QUADRATIC RECIPROCITY LAW

MING-LUN HSIEH

1. Equations over finite fields

Denote by $\mathbf{Z}$ the set of integers is denoted by and and by $\mathbf{Q}$ the set of rational numbers. Let p be a rational prime. We write $\mathbb{F}_p = \mathbf{Z}/p\mathbf{Z}$. Let $\mathbb{F}_p^\times$ be the multiplicative group given by

$$\mathbb{F}_p^\times := \{x \neq 0 \in \mathbb{F}_p\}.$$

We know that $\mathbb{F}_p$ is a finite field and $x^{p-1} = 1$ for each $x \in \mathbb{F}_p^\times$.

Proposition 1.1. *The group $\mathbb{F}_p^\times \simeq \mathbf{Z}/(p-1)\mathbf{Z}$ is a cyclic group of order $p-1$. In other words, there exists $\alpha \in \mathbb{F}_p^\times$ such that*

$$\mathbb{F}_p^\times =< \alpha >:= \left\{1, \alpha, \alpha^2, \cdots, \alpha^{p-2}\right\}.$$

Proof. See Serre's book [Ser73, Theorem 2, p. 4]. □

Lemma 1.2. *Let $a \in \mathbf{Z}_+$. Then*

$$\sum_{y \in \mathbb{F}_p} y^a = \begin{cases} 0 & \text{if } p-1 \nmid a, \\ -1 & \text{if } p-1 \mid a. \end{cases}$$

Proof. Put

$$S := \sum_{y \in \mathbb{F}_p} y^a \in \mathbb{F}_p.$$

If $p-1 \mid a$ then $y^a = 1$ if $y \neq 0$, so $S = (p-1) = -1$. If $p-1 \nmid a$, then there exists $\alpha \in \mathbb{F}_p$ such that $\alpha \neq 1$. We have $\alpha S = S \Rightarrow S = 0$. □

Definition 1.3. For $f \in \mathbf{Z}[x_1, \cdots x_n]$ a polynomial of n-variables, we put

$$X_f(R) := \{(a_1, \cdots, a_n) \in R^n \mid f(a_1, \cdots, a_n) = 0\}.$$

Here R can be $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{Z}/p^n\mathbf{Z}$ or $\mathbb{F}_p$. We denote by $\#X_f(R)$ the cardinality of the set $X_f(R)$.

Theorem 1.4 (Chevalley-Warning). *Let $f \in \mathbf{Z}[x_1, \cdots, x_n]$. If $\deg f < n$, then*

$$\#X_f(\mathbb{F}_p) \equiv 0 \,(mod\ p).$$

Proof. Consider the polynomial

$$P(x_1, \ldots, x_n) := 1 - \bar{f}(x_1, \ldots, x_n)^{p-1} \in \mathbb{F}_p[x_1, \ldots, x_n].$$

Then it is clear that if $a = (a_1, \ldots, a_n) \in \mathbb{F}_p^n$,

$$P(a) = \begin{cases} 1 & \text{if } f(a) = 0, \\ 0 & \text{if } f(a) \neq 0, \end{cases}$$

Date: September 6, 2025.

so

$$\#X_f(\mathbb{F}_p) \equiv \sum_{a\in\mathbb{F}_p^n} P(a) = \sum_{(m_1,m_2,\dots,m_n)} \sum_{a\in\mathbb{F}_p^n} a_1^{m_1}a_2^{m_2}\dots a_n^{m_n}.$$

Since $\deg f < n$, we find that $\deg P < (p-1)n$, and hence $m_j < p-1$ for some j. This shows that $\#X_f(\mathbb{F}_p) \equiv 0 \pmod{p}$ by Lemma 1.2. □

2. Quadratic reciprocity law

Definition 2.1 (Legendre symbol)**.** Suppose that $p > 2$ is an odd pirme. For $a \in \mathbb{F}_p$, we define

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \cdots a \in (\mathbb{F}_p^\times)^2, \\ -1 & \cdots a \notin (\mathbb{F}_p^\times)^2, \\ 0 & \cdots a = 0. \end{cases}$$

By definition,

$$\#\left(\left\{b \in \mathbb{F}_p \mid b^2 = a\right\}\right) = \left(\frac{a}{p}\right) + 1.$$

Example 2.2. $\left(\frac{2}{3}\right) = \left(\frac{3}{5}\right) = -1$.

Since $p > 2$, we can distinguish $+1$ and -1 in $\mathbb{F}_p$ and view the legendre symbol valued in $\mathbb{F}_p$. Denote by $\overline{\mathbb{F}_p}$ the algebraic closure of $\mathbb{F}_p$.

Proposition 2.3. *Let $a \in \mathbb{F}_p^\times$ and $y \in \overline{\mathbb{F}_p}$ with $y^2 = a$. Then*

$$\left(\frac{a}{p}\right) = y^{p-1} = a^{\frac{p-1}{2}} \in \mathbb{F}_p.$$

Proof. Note that $(y^{p-1})^2 = a^{p-1} = 1$, so $y^{p-1} = \pm 1$, and

$$\left(\frac{a}{p}\right) = 1 \iff y \in \mathbb{F}_p \iff y^p = y \iff y^{p-1} = 1.$$

The lemma follows immediately. □

Corollary 2.4. *The map*

$$\mathbb{F}_p^\times \to \{\pm 1\}, \quad a \mapsto \left(\frac{a}{p}\right)$$

is a surjective group homomorphism.

Proposition 2.5. *We have the following formulas.*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$
$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Proof. It suffices to show the second formula. Let α be a 8-th primitive root of unity in $\overline{\mathbb{F}_p}$ and put $y = \alpha + \alpha^{-1}$. Then $y^2 = 2$, and by Proposition 2.3

$$\left(\frac{2}{p}\right) = y^{p-1} \in \mathbb{F}_p.$$

Since $y^p = y$ if $p \equiv \pm 1 \pmod{8}$ and $y^p = -y$ if $p \equiv \pm 3 \pmod{8}$, we find that $y^{p-1} = (-1)^{\frac{p^2-1}{8}}$. □

The following theorem is referred to the quadratic reciprocity law.

Theorem 2.6 (Gauss)**.** *Let p, q be two distinct odd primes. Then*

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

There are several proofs in the literature. We shall explain two proofs. The first one is simpler but uses "Gauss sum" in finite fields. The other one is elementary and combinatorial.

The first proof. Let ζ be a primitive q-th root of unity in $\overline{\mathbb{F}_p}$ (the existence?). Define the Gauss sum

$$G := \sum_{i\in\mathbb{F}_q^\times}\left(\frac{i}{q}\right)\zeta^i \in \overline{\mathbb{F}_p}.$$

It is clear that $G^p = \left(\frac{p}{q}\right) G$ and a direct computation shows that

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

It follows that $G \neq 0 \in \overline{\mathbb{F}_p}^\times$ and

$$\left(\frac{p}{q}\right) = G^{p-1} = q^{\frac{p-1}{2}}(-1)^{(\frac{p-1}{2})(\frac{q-1}{2})} = \left(\frac{q}{p}\right)(-1)^{(\frac{p-1}{2})(\frac{q-1}{2})} \in \overline{\mathbb{F}_p}.$$

The second proof. We begin with a lemma of Gauss.

Lemma 2.7 (Gauss)**.** *Let $a \in \mathbb{F}_p^\times$. For each $1 \le i \le \frac{p-1}{2}$, let r_i be the unique integer such that $r_i \equiv ia \,(mod\ p)$ and $-\frac{p-1}{2} \le r_i \le \frac{p-1}{2}$. Then*

$$\left(\frac{a}{p}\right) = (-1)^s,$$

where $s = \#\left\{0 < i < \frac{p}{2} \mid r_i < 0\right\}$.

Proof. Let $\left\{-u_1, -u_2, \dots, -u_s, v_1, \dots, v_{\frac{p-1}{2}-s}\right\}$ be the residue of $\left\{a, 2a, \dots, \frac{p-1}{2}a\right\}$ modulo p with $1 \le u_i, v_j \le \frac{p-1}{2}$. Then one verifies that

$$\left\{u_1, \dots, u_s, v_1, \dots, v_{\frac{p-1}{2}-s}\right\} = \left\{1, \dots, \frac{p-1}{2}\right\}$$

for u_i, v_j are distinct. It follows that

$$\left(\frac{p-1}{2}\right)! = \prod_{i=1}^{s} u_i \prod_{j=1}^{\frac{p-1}{2}-s} v_j = (-1)^s \prod_{i=1}^{\frac{p-1}{2}} ia = (-1)^s\left(\frac{p-1}{2}\right)!\cdot a^{\frac{p-1}{2}} \in \mathbb{F}_p.$$

This shows that

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

□

Let R be the rectangle

$$R = \left\{(x,y) \in \mathbf{Z}^2 \mid 0 < x < p/2, \quad 0 < y < q/2\right\}.$$

Consider the subsets

$$\begin{aligned} S_{qp} &= \{(x,y) \in R \mid 0 < yp - xq < p/2\}, \\ S_{pq} &= \{(x,y) \in R \mid 0 < xq - yp < q/2\}, \\ T_+ &= \left\{(x,y) \in R \mid yp - xq \geq \frac{p+1}{2}\right\}; \\ T_- &= \left\{(x,y) \in R \mid xq - yp \geq \frac{q+1}{2}\right\}. \end{aligned}$$

It is clear that

$$R = S_{pq} \sqcup S_{qp} \sqcup T_+ \sqcup T-,$$

and by Lemma 2.7, we find that

$$\left(\frac{q}{p}\right) = (-1)^{\#S_{qp}}; \quad \left(\frac{p}{q}\right) = (-1)^{\#S_{pq}}.$$

The map $(x,y) \mapsto (\frac{p+1}{2} - x, \frac{q+1}{2} - y)$ gives a bijection between T_+ and T_-, so we see

$$\#(T_+) = \#(T_-).$$

It follows that

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\#R - 2\#T_+} = (-1)^{\#R} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Example 2.8. We can use the quadratic reciprocity law to compute Legendre symbols. For example,

$$\begin{aligned} \left(\frac{3}{149}\right) &= \left(\frac{149}{3}\right)(-1)^{\frac{148}{2}} = \left(\frac{2}{3}\right) = -1 \\ \left(\frac{12}{23}\right) &= \left(\frac{2}{23}\right)^2\left(\frac{3}{23}\right) = -\left(\frac{23}{3}\right) = -\left(\frac{2}{3}\right) = 1. \end{aligned}$$

References

[Ser73] J.-P. Serre, *A course in arithmetic*, Springer-Verlag, New York, 1973, Translated from the French, Graduate Texts in Mathematics, No. 7.

Homework 2: Due date (9/19)

In these exercises, the letter p always denotes an odd prime.

Exercise 1 (10 pts)**.** Let

$$f(x,y) = y^2 - y - x^3 + x^2 \in \mathbf{Z}[x,y].$$

For $n \in \mathbf{Z}_+$, put $\mathbf{a}(p^n) := \#X_f(\mathbf{Z}/p^n\mathbf{Z})$. Show that

(1) $\mathbf{a}(p^n) = p^{n-1}\mathbf{a}(p)$ if $p \neq 11$.

(2) $\mathbf{a}(p^n) = p^n - 2p^{n-1}$ if $p = 11$ and $n > 1$.

Note that $p = 11$ is special because it is the only prime p such that the system of equations

$$f(x,y) = \frac{\partial f}{\partial x} = \frac{\partial f}{\partial y} = 0$$

has a solution in $\mathbb{F}_p$.

Hint for (1): We need to prove $\mathbf{a}(p^n) = p\mathbf{a}(p^{n-1})$ for $n > 1$. Given $(a,b) \in \mathbf{Z}^2$ with $f(a,b) \equiv 0 \pmod{p^{n-1}}$, you may use the Taylor expansion of $f(x,y)$ around (a,b) to show there are p solutions $f(x,y) = 0$ in $\mathbf{Z}/p^n\mathbf{Z}$ with $(x,y) \equiv (a,b) \pmod{p^{n-1}}$.

Exercise 2 (5pts)**.** Use quadratic reciprocity law to show that

$$\left(\frac{-6}{p}\right) = 1 \iff p \equiv 1, 5, 7, 11 \pmod{24}.$$

Exercise 3 (5 pts)**.** Let

$$f(x) = (x^2 - 11)(x^2 - 17)(x^2 - 187) \in \mathbf{Z}[x].$$

Show that $X_f(\mathbb{F}_p) \neq \emptyset$ for all primes p, but $X_f(\mathbf{Q}) = \emptyset$.

Exercise 4 (5pts)**.** Let $a \in \mathbb{F}_p^\times$ with $\left(\frac{a}{p}\right) = 1$. Show that

$$\#\left(\left\{m \in \mathbb{F}_p \mid \left(\frac{m^2 - a}{p}\right) = -1\right\}\right) = \frac{p-1}{2}.$$

Exercise 5 (10 pts)**.** Let

$$f(x,y) = y^2 - x^3 + x \in \mathbf{Z}[x,y].$$

Let $p > 2$ be an odd prime. Show that

(1)

$$\#X_f(\mathbb{F}_p) = \sum_{x \in \mathbb{F}_p} 1 + \left(\frac{x^3 - x}{p}\right).$$

(2) $\#X_f(\mathbb{F}_p) \equiv 3 \pmod 4$.

(3) If $p \equiv -1 \pmod 4$, then $\#X_f(\mathbb{F}_p) = p$.

Exercise 6 (5 pts)**.** Let $c \in \mathbb{F}_p^\times$ and let

$$f(x,y) = y^2 - x^3 - c.$$

Show that $\#X_f(\mathbb{F}_p) = p$ if $p \equiv 2 \pmod 3$.