Homework 2

Fermat's last theorem seminar

Due Monday, November 18 at 1 PM

Choose *one* of the following exercises and solve it. Write up your solution carefully; it should be not only mathematically correct but also clear and easy to read and follow.

Problem 1. Exercise 3.27 from the textbook (the Hasse principal for conics): let a, b, and c be three nonzero integers, and consider the projective conic curve defined by the equation $L_{a,b,c}$

$$ax^2 + by^2 + cz^2 = 0.$$

The goal of this problem is to find a necessary and sufficient condition for this equation to admit a rational solution (in the projective plane, i.e. other than the trivial solution $x = y = z = 0$). We can assume that a, b, and c are squarefree and pairwise relatively prime.

(a) Show that if $L_{a,b,c}$ admits a rational point, then it admits a point in $\mathbb{R}$ and in $\mathbb{Q}_p$ for each prime p (this is fairly straightforward, don't overcomplicate).

We want to show the converse. Parts of this are annoyingly technical, but these can be summed up by the following fact, due to Legendre: the curve $L_{a,b,c}$ has a nontrivial rational solution if and only if $-ab$ is a square modulo c, $-bc$ is a square modulo a, and $-ca$ is a square modulo b. Thus we henceforth *assume* that $L_{a,b,c}$ admits a real solution and a p-adic solution for every p, and we aim to prove these modular conditions given this assumption.

(b) Show that if $p|c$ and (u, v, w) is a solution of $L_{a,b,c}$ in $\mathbb{Q}_p$, then we can find a solution (u', v', w') such that $\max(|u'|_p, |v'|_p, |w'|_p) = 1$, so we can assume that $\max(|u|_p, |v|_p, |w|_p) = 1$. Show that in fact in this case we must have $|u|_p = |v|_p = 1$.

(c) Deduce that $-ab$ is a square modulo p.

(d) Using the previous part, deduce that $-ab$ is a square modulo c. Argue briefly that the other two similar facts are proved in a similar manner, given our assumption.

Problem 2. The Fermat equation $x^3 + y^3 = z^3$ for $n = 3$ is a projective cubic curve over $\mathbb{Q}$.

(a) Show that it is smooth and has at least one rational point, and therefore defines an elliptic curve.

(b) Write the above curve in Weierstrass form, i.e. use a coordinate transformation to put it in the (dehomogenized) form $Y^2 = X^3 + aX + b$ for some rational numbers a, b.

(c) Using this form, look up the resulting curve in LMFDB; it should have rank 0, i.e. its Mordell–Weil group should be finite. This group however is *not* trivial, i.e. there do exist solutions to the resulting equation over the rational numbers. Which solutions to the original equation do these correspond to? Does this violate Fermat's last theorem for $n = 3$?

Problem 3. Suppose that E is a modular elliptic curve over $\mathbb{Q}$, associated to the weight 2 Hecke eigenform

$$f = \sum_{n \geq 1} a_n q^n.$$

(a) Using the Hasse bound on the number of $\mathbb{F}_p$-points of an elliptic curve, show that $|a_p| \leq 2\sqrt{p}$ for every prime p.

(b) Use the relation on Hecke operators

$$T_{p^n} = T_{p^{n-1}} T_p - p T_{p^{n-2}}$$

for prime p together with part (a) to show that for each $n \geq 1$

$$|a_{p^n}| \leq c_n p^{n/2}$$

where c_n satisfy $c_0 = 1$, $c_1 = 2$, and $c_n = 2c_{n-1} + c_{n-2}$, corresponding to the sequence $1, 2, 5, 12, 29, 70, \ldots$.

(c) If n has prime factorization $n = \prod_p p^{e_p}$, set $C_n = \prod_p c_{e_p}$, so for example for $n = 60 = 2^2 \cdot 3 \cdot 5$ we have $C_{60} = c_2 \cdot c_1 \cdot c_1 = 5 \cdot 2 \cdot 2 = 20$, or if n is squarefree, so each c_p is either 0 or 1, then $C_n = 2^r$ where r is the number of prime factors of n. Show that

$$|a_n| \leq C_n \sqrt{n}$$

for all n.

(d) Optional: show that C_n has at most polynomial growth for 100% of integers n, and show that nevertheless for certain values of n the size of C_n grows exponentially. (In other words, show that it is possible to find a subset S of the positive integers of density 0 such that on $\mathbb{N} \setminus S$, the function $n \mapsto C_n$ has at most polynomial growth.) Argue, using the convergence of modular forms, that nevertheless all actually occurring a_n have subexponential growth (on all positive integers n).

Problem 4. Choose an elliptic curve E with integer coefficients (make sure it really is an elliptic curve, i.e. smooth and with a rational point). Compute the first view values of $a_p = p + 1 - \#E(\mathbb{F}_p)$. Use this, together with the multiplicativity of coefficients of Hecke eigenforms, the formula for Hecke operators at prime powers in problem 3, and the fact that (normalized) cusp forms have zeroth coefficient 0 and first coefficient 1 to write out the first few terms of the q-series for the corresponding modular form. Look up the result in LMFDB (if there's more than one possibility in weight 2 with trivial character, compute more terms!), and find out what its level is; use this to determine the conductor of the original elliptic curve.