1 & E \\
C_0 + C_1 + C_2 &= C_2 & E
\end{align*}
give us the equation $3En + D = n^3$. Substituting (34) into this equation we obtain

$$3 \left( X_{0,0,0}D + X_{0,0,1}^2n + X_{0,0,2}^2n \right) + D = n^3 \quad (35)$$

(32) and (33) give

$$X_{0,1,2} = D/n = X_{0,0,0} + 1 \quad (36)$$

That is $D = (X_{0,0,0} + 1)n$. Substituting this equation into (35) we obtain

$$3X_{0,0,0}^2 + 3X_{0,0,1}^2 + 3X_{0,0,2}^2 + 4X_{0,0,0} + 1 = n^2 \quad (37)$$

(37) and (32) give

$$X_{0,0,0}^2 + X_{0,0,1}^2 + X_{0,0,2}^2 + X_{0,0,0}$$
$$- X_{0,0,1} - X_{0,0,2} - X_{0,0,0}X_{0,0,1} - X_{0,0,0}X_{0,0,2} - X_{0,0,1}X_{0,0,2} = 0 \quad (38)$$

Let us write ( where $b$ and $c$ will be certain integers)

$$X_{0,0,1} = X_{0,0,0} + b \quad X_{0,0,2} = X_{0,0,0} + c \quad (39)$$

Substituting (39) into (38) we find that

$$X_{0,0,0} = b^2 + c^2 - bc - b - c \quad (40)$$

(32), (39), (34) and (40) give

$$n = 3b^2 + 3c^2 - 3bc - 2b - 2c + 1$$

Consequently

$$p = 3n + 1 = 9b^2 + 9c^2 - 9bc - 6b - 6c + 4 = \frac{(3b - 3c + 4)^2 + 3(-3c + 3b)^2}{4}$$

That is

$$4p = (3b - 3c + 4)^2 + 3(-3c + 3b)^2 \quad (41)$$

It is well known if $4p = F^2 + 3G^2$ and $G$ is multiple of 3, then $|F|$ and $|G|$ are unique ( there exist elementary proofs on this subject, see [1], page 101).

Let us write ( note that $F \equiv 1 \ (mod \ 3)$ )

$$F = -3b - 3c + 4$$
$$G = -3c + 3b$$

That is

$$F - 4 = -3b - 3c$$
$$G = 3b - 3c \quad (42)$$
Let us consider the other possibility (the sign of $G$ is changed)

$$F - 4 = -3x - 3y$$

$$-G = 3x - 3y$$

In this last case we obtain the permutation $x = c$ and $y = b$. This solution permutes the values of $X_{0,0,1}$ and $X_{0,0,2}$ leaving $X_{0,0,0}$ unchanged (see (39) and (40)). This is not surprising since the elements in the sets $C'1$ and $C'2$ can be permuted (see example 1) depending of the primitive root $g$ used.

From (42) we obtain

$$b = \frac{-F + G + 4}{6}$$

$$c = \frac{-F - G + 4}{6}$$

(43)

On the other hand, (32) and (39) give

$$9X_{0,0,0} = p - 3b - 3c - 4$$

(44)

Consequently (see (42))

$$9X_{0,0,0} = p + F - 8$$

(45)

Substituting (45) and (43) into (39) and (36) we obtain (27).

Therefore the two possible sets of cyclotomic numbers $X_{0,j,k}$ are determined by equation (41). The theorem is proved.

4 An Application, the Cubic Character of 2

The following theorem was conjectured by Euler (see [3], pages 13, 14 and 223) and first proved by Gauss (see [3], page 199). There exist others proofs by Chowla, Dedekind and others (see [3], pages 225 and 226)

**Theorem 4.1** 2 is a cubic residue of a prime $p$ if and only if $p = A^2 + 27B^2$

Proof. We can suppose 2 is a $C1$ if it is not a cubic residue (since we can change the primitive root if it is necessary).

Let us consider the number $X'_{0,0,0}$ of sums of two cubic residues whose result is a fixed cubic residue (the order of the summands is irrelevant).

Hence if 2 is a cubic residue (that is, if 2 is a $C0$),

$$2X'_{0,0,0} - 1 = X_{0,0,0}$$

(46)

Analogously let us consider the number $X'_{0,0,1}$ of sums of two cubic residues whose result is a fixed $C1$ (the order of the summands is irrelevant).
Hence if 2 is not a cubic residue (that is, if 2 is a $C_1$),

$$2X'_{0,0,1} - 1 = X_{0,0,1}$$  \hspace{1cm} (47)

Suppose that 2 is a cubic residue, (40) and (46) give

$$X'_{0,0,0} = \frac{b^2 + c^2 - bc - b - c + 1}{2}$$

Consequently $b$ and $c$ are odd.

Substituting $b = 2b' + 1$ and $c = 2c' + 1$ into (41) we obtain

$$p = (3b' + 3c' + 1)^2 + 3(3c' - 3b')^2$$  \hspace{1cm} (48)

Now suppose that 2 is not a cubic residue, (39) and (47) give

$$X'_{0,0,1} = \frac{b^2 + c^2 - bc - b - c + 1}{2}$$

Consequently $b$ is odd and $c$ is even.

Substituting $b = 2b' + 1$ and $c = 2c'$ into (41) we obtain

$$p = \frac{(6b' + 6c' - 1)^2 + 3(6c' - 6b' - 3)^2}{4}$$

From the identity

$$\left(a_1^2 + 3b_1^2\right)\left(a_2^2 + 3b_2^2\right) = (a_1a_2 - 3b_1b_2)^2 + 3(a_1b_2 + b_1a_2)^2$$

we find that

$$p = \frac{(1^2 + 3.1^2)\left((6b' + 6c' - 1)^2 + 3(6c' - 6b' - 3)^2\right)}{4^2}$$

$$= \frac{(6b' - 3c' + 2)^2 + 3(3c' - 1)^2}{4}$$  \hspace{1cm} (49)

It is well known if $p = F^2 + 3G^2$, then $|F|$ and $|G|$ are unique (there exist elementary proofs on this subject discovered first by P. Fermat, see [1], page 101). The theorem is then a direct consequence of (48) and (49).

5 The Quartic Equation

Theorem 5.1 If $d = 4$, the 16 cyclotomic numbers $X_{0,j,k}$ can be determined in an elementary way. We have if $n$ is even

$$X_{0,0,0}$$
Equations in $F_p$

\begin{align*}
X_{0,0,1} &= X_{0,1,0} = X_{0,3,3} \\
X_{0,0,2} &= X_{0,2,0} = X_{0,2,2} \\
X_{0,0,3} &= X_{0,1,1} = X_{0,3,0} \\
X_{0,1,2} &= X_{0,1,3} = X_{0,2,1} = X_{0,2,3} = X_{0,3,1} = X_{0,3,2} \\
& \text{(50)}
\end{align*}

On the other hand, if $n$ is odd

\begin{align*}
X_{0,0,0} &= X_{0,2,0} = X_{0,2,2} \\
X_{0,0,1} &= X_{0,1,3} = X_{0,3,2} \\
X_{0,0,2} &= \\
X_{0,0,3} &= X_{0,1,2} = X_{0,3,1} \\
X_{0,1,0} &= X_{0,1,1} = X_{0,2,1} = X_{0,2,3} = X_{0,3,0} = X_{0,3,3} \\
& \text{(51)}
\end{align*}

They are given by the following polynomials of rational coefficients in the three variables $F$, $G$ and $p$.

If $n$ is even they are

\begin{align*}
16X_{0,0,0} &= p + 6F - 11 \\
16X_{0,0,1} &= p - 2F + 4G - 3 \\
16X_{0,0,2} &= p - 2F - 3 \\
16X_{0,0,3} &= p - 2F - 4G - 3 \\
16X_{0,1,2} &= p + 2F + 1 \\
& \text{(52)}
\end{align*}

Where the integers $F$ and $G$ are given by

\begin{align*}
p &= F^2 + G^2, \quad F \equiv -1 \pmod{4}
\end{align*}

The sign of $G$ depend of the primitive root $g$ used.

If $n$ is odd they are

\begin{align*}
16X_{0,0,0} &= p + 2F - 7 \\
16X_{0,0,1} &= p + 2F + 4G + 1 \\
16X_{0,0,2} &= p - 6F + 1 \\
16X_{0,0,3} &= p + 2F - 4G + 1 \\
16X_{0,1,0} &= p - 2F - 3 \\
& \text{(53)}
\end{align*}

Where the integers $F$ and $G$ are given by

\begin{align*}
p &= F^2 + G^2, \quad F \equiv 1 \pmod{4}
\end{align*}
The sign of $G$ depend of the primitive root $g$ used.

Consequently the quartic equation

$$A_1x_1^4 + \ldots + A_kx_k^4 = A$$

where the number of coefficients in each set $C^i$ ($i = 0, 1, 2, 3$) is fixed and $A$ is a fixed $C^i$ ($i = 0, 1, 2, 3$) or 0, can be solved using elementary methods by application of theorem 2.1. The number $N$ of solutions to this equation is given by a polynomial of rational coefficients in the three variables $F$, $G$ and $p$

Proof. The 16 unknowns $X_{0,j,k}$ can be reduced to 10. Since (conmutative property and (25))

$$X_{0,2,2} = X_{0,2,0} \quad X_{0,2,3} = X_{0,2,1} \quad X_{0,3,0} = X_{0,1,1}$$

$$X_{0,3,1} = X_{0,1,2} \quad X_{0,3,2} = X_{0,1,3} \quad X_{0,3,3} = X_{0,1,0}$$

Case 1) $n$ is even.

The following sets of sums have the same number $S$ of sums.

$$C0 + C1 + C2 = 0 \quad S$$
$$C0 + C1 + C3 = 0 \quad S$$
$$C1 + C2 + C3 = 0 \quad S$$
$$C0 + C2 + C3 = 0 \quad S$$

Therefore we have

$$C0 + C1 = C2 \quad X_{0,1,2} = S/n$$
$$C0 + C2 = C1 \quad X_{0,2,1} = S/n$$
$$C0 + C1 = C3 \quad X_{0,1,3} = S/n$$

On the other hand, we have

$$X_{0,1,0} = X_{0,0,1} \quad X_{0,3,0} = X_{0,0,3} \quad X_{0,2,0} = X_{0,0,2}$$

For sake of simplicity we shall write

$$X_{0,0,0} = X_0 \quad X_{0,0,1} = X_1 \quad X_{0,0,2} = X_2 \quad X_{0,0,3} = X_3$$

Consequently the number of unknowns is now 5, $X_0, X_1, X_2, X_3, S/n$. Therefore (50) is proved.

The sets of sums

$$C0 + C0 = C0 \quad X_0$$
$$C0 + C0 = C1 \quad X_1$$
Equations in $F_p$

\begin{align*}
  C_0 + C_0 &= C_2 & X_2 \\
  C_0 + C_0 &= C_3 & X_3 \\
\end{align*}

give us the equation

\[ X_0 + X_1 + X_2 + X_3 + 1 = n \]  \hspace{1cm} (54)

The following sets of sums (use (50))

\begin{align*}
  C_0 + C_1 &= C_0 & X_1 \\
  C_0 + C_1 &= C_1 & X_3 \\
  C_0 + C_1 &= C_2 & S/n \\
  C_0 + C_1 &= C_3 & S/n \\
\end{align*}

give us the equation

\[ nX_1 + nX_3 + 2S = n^2 \]  \hspace{1cm} (55)

The following sets of sums

\begin{align*}
  C_0 + C_2 &= C_0 & X_2 \\
  C_0 + C_2 &= C_1 & S/n \\
  C_0 + C_2 &= C_2 & X_2 \\
  C_0 + C_2 &= C_3 & S/n \\
\end{align*}

give us the equation

\[ 2nX_2 + 2S = n^2 \]  \hspace{1cm} (56)

Let us consider the following set of sums which have $T$ sums.

\[ C_0 + C_1 + C_2 + C_3 = 0 \quad T \]

The following sets of sums

\begin{align*}
  C_0 + C_1 + C_2 &= 0 & S \\
  C_0 + C_1 + C_2 &= C_0 & X_{0,1,2,0} \\
  C_0 + C_1 + C_2 &= C_1 & X_{0,1,2,1} \\
  C_0 + C_1 + C_2 &= C_2 & X_{0,1,2,2} \\
  C_0 + C_1 + C_2 &= C_3 & T/n \\
\end{align*}

give us the equation

\[ S + nX_{0,1,2,0} + nX_{0,1,2,1} + nX_{0,1,2,2} + T = n^3 \]  \hspace{1cm} (58)
Let us consider the following sets of sums (use (50) and (25))

\[
\begin{align*}
C_0 + 0 &= C_0 & 1 \\
C_0 + C_0 &= C_0 & X_0 \\
C_0 + C_1 &= C_0 & X_1 \\
C_0 + C_2 &= C_0 & X_2 \\
C_0 + C_3 &= C_0 & X_3 \\
\end{align*}
\]

(59)

and

\[
\begin{align*}
C_1 + C_2 &= 0 & 0 \\
C_1 + C_2 &= C_0 & S/n \\
C_1 + C_2 &= C_1 & X_1 \\
C_1 + C_2 &= C_2 & X_3 \\
C_1 + C_2 &= C_3 & S/n \\
\end{align*}
\]

Consequently (multiply in order) the number of sums \(X_{0,1,2,0}\) in the set of sums \(C_0 + C_1 + C_2 = C_0\) will be

\[
X_{0,1,2,0} = X_0 \frac{S}{n} + X_1^2 + X_2 X_3 + X_3 \frac{S}{n}
\]

(60)

The sets of sums \(C_0 + C_1 + C_2 = C_1\) and \(C_0 + C_1 + C_3 = C_0\) have the same number of sums.

Let us consider the sets of sums (59) and the following sets of sums

\[
\begin{align*}
C_1 + C_3 &= 0 & 0 \\
C_1 + C_3 &= C_0 & S/n \\
C_1 + C_3 &= C_1 & X_2 \\
C_1 + C_3 &= C_2 & S/n \\
C_1 + C_3 &= C_3 & X_2 \\
\end{align*}
\]

Consequently (multiply in order) the number of sums \(X_{0,1,2,1}\) in the set of sums \(C_0 + C_1 + C_2 = C_1\) will be

\[
X_{0,1,2,1} = X_0 \frac{S}{n} + X_1 X_2 + X_2 \frac{S}{n} + X_3 X_2
\]

(61)

The sets of sums \(C_0 + C_1 + C_2 = C_2\) and \(C_0 + C_2 + C_3 = C_0\) have the same number of sums.
Let us consider the sets of sums (59) and the following sets of sums

\[
\begin{align*}
C2 + C3 &= 0 \quad 0 \\
C2 + C3 &= C0 \quad S/n \\
C2 + C3 &= C1 \quad S/n \\
C2 + C3 &= C2 \quad X_1 \\
C2 + C3 &= C3 \quad X_3
\end{align*}
\]

Consequently (multiply in order) the number of sums \(X_{0,1,2,2}\) in the set of sums \(C0 + C1 + C2 = C2\) will be

\[
X_{0,1,2,2} = X_0 \frac{S}{n} + X_1 \frac{S}{n} + X_2X_1 + X_3^2
\]

(62)

Substituting (60), (61) and (62) into (58) we obtain

\[(3X_0 + X_1 + X_2 + X_3 + 1)S + (X_1^2 + X_3^2 + 2X_2X_3 + 2X_1X_2)n + T = n^3\]  

(63)

The following sets of sums

\[
\begin{align*}
C0 + C1 + C2 + C3 &= 0 \quad T \\
C0 + C1 + C2 + C3 &= C0 \quad Q \\
C0 + C1 + C2 + C3 &= C1 \quad Q \\
C0 + C1 + C2 + C3 &= C2 \quad Q \\
C0 + C1 + C2 + C3 &= C3 \quad Q
\end{align*}
\]

give us the equation

\[4nQ + T = n^4\]  

(64)

Let us consider the sets of sums (59) and the following sets of sums

\[
\begin{align*}
C1 + C2 + C3 &= 0 \quad S \\
C1 + C2 + C3 &= C0 \quad T/n \\
C1 + C2 + C3 &= C1 \quad X_{0,1,2,0} \\
C1 + C2 + C3 &= C2 \quad X_{0,1,2,1} \\
C1 + C2 + C3 &= C3 \quad X_{0,1,2,2}
\end{align*}
\]

Consequently (multiply in order) the number \(Q\) of sums in the set of sums \(C0 + C1 + C2 + C3 = C0\) will be

\[
Q = S + X_0 \frac{T}{n} + X_1X_{0,1,2,0} + X_2X_{0,1,2,1} + X_3X_{0,1,2,2}
\]

(65)
Substituting (65), (60), (61) and (62) into (64) we obtain

\[ T(4X_0 + 1) + 4S(n + X_0X_1 + X_0X_2 + X_0X_3 + 2X_1X_3 + X_2^2) + 4n(X_1^3 + X_3^3 + 2X_1X_2X_3 + X_1X_2^2 + X_3X_2^2) = n^4 \] (66)

That is

\[ \frac{T}{n}(4X_0 + 1) + \frac{4S}{n}(n + X_0X_1 + X_0X_2 + X_0X_3 + 2X_1X_3 + X_2^2) + 4(X_1^3 + X_3^3 + 2X_1X_2X_3 + X_1X_2^2 + X_3X_2^2) = n^3 \] (67)

(55) and (56) give

\[ \frac{S}{n} = \frac{X_0 + X_2 + 1}{2} \] (68)

(63) gives

\[ \frac{T}{n} = n^2 - \frac{S}{n}(3X_0 + X_1 + X_2 + X_3 + 1) - (X_1^2 + X_3^2 + 2X_2X_3 + 2X_1X_2) \] (69)

Substituting (68), (69) and (55) into (67) we obtain

\[ 6X_0^3 - 6X_1^3 - 2X_2^3 - 6X_3^3 - 3 + 3X_0^2 + 6X_1^2 - 3X_2^2 + 6X_3^2 - 6X_0 - X_1 - 4X_2 - X_3 + 12X_0X_1X_2 - 12X_0X_1X_3 + 12X_0X_2X_3 - 12X_1X_2X_3 - 11X_0X_1 - 8X_0X_2 - 11X_0X_3 + 9X_1X_2 + 9X_2X_3 + 6X_0X_1^2 - 6X_0X_2^2 + 6X_0X_3^2 - 10X_1X_2X_3 + 2X_2X_3^2 - 10X_3X_0^2 - 2X_1X_2^2 + 6X_1X_3^2 + 6X_2X_2^2 + 6X_3X_0^2 + 6X_2X_3^2 - 2X_3X_2^2 = 0 \] (70)

(56) and (57) give

\[ X_2 = \frac{X_1 + X_3}{2} \] (71)

Substituting (71) into (70) we obtain

\[ 24X_0^3 - 15X_1^3 - 15X_3^3 - 12X_0X_1X_3 + 42X_0X_1^2 + 42X_0X_3^2 - 36X_1X_0^2 - 36X_3X_0^2 + 3X_1X_3^2 + 3X_3X_1^2 + 12X_0^2 + 39X_1^2 + 39X_3^2 - 60X_0X_1 - 60X_0X_3 + 30X_1X_3 - 24X_0 - 12X_1 - 12X_3 - 12 = 0 \] (72)

Let us write

\[ X_1 = X_0 + a \quad X_3 = X_0 + b \] (73)

Substituting (73) into (72) we obtain

\[ 16X_0(a + b - 1) = 5a^2 + 5b^2 - ab^2 - a^2b - 13a^2 - 13b^2 - 10ab + 4a + 4b + 4 \]

That is

\[ 16X_0(a + b - 1) = (a + b - 1)(5a^2 + 5b^2 - 6ab - 8a - 8b - 4) \] (74)
(73) and (71) imply that $a + b - 1$ is odd. Therefore (74) gives

$$X_0 = \frac{5a^2 + 5b^2 - 6ab - 8a - 8b - 4}{16} \quad (75)$$

(55), (75), (73) and (71) give

$$n = \frac{5a^2 + 5b^2 - 6ab - 2a - 2b}{4}$$

Note that this equation and (75) imply

$$a + b = 2(2k + 1) = 4k + 2 \quad (76)$$

On the other hand, we have

$$p = 4n + 1 = 5a^2 + 5b^2 - 6ab - 2a - 2b + 1 = (-a - b + 1)^2 + (2a - 2b)^2 \quad (77)$$

It is well known if $p = F^2 + G^2$ where $F$ is odd and $G$ is even, then $|F|$ and $|G|$ are unique (there exist elementary proofs on this subject discovered first by P. Fermat, see [1], page 101).

Let us write (note that $F \equiv -1 \pmod{4}$, see (76))

$$F = -a - b + 1$$
$$G = 2a - 2b$$

That is

$$F - 1 = -a - b$$
$$G = 2a - 2b \quad (78)$$

Let us consider the other possibility (the sign of $G$ is changed)

$$F - 1 = -x - y$$
$$-G = 2x - 2y$$

In this last case we obtain the permutation $x = b$ and $y = a$. This solution permutes the values of $X_1$ and $X_3$ leaving to $X_0$ and $X_2$ unchanged (see (73), (75) and (71)). This is not surprising since the elements in the sets $C'1$ and $C'3$ can be permuted depending of the primitive root $g$ used.

From (78) we obtain

$$a = \frac{G - 2F + 2}{4} \quad b = \frac{-G - 2F + 2}{4} \quad (79)$$

On the other hand, (55), (71) and (73) give

$$16X_{0,0,0} = p - 6a - 6b - 5 \quad (80)$$
Consequently (see (78))

\[ 16X_{0,0,0} = p + 6F - 11 \] 

(81)

Substituting (81) and (79) into (73), (71) and (68) we obtain (52).

Therefore the two possible sets of cyclotomic numbers \( X_{0,j,k} \) are determined by equation (77). The theorem is proved when \( n \) is even.

Case 2) \( n \) is odd.

The following sets of sums have the same number \( S \) of sums.

\[
\begin{align*}
C0 + C1 + C2 &= 0 \quad S \\
C0 + C1 + C3 &= 0 \quad S \\
C1 + C2 + C3 &= 0 \quad S \\
C0 + C2 + C3 &= 0 \quad S
\end{align*}
\]

Therefore we have

\[
\begin{align*}
C0 + C1 &= C0 \quad X_{0,1,0} = S/n \\
C0 + C1 &= C1 \quad X_{0,1,1} = S/n \\
C0 + C2 &= C1 \quad X_{0,2,1} = S/n
\end{align*}
\]

On the other hand, we have

\[
X_{0,1,2} = X_{0,0,3} \quad X_{0,3,2} = X_{0,0,1} \quad X_{0,2,2} = X_{0,0,0}
\]

For sake of simplicity we shall write

\[
X_{0,0,0} = X_0 \quad X_{0,0,1} = X_1 \quad X_{0,0,2} = X_2 \quad X_{0,0,3} = X_3
\]

Consequently the number of unknowns is now 5, \( X_0, X_1, X_2, X_3, S/n \). Therefore (51) is proved.

The sets of sums (54) give us the equation

\[ X_0 + X_1 + X_2 + X_3 = n \] 

(82)

The following sets of sums (use (51))

\[
\begin{align*}
C0 + C1 &= C0 \quad S/n \\
C0 + C1 &= C1 \quad S/n \\
C0 + C1 &= C2 \quad X_3 \\
C0 + C1 &= C3 \quad X_1
\end{align*}
\]
Equations in $F_p$

\[ nX_1 + nX_3 + 2S = n^2 \]  \hspace{1cm} (83)

The following sets of sums

\[ \begin{align*}
C0 + C2 &= C0 \quad X_0 \\
C0 + C2 &= C1 \quad S/n \\
C0 + C2 &= C2 \quad X_0 \\
C0 + C2 &= C3 \quad S/n
\end{align*} \]

give us the equation

\[ 2nX_0 + 2S = n^2 - n \]  \hspace{1cm} (84)

Let us consider the following set of sums which have $T$ sums.

\[ C0 + C1 + C2 + C3 = 0 \quad T \]

The following sets of sums

\[ \begin{align*}
C0 + C1 + C2 &= 0 \quad S \\
C0 + C1 + C2 &= C0 \quad X_{0,1,2,0} \\
C0 + C1 + C2 &= C1 \quad T/n \\
C0 + C1 + C2 &= C2 \quad X_{0,1,2,2} \\
C0 + C1 + C2 &= C3 \quad X_{0,1,2,3}
\end{align*} \]

give us the equation

\[ S + nX_{0,1,2,0} + nX_{0,1,2,2} + nX_{0,1,2,3} + T = n^3 \]  \hspace{1cm} (85)

Let us consider the following sets of sums (use (51) and (25))

\[ \begin{align*}
C0 + 0 &= C0 \quad 1 \\
C0 + C0 &= C0 \quad X_0 \\
C0 + C1 &= C0 \quad S/n \\
C0 + C2 &= C0 \quad X_0 \\
C0 + C3 &= C0 \quad S/n
\end{align*} \]

and

\[ \begin{align*}
C1 + C2 &= 0 \quad 0 \\
C1 + C2 &= C0 \quad X_1
\end{align*} \]
\[ C1 + C2 = C1 \quad S/n \]
\[ C1 + C2 = C2 \quad S/n \]
\[ C1 + C2 = C3 \quad X_3 \]

Consequently the number of sums \( X_{0,1,2,0} \) in the set of sums \( C0+C1+C2 = C0 \) will be
\[
X_{0,1,2,0} = X_0 X_1 + \left( \frac{S}{n} \right)^2 + X_0 \frac{S}{n} + X_3 \frac{S}{n} \quad (87)
\]

The sets of sums \( C0 + C1 + C2 = C2 \) and \( C0 + C2 + C3 = C0 \) have the same number of sums.

Let us consider the sets of sums (86) and the following sets of sums
\[
C2 + C3 = 0 \quad 0 \\
C2 + C3 = C0 \quad X_3 \\
C2 + C3 = C1 \quad X_1 \\
C2 + C3 = C2 \quad S/n \\
C2 + C3 = C3 \quad S/n
\]

Consequently the number of sums \( X_{0,1,2,2} \) in the set of sums \( C0+C1+C2 = C2 \) will be
\[
X_{0,1,2,2} = X_0 X_3 + X_1 \frac{S}{n} + X_0 \frac{S}{n} + \left( \frac{S}{n} \right)^2 \quad (88)
\]

Let us consider the following sets of sums
\[
C0 + 0 = C3 \quad 0 \\
C0 + C0 = C3 \quad X_3 \\
C0 + C1 = C3 \quad X_1 \\
C0 + C2 = C3 \quad S/n \\
C0 + C3 = C3 \quad S/n
\]

and
\[
C1 + C2 = 0 \quad 0 \\
C1 + C2 = C0 \quad X_1 \\
C1 + C2 = C1 \quad S/n \\
C1 + C2 = C2 \quad S/n \\
C1 + C2 = C3 \quad X_3
\]
Consequently the number of sums $X_{0,1,2,3}$ in the set of sums $C0 + C1 + C2 = C3$ will be

$$X_{0,1,2,3} = X_1X_3 + X_1 \frac{S}{n} + \left( \frac{S}{n} \right)^2 + X_3 \frac{S}{n} \quad (89)$$

Substituting (87), (88) and (89) into (85) we obtain

$$3 \left( \frac{S}{n} \right)^2 + \left( 1 + 2X_0 + 2X_1 + 2X_3 \right) \frac{S}{n} + (X_0X_1 + X_0X_3 + X_1X_3) + \frac{T}{n} = n^2 \quad (90)$$

The following sets of sums

$$C0 + C1 + C2 + C3 = 0 \quad T$$
$$C0 + C1 + C2 + C3 = C0 \quad Q$$
$$C0 + C1 + C2 + C3 = C1 \quad Q$$
$$C0 + C1 + C2 + C3 = C2 \quad Q$$
$$C0 + C1 + C2 + C3 = C3 \quad Q$$

give us the equation $4nQ + T = n^4$. That is

$$4Q + \frac{T}{n} = n^3 \quad (91)$$

Let us consider the sets of sums (86) and the following sets of sums

$$C1 + C2 + C3 = 0 \quad S$$
$$C1 + C2 + C3 = C0 \quad X_{0,1,2,3}$$
$$C1 + C2 + C3 = C1 \quad X_{0,1,2,0}$$
$$C1 + C2 + C3 = C2 \quad T/n$$
$$C1 + C2 + C3 = C3 \quad X_{0,1,2,2}$$

Consequently the number $Q$ of sums in the set of sums $C0 + C1 + C2 + C3 = C0$ will be

$$Q = S + X_0X_{0,1,2,3} + \frac{S}{n}X_{0,1,2,0} + X_0 \frac{T}{n} + \frac{S}{n}X_{0,1,2,2} \quad (92)$$

Substituting (92), (87), (88) and (89) into (91) we obtain

$$\frac{T}{n}(4X_0 + 1) + 8 \left( \frac{S}{n} \right)^3 + (12X_0 + 4X_3 + 4X_1) \left( \frac{S}{n} \right)^2$$

$$+ (8X_0X_1 + 8X_0X_3 + 4n) \frac{S}{n} + 4X_0X_1X_3 = n^3 \quad (93)$$
(82) and (83) give
\[ S \frac{n}{n} = \frac{X_0 + X_2}{2} \]  
(94)

(90) gives
\[ T \frac{n}{n} = n^2 - 3 \left( \frac{S}{n} \right)^2 - (1 + 2X_0 + 2X_1 + 2X_3) \frac{S}{n} - (X_0X_1 + X_0X_3 + X_1X_3) \]  
(95)

Substituting (94), (95) and (82) into (93) we obtain
\[ -4X_3^2 - 4X_3^3 - 3X_0^2 + 4X_1^2 + 9X_2^2 + 4X_3^2 - 2X_0 - 2X_2 + 16X_0X_1X_2 \\
+ 8X_0X_1X_3 + 16X_0X_2X_3 - 24X_1X_2X_3 + 6X_0X_2 + 12X_1X_2 + 4X_1X_3 \\
+ 12X_2X_3 + 8X_0X_1 + 8X_0X_3 + 4X_0X_1^2 + 16X_0X_3^2 + 4X_0X_2^2 + 16X_2X_0^2 \\
+ 8X_1X_0^2 + 8X_3X_0^2 - 8X_3X_2^2 - 8X_1X_2^2 - 12X_1X_3^2 - 12X_2X_1^2 - 12X_3X_1^2 \\
- 12X_2X_3^2 = 0 \]  
(96)

(83) and (84) give
\[ X_3 = 2X_0 - X_1 + 1 \]  
(97)

Substituting (97) into (96) we obtain
\[ 5X_0^2 + 4X_1^2 + X_2^2 - 8X_0X_1 - 2X_0X_2 + 2X_0 - 4X_1 - 2X_2 = 0 \]  
(98)

Let us write
\[ X_1 = X_0 + a \quad X_2 = X_0 + b \]  
(99)

Substituting (99) into (98) we obtain
\[ X_0 = \frac{4a^2 + b^2 - 4a - 2b}{4} \]  
(100)

Substituting (99), (97) and (100) into (82) we obtain
\[ n = 4a^2 + b^2 - 4a - b + 1 \]

Therefore
\[ p = 4n + 1 = 16a^2 + 4b^2 - 16a - 4b + 5 = (-2b + 1)^2 + (4a - 2)^2 \]  
(101)

It is well known if \( p = F^2 + G^2 \) where \( F \) is odd and \( G \) is even, then \(|F|\) and \(|G|\) are unique (there exist elementary proofs on this subject discovered first by P. Fermat).

Note that (100) imply \( b \) is even.

Let us write (note that \( F \equiv 1 \mod{4} \))
\[ F = -2b + 1 \]
\[ G = 4a - 2 \]  
(102)

Let us consider the other possibility (the sign of \( G \) is changed)

\[ F = -2x + 1 \]

\[ -G = 4y - 2 \]

In this last case we obtain \( x = b \) and \( y = -a + 1 \). This solution permutes the values of \( X_1 \) and \( X_3 \) leaving to \( X_0 \) and \( X_2 \) unchanged (see (97), (99) and (100)). This is not surprising since the elements in the sets \( C'1 \) and \( C'3 \) can be permuted depending of the primitive root \( g \) used.

From (102) we obtain

\[ a = \frac{G + 2}{4} \quad b = \frac{-F + 1}{2} \]  
(103)

On the other hand, (82), (97) and (99) give

\[ 16X_{0,0,0} = p - 4b - 5 \]  
(104)

Consequently (see (102))

\[ 16X_{0,0,0} = p + 2F - 7 \]  
(105)

Substituting (105) and (103) into (99), (97) and (94) we obtain (53).

Therefore the two possible sets of cyclotomic numbers \( X_{0,j,k} \) are determined by equation (101). The theorem is proved when \( n \) is odd. The proof is complete.

### 6 An Application, the Quartic Character of 2

The following theorem was conjectured by Euler (see [3], pages 13 and 14) and first proved by Gauss (see [3], page 174). There exist others proofs by Dirichlet, Halphén, Hensel, Lebesgue, Mordell, Pépin and others (see [3], page 174)

**Theorem 6.1** 2 is a quartic residue of a prime \( p \) if and only if \( p = A^2 + 64B^2 \)

Proof. Suppose that \( n \) is even. In this case \( p = 4n + 1 = 8k + 1 \) and therefore (quadratic character of 2) 2 is a quadratic residue. Consequently 2 \( \in C'0 \) or 2 \( \in C'2 \). Let us consider the number of sums \( X'_{0,0,1} \) of two quartic residues whose result is a fixed \( C1 \) (the order of the summands is irrelevant). We have:
If 2 is a quartic residue (that is, if $2 \in C'0$)

$$2X'_{0,0,1} = X_{0,0,1} \quad (106)$$

If $2 \in C'2$

$$2X'_{0,0,1} = X_{0,0,1} \quad (107)$$

Let us consider the number of sums $X'_{0,0,2}$ of two quartic residues whose result is a fixed $C2$ (the order of the summands is irrelevant). We have:

If $2 \in C'0$

$$2X' = X_{0,0,2} \quad (108)$$

If $2 \in C'2$

$$2X' - 1 = X_{0,0,2} \quad (109)$$

Suppose that $2 \in C'0$. 

(106) and (73) give

$$X'_{0,0,1} = \frac{5a^2 + 5b^2 - 6ab + 8a - 8b - 4}{32} \quad (110)$$

(108) and (71) give

$$X'_{0,0,2} = \frac{5a^2 + 5b^2 - 6ab - 4}{32} \quad (111)$$

(110) and (111) imply

$$a - b = 4k \quad (112)$$

Suppose that $2 \in C'2$. 

(107) and (73) give

$$X'_{0,0,1} = \frac{5a^2 + 5b^2 - 6ab + 8a - 8b - 4}{32} \quad (113)$$

(109) and (71) give

$$X'_{0,0,2} = \frac{5a^2 + 5b^2 - 6ab + 12}{32} \quad (114)$$

(113) and (114) imply

$$a - b = 4k + 2 \quad (115)$$

Now, suppose $n$ is odd. In this case $p = 4n + 1 = 8k + 5$ and therefore (quadratic character of 2) 2 is a quadratic nonresidue. Consequently 2 is a quartic nonresidue. The theorem is a direct consequence of (77), (112), (115) and (101). The proof is complete.
7 The Quintic Equation

Theorem 7.1 If \( d = 5 \), the 25 cyclotomic numbers \( X_{0,j,k} \) can be determined in an elementary way. We have

\[
\begin{align*}
X_{0,0,0} &= p - 14 + 3x \\
X_{0,0,1} &= X_{0,1,0} = X_{0,4,4} \\
X_{0,0,2} &= X_{0,2,0} = X_{0,3,3} \\
X_{0,0,3} &= X_{0,2,2} = X_{0,3,0} \\
X_{0,0,4} &= X_{0,1,1} = X_{0,4,0} \\
X_{0,1,2} &= X_{0,2,1} = X_{0,3,4} = X_{0,4,1} = X_{0,4,3} = X_{0,1,4} \\
X_{0,1,3} &= X_{0,2,3} = X_{0,2,4} = X_{0,3,1} = X_{0,3,2} = X_{0,4,2} 
\end{align*}
\]

They are given by the following polynomials of rational coefficients in the five variables \( u, v, x, w \) and \( p \).

\[
25X_{0,0,0} = p - 14 + 3x \\
100X_{0,0,1} = 4p - 16 - 3x + 25w + 50v \\
100X_{0,0,2} = 4p - 16 - 3x - 25w + 50u \\
100X_{0,0,3} = 4p - 16 - 3x - 25w - 50u \\
100X_{0,0,4} = 4p - 16 - 3x + 25w - 50v \\
100X_{0,1,2} = 4p + 4 + 2x - 50w \\
100X_{0,1,3} = 4p + 4 + 2x + 50w 
\]

(117)

Where the integers \( u, v, x, w \) are given by the Dickson's diophantine system

\[
16p = x^2 + 125w^2 + 50v^2 + 50u^2, \quad x \equiv 1 \pmod{5} \\
xw = v^2 - 4vu - u^2 
\]

(118)

This system has four integral solutions, if \( (x, w, v, u) \) is an integral solution then all integral solutions are given by \( (x, w, v, u) \), \( (x, w, -v, -u) \), \( (x, -w, -u, v) \) and \( (x, -w, u, -v) \).

The solution that correspond in (117) is determined by the primitive root \( g \) used.

Consequently the quintic equation

\[
A_1x_1^5 + \ldots + A_kx_k^5 = A 
\]

where the number of coefficients in each set \( C' \) \((i = 0, 1, 2, 3, 4)\) is fixed and \( A \) is a fixed \( C' \) \((i = 0, 1, 2, 3, 4)\) or 0, can be solved using elementary methods by application of theorem 2.1. The number \( N \) of solutions to this equation is given by a polynomial of rational coefficients in the five variables \( u, v, x, w \) and \( p \).
Proof. See [1] (pages 93, 94 and 99) for an elementary proof of (117). The original elementary proof that the system (118) has the four solutions mentioned is given in [2] (pages 402-404). The rest is an immediate consequence of theorem 2.1.

8 Theorem 2.1. Examples

1) The number of solutions $A_0^2$ to the equation $x_1^3 + x_2^3 = 1$ is (see (4) and (27))

$$A_0^2 = 9X_{0,0,0} + 6 = p + F - 2$$  (119)

2) If $n$ is even, the number of solutions $A_0^2$ to the equation $x_1^4 + x_2^4 = 1$ is (see (4) and (52))

$$A_0^2 = 16X_{0,0,0} + 8 = p + 6F - 3$$

3) If $n$ is odd, the number of solutions $A_0^2$ to the equation $x_1^4 + x_2^4 = 1$ is (see (5) and (53))

$$A_0^2 = 16X_{0,0,0} + 8 = p + 2F + 1$$

These results are due to Gauss (see [1], page 323 and 338).

4) The number of solutions $A_0^2$ to the equation $x_1^5 + x_2^5 = 1$ is (see (4) and (117))

$$A_0^2 = 25X_{0,0,0} + 10 = p + 3x - 4$$

This result is due to Dickson (see [1], page 323 and 338, and [2], page 402).

5) The number of solutions $A_0^3$ to the equation $x_1^3 + x_2^3 + x_3^3 = 1$ is (see (8), (25) and (4))

$$A_0^3 = A_0^2 + 3 \sum_{i=0}^{2} A_i^2 X_{i,0,0} + 3B^2$$

$$= A_0^2 + 3A_0^2 X_{0,0,0} + 3A_1^2 X_{1,0,0} + 3A_2^2 X_{2,0,0} + 3B^2$$

$$= A_0^2 + 3A_0^2 X_{0,0,0} + 3A_1^2 X_{0,2,2} + 3A_2^2 X_{0,1,1} + 3B^2$$

$$= 27X_{0,0,0} + 27X_{0,0,0}^2 + 27X_{0,0,1}X_{0,2,2} + 27X_{0,0,2}X_{0,1,1} + 9p$$

That is (see (26), (27) and (28))

$$A_0^3 = 27X_{0,0,0} + 27X_{0,0,0}^2 + 27X_{0,0,1}^2 + 27X_{0,0,2}^2 + 9p = p^2 + 6p - F$$  (120)

6) The number of solutions $B^4$ to the equation $x_1^3 + x_2^3 + x_3^3 + x_4^3 = 0$ is (see (12), (4), (119) and (120))

$$B^4 = B^3 + A_0^3(p - 1) = B^3 + A_0^2(p - 1) + A_0^3(p - 1)$$

$$= 3p - 2 + A_0^2(p - 1) + A_0^3(p - 1) = p^3 + 6p^2 - 6p$$

This result is in [1], page 335.
7) If $n$ is odd, the number of solutions $B^3$ to the equation $x_1^4 + x_2^4 + x_3^4 = 0$ is (see (13), (5) and (53))

$$B^3 = B^2 + A_2^2 (p - 1) = 1 + 16X_{0,0,2}(p - 1) = p^2 - 6pF + 6F$$

8) The number of solutions $A_3^3$ to the equation $x_1^5 + x_2^5 + x_3^5 = C1$ is (see (10), (25), (4), (116) and (117))

$$A_3^3 = A_1^3 + 5 \sum_{j=0}^4 A_j^2 X_{j,0,1}$$

$$= A_1^3 + 5A_0^2 X_{0,0,1} + 5A_1^2 X_{1,0,1} + 5A_2^2 X_{2,0,1} + 5A_3^2 X_{3,0,1} + 5A_4^2 X_{4,0,1}$$

$$= A_1^3 + 5A_0^2 X_{0,0,1} + 5A_1^2 X_{0,4,0} + 5A_2^2 X_{0,3,4} + 5A_3^2 X_{0,2,3} + 5A_4^2 X_{0,1,2}$$

$$= 75X_{0,0,1} + 125X_{0,0,0}X_{0,0,1} + 125X_{0,0,1}X_{0,0,4} + 125X_{0,0,2}X_{0,1,2}$$

$$+ 125X_{0,0,3}X_{0,1,3} + 125X_{0,0,4}X_{0,1,2} = (1/16)(16p^2 - 64p - 9x^2 + 50xw)$$

$$+ 100xv - 48x - 125w^2 + 500wv - 1000wu - 500v^2)$$

**ACKNOWLEDGEMENTS.** The author is very grateful to Universidad Nacional de Luján.

**References**


**Received: February, 2009**