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.*

The first thing you have to do is find a rational point on the cubic $x^3 + y^3 = 6$. Clearing denominators, we see that we have to find integers $x^3 + y^3 = 6z^3$. Finding small positive solutions is easy; ordering them with respect to z suggests the following pari program:

```
{for(z=1,50,for(x=0,6^(1/3)*z,y=round((6*z^3-x^3)^(1/3)):
 if(x^3+y^3-6*z^3,,print(x,"   ",y,"   ",z))))}
```

Note that $y \approx \sqrt[3]{6z^3 - x^3}$, so you don't have to search through all possible values. The program finds $P = (x, y, z) = (17, 37, 21)$ within fractions of a second.

The next step is to use the chord and tangent method to find other points with positive coordinates; if you only use tangents (instead of tangents and chords), the smallest solution you will find is rather large.

Here's a slightly different approach. The cubic $X^3 + Y^3 - 6Z^3 = 0$ has a point $[-1 : 1 : 0]$ at infinity with tangent $X + Y = 0$. This tangent intersects the curve with multiplicity 3, hence is a flex. Thus we can transform the cubic into Weierstrass form by moving $[-1 : 1 : 0]$ to $[0 : 1 : 0]$ and the line $X + Y = 0$ to $Z = 0$ with the projective transformation $X = z - y$, $Y = y$, $Z = x$; dehomogenizing after the transformation gives $3y^2 - 3y = 6x^3 - 1$. Multiply through by $2^2 \cdot 3^5$ and put $v = 27(2y - 1)$ and $u = 18x$; this gives $v^2 = u^3 - 243$. The overall transformation is $u = 18\frac{Z}{X+Y}$, $v = 27(\frac{2Y}{X+Y} - 1)$, hence moves $[17 : 37 : 21]$ to the point $(u, v) = (7, 10)$.

Now we can use pari for adding points: initialize with

```
e = ellinit([0,0,0,0,-243]):P=[7,10]
```

and then multiply:

```
for(n=1,6,print(n,"   ",ellpow(e,P,n)))
```

Since we can write the points in the form $x = n/e^2$, $y = m/e^3$, it is sufficient to give n, m, e:

n	n	m	e
1	7	10	1
2	16009	-2021723	40
3	2838722167	146917312265870	13209
4	67675356206662561	$-155558129143226117492354 41$	80868920

Here are the coordinates of $5P$:

$$n = 333109779867069842893772887$$
$$m = 607927020969104408064577263124060104445 0$$
$$e = 1657724328329$$

and of $6P$:

$$n = 942484510461619169237406737948912444 89$$
$$m = -805497926568577145405911895679691637832293070392819207 63$$
$$e = 3881261555439753660$$

Transforming back to $[X : Y : Z]$ via $\frac{Y}{Z} = \frac{9}{u}(\frac{v}{27} + 1)$ gives

$$P = [17 : 37 : 21]$$
$$2P = [3749723 : -293723 : 1921080]$$
$$3P = [-84691068680987 : 209143555850753 : 112490043311709]$$

and finally we find that $6P$ has positive coordinates, leading to

$$A = 165918758567183281704526025160016369620426670803613511276 3$$
$$B = 109740866911564163927429722772921473450029250338297773922 0$$
$$C = 149808800035811738796407787246422536863780809395757127123 7$$
$$D = 109740866911564163927429722772921473450029250338297773922 0$$

(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 $E_{\mathrm{ns}}(K) = E(K) \setminus \{O\}$ by declaring that $P + Q + R = \mathcal{O} = [0 : 1 : 0]$ if and only if P, Q, R are collinear.*

It is easily checked that $(0, 0)$ is singular; since the cubic is irreducible, it must be the only singular point. The technique of sweeping lines gives us the parametrization $(x, y) = (t^2, t^3)$.

(a) *Parametrize $E_{\mathrm{ns}}(K)$ 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 $\frac{1}{t_1} + \frac{1}{t_2} + \frac{1}{t_3} = 0$.*

The three points with parameters r, s, t (assumed to be pairwise distinct for simplicity) are collinear if and only if $\frac{s^3 - r^3}{s^2 - r^2} = \frac{t^3 - r^3}{t^2 - r^2}$, which after some calculation and division by $rst \neq 0$ yields $\frac{1}{r} + \frac{1}{s} + \frac{1}{t} = 0$.

(b) *Show that* $E_{\mathrm{ns}}(K) \simeq (K,+)$*, the additive group of* K*.*

The map $K \longrightarrow E_{\mathrm{ns}}(K) : t \longmapsto (t^{-2}, t^{-3})$ and $0 \longmapsto \mathcal{O}$ is easily checked to respect the group law. Since it is bijective, it must be an isomorphism.

(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* $E_{\mathrm{ns}}(K) \longrightarrow C(K)$*.*

We find $Q = Q_t = (t^{-2}, t^{-1})$ and $P = P_t = (t^2, t^3)$, hence the map $(x,y) \longmapsto (\frac{1}{x^2}, \frac{y}{x})$ gives the bijection $\phi : E \longrightarrow C$ (with $\mathcal{O}$ going to the origin). The inverse map ψ sends $(x,y) \in C$ to $(\frac{1}{y^2}, \frac{1}{y^3})$.
The addition law on C is given by the addition of the y-coordinates. Thus the map $Q_t \longmapsto t^{-1}$ is an isomorphism $C \longrightarrow K$. Now ψ is the composition of the isomorphism $C \longrightarrow K : (x,y) \longmapsto y$ and the isomorphism $K \longrightarrow E : y \longmapsto (\frac{1}{y^2}, \frac{1}{y^3})$. Thus ψ is an isomorphism, and so is ϕ.

(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* $(d/p) = +1$*.*

If $d \equiv r^2 \bmod p$ is a square, then $u = ry$, $v = x$ is an admissible transformation (i.e., an isomorphism in the category of elliptic curves) mapping the elliptic curve E_d to E.

Assume therefore that d is a nonsquare modulo p. For each $x \in \mathbb{F}_p$, there are $1 + \chi(x)$ affine points of the form (x,y) on $E : y^2 = f(x)$, where $\chi(x) = (\frac{f(x)}{p})$. Thus the number of all points in $E(\mathbb{F}_p)$ is $p+1+\sum_{x=0}^{p-1} \chi(x)$. Similarly, on the curve $(dy)^2 = df(x)$ is $p+1+(d/p)\sum_{x=0}^{p-1} \chi(x)$. This proves the claims.

(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* $\Delta(E) = 1$*.*

Look at the output for several small primes $p \equiv 3 \bmod 4$*, make a conjecture and prove it.*

The conjecture is that the sum vanishes for all $p \equiv 3 \bmod 4$. More exactly, it seems that $a_p(E_{a,b}) = -a_p(E_{a,-b})$. This would clearly imply the conjecture, since $a_p(E_{a,0}) = 0$ for primes $p \equiv 3 \bmod 4$ (the proof in the lectures for $a = 1$ works in general).

Now the quadratic twist of $E_{a,b}$ by -1 is $-y^2 = x^3 + ax + b$, and replacing x by $-x$ shows that this is $E_{a,-b}$. Since -1 is a nonsquare modulo $p \equiv$

3 mod 4, the last exercise shows that $a_p(E_{a,b}) = -a_p(E_{a,-b})$, and we are done.

For explaining the nonzero results, 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.

The following table gives the sums $S_p = \sum a_p(E_{a,b})$ for curves with $\Delta = 1$ for primes $p \equiv 1 \bmod 4$, as well as the integers a, b (a odd) for which $p^2 = a^2 + b^2$:

p	5	13	17	29	37
S_p	6	-10	30	-42	70
a	3	-5	15	-21	35
b	4	12	8	20	12

Here we have chosen the sign of a in such a way that $a \equiv 3 \bmod 4$. It seems that we have $S_p = 2a$ with these conventions.

Note: for primes $p \equiv 1 \bmod 4$, these conjectures (apparently due to N. Katz – the Princeton prof who eventually discovered the gap in Wiles' first proof of Fermat's Last Theorem) have not yet been proved.

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

For curves with $\Delta = 2$ we get the following results:

p	5	13	17	29	37
S_p	-8	24	-30	-40	24
a	3	-5	15	-21	35
b	4	12	8	20	12

Up to sign it seems that $S_p = \pm a$ if $(2/p) = +1$, and $S_p = \pm b$ if $(2/b) = -1$. Something similar seems to go on in general.

(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 $\mathbb{F}_5$?*

The number of points satisfies $|\#E(\mathbb{F}_5) - 6| \leq 4$, hence $2 \leq \#E(\mathbb{F}_5) \leq 10$.

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

All the possible values 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).*

Again, $E_{a,-b}$ is the twist by -1 of $E_{a,b}$, hence $E_{a,-b}(\mathbb{F}_p) \simeq E_{a,b}(\mathbb{F}_p)$.

(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 $\#E(\mathbb{F}_5) = 9$.*

If $E(\mathbb{F}_5)$ has nine points, then thw two choices are $E(\mathbb{F}_5) \simeq \mathbb{Z}/3 \oplus \mathbb{Z}/3$ and $E(\mathbb{F}_5) \simeq \mathbb{Z}/9$. The first one does not agree with the theorem, hence the second possibility must hold.

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

Note that the theorem allows the two possibilities $E(\mathbb{F}_5) \simeq \mathbb{Z}/2 \oplus \mathbb{Z}/4$ and $E(\mathbb{F}_5) \simeq \mathbb{Z}/8$.
For $E : y^2 = x^3 + 4x = x(x+2)(x-2)$ we find that there are three points of order 2, hence $E(\mathbb{F}_5) \simeq \mathbb{Z}/2 \oplus \mathbb{Z}/4$.
For $E : y^2 = x^3 + 4x + 1$, the point $P = (0, 1)$ satisfies $4P = (-2, 0)$, hence we have $E(\mathbb{F}_5) \simeq \mathbb{Z}/8$.
The last calculation can be done with pari:

```
e = ellinit([0,0,0,Mod(4,5),Mod(1,5)]);
ellpow(e,[0,1],4)
```

gives the result `[Mod(3,5),Mod(0,5)]`, i.e., $4P = (-2, 0)$.