BASIC NUMBER THEORY: LECTURE 1

WENHAN DAI

1. Introduction: primes with the form $p = x^2 + y^2$

The course begins with the conjecture of Fermat that is proved by Euler.

Theorem 1 (Euler)**.** *Let p be a prime number. Then there exists integers x, y such that $p = x^2 + y^2$ if and only if $p \equiv 1 \bmod 4$.*

Proof. The proof is divided into two steps.

(1) **The reciprocity step.**
We claim that given p, there are $x, y \in \mathbb{Z}$ such that $p \nmid xy$ and $p \mid x^2 + y^2$, if and only if $p \equiv 1 \bmod 4$.

- Suppose there are x, y such that $x^2 \equiv -y^2 \bmod p$ and $p \nmid xy$. Then
$$x^{p-1} \equiv (-1)^{(p-1)/2} y^{p-1} \bmod p.$$
On the other hand, Fermat's little theorem dictates that if $p \nmid a$ then $a^{p-1} \equiv 1 \bmod p$. By this, as $p \nmid xy$, we get
$$x^{p-1} \equiv y^{p-1} \equiv 1 \bmod p \implies (-1)^{(p-1)/2} \equiv 1 \bmod p.$$
Therefore, $2 \mid (p-1)/2$ and hence $p \equiv 1 \bmod 4$.
- As for the converse direction of the claim, it is equivalent to show that there is some $x \in \mathbb{Z}$ such that $x^2 + 1 \equiv 0 \bmod p$ for $p = 4k + 1$ with $k \in \mathbb{Z}$. Note that the polynomial $x^{4k} - 1 = (x^{2k} + 1)(x^{2k} - 1)$ splits over $\mathbb{F}_p$, i.e. $x^{4k} = 1$ has $4k = p - 1$ distinct roots in $\mathbb{F}_p$, and so also does $x^{2k} - 1$. Then there is some $x \in \mathbb{Z}$ such that $p \mid x^{2k} + 1 = (x^k)^2 + 1$.

(2) **The descent step.**
Given p, suppose there are $x, y \in \mathbb{Z}$ such that $p \mid x^2 + y^2$ and $p \nmid xy$. We assert that if $x^2 + y^2 > p$ then there is a smaller (x', y') such that $p \mid x'^2 + y'^2$ again. Granting this assertion, the proof could be completed by inferring $p = x^2 + y^2$.
To prove the assertion, first observe that by replacing (x, y) with $(\pm x, \pm y) \bmod p$, the result keeps invariant. For this, may suppose $|x|, |y| < p/2$ and $(x, y) = 1$. Then $x^2 + y^2 = pm < p^2/2$ for some m, which implies $m < p$. Let q be a prime divisor of m with $q < p$.

Claim. There exist $a, b \in \mathbb{Z}$ such that $q = a^2 + b^2$.
The claim is apparent when $q = 2$. Suppose q is an odd prime. Note that $q \nmid xy$ and $q \mid x^2 + y^2$. By Step (1), $q \equiv 1 \bmod 4$. Using the induction, we find a solution that $(a, b) = (\pm x, \pm y)$ or $(\pm y, \pm x) \bmod q$.

Date: September 22, 2020.

Without loss of generality, we only consider the case when $(a,b) \equiv (x,y) \bmod q$. Then $q \mid ay - bx$ and $q \mid ax + by$. This then leads to

$$pmq = (x^2+y^2)(a^2+b^2) = (ay-bx)^2 + (ax+by)^2.$$

However, this allows the descent via

$$p \cdot \frac{m}{q} = \left(\frac{ay-bx}{q}\right)^2 + \left(\frac{ax+by}{q}\right)^2.$$

This completes the proof of (1)(2). □

Using the similar strategy, one can prove the following results.

Proposition 2. *Let p be a prime number. Then*

(1) *there are $x, y \in \mathbb{Z}$ such that $p = x^2 + 2y^2$ if and only if $p \equiv 1, 3 \bmod 8$;*
(2) *there are $x, y \in \mathbb{Z}$ such that $p = x^2 + 3y^2$ if and only if $p \equiv 1 \bmod 3$.*

2. The quadratic reciprocity law

Definition 3. The *Legendre symbol* is defined as follows.

$$\left(\frac{a}{p}\right) := \begin{cases} 0, & p \mid a; \\ 1, & a \text{ is a quadratic residue mod } p; \\ -1, & \text{otherwise.} \end{cases}$$

Here $a \in \mathbb{Z}$ is called a *a quadratic residue modulo p* if the congruence equation $x^2 \equiv a \bmod p$ has a solution $x \in \mathbb{Z}$.

We can rewritten the reciprocity step of Theorem 1 and Proposition 2 as below.

Proposition 4. *We obtain*

$$\begin{aligned} \left(\frac{-1}{p}\right) = 1 &\iff p \equiv 1 \bmod 4; \\ \left(\frac{-2}{p}\right) = 1 &\iff p \equiv 1, 3 \bmod 8; \\ \left(\frac{-3}{p}\right) = 1 &\iff p \equiv 1 \bmod 3 \\ &\iff p \equiv 1, 7 \bmod 12. \end{aligned}$$

Moreover, Euler had made more conjectures of this type via his elementary calculations.

Proposition 5 (Euler's conjecture)**.**

$$\begin{aligned} \left(\frac{-5}{p}\right) = 1 &\iff p \equiv 1, 3, 7, 9 \bmod 20; \\ \left(\frac{-7}{p}\right) = 1 &\iff p \equiv 1, 9, 11, 15, 23, 25 \bmod 28; \\ \left(\frac{3}{p}\right) = 1 &\iff p \equiv \pm 1 \bmod 12; \end{aligned}$$

$$\begin{aligned}\left(\frac{5}{p}\right) = 1 \quad &\Longleftrightarrow \quad p \equiv \pm 1, \pm 9 \bmod 20;\\ \left(\frac{7}{p}\right) = 1 \quad &\Longleftrightarrow \quad p \equiv \pm 1, \pm 9, \pm 25 \bmod 28.\end{aligned}$$

By looking at the last three relations in the proposition, one may guess that

Conjecture 6. *Let $p \neq q$ be distinct odd primes. Then*

$$\left(\frac{q}{p}\right) = 1 \quad \Longleftrightarrow \quad p \equiv \pm \Box \bmod 4q,$$

where $\Box$ denotes a perfect square number of an integer.

In fact, this is a phenomenon of the quadratic reciprocity law.

Theorem 7 (Quadratic reciprocity law)**.**

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = \begin{cases} 1, & \textit{if either of } p, q \equiv 1 \bmod 4;\\ -1, & \textit{if } p, q \equiv 3 \bmod 4.\end{cases}$$

Before going further, we need to point out that Conjecture 6 is not just a one-sided phenomenon of the quadratic reciprocal law; it actually implies Theorem 7 entirely.

Proposition 8. *Theorem 7 and Conjecture 6 are equivalent.*

Proof. The proof is constructed by explicit computation. Consider the following cases.

(1) Either of $p, q \equiv 1 \bmod 4$. Suppose $q \equiv 1 \bmod 4$. For this, we obtain

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

On Conjecture 6, consider

$$\left(\frac{q}{p}\right) = 1 \Longleftrightarrow p \equiv \Box \bmod q \Longleftrightarrow p \equiv \pm\Box \bmod 4q.$$

(2) Suppose $p, q \equiv 3 \bmod 4$. Then

$$\begin{aligned}\left(\frac{q}{p}\right) = 1 \Longleftrightarrow \left(\frac{p}{q}\right) &= -1\\ \Longleftrightarrow p &\equiv -\Box \bmod q\\ \Longleftrightarrow p &\equiv -\Box \bmod 4q\\ \Longleftrightarrow p &\equiv \pm\Box \bmod q.\end{aligned}$$

This completes the proof. □

A comment by the note-taker. From the aspect of field theory (or algebraic number theory), here comes an important argument to understand the quadratic reciprocity law. Consider the unit group $\mathbb{F}_p^\times$ of the finite field $\mathbb{F}_p$, which is a multiplicative group of order $p-1$ and consists of the elements that are invertible in $\mathbb{F}_p$, i.e., those ($x \bmod p$) such that there exists some ($y \bmod p$) such that $xy \equiv 1 \bmod p$. Let $(\mathbb{F}_p^\times)^2$ denote the subgroup generated by the square elements, which set-theoretically contains the elements x^2 when x runs through all elements in $\mathbb{F}_p^\times$. Then for each $a \in \mathbb{F}_p^\times$, it further lies in $(\mathbb{F}_p^\times)^2$ if and only if it is a quadratic residue modulo p; or equivalently, $\left(\frac{a}{p}\right) = 1$. This induces a group homomorphism

$$\varphi : \mathbb{F}_p^\times \longrightarrow \{\pm 1\}, \quad a \longmapsto \left(\frac{a}{p}\right).$$

Note that $\ker\varphi = (\mathbb{F}_p^\times)^2$ and hence by the first group isomorphism theorem,

$$\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2 \cong \{\pm 1\}.$$

From this, we conclude two properties:

(i) As both sides are multiplicative groups, for each a, b,

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

Moreover, this can be also deduced from

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

(ii) The quadratic residue is "equidistributed" in $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{F}_p^\times$, i.e. there are exactly $(p-1)/2$ elements in $(\mathbb{Z}/p\mathbb{Z})^\times$ that are quadratic residues modulo p, and the other $(p-1)/2$ elements are not.

Remark 9. In practice, the quadratic reciprocity law gives rise to an algorithm to compute Legendre symbols $\left(\frac{p}{q}\right)$.

3. On higher reciprocity laws

More phenomena. Historically, Euler has discovered some properties that are beyond the quadratic reciprocity law.

(1) When $p \neq 5$ is an odd prime,

$$p = x^2 + 5y^2 \iff p \equiv 1, 9 \bmod 20,$$
$$2p = x^2 + 5y^2 \iff p \equiv 3, 7 \bmod 20.$$

(2) When $p \neq 5$ is an odd prime,

$$p = x_1^2 + 14y_1^2 \iff p = 2x_2^2 + 7y_2^2 \iff p \equiv 1, 9, 15, 23, 25, 39 \bmod 56,$$
$$3p = x^2 + 14y^2 \iff p \equiv 3, 5, 13, 19, 27, 45 \bmod 56.$$

(3) When p is any odd prime,

(i) $p = x^2 + 27y^2$ if and only if $p \equiv 1 \mod 3$, and 2 is a cubic residue of p, i.e. the congruent equation $x^3 \equiv 2 \bmod p$ has a solution.

(ii) $p = x^2 + 64y^2$ if and only if $p \equiv 1 \bmod 4$ and 2 is a biquadratic residue of p, i.e. the congruent equation $x^4 \equiv 2 \bmod p$ has a solution.

One of the main goal of this course is to understanding some generalization of the quadratic reciprocity as a "higher reciprocity law". The main obstruction lies in the language: the reciprocity law together with the Legendre symbol only describes the relation between two primes. It is necessary to find out a new approach to describe the relations via the "class group".

Theorem 10 (The main theorem of the course)**.** *Fix a positive integer $n \in \mathbb{Z}_{>0}$. Then there exists a monic irreducible polynomial $f_n(x) \in \mathbb{Z}[x]$ of degree $h(-4n)$, where $h(\cdot)$ denotes the class number, such that: for each odd prime $p \nmid n$, the following are equivalent.*

(*a*) *There are $x, y \in \mathbb{Z}$ such that $p = x^2 + ny^2$;*
(*b*) *there is an integer solution for $f_n(x) \equiv 0 \bmod p$ and $\left(\frac{-n}{p}\right) = 1$.*

Here Theorem 10 appears in a relatively elementary appearance, but the properties of $f_n(x)$ have a deep connection with classical algebraic number theory. For example,

- the existence of $f_n(x)$ comes from the class field theory, and
- to compute $f_n(x)$, we need the complex multiplication on elliptic curves.

School of Mathematical Sciences, Peking University, 100871, Beijing, China
Email address: daiwenhan@pku.edu.cn