Chapter 5: Quadratic Reciprocity

Author: Meng-Gen Tsai
Email: plover@gmail.com

Exercise 5.2. *Show that the number of solutions to $x^2 \equiv a\ (p)$ is given by $1 + (a/p)$.*

p is an odd prime.

Proof.

(1) If $x \equiv t\,(p)$ is a solution of the equation $x^2 \equiv a\,(p)$, then $x \equiv -t\,(p)$ is also a solution. Notice that $t \not\equiv -t\ (p)$ if $t \not\equiv 0\ (p)$ by using the fact that p is odd.

(2) (Lemma 4.1.) Let $f(x) \in k[x]$, k a field. Suppose that $\deg f(x) = n$. Then f has at most n distinct roots.

(3) If $a = 0$, then $x^2 \equiv 0\ (p)$ has only one solution $x \equiv 0\ (p)$, or $1 + (a/p)$ solution (where $(a/p) = 0$ in this case).

(4) If $a \neq 0$ is a quadratic residue mod p, then by (1)(2) the equation $x^2 \equiv a(p)$ has exactly 2 solutions, or $1 + (a/p)$ solutions (where $(a/p) = 1$ in this case).

(5) If a is not a quadratic residue mod p, then there is no solutions of the equation $x^2 \equiv a\ (p)$, or $1 + (a/p)$ solutions (where $(a/p) = -1$ in this case).

By (3)(4)(5), in any case the number of solutions to $x^2 \equiv a\ (p)$ is given by $1 + (a/p)$. □

Exercise 5.4. *Prove that* $\sum_{a=1}^{p-1}(a/p) = 0$.

Note. $\sum_{a=0}^{p-1}(a/p) = 0$ since $(0/p) = 0$.

Proof. There are as many residues as nonresidues mod p (Corollary to Proposition 5.1.2). □

Exercise 5.5. *Prove that* $\sum_{x=0}^{p-1}\left(\frac{ax+b}{p}\right) = 0$ *provided that* $p \nmid a$.

Proof. Since x $(x = 1, \dots, p-1)$ is a reduced residue system modulo p, ax $(x = 1, \dots, p-1)$ is again a reduced residue system modulo p if $p \nmid a$ (Exercise

3.6). Hence

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

Note that $\left(\frac{0}{p}\right) = 0$, and thus $0 = \sum_{x=0}^{p-1} \left(\frac{ax}{p}\right) = \sum_{x=0}^{p-1} \left(\frac{a(x+a^{-1}b)}{p}\right) = \sum_{x=0}^{p-1} \left(\frac{ax+b}{p}\right)$.
$\square$

Exercise 5.6. *Show that the number of solutions to $x^2 - y^2 \equiv a\,(p)$ is given by*

$$\sum_{y=0}^{p-1} \left(1 + \left(\frac{y^2+a}{p}\right)\right).$$

Proof. Write $x^2 \equiv y^2 + a\,(p)$. For every fixed $y = 0, \ldots, p-1$, the number of solutions x to $x^2 \equiv y^2 + a\,(p)$ is given by $1 + \left(\frac{y^2+a}{p}\right)$ (Exercise 5.2). Hence, the number of solutions (x, y) to $x^2 - y^2 \equiv a\,(p)$ is

$$\sum_{y=0}^{p-1} \left(1 + \left(\frac{y^2+a}{p}\right)\right).$$

$\square$

Exercise 5.7. *By calculating directly show that the number of solutions to $x^2 - y^2 \equiv a\,(p)$ is $p-1$ if $p \nmid a$ and $2p-1$ if $p \mid a$. (Hint: Use the change of variables $u = x+y, v = x-y$.)*

Proof (Hint). Write $(x+y)(x-y) \equiv a(p)$ or $uv \equiv a(p)$ where $u = x+y, v = x-y$. For any a, either $a \equiv 0\,(p)$ or $a \not\equiv 0\,(p)$.

(1) $a \equiv 0\,(p)$. Then $u = 0$ or $v = 0$. Consider three possible cases (may be overlapped).

 (a) $u = 0$, or $x + y = 0$. In this case, the number of solutions is p. ($x = k, y = -k$ for $k = 0, \ldots, p-1$.)

 (b) $v = 0$. Similar to (a), the number of solutions is p. ($x = k, y = k$ for $k = 0, \ldots, p-1$.)

 (c) $u = v = 0$. $x = y = 0$.

 By (a)(b)(c), there are $2p-1$ solutions to $x^2 - y^2 \equiv 0\,(p)$.

(2) $a \not\equiv 0\,(p)$. $u \neq 0$ and $v \neq 0$. For each $u = k$ for $k = 1, \ldots, p-1$, there is one unique $v = ak^{-1}$ such that $uv \equiv a\,(p)$. Solve u and v to get $(x, y) = (2^{-1}(k + ak^{-1}), 2^{-1}(k - ak^{-1})) \in \mathbb{Z}/p\mathbb{Z}$ for $k = 1, \ldots, p-1$. So there are $p-1$ solutions to $x^2 - y^2 \equiv a\,(p)$ where $a \not\equiv 0\,(p)$.

By (1)(2), the result holds. $\square$

Exercise 5.8. *Combining the results of Exercise 5.6 and 5.7 show that*

$$\sum_{y=0}^{p-1} \left(\frac{y^2+a}{p}\right) = \begin{cases} -1, & \text{if } p \nmid a, \\ p-1, & \text{if } p \mid a. \end{cases}$$

Proof. By Exercise 5.6 and 5.7,

$$\sum_{y=0}^{p-1} \left(1 + \left(\frac{y^2+a}{p}\right)\right) = \begin{cases} p-1, & \text{if } p \nmid a, \\ 2p-1, & \text{if } p \mid a. \end{cases}$$

Hence the result holds. $\square$