TAKE HOME EXAM 1

TOPICS IN ALGEBRAIC GEOMETRY: ELLIPTIC CURVES

(1) Every year, the Sunday Telegraph in London has a New Year's Quiz. In 1995, two of the questions were the following:
 (a) Solve the equation $A^3/B^3 + C^3/D^3 = 6$, where A, B, C, D are all positive whole numbers below 100.
 (b) A special question with a £450 prize. Either give a second solution to the above equation where the four variables are all whole numbers above 100 (A, B and C, D relatively prime), or demonstrate that no such second solution can exist.

 It's too late to earn the £450 (sorry!), but using pari you can solve the problem.

(2) Consider the cubic $y^2 = x^3$ over some field K of characteristic $\neq 2, 3$. Show that $O = [0 : 0 : 1]$ is the only singularity, and define an addition on $E_{\rm ns}(K) = E(K) \setminus \{O\}$ by declaring that $P + Q + R = \mathcal{O} = [0 : 1 : 0]$ if and only if P, Q, R are collinear.
 (a) Parametrize $E_{\rm ns}(K)$ using lines with slope t through O; show that the points corresponding to the parameters t_1, t_2, t_3 are collinear if and only if $\frac{1}{t_1} + \frac{1}{t_2} + \frac{1}{t_3} = 0$.
 (b) Show that $E_{\rm ns}(K) \simeq (K, +)$, the additive group of K.
 (c) Consider the parabola $C : y^2 = x$ with neutral element O; every line through O with slope t intersects E in some point P and C in some point Q; describe the map sending P to Q in coordinates and show that it induces a group homomorphism $E_{\rm ns}(K) \longrightarrow C(K)$.

(3) Let $E : y^2 = x^3 + ax + b$ be an elliptic curve defined over a finite field $\mathbb{F}_p$. Let d be an integer not divisible by p and consider the quadratic twist $E_d : dy^2 = x^3 + ax + b$.

 Show that if $\#E(\mathbb{F}_p) = p + 1 - a_p$, then

$$\#E_d(\mathbb{F}_p) = \begin{cases} p + 1 - a_p & \text{if } (d/p) = +1, \\ p + 1 + a_p & \text{if } (d/p) = -1. \end{cases}$$

 Also show that $E(\mathbb{F}_p) \simeq E_d(\mathbb{F}_p)$ if $(d/p) = +1$. (Hint: all you need is elementary number theory.)

(4) Consider the family of all elliptic curves $E : y^2 = x^3 + ax + b$ over $\mathbb{F}_p$ $(p > 2)$ with discriminant $\Delta(E) = -4a^3 - 27b^3 = 1$. Its number of points can be written as $N_p = p + 1 - a_p(E)$, where $|a_p(E)| < 2\sqrt{p}$. Now form the sum over all $a_p(E)$ with $\Delta(E) = 1$.

For a fixed prime p, the following pari program computes this sum:

```
{p=5:s=0:for(a=0,p-1,for(b=0,p-1,d=Mod(-4*a^3-27*b^2,p):
 d=lift(d):if(d-1,,e=ellinit([0,0,0,a,b]):s=s+ellap(e,p):
 print(a,"  ",b,"  ",Mod(d,p),"  ",s)))))}
```

The sum of all the a_p is the last number in the output. Look at the output for several small primes $p \equiv 3 \bmod 4$, make a conjecture and prove it. For getting more data on the sums when they are nonzero, modify the program slightly:

```
{forstep(p=5,100,4,if(isprime(p),
 s=0:for(a=0,p-1,for(b=0,p-1,d=Mod(-4*a^3-27*b^2,p):
 d=lift(d):if(d-1,,e=ellinit([0,0,0,a,b]):s=s+ellap(e,p)))):
 print(p,"  ",s),))}
```

Recall that primes $p \equiv 1 \bmod 4$ can be written as a sum of two squares; the same holds for p^2, by the way.

What happens if you replace the elliptic curves with discriminant 1 by curves with discriminant 2 (or 3)?

Note: for primes $p \equiv 1 \bmod 4$, these conjectures (apparently due to N. Katz) have not yet been proved.

(5) What does the Hasse bound tell you about the number of points on elliptic curves $E_{a,b} : y^2 = x^3 + ax + b$ over $\mathbb{F}_5$?

(a) Use pari to do a complete search over all elliptic curves and list the orders of $E(\mathbb{F}_p)$ that occur.

(b) Use the fact that -1 is a square mod 5 to explain why the elliptic curves $E_{a,b}$ and $E_{a,-b}$ have the same number of points (and, as a matter of fact, the same group structure).

(c) For squarefree orders, the group structure of $E(\mathbb{F}_p)$ is uniquely determined. I mentioned that we know $E(\mathbb{F}_p) = \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z}$ with $n_2 \mid n_1$ and $n_2 \mid (p-1)$. Use this result to determine the group structure for the curves with $\#E(\mathbb{F}_5) = 9$.

(d) Use explicit calculations to determine the group structure for the curves with $\#E(\mathbb{F}_5) = 8$.