Chapter 14

Counting integral and rational points on curves, modulo p

14.1. Diagonal quadratics

Exercise 14.1.1. Prove that if odd prime p does not divide n, then

$$\sum_{x \pmod p} \left(\frac{x^2-n}{p}\right) = \sum_{y \pmod p} \left(\frac{y(y+n)}{p}\right) = -1.$$

Exercise 14.1.2. Suppose that odd prime p does not divide n.

(a) Show that there are $\frac{1}{4}(p-3-(\frac{n}{p})(1+(\frac{-1}{p})))$ residues $m \pmod p$ for which m and $m+n$ are both quadratic residues mod p.

(b) Show that there are $\frac{1}{4}(p-3+(\frac{n}{p})(1+(\frac{-1}{p})))$ residues $\ell \pmod p$ for which ℓ and $\ell+n$ are both quadratic non-residues mod p.

14.2. Counting solutions to a quadratic equation and another proof of quadratic reciprocity

14.3. Cubic equations modulo p

Exercise 14.3.1. Let p be a prime $\equiv 2 \pmod 3$.

(a) Prove that for every $a \pmod p$ there is exactly one $b \pmod p$ for which $b^3 \equiv a \pmod p$.

(b) Deduce that if $p \nmid (a,b,c)$, then $N(a,b,c) = p^2$.

Exercise 14.3.2. Let p be a prime $\equiv 1 \pmod 3$ with a primitive root g, and suppose $p \nmid abc$.

(a) Show that if $p \nmid rst$, then $N(ar^3, bs^3, ct^3) = N(a,b,c)$.

(b) Show that $N(1,1,1) + N(1,1,g) + N(1,1,g^2) = p^2$.

(c) Show that $N(1,g,1) + N(1,g,g) + N(1,g,g^2) = p^2$.

(d) Deduce that $N(1,g,g^2) = N(1,1,1)$.

(e) Show that $N(a,b,c) = N(1,1,abc)$.

14.4. The equation $E_b:\ y^2 = x^3 + b$

Exercise 14.4.1. Let p be a prime $\equiv 1 \pmod 3$ with a primitive root g and suppose $(\ell, p) = 1$.

(a) Prove that if $L \equiv \ell r^3 \pmod p$, then $S_L = \left(\frac{r}{p}\right) S_\ell$.

Define $T_\ell := \left(\frac{\ell}{p}\right) S_\ell$, so that $T_L = T_\ell$.

(b) Prove that if $\ell \equiv g^k \pmod p$ and i is the least residue of $k \pmod 3$, then $T_\ell = T_{g^i}$.

(c) Prove that T_1 is even, whereas T_g and T_{g^2} are odd.

(d) Prove that each $T_\ell \equiv 1 \pmod 3$.

Therefore there exist integers A, B, C such that $T_1 = 2A, T_g = -A + 3B$, and $T_{g^2} = -A - 3C$.

Exercise 14.4.2.† (a) Prove that if p does not divide abc, then

$$\#\{x, y \pmod p :\ ax^3 + by^3 \equiv c \pmod p\} = p - \chi(a/b) - \chi(b/a) + u,$$

where the character $\chi \pmod p$ has order 3.

(b) Deduce that $\#\{w, x, y, z \pmod p :\ x^3 + y^3 \equiv w^3 + z^3 \pmod p\} = p^3 + 6p(p-1)$.

14.5. The equation $y^2 = x^3 + ax$

Exercise 14.5.1. Let p be a prime $\equiv 3 \pmod 4$. Observing that $(-n)^3 + a(-n) = -(n^3 + an)$ deduce that $S_a = 0$, so that $N_p(a) = p$.

Exercise 14.5.2. Let p be a prime $\equiv 1 \pmod 4$ with a primitive root g and suppose $(\ell, p) = 1$.

(a) Prove that S_ℓ is even, so there exist integers A, B such that $S_1 = 2A$ and $S_g = 2B$.

(b) Using that $\left(\frac{(-n)^3 + \ell(-n)}{p}\right) = \left(\frac{n^3 + \ell n}{p}\right)$ establish that $S_\ell \equiv 3 - \left(\frac{\ell}{p}\right) \pmod 4$.

(c) Deduce that A is odd and B is even.

(d) Prove that if $c \equiv \ell r^2 \pmod p$, then $S_c = \left(\frac{r}{p}\right) S_\ell$.

(e) Deduce that $S_{-1} = (-1)^{\frac{p-1}{4}} \cdot 2A$.

14.6. A more general viewpoint on counting solutions modulo p

Exercise 14.6.1. Use (14.6.1) to show that if $h(x) \pmod p$ is a polynomial of degree $d \geq 2$ without repeated roots, then

$$\left| \sum_{n \pmod p} \left(\frac{h(n)}{p}\right) \right| < (d-1)\sqrt{p}.$$

Exercise 14.6.2. Prove that the number of $n \pmod p$ for which $\left(\frac{n^2+1}{p}\right) = \left(\frac{n^2+2}{p}\right) = 1$ equals $p/4$ plus or minus an error of at most $4\sqrt{p}$.

Exercise 14.6.3.† Let p be an odd prime which can be written as $p = a^2 + b^2$ with $a \equiv 3 \pmod 4$. Prove that the number of $n \pmod p$ for which $\left(\frac{n-1}{p}\right) = \left(\frac{n}{p}\right) = \left(\frac{n+1}{p}\right) = 1$ equals $\frac{p+1+2a}{8} - 2$ if $p \equiv 1 \pmod 8$, and equals $\frac{p+1-2a}{8} - 1$ if $p \equiv 5 \pmod 8$.

Exercise 14.6.4. Prove that the number of $n \pmod p$ for which $\left(\frac{n+1}{p}\right) = \cdots = \left(\frac{n+k}{p}\right) = 1$ with $k \leq \log p$, equals $p/2^k$ plus or minus an error of at most $k\sqrt{p}$.

Exercise 14.6.5. Let $\delta_1, \dots, \delta_k$ be an arbitrary sequence of 1's and -1's, with $k \leq \log p$. Prove that the number of $n \pmod p$ for which $\left(\frac{n+j}{p}\right) = \delta_j$ for $j = 1, 2, \dots, k$, equals $p/2^k$ plus or minus an error of at most $k\sqrt{p}$.

Appendix 14A. Gauss sums

14.7. Identities for Gauss sums

14.8. Dirichlet L-functions at $s = 1$

Exercise 14.8.1. (a) Prove that $\arg(1 - e^{i\theta}) \in (-\frac{\pi}{2}, \frac{\pi}{2})$.
(b) Deduce that if $0 < \theta < 2\pi$, then $\log(1 - e^{i\theta}) - \log(1 - e^{-i\theta}) = i(\theta - \pi) \in (-\pi, \pi)$.

14.9. Jacobi sums

14.10. The diagonal cubic, revisited

Exercise 14.10.1. Prove that if $p \nmid a$, then

$$\#\{x \pmod p : ax^3 \equiv u \pmod p\} = 1 + \chi(a^{-1}u) + \chi^2(a^{-1}u).$$