MATH 571, SPRING 2025, PROBLEMS 12

Due 21st April

As usual, given a character χ modulo q, $\tau(\chi) = \sum_{x=1}^{q} \chi(x)e(x/q)$.

1. (i) Show that

$$\frac{1}{\varphi(q)} \sum_{\chi} \overline{\chi}(a)\tau(\chi) = \begin{cases} e(a/q) & (a,q) = 1, \\ 0 & \text{otherwise.} \end{cases}$$

(ii) Show that for all integers a,

$$e(a/q) = \sum_{\substack{d|q \\ d|a}} \frac{1}{\varphi(q/d)} \sum_{\chi \pmod{q/d}} \overline{\chi}(a/d)\tau(\chi).$$

2. 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

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

and deduce that $|N(p) - p| \le 2\sqrt{p}$. This is the Riemann hypothesis for the elliptic curve $y^2 = x^3 + 7$.

(c) Deduce that $N(p) > 0$ for all p.

(d) Show that $N(2^k) = 2^{k-1}$ for $k \ge 2$, that $N(3^k) = 2 \cdot 3^{k-1}$ for $k \ge 2$, that $N(7^k) = 6 \cdot 7^{k-1}$ for $k \ge 2$, 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. In fact it has no rational solutions either and the local to global principle is false for this curve.