

## Return by Monday 5th November

1. Let  $N(q)$  denote the number of pairs  $x, y$  of residue classes (mod  $q$ ) such that  $y^2 \equiv x^3 + 7 \pmod{q}$ .
- (a) Show that  $N(q)$  is a multiplicative function of  $q$ , that  $N(2) = 2$ ,  $N(3) = 3$ ,  $N(7) = 7$ , and that  $N(p) = p$  when  $p \equiv 2 \pmod{3}$ .
- (b) Suppose that  $p \equiv 1 \pmod{3}$ . Let  $\chi_1(n)$  be a cubic character modulo  $p$ , and let  $\chi_2(n) = \left(\frac{n}{p}\right)$  be the quadratic character modulo  $p$ . Show that

$$\begin{aligned} N(p) &= \frac{1}{p} \sum_{a=1}^p e(7a/p) \left( \sum_{h=1}^p (1 + \chi_1(h) + \chi_1^2(h)) e(ah/p) \right) \left( \sum_{k=1}^p (1 + \chi_2(k)) e(-ak/p) \right) \\ &= p + \frac{2}{p} \Re(\tau(\chi_1)\tau(\chi_2)\tau(\chi_1^2\chi_2)\chi_1\chi_2(-7)), \end{aligned}$$

and deduce that  $|N(p) - p| \leq 2\sqrt{p}$ .

- (c) Deduce that  $N(p) > 0$  for all  $p$ .
- (d) Show that  $N(2^k) = 2^{k-1}$  for  $k \geq 2$ , that  $N(3^k) = 2 \cdot 3^{k-1}$  for  $k \geq 2$ , that  $N(7^k) = 6 \cdot 7^{k-1}$  for  $k \geq 2$ , and that  $N(p^k) = N(p)p^{k-1}$  for all other primes.
- (e) Conclude that the congruence  $y^2 \equiv x^3 + 7 \pmod{q}$  has solutions for every positive integer  $q$ .
- (f) Suppose that  $x$  and  $y$  are integers such that  $y^2 = x^3 + 7$ . Show that  $2 \mid y$ ,  $x \equiv 1 \pmod{4}$ , and that  $x > 0$ . Note that  $y^2 + 1 = (x+2)(x^2 - 2x + 4)$ , so that  $y^2 + 1$  is composed of primes  $\equiv 1 \pmod{4}$ , and yet  $x+2 \equiv 3 \pmod{4}$ . Deduce that this equation has no solution in integers.

2. (a) Show that if  $p > 2$  and  $p \nmid b$  then

$$\sum_{n=1}^p \left(\frac{n}{p}\right) \left(\frac{n+b}{p}\right) = -1.$$

- (b) Suppose that  $p > 2$  and that  $p \nmid d$ . Explain why

$$\sum_{x=1}^p \left(\frac{x^2 - d}{p}\right) = \sum_{n=1}^p \left(1 + \left(\frac{n}{p}\right)\right) \left(\frac{n-d}{p}\right),$$

and deduce that this sum is  $-1$ .

- (c) Put  $d = b^2 - 4ac$ , and suppose that  $p > 2$ ,  $p \nmid d$ . Show that

$$\sum_{x=1}^p \left(\frac{ax^2 + bx + c}{p}\right) = \left(\frac{a}{p}\right).$$

3. Let  $p$  be a prime,  $p \equiv 1 \pmod{4}$ , and let  $\mathcal{N}$  be a set of  $Z$  residue classes modulo  $p$ .

- (a) Explain why

$$\sum_{m \in \mathcal{N}} \sum_{n \in \mathcal{N}} \left(\frac{m-n}{p}\right) = \frac{1}{\sqrt{p}} \sum_{a=1}^p \left(\frac{a}{p}\right) \left| \sum_{n \in \mathcal{N}} e(an/p) \right|^2.$$

- (b) Suppose that  $\left(\frac{m-n}{p}\right) = 1$  whenever  $m \in \mathcal{N}$ ,  $n \in \mathcal{N}$ , and  $m \neq n$ . Show that  $Z \leq \sqrt{p}$ .