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 $1 + (a/p)$. $\square$

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). $\square$