DRP REPORT
QUADRATIC NUMBER FIELDS

MOCHAMMAD ZULFIKAR ADITYA

Contents

1. Introduction

The idea of having a Diophantine equation (an equation with integral solutions) already emerges from Theorem of Pythagoras involving a right angle triangle with sides a, b, and c. The theorem states that if sides c located on the opposite of the right angle, then we have $a^2 + b^2 = c^2$. One of the natural questions regarding to this theorem are the existence of integral solutions. Name the triple (a, b, c) as the triple Pythagoras and solutions to $a^2 + b^2 = c^2$.

One of the classic example of triple Pythagoras is $(3, 4, 5)$. Another question arise: Is there any other integral solutions? Can we generate those solutions? Many attempts and parametrizations are given in order to generate another solution of triples include one from Diophantus.

Another problem of Diophantine equation arise in the form of $y^2 + 2 = x^3$ proposed by Bachet. This type of equation later called as an elliptic curve. It's slightly harder than Pythagoras Theorem with the same question of whether this equation have integral solutions. To get any better point of view, mathematicians take this equation into finding a rational solutions first through many form of parametrization includes some works of Fermat and Euler.

Gauss considered another possibilities to solve Bachet's equation involving a number in a form of $a + bi$ where $i = \sqrt{-1}$. This type of number later called as Gaussian number and it also motivates to construct a bigger number structure in order to solve the equation based on more general structures.

Date: Update: November 12, 2023.

2. Preliminaries

This section will contains many different concept (related or unrelated) that we needed to dive deeper into Quadratic Number Field such as it's definition and properties, Modularity Theorem, and Elliptic Curves.

2.1. Quadratic Number Fields.

Let's define what is a Quadratic Number Fields according to [1]

Definition 2.1. Let m be a *squarefree* integer not equal to 0 or 1. The set

$$k = \mathbb{Q}(\sqrt{m}) = \{a + b\sqrt{m} : a, b \in \mathbb{Q}\}$$

is called *quadratic number field.*

Set an element $\alpha = a + b\sqrt{m} \in k$, it can be viewed as a root of quadratic polynomial $P_\alpha(x) = x^2 - 2ax + a^2 - mb^2$. Based on those motivation, next we called the other roots of $P_\alpha(x)$, $\alpha' = a - b\sqrt{m}$ as the *conjugate* of α. Another term that we defined in the quadratic number field are :

- The *norm* of α: $N\alpha = \alpha\alpha' = a^2 - mb^2$,
- The *trace* of α: $\mathrm{Tr}\alpha = \alpha + \alpha' = 2a$, and
- The *discriminant* of α: $\mathrm{disc}(\alpha) = (\alpha - \alpha')^2 = 4mb^2$.

2.2. Quadratic Residue.

Concept of quadratic residue plays a big role in finding the number of 'points' on a curves. By defining 'points' means we observe another type of points than our usual integral points. The other type of points usually rely on different structure than $\mathbb{Z}$ (since $\mathbb{Z}$ is not a field). It could be $\mathbb{Q}$, $\mathbb{F}_q$, or any kind of fields available.

Definition 2.2. Let k a field and $f(x, y) = 0$ be a curve. A point (a, b) is called *k-rational point* on curve $f(x, y) = 0$ if $a, b \in k$ and $f(a, b) = 0$.

The type of curves we often consider are the one with quadratic variables such as Pell's conic $x^2 - my^2 = 1$. To get a better understanding about it, we consider all the $\mathbb{F}_p$-rational points on $x^2 - my^2 = 1$. In other words, all the solutions of (x, y) over modulo p where p is a prime. Finding everything one by one would be a hassle, so instead we observe for arbitrary y are there any solution of $x^2 = 1 + my^2$. From those, we need to define what is the 'solvability' for x in $x^2 = 1 + my^2$.

Definition 2.3. Let p odd prime and a is an integer. If a is not divisible by p, define a is a *quadratic residue* modulo p if $x^2 \equiv a \mod p$ is solvable in integers. If there are no integer solutions of $x^2 \equiv a \mod p$, define it as *not quadratic residue.* Define the Legendre symbol $(\frac{a}{p})$ by

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } p|a \\ 1, & \text{if } p \nmid a \text{ and } a \text{ quadratic residue modulo } p \\ -1, & \text{if } p \nmid a \text{ and } a \text{ not quadratic residue modulo } p \end{cases}$$

This Legendre symbol also represent as a group homomorphism between $(\mathbb{Z}/p\mathbb{Z})^\times$ and ± 1 by the consequence of $(\mathbb{Z}/p\mathbb{Z})^\times$ being a cyclic group. It also means that

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

Another interesting consequences of $(\mathbb{Z}/p\mathbb{Z})^\times$ being a cyclic group is that we can define a closed form for Legendre symbols $(\frac{a}{p})$.

Proposition 2.4. *For all integers a that is not divisible by the odd prime number p we have*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$$

Proof. Let $p = 2m + 1$ for positive integer m. We already know that $(\mathbb{Z}/p\mathbb{Z})^\times$ is a cyclic group (which actually not that trivial, I'll attach the proof on the last section), so there exist $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ such that for every $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ there always exist positive integers k that satisfy

$$a \equiv g^k \mod p$$

Also notice that for every $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ it holds $a^{p-1} \equiv 1 \mod p$. We will observe in two different cases

- If $a \equiv g^k \mod p$ where k is even, let $k = 2l$. Then $x^2 \equiv a \mod p \equiv g^{2l} \mod p$ immediately solvable and $(\frac{a}{p}) = +1$. Meanwhile

$$\begin{aligned} a^{\frac{p-1}{2}} &= a^m \\ &\equiv (g^k)^m \mod p \\ &\equiv g^{km} \mod p \\ &\equiv (g^{2m})^{k/2} \mod p \\ &\equiv 1 \mod p \end{aligned}$$

- If $a \equiv g^k \mod p$ where k is odd, let $k = 2l+1$. Then $x^2 \equiv a \mod p \equiv g^{2l+1} \mod p$ is not solvable and $(\frac{a}{p}) = -1$. Meanwhile

$$\begin{aligned} a^{\frac{p-1}{2}} &= a^m \\ &\equiv (g^{2l+1})m \mod p \\ &\equiv g^{2lm}g^m \mod p \\ &\equiv (+1)\cdot(-1) \mod p \\ &\equiv -1 \mod p \end{aligned}$$

We can conclude that $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \mod p$. □

Sometimes when we fixed the numerator on Legendre Symbol, we can determine the value of those notations solely by the congruences of the modulo. One of the example is:

Proposition 2.5. *For odd positive prime numbers p we have*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \mod 4 \\ -1, & \text{if } p \equiv 3 \mod 4 \end{cases}$$

Proof. Let $p = 2k + 1$. Apply the previous proposition and we would have

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \mod p \equiv (-1)^k \mod p$$

The value of $(\frac{-1}{p})$ solely depend on the parity of k.

- If k is even, then $p \equiv 1 \mod 4$ and $(-1)^k = +1$.
- If k is odd, then $p \equiv 3 \mod 4$ and $(-1)^k = -1$.

□

Later it became our point of interest when we have a fixed integer a, can we find any congruences over modulo N such that for any prime numbers p and q (next it also applies for non prime numbers too) that satisfy $p \equiv q \mod N$ then we have

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$$

Another method to calculate any Legendre notation by using some method called Gauss Lemma. The Gauss Lemma instead of multiplying the same number $p-1/2$ times, instead we consider what is called to be a *Half System*.

Definition 2.6. Let p be odd prime number, and we can write $p = 2m+1$ for some positive integer m. A *half system* modulo p is defined as a set of $\{a_1, a_2, ..., a_m\}$ where every coprime residue class is represented by an element in the form of $\pm a_j$. Let a be an integer coprime to p and for $1 \leq i \leq m$, consider the equation

$$a \cdot a_i \equiv \varepsilon_i \cdot a_i' \mod p$$

where $\varepsilon_i \in \{-1, 1\}$ and $a_i' \in \{a_1, a_2, ..., a_m\}$. Multiply all the possible equations and canceling some terms, we would get that

$$\left(\frac{a}{p}\right) = \prod_{i=i}^{m} \varepsilon_i$$

Gauss Lemma rather be simple to applied than try to find the congruences by the exponent of $(p-1)/2$. One of those examples are finding the value of $(\frac{2}{p})$.

Proposition 2.7. *For odd prime number p, we have*

$$\left(\frac{2}{p}\right) = \begin{cases} +1, & \text{if } p \equiv \pm 1 \mod 8 \\ -1, & \text{if } p \equiv \pm 3 \mod 8 \end{cases}$$

Proof. Apply Gauss Lemma with $a = 2$. Since it rather tricky to solve all in one go, we divide the case of $p \equiv 1 \mod 4$ and $p \equiv 3 \mod 4$. (I'll write the rest of the proof later). □

The concept of Legendre notation only limited over prime modulo, while most of the scenarios we also deals with arbitrary odd number modulo. We need to define those case by define it into Jacobi notation

Definition 2.8. Let m be an odd prime numbers and set $m = \prod p$ as the product of all the odd primes. Then *Jacobi notation* $(\frac{a}{m})$ defined as

$$\left(\frac{a}{m}\right) = \prod_{p} \left(\frac{a}{p}\right)$$

Set an example of $(\frac{2}{15}) = (\frac{2}{3})(\frac{2}{5}) = (-1) \cdot (-1) = +1$. Unfortunately Jacobi notation are less intuitive than Legendre notation. Legendre notation $(\frac{a}{p})$ states clearly the solvability of $x^2 \equiv a \mod p$ by the plus or minus sign of the notation, meanwhile Jacobi notation with $(\frac{a}{m}) = 1$ doesn't always imply the solvability of $x^2 \equiv 2 \mod 15$. In fact, there are no integers that satisfy $x^2 \equiv 2 \mod 15$.

3. Rational Points on Curves

One of the main goals that mathematicians wish to achieved are to solve a Diophantine equation that isn't trivial enough by only using elementary number theory. Because it is completely difficult especially working on $\mathbb{Z}$, we approach the solutions over fields (finite or not finite). Keep in mind that working this rational points benefit other branch of mathematics to develop their research like cryptography. For this section, we will working on $\mathbb{F}_p$ for a prime number p.

For starters, let K be a field and $f(x) \in K[x]$ a polynomial. We say that $\mathcal{C} : y^2 = f(x)$ is a plane algebraic curve. A point $(x, y) \in K \times K$ satisfying this equation is called an affine point on $\mathcal{C}$. If $\deg f = 2$, the curve $\mathcal{C} : y^2 = f(x)$ is called a conic.

We start this section with a nice Lemma involving quadratic residue notation.

Lemma 3.1. *Let $\mathcal{C} : y^2 = f(x)$ be algebraic curve with $f(x) = \mathbb{Z}[x]$. The number of affine $\mathbb{F}_p$-rational points on $\mathcal{C}$ is given by*

$$N_p(\mathcal{C}) = \#\mathcal{C}(\mathbb{F}_p) = p + \sum_{t=0}^{p-1} \left(\frac{f(t)}{p}\right)$$

Proof. Let $x \in \mathbb{F}_p$, then the number of solutions of $y^2 = f(x)$ over $\mathbb{F}_p$ depends on the value of $\left(\frac{f(x)}{p}\right)$. Recall that $\left(\frac{f(x)}{p}\right)$ if and only if $y^2 = f(x)$ has $\left(\frac{f(x)}{p}\right) + 1$ solutions of y for a specified $x \in \mathbb{F}_p$.

So, the number of affine $\mathbb{F}_p$-rational points on $\mathcal{C}$ is

$$N_p(\mathcal{C}) = \#\mathcal{C}(\mathbb{F}_p) = \sum_{t=0}^{p-1} 1 + \left(\frac{f(t)}{p}\right) = p + \left(\frac{f(t)}{p}\right)$$

□

Character sums of the form $\sum \left(\frac{f(x)}{p}\right)$ is called *Jacobsthal sums* after Ernst Jacobsthal (1882-1965). This sums have many improvements and development especially on certain primes such as : $p \equiv 1 \mod 3$ in the form of $p = a^2 + 3b^2$ and $p \equiv 1 \mod 8$ in the form of $p = a^2 + 2b^2$.

On this section, we will cover for some general and specified cases of p with polynomial $f(x) \in \mathbb{Z}[x]$ of degree one, two, and three.

3.1. Jacobsthal Sums for Linear Function.

Starting with a simple Lemma with easy proof of observation

Lemma 3.2. *For each odd prime p, we have*

$$\sum_{t=0}^{p-1} \left(\frac{t}{p}\right) = 0$$

Proof. As a consequences of $\mathbb{F}_p^\times$ being cyclic with order of even number, we expect the number of quadratic residue over mod p is equal to the number of non quadratic residue over mod p. Hence, the sum of all characters over mod p is equal to 0.

Another proof to consider : let $S = \sum_{t=0}^{p-1} \left(\frac{t}{p}\right)$ and choose nonquadratic residue n. Then $-S = \left(\frac{n}{p}\right) S = \sum_{t=0}^{p-1} \left(\frac{nt}{p}\right)$. Since n are prime relative to p, then tn are

a complete residue of modulo p and $-S = \sum_{t=0}^{p-1} \left(\frac{nt}{p}\right) = S$. Finally we can get $S = 0$. □

With this Lemma 3.2, we can easily proceed to the next proposition of Jacobsthal Sums over Linear Function

Proposition 3.3. *Let $f(x) = ax + b$ with $p \nmid a$. Then*

$$\sum_{t=0}^{p-1} \left(\frac{f(t)}{p}\right) = 0$$

Proof. As long as we can prove that $f(x)$ is a bijective map from $\mathbb{F}_p$ to $\mathbb{F}_p$, it is the same proof as of Lemma 3.2.

Let $k, l \in \mathbb{F}_p$ such that $f(k) = f(l)$. Then we have

$$\begin{aligned} f(k) &= f(l) \\ ak + b &= al + b \\ ak &= al \\ a^{-1}ak &= a^{-1}al \\ k &= l \end{aligned}$$

and $f(x)$ is injective. As for the surjective one, let $r \in \mathbb{F}_p$. Then, it's easy to pick $s = a^{-1}(r - b) \in \mathbb{F}_p$ such that

$$\begin{aligned} f(s) &= a(a^{-1}(r - b)) + b \\ &= r - b + b \\ &= r \end{aligned}$$

and $f(x)$ is also surjective. We conclude $f(x)$ is bijective, and $at + b$ serves as the complete residue of modulo p for $t = 0, 1, ..., p - 1$. Finally,

$$\sum_{t=0}^{p-1} \left(\frac{f(t)}{p}\right) = 0$$

□

3.2. **Jacobsthal Sums for Quadratic Polynomial.** Now let's analyze the sum for quadratic polynomial. For starter, let $f(x) = ax^2 + bx + c$ with $p \nmid a$ for p odd prime number. We could simplify $f(x)$ by completing a square. In this case, we rather completing the square of $4af(x)$.

$$\begin{aligned} 4af(x) &= 4a^2x^2 + 4abx + 4ac \\ &= 4a^2x^2 + 4abx + b^2 - b^2 + 4ac \\ &= (2ax + b)^2 - (b^2 - 4ac) \end{aligned}$$

Set $\Delta = b^2 - 4ac$ and now we have $4af(x) = (2ax+b)^2 - \Delta$. Proceeding into the Jacobsthal sum,

$$\begin{aligned}\sum_{t=0}^{p-1}\left(\frac{f(t)}{p}\right) &= \sum_{t=0}^{p-1}\left(\frac{4a^2}{p}\right)\left(\frac{f(t)}{p}\right)\\ &= \left(\frac{a}{p}\right)\sum_{t=0}^{p-1}\left(\frac{4af(t)}{p}\right)\\ &= \left(\frac{a}{p}\right)\sum_{t=0}^{p-1}\left(\frac{(2at+b)^2-\Delta}{p}\right)\end{aligned}$$

Again since any linear mapping with coeffiecient not divisible by p is a bijective mapping from $\mathbb{F}_p$ to $\mathbb{F}_p$, then

$$\sum_{t=0}^{p-1}\left(\frac{f(t)}{p}\right) = \left(\frac{a}{p}\right)\sum_{t=0}^{p-1}\left(\frac{(2at+b)^2-\Delta}{p}\right) = \left(\frac{a}{p}\right)\sum_{t=0}^{p-1}\left(\frac{t^2-\Delta}{p}\right)$$

Now the Jacobsthal sums of Quadratic Polynomial depends on coefficients and constant of it's polynomial in such a good way since a act as the leading coeffieient and Δ is a discriminant of a quadratic polynomial. Next we consider a simple quadratic polynomial $f(t) = t^2 - D$ yet so impactful it can represent the behaviour of all quadratic polynomial. Define

$$\psi(D) = \sum_{t=0}^{p-1}\left(\frac{t^2-D}{p}\right)$$

We will further explore about some characteristic of $\psi(D)$. As for starter, obviously $\psi(0) = p-1$ since $\psi(0) = \sum_{t=0}^{p-1}\left(\frac{t^2}{p}\right) = p-1$.

Lemma 3.4. *We have $\psi(a^2D) = \psi(D)$ for all integers a with $p \nmid a$.*

Proof. Starting from $\psi(a^2D)$, we have

$$\psi(a^2D) = \sum_{t=0}^{p-1}\left(\frac{t^2-a^2D}{p}\right)$$

Since $p \nmid a$, consider a linear function $f(t) = at$ which is bijective on $\mathbb{F}_p$. Then t can be represent as as for s running from 0 to $p-1$ since it's a complete residue over modulo p.

$$\sum_{t=0}^{p-1}\left(\frac{t^2-a^2D}{p}\right) = \sum_{s=0}^{p-1}\left(\frac{a^2s^2-a^2D}{p}\right) = \sum_{s=0}^{p-1}\left(\frac{s^2-D}{p}\right) = \psi(D)$$

□

Moving on to a more trickier lemma.

Lemma 3.5. *We have $\psi(1) = -1$.*

Proof.

$$\begin{aligned}\psi(1) &= \sum_{t=0}^{p-1}\left(\frac{t^2-1}{p}\right)\\ &= \sum_{t=0}^{p-1}\left(\frac{t-1}{p}\right)\left(\frac{t+1}{p}\right)\end{aligned}$$

Set $s = t-1$ in order to get

$$\begin{aligned}\sum_{t=0}^{p-1}\left(\frac{t-1}{p}\right)\left(\frac{t+1}{p}\right) &= \sum_{s=0}^{p-1}\left(\frac{s}{p}\right)\left(\frac{s+2}{p}\right)\\ &= \sum_{s=1}^{p-1}\left(\frac{s}{p}\right)^{-1}\left(\frac{s+2}{p}\right)\\ &= \sum_{s=1}^{p-1}\left(\frac{s^{-1}(s+2)}{p}\right)\\ &= \sum_{s=1}^{p-1}\left(\frac{1+2s^{-1}}{p}\right)\end{aligned}$$

Variable s ranging from 1 to $p-1$, so there exist $r \in \mathbb{F}_p$ such that $rs \equiv 1 \mod p$. Furthermore, r also ranging from 1 to $p-1$ over modulo p, so we can set $s^{-1} = r$ and the summation over r.

$$\begin{aligned}\sum_{s=1}^{p-1}\left(\frac{1+2s^{-1}}{p}\right) &= \sum_{r=1}^{p-1}\left(\frac{1+2r}{p}\right)\\ &= -\left(\frac{1+2(0)}{p}\right) + \sum_{r=0}^{p-1}\left(\frac{1+2s}{p}\right)\\ &= -1\end{aligned}$$

□

Here are some of the bigger questions yet to reveal: can we find another value of $\psi(D)$? Sometimes it can be a good way to consider all at once rather than find them one by one. By this, we will jump into the sum of all possible $\psi(D)$.

$$\sum_{D=0}^{p-1}\psi(D) = \sum_{D=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{t^2-D}{p}\right) = \sum_{t=0}^{p-1}\sum_{D=0}^{p-1}\left(\frac{t^2-D}{p}\right) = 0$$

since $\sum_{D=0}^{p-1}\left(\frac{t^2-d}{p}\right) = 0$ by Proposition 3.3.

There are another ways to count the summation of $\sum\psi(D)$. If we observe carefully, $\psi(D)$ only depends on $\left(\frac{D}{p}\right)$ for $p \nmid D$. Why? If D is a quadratic residue modulo p, we can treat the value of $\psi(D)$ just like what Lemma 3.5 did and having the same result. If D is a non quadratic residue modulo p, refer again to Lemma 3.4 that basically said every non quadratic residue D would have the same value of $\psi(D)$.

To elaborate more, let n be non quadratic residue modulo p and we can conclude that

$$\sum_{D=0}^{p-1} \psi(D) = \psi(0) + \frac{p-1}{2}(\psi(1) + \psi(n)) = (p-1) + \frac{p-1}{2}(-1 + \psi(n)) = 0$$

Simple arithetic resulting us that $\psi(n) = -1$. Finally, we can summarize the results into a proposition.

Proposition 3.6. *We have*

$$\psi(D) = \sum_{t=0}^{p-1} \left(\frac{t^2 - D}{p} \right) = \begin{cases} -1 & \text{if } p \nmid D \\ p-1 & \text{if } p \mid D \end{cases}$$

3.3. **Jacobsthal Sums for Cubic Polynomial.** The cubic polynomial itself actually quite hard (at least stated in the [1]), but actually there's some good reason behind that. Using some substitution, we can reduce a polynomial of general form $ax^3 + bx^2 + cx + d$ into $x^3 + kx + l$. Due to respect the content of Lemmermeyer, we will consider the cubic polynomial of the form $f(x) = x^3 - x$. If we have more time, we could explore more about the general simplified cubic polynomial $f(x) = x^3 + kx + l$ for $l = 0$ and $l \neq 0$.

Let us define

$$\phi_p(k) = \phi(k) = \sum_{t=0}^{p-1} \left(\frac{t}{p} \right) \left(\frac{t^2 - k}{p} \right)$$

We wish to prove this property first.

Proposition 3.7. *We have* $\phi(a^2 k) = \left(\frac{a}{p} \right) \phi(k)$ *for each* a *coprime to* p.

Proof. We have a coprime to p, then at will set as a complete residue of modulo p when t is also a complete residue of modulo p. Immediately we have

$$\begin{aligned} \phi(a^2 k) = \sum_{t=0}^{p-1} \left(\frac{t}{p} \right) \left(\frac{t^2 - a^2 k}{p} \right) &= \sum_{t=0}^{p-1} \left(\frac{(at)}{p} \right) \left(\frac{(at)^2 - a^2 k}{p} \right) \\ &= \left(\frac{a}{p} \right) \sum_{t=0}^{p-1} \left(\frac{t}{p} \right) \left(\frac{t^2 - k}{p} \right) \\ &= \left(\frac{a}{p} \right) \phi(k) \end{aligned}$$

and it completes the proof. □

One theorem that we also wish to claim is

Theorem 3.8. *Let* $p \equiv 1 \mod 4$ *be a prime number, and write down* $p = a^2 + 4b^2$. *Then*

$$\phi(1) = \sum_{k=0}^{p-1} \left(\frac{t}{p} \right) \left(\frac{t^2 - 1}{p} \right) = 2a$$

where the sign of a *is chosen in such a way that* $a \equiv -\left(\frac{2}{p} \right) \mod 4$.

In particular, the number of $\mathbb{F}_p$*-rational points on the olliptic curve* $y^2 = x^3 - x$ *is* $N_p = p + 1 - 2a$.

Seems like the theorem are hard to believe and to be accepted right away. Nonetheless, we consider the summation of $\sum \phi(k)^2$ as our path to prove the value of $\phi(1)$. Why it should be $\sum \phi(k)^2$? Again, we can consider things as a whole rather than seeking all of them one by one.

Furthermore, we can utilize Proposition 3.7 to our fullest. Because all of our $\phi(r)^2$ having the same value for r any quadratic residue modulo p and also happens with $\phi(n)^2$ for n is a non quadratic residue modulo p. We claim that $\phi(r)^2 = 4x^2$ and $\phi(r)^2 = 4y^2$, then our summation $\sum \phi(k)^2$ is equal to

$$\sum_{k=0}^{p-1} \phi(k)^2 = \frac{p-1}{2}(4x^2 + 4y^2) = 2(p-1)(x^2+y^2)$$

We claim that $p = x^2 + y^2$ and wish to prove them. Using the double counting method, we want to calculate $\sum \phi(k)^2$ directly. Before moving on to the calculation, another lemma was needed.

Lemma 3.9. *We have*

$$\sum_{k=0}^{p-1} \left(\frac{k}{p}\right)\left(\frac{k+b}{p}\right) = \begin{cases} -1 & \text{if } p \nmid b \\ p-1 & \text{if } p \mid b \end{cases}$$

Proof. This is just a similar version of Proposition 3.6 since we have

$$\begin{aligned} \sum_{k=0}^{p-1} \left(\frac{k}{p}\right)\left(\frac{k+b}{p}\right) &= \sum_{k=0}^{p-1} \left(\frac{k^2+kb}{p}\right) = \sum_{k=0}^{p-1} \left(\frac{4k^2+4kb}{p}\right) \\ &= \sum_{k=0}^{p-1} \left(\frac{(2k+b)^2 - b^2}{p}\right) = \sum_{t=0}^{p-1} \left(\frac{t^2-b^2}{p}\right) \end{aligned}$$

□

Now we are ready to calculate $\sum \phi(k)^2$.

$$\begin{aligned} \sum_{k=0}^{p-1} \phi(k)^2 &= \sum_{k=0}^{p-1} \left(\sum_{s=0}^{p-1} \left(\frac{s}{p}\right)\left(\frac{s^2-k}{p}\right)\right)\left(\sum_{t=0}^{p-1} \left(\frac{t}{p}\right)\left(\frac{t^2-k}{p}\right)\right) \\ &= \sum_{0 \le s,t \le p-1} \left(\frac{st}{p}\right) \sum_{k=0}^{p-1} \left(\frac{s^2-k}{p}\right)\left(\frac{t^2-k}{p}\right) \end{aligned}$$

Let $s^2 - k = l$ and $t^2 - k = t^2 - s^2 + l$. Next we will count $\sum \left(\frac{s^2-k}{p}\right)\left(\frac{t^2-k}{p}\right)$.

$$\sum_{k=0}^{p-1} \left(\frac{s^2-k}{p}\right)\left(\frac{t^2-k}{p}\right) = \sum_{l=0}^{p-1} \left(\frac{l}{p}\right)\left(\frac{l+t^2-s^2}{p}\right) = \begin{cases} -1 & , s \not\equiv \pm t \\ p-1 & , s \equiv \pm t \end{cases}$$

The last statement follows from Lemma 3.9. So,

$$\begin{aligned}\sum_{k=0}^{p-1}\phi(k)^2 &= (p-1)\left[\sum_{s=t}\left(\frac{t^2}{p}\right)+\sum_{s=-t}\left(\frac{-t^2}{p}\right)\right]-\sum_{s\not\equiv\pm t}\left(\frac{st}{p}\right)\\ &= p\left[\sum_{s=t}\left(\frac{t^2}{p}\right)+\sum_{s=-t}\left(\frac{-t^2}{p}\right)\right]-\sum_{s,t}\left(\frac{st}{p}\right)\\ &= p\left[(p-1)+\left(\frac{-1}{p}\right)(p-1)\right]\end{aligned}$$

If we consider the case of $p \equiv 1 \mod 4$, then $\left(\frac{-1}{p}\right) = 1$. Finally, we have

$$\sum_{k=0}^{p-1}\phi(k)^2 = p[2(p-1)] = 2p(p-1)$$

4. Appendix

This section dedicated for proving something we consider trivial from the early part but in actual, it isn't.

4.1. Cyclic Group of $\mathbb{F}_q^\times$.

It is mentioned many times on group theory the incredible structure of multiplication group of finite field $\mathbb{F}_q^\times$ for $q = p^k$ with prime number p and non negative integer k. In fact, the proof those groups are cyclic groups is rather not a direct proof but need some additional Lemmas. We decicate the whole subchapter as a ground for proving all theorems and lemmas needed. For more details, refer to [2].

We will start with such a good statement about polynomial over field.

Theorem 4.1. *Let F be a field and $f(t)$ be a non-constant polynomial with coefficients in F of degree d. Then $f(t)$ has at most d roots in F.*

It's such a strong statement. In order to prove it, we need to prove a preliminary lemma.

Lemma 4.2. *Let F be a field and $f(t)$ be a non-constant polynomial with coefficients in F. For $a \in F$, $f(a) = 0$ if and only if $t - a$ is a factor of $f(t)$.*

Proof. If $t-a$ is a factor of $f(t)$, we can write $f(t) = (t-a)g(t)$ for some polynomial $g(t)$, and substituting a into $f(t)$ give us $f(a) = (a-a)g(a) = 0$.

Conversely, suppose $f(a) = 0$. Write $f(t)$ as

$$f(t) = c_n t^n + c_{n-1}t^{n-1} + ... + c_1 t + c_0$$

where $c_i \in F$. Then

$$f(a) = 0 = c_n a^n + c_{n-1}a^{n-1} + ... + c_1 a + c_0$$

Substract $f(t)$ by $f(a)$ in order to get

$$\begin{aligned} f(t) - f(a) &= \sum_{k=1}^{n} c_k(t^k - a^k) \\ f(t) &= \sum_{k=1}^{n} c_k(t-a)(t^{k-1} + t^{k-2}a + \cdots + ta^{k-2} + a^{k-1}) \\ &= (t-a)\sum_{k=1}^{n} c_k \sum_{j=0}^{k-1} t^j a^{k-1-j} \end{aligned}$$

and $f(t) = (t-a)h(t)$ for $h(t) = \sum_{k=1}^{n} c_k \sum_{j=0}^{k-1} t^j a^{k-1-j}$, our proof is complete. □

Now we are ready to prove Theorem 4.1

Proof. We will use induction on the degree of $f(t)$. Note that $d \geq 1$.

Let $f(t) = at + b$ a polynomial with degree 1, $a, b \in F$, and $a \neq 0$. This polynomial has one root in F, which is $-b/a$ and we have a polynomial of degree one having at most 1 root in F.

For $d \geq 1$, assume the theorem holds for all polynomials in $F[t]$ (or polynomial with all coefficients in F) with degree d. We will prove the theorem also holds for all polynomials in $F[t]$ with degree of $d+1$. Write down the polynomial of degree $d+1$ as

$$f(t) = c_{d+1}t^{d+1} + c_d t^d + \cdots + c_1 t + c_0$$

where $c_{d+1} \neq 0$.

If $f(t)$ has no roots in F, we're done since it's having at most $d+1$ roots in F. Else, let $f(t)$ has a root in F. Name them $r \in F$. By Lemma 4.2, $f(t) = (t-r)g(t)$ for some polynomial $g(t)$ with all coefficients in F and having degree of d. Using the inductive hypothesis, $g(t)$ has at most d roots in F.

Observe again that $f(t) = (t-r)g(t)$ and since F is a field, then $f(t) = 0$ if and only if $t - r = 0$ or $g(t) = 0$. That means every root of $f(t)$ in F are either r or the root of $g(t)$. Then $f(t)$ has at most $d+1$ roots in F. □

Now we will seek them from the perspective of group theory, although Theorem 4.1 would be useful later.

Lemma 4.3. *Let G be a finite abelian group. If n is the maximal order among the elements in G, then the order of every element divides n.*

Proof. Let g have the maximal order n. Let $h \in G$ with order m. We will prove no matter the choice of h, we will always have $m|n$. By contradiction, assume m does not divide n (also implies $m > 1$) and we wish to construct an element with order exceeding n and contradict the maximality of n.

If $\gcd(m, n) = 1$, then gh will have order of mn, and of course it's already solved. But what about $\gcd(m, n) > 1$? Let us set for a general case. Before moving into the next step, for prime number p and integer q, define $v_p(q)$ as the non-negative integer k such that $p^k|q$ and $p^{k+1} \nmid q$.

Back to the proof, since $m \nmid n$ there exist prime number p such that $v_p(m) > v_p(m)$. Let $v_p(m) = e$ and $v_p(n) = f$. Next, consider elements g^{p^f} and h^{m/p^e}. Element g^{p^f} has order n/p^f and element h^{m/p^e} has order p^e. Observe that n/p^f

is not divisible by p meanwhile p^e is just a p-power. These numbers are relatively prime.

In an abelian group, if g_1 has order n_1 and g_2 has order n_2 with $\gcd(n_1, n_2) = 1$, then $g_1 g_2$ has order $n_1 n_2$. So, $g^{p^f} h^{m/p^e}$ has order

$$\frac{n}{p^f} p^e = n p^{e-f} > n$$

This contradict the maximality of n as an order in G. □

The following theorem will be the criterion for showing a group is cyclic. Recall for a cyclic group, there is just one subgroup of each size that occurs. Assuming the group is abelian, the converse holds.

Theorem 4.4. *Let G be a finite abelian group with at most one subgroup per size. Then G is cyclic.*

Proof. Let n be the maximal order among all elements in G and let $g \in G$ with order n. We will prove every element is a power of g, so $\langle g \rangle = G$.

Pick $h \in G$ with order d. By Lemma 4.3, we have $d|n$ and there exist another element with order d: $g^{n/d}$. We have two subgroups of order d: $\langle h \rangle$ and $\langle g^{n/d} \rangle$. Since by the statement, only at most one subgroup per size, consequently $\langle h \rangle = \langle g^{n/d} \rangle$. It also implies $h \in \langle g^{n/d} \rangle$ and there exist $k \in \mathbb{Z}$ such that $h = g^{kn/d}$, so h is a power of g. Since every element in G is a power of g, we can conclude $G = \langle g \rangle$. □

Now we are ready to show $\mathbb{F}_q^\times$ is cyclic.

Theorem 4.5. *Let $q = p^k$ for prime number p and positive integer k. Then $\mathbb{F}_q^\times$ is cyclic.*

Proof. Based on the Theorem 4.4, we only need to show that $F_q^\times$ only have at most one subgroup per size. Let $H \subset \mathbb{F}_q^\times$ be a subgroup of size d. Then every $a \in H$ satisfy $a^d = 1$ and H also a subset of the solutions to $x^d = 1$. But based on Theorem 4.1, $x^d = 1$ have at most d solutions in $\mathbb{F}_q^\times$. And since d is the size of H, we can redefine H as

$$H = \{x \in \mathbb{F}_q^\times : x^d = 1\}$$

The value of d are arbitrary, and we proved there is at most one subgroup of $\mathbb{F}_q^\times$. Refer again to Theorem 4.4, we conclude $\mathbb{F}_q^\times$ is cyclic. □

References

[1] Franz Lemmermeyer. *Quadratic Number Fields*. Springer International Publishing. 2021.
[2] Keith Conrad. *Cyclicity of $(Z/(p))^\times$*. https://kconrad.math.uconn.edu/blurbs/grouptheory/cyclicmodp.pdf