Introduction to Number Theory

Math 110 | Winter 2023

Xu Gao

March 8, 2023

What we have seen last time:

- Qudratic residues and non-residues
- Euler’s theorem
- Method of Partnership
- Wilson’s theorem
- Legendre symbol

Today, we will move to the ***reciprocity laws***.

Quadratic Reciprocity Laws

What is a reciprocity law?

A ***reciprocity law*** would relate

- a property about the congruence class of a modulo m and
- a property about the congruence class of $f(m)$ modulo $g(a)$.

What important is that the roles of a and m are exchanged: in the second property, the congruence class only depends on m, while the modulus only depends on a.

Theorem 22.1 (First Quadratic Reciprocity Law)

Let p be an odd prime number. Then

congruence

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

Congruence

modulus

modulus

Proof. Corollary 21.10 tell us that -1 is a quadratic residue modulo p if and only if $p \equiv 1 \pmod{4}$, and it is a quadratic non-residue modulo p if and only if $p \equiv 3 \pmod{4}$. $\square$

Theorem 22.2 (Second Quadratic Reciprocity Law)

Let p be an odd prime number. Then

congruence

congruence

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

modulus

modulus

Proof. We will use the method of partnership, investigating the following three products:

$$A = 1 \cdot 2 \cdot \cdots \cdot \frac{p-3}{2} \cdot \frac{p-1}{2}, \qquad \text{(first half of } \Phi(p))$$

$$B = 2 \cdot 4 \cdot \cdots \cdot (p-3) \cdot (p-1), \qquad \text{(evens in } \Phi(p))$$

$$C = 1 \cdot 3 \cdot \cdots \cdot (p-4) \cdot (p-2). \qquad \text{(odds in } \Phi(p))$$

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

$\underset{\text{even}}{x} \leq \frac{p-1}{2} \rightsquigarrow \underset{\text{odd}}{p - x} > \frac{p-1}{2}$

The product B can be obtained from A by multiplying each factor by 2. Hence, $B = 2^{\frac{p-1}{2}} A$. The product C are related to B by the bijection $x \mapsto p - x$. Hence, $C = (-1)^{\frac{p-1}{2}} B$. Finally, if we replace each even factor x in A by $p - x$, we get C. Hence, $C = (-1)^{\lfloor \frac{p-1}{4} \rfloor} A$. (Note that there are $\lfloor \frac{p-1}{4} \rfloor$ evens in the first half of $\Phi(p)$.)

If we combine above, we get

$$(-1)^{\lfloor \frac{p-1}{4} \rfloor} \equiv (-1)^{\frac{p-1}{2}} \cdot 2^{\frac{p-1}{2}} \pmod{p}.$$

Therefore, by Euler's theorem,

$$\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \equiv (-1)^{\lfloor \frac{p-1}{4} \rfloor + \frac{p-1}{2}} \pmod{p}.$$

We list all possibilities of the values:

$p \pmod{8}$	$\frac{p-1}{2} \pmod{2}$	$\lfloor \frac{p-1}{4} \rfloor \pmod{2}$	$\left(\frac{2}{p}\right)$
1	0	0	1
3	1	0	-1
5	0	1	-1
7	1	1	1

Then the statement follows. $\square$

Theorem 22.3 (Third Quadratic Reciprocity Law)

Let p and q be two distinct odd prime numbers. Then

Cong. cong.

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

mod. mod.

We introduce $p^* := (-1)^{\frac{p-1}{2}} \cdot p$. Then the above formula tells us:

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right).$$

Quadratic Reciprocity Laws

± sign

$$\left(\frac{n}{p}\right) = \left(\frac{-1}{p}\right)^{\nu_{-1}(n)} \cdot \left(\frac{2}{p}\right)^{\nu_2(n)} \cdot \prod_{\substack{q \\ \in \\ \text{odd prime}}} \left(\frac{q}{p}\right)^{\nu_q(n)}$$

Note that the prime factorization of integers and the complete multiplicativity of $\left(\frac{-}{p}\right)$ together tells us that its value is completely determined by $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$, and $\left(\frac{q}{p}\right)$ (for prime q). Hence, the three quadratic reciprocity laws help us to completely translate quadratic residue problems in a reciprocal way.

Applications of Quadratic Reciprocity Laws

Example 22.4

Is 10 a quadratic residue modulo 10337?

Since $10 = 2 \cdot 5$, $\left(\frac{10}{10337}\right) = \left(\frac{2}{10337}\right)\left(\frac{5}{10337}\right)$.

We can use the second quadratic reciprocity law to compute $\left(\frac{2}{10337}\right)$:

$$10337 \equiv 337 \equiv 1 \pmod{8}.$$

Hence, $\left(\frac{2}{10337}\right) = 1$.

We then use the third quadratic reciprocity law to compute $\left(\frac{5}{10337}\right)$:

$10337 \equiv 1 \bmod 4$

$$\left(\frac{5}{10337}\right) = \left(\frac{10337^*}{5}\right) = \left(\frac{10337}{5}\right) = \left(\frac{2}{5}\right) = -1,$$

$2^{\frac{5-1}{2}} = 2^2 \equiv -1 \bmod 5$

$1^2 \equiv 1 \quad 4^2 \equiv 1$
$2^2 \equiv 4 \quad 0^2 \equiv 0$
$3^2 \equiv 4 \quad (\bmod 5)$

here the last equality follows from the second quadratic reciprocity law. We conclude that 10 is a quadratic non-residue modulo 10337.

Irreducibility of modular polynomials

Example 22.5

Consider the integer polynomial $f(T) = T^2 - 2T + 4$. Modulo which prime p, the polynomial $f(T)$ is irreducible.

We first complete the square:

$$f(T) = T^2 - 2T + 4 = (T-1)^2 + 3.$$

Then $\quad f(T)$ is ~~ir~~reducible modulo p

$\iff$ there is an integer a such that $(a-1)^2 \underline{+3} \equiv 0 \pmod{p}$

$\iff$ -3 is a quadratic residue modulo p.

By looking at the contrapositive, we have

$$f(T) \text{ is irreducible modulo } p \iff \left(\frac{-3}{p}\right) = -1.$$

$(-1)^{\frac{3-1}{2}} = -1$ $\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right)$

Note that $3^* = -3$. Hence, by the third reciprocity law,

$$\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right).$$

Among $\Phi(3) = \{1, 2\}$, 2 is the only quadratic non-residue. Hence,

$$\left(\frac{-3}{p}\right) = -1 \iff p \equiv 2 \pmod 3$$

We thus conclude that $T^2 - 2T + 4$ is irreducible modulo p if and only if $p \equiv 2 \pmod 3$.

Question

Given modulus m and $a \in \Phi(m)$, show that there are infinitely many prime numbers p such that

$$p \equiv a \pmod{m}.$$

Using quadratic reciprocity laws, we can prove the following weak version:

Theorem 22.6

Fix an integer a. There are infinitely many prime numbers p such that $\left(\frac{a}{p}\right) = 1$.

Lemma 22.7

Let $f(T)$ be a nonzero integer polynomial. Then there are infinitely many prime numbers p such that $p \mid f(n)$ for some integer n.

Proof. Suppose $f(T) = a_d T^d + \cdots + a_1 T + a_0$.

For the sake of contradiction, suppose $p_1, \cdots, p_r$ are all the prime numbers such that $p \mid f(n)$ for some integer n, saying $p_i \mid f(n_i)$.

Let $P = p_1 \cdots p_r$. Then for any integer x, we have

$$\frac{1}{a_0} f(a_0 PT) = \frac{1}{a_0}\left(a_d(a_0PT)^d + \cdots + a_1(a_0PT) + a_0\right)$$
$$= \underbrace{a_d a_0^{d-1} P^d T^d + \cdots + a_1 PT}_{\equiv 0 \bmod P} + 1.$$

Infinitude of primes in arithmetic progressions

$$\begin{aligned}\frac{1}{a_0}f(a_0PT) &= \frac{1}{a_0}\left(a_d(a_0PT)^d + \cdots + a_1(a_0PT) + a_0\right)\\ &= \underbrace{a_d a_0^{d-1}P^dT^d + \cdots + a_1PT}_{\equiv 0 \bmod P} + 1.\end{aligned}$$

Note that the right-hand side is a nonzero integer polynomial with all non-constant coefficients being a multiple of P. Hence, there are integers x such that $\frac{1}{a_0}f(a_0Px)$ is an integer larger than 1 and coprime to P. But this implies that there must be a prime p distinct from $p_1, \cdots, p_r$ such that $p \mid f(a_0Px)$. A contradiction! □

Proof. (Of theorem 22.6) Apply the lemma to $T^2 - a$. We see that there are infinitely many prime numbers p such that $p \mid n^2 - a$, namely $n^2 \equiv a \pmod{p}$, for some integer n. Among these primes, there are only finitely many can divide a. Hence, there are infinitely many prime numbers p such that $\left(\frac{a}{p}\right) = 1$. $\square$

Infinitude of primes in arithmetic progressions

Apply Quadratic Reciprocity Laws to Theorem 22.6, we have

- There are infinitely many prime numbers $\equiv 1 \pmod{4}$.
  Proof. Take $a = -1$ and note that $\left(\frac{-1}{p}\right) = 1 \Leftrightarrow p \equiv 1 \pmod{4}$. $\square$
- There are infinitely many prime numbers $\equiv 1 \pmod{3}$.
  Proof. Take $a = -3$ and note that $\left(\frac{-3}{p}\right) = 1 \Leftrightarrow p \equiv 1 \pmod{3}$. $\square$
- There are infinitely many prime numbers $\equiv \pm 1 \pmod{8}$.
  Proof. Take $a = 2$ and note that $\left(\frac{2}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \pmod{8}$. $\square$
- $\ldots\ldots$