KMB, 18/11/10

Number Theory: Elliptic Curves, Problem Sheet 3

The questions on this sheet are not logically essential for your understanding of the course, and some do not even test your ability to apply theorems from the course—they are just there to give you some background to some of the statements I have made recently in the course. I will perhaps make use of Q3 and Q7 in the course, but this doesn't mean you have to do the questions, it just means that you have to have read the statements. Q1 is quite good, it won't teach you too much about cubics, but it will make you good at applying Hensel's lemma, which is important.

1) Here is a sketch of a proof there are solutions to $3x^3 + 4y^3 = 5$ in $\mathbf{Q}_p$ for any prime p. I claimed this without proof in the course. If you do this question then it will teach you a bit about the "power of Hensel's lemma". Note that there are obviously real solutions to $3x^3 + 4y^3 = 5$ and hence this question shows that there are solutions to $3x^3 + 4y^3 = 5$ in any completion of $\mathbf{Q}$.

a) Prove that there exists $y \in \mathbf{Q}_3$ such that $4y^3 = 5$. Deduce that there is a solution to $3x^3 + 4y^3 = 5$ in $\mathbf{Q}_3$.

b) Prove that there is $x \in \mathbf{Q}_5$ such that $3x^3 = 1$. Deduce that there is a solution to $3x^3+4y^3 = 5$ in $\mathbf{Q}_5$.

Clearly strategies like the above may well deal with any fixed p that you can think of. But how to deal with all p at once? There are "pure thought" methods, coming from deeper results about the existence of mod p solutions to cubic equations, but here is an elementary approach that works for the cubic in question. Let p be any prime that is not 3 or 5.

c) Prove that either 3, 5, 15 or 45 is a cube mod p. Hint: consider $(\mathbf{Z}/p\mathbf{Z})^\times$ quotiented out by the subgroup of cubes. If this doesn't have order 1 then it has order 3.

d)

(i) If 3 is a cube mod p then check that there is a $\mathbf{Q}_p$-solution to $3x^3 + 4y^3 = 5$ with $y = 1$.

(ii) If 5 is a cube mod p then check that there is a solution with $x = -y$.

(iii) If 45 is a cube mod p then check that there is a solution with $y = 0$.

(iv) If 15 is a cube mod p then check that there is a solution with $y = 5/7$.

Conclude that there is a solution to $3x^3 + 4y^3 = 5$ in $\mathbf{Q}_p$ for any prime p.

In fact this proof is elementary but rather artificial and if you knew the standard but tricky fact that smooth cubic curves over finite fields always had points then the result (and many more like it) follows easily from Hensel's lemma

2) Here as promised is the change of coordinates which takes an irreducible cubic with a given smooth point $\mathcal{O}$ into the form

$$y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x + a_6) = 0.$$

We work over a field k. The exercise is to check the details. Firstly draw the tangent line to the cubic at $\mathcal{O}$. The tangent line will meet the cubic at three points, at least two of which will be $\mathcal{O}$.

CASE 1: the third point of intersection is also $\mathcal{O}$. In this case a linear change in coordinates (i.e., $X_1 = aX+bY+cZ$, $Y_1 = eX+fY+gZ$, $Z_1 = hX+iY+jZ$) will suffice: change variables of the homogeneous equation by a linear transformation so that $\mathcal{O}$ goes to $[0 : 1 : 0]$ and the tangent line goes to the line $Z_1 = 0$ in projective 2-space, that is, the line at infinity. Check that this does it.

CASE 2: the third point of intersection is P, a point not equal to $\mathcal{O}$. Make a linear change of variables so that P is at $(0, 0)$ and that the tangent to $\mathcal{O}$ is the y-axis in the x, y-plane. Let's work with the inhomogeneous cubic $f(x, y) = 0$. The fact that $(0, 0)$ is on the cubic implies that the constant term of f is zero, so we can write

$$f(x, y) = f_1(x, y) + f_2(x, y) + f_3(x, y)$$

where f_i is homogeneous of degree i.

We know that the intersection of $f = 0$ with the line $x = 0$ (that is, the y-axis) is $(0, 0)$ with multiplicity 1 and some other root (namely $\mathcal{O}$) with multiplicity 2. Hence, setting $x = 0$, we deduce that the quadratic $f_1(0, 1) + yf_2(0, 1) + y^2 f_3(0, 1)$ has a double root and hence $f_2(0, 1)^2 = 4f_1(0, 1)f_3(0, 1)$.

Now draw lines through the origin. The line $y = tx$ (think of t as a constant) meets the curve at three points whose x-coordinates are the three roots of $xf_1(1, t) + x^2 f_2(1, t) + x^3 f_3(1, t)$ so this line hits a k-point other than $(0, 0)$ if and only if the quadratic $x^2 f_3(1, t) + xf_2(1, t) + f_1(1, t)$ has roots in k, which happens iff $f_2(1, t)^2 - 4f_1(1, t)f_3(1, t)$ is a square in k. Hence if we write

$$s^2 = f_2(1, t)^2 - 4f_1(1, t)f_3(1, t)$$

then the formula for the roots of a quadratic equation give us, for every solution to this equation, a root of $x^2 f_3(1, t) + xf_2(1, t) + f_1(1, t)$, namely $x = (-f_2(1, t) + s)/2f_3(1, t)$.

The punchline however is that $G(t) := f_2(1, t)^2 - 4f_1(1, t)f_3(1, t)$, which looks like an equation of degree 4 in t, is actually of degree 3 because $f_2(0, 1)^2 = 4f_1(0, 1)f_3(0, 1)$. Hence the cubic has now become an equation of the form $s^2 = G(t)$ with G a cubic, which is what we were after.

3) An example of the easy case of the algorithm presented in Q2. Let d be a non-zero constant, and let's consider the cubic $F(X, Y, Z) = X^3 + Y^3 + dZ^3$, over a field of characteristic not equal to 2 or 3.

(i) Prove that $F = 0$ has no singular points.

(ii) Prove that the point $[1 : -1 : 0]$ is a point of inflexion.

(iii) Write down a linear change of coordinates (i.e., $X_1 = aX + bY + cZ$, $Y_1 = eX + fY + gZ$, $Z_1 = hX + iY + jZ$) that takes this point to $[0 : 1 : 0]$ and which takes the tangent line at this point to the line $Z_1 = 0$.

If you did it right, and then tidy up and complete the square and cube if necessary, you should be left with an equation of the form $Y_1^2 Z_1 = X_1^3 - 432d^2 Z_1^3$, whose corresponding dehomogenisation is $y^2 = x^3 - 432d^2$. These are exactly the kinds of curves we will deal with later.

4) Here is the beginning of a proof that $3x^3 + 4y^3 = 5$ has no rational solutions, but it assumes a little Galois theory, or some common sense. Say there were a solution. Then by clearing denominators we get integers u, v, w, not all zero (and hence all non-zero), such that $3u^3 + 4v^3 + 5w^3 = 0$ (change the sign of w if necessary). Now set $\rho = e^{2\pi i/3}$, a non-trivial cube root of 1, and work in the field $\mathbf{Q}(\rho) = \mathbf{Q}(\sqrt{-3})$. Set $\alpha = 3u^3 + 4\rho v^3 + 5\rho^2 w^3$ and let β be the complex conjugate of α (note that the conjugate of ρ is ρ^2). Check that $\alpha + \beta = 9u^3$ (recall $\rho + \rho^2 = -1$), that $\rho\alpha + \rho^2\beta = 15w^3$ and that $\rho^2\alpha + \rho\beta = 12v^3$. Deduce that $\alpha^3 + \beta^3 = 60\gamma^3$, where $\gamma = 3uvw$.

Now $P := (\alpha/\gamma, \rho\beta/\gamma)$ is a point on $x^3 + y^3 = 60$ defined over $\mathbf{Q}(\sqrt{-3})$, and so is its complex conjugate $\overline{P}$. Draw the line through P and $\overline{P}$; this meets the cubic $x^3 + y^3 = 60$ at P and $\overline{P}$ and a third point Q; applying complex conjugation to everything we deduce that $Q = \overline{Q}$ and hence that Q has rational coordinates. Furthermore, the point Q is not the point at infinity, as the general line through infinity is of the form $x + y = c$ with c constant, and $\alpha + \rho\beta$ cannot be rational.

We conclude that *if* there is a rational solution to $3x^3 + 4y^3 = 5$ then there is a rational solution to $x^3 + y^3 = 60$. By Q3, we deduce that there is a rational solution to $s^2 = t^3 - 60.432$. Later on in the course we'll see how to prove that the only solution to this equation over the rationals is the point at infinity, and finally our proof of the statement "$3x^3 + 4y^3 = 5$ has p-adic points for all p, and real points, but no rational points" will be complete.

5) It turns out that there are other equations that can be put into the form $y^2 = f(x)$ with f a cubic. For example, perhaps surprisingly, the equation $y^2 = g(x)$ with $g(x)$ of degree 4, can be put into this form, as long as a smooth point is known. Read the proof on p35 of Cassels' book.

6) Similarly, the intersection of two quadric surfaces, that is, the simultaneous solutions to two homogeneous equations of degree 2 in 4 variables, can be put into this form, if a smooth point is known. Read the proof on p36 of Cassels' book.

7) Check that $\mathrm{disc}(x^3 + ax + b) = 4a^3 + 27b^2$. One can do this for example by calling the roots α, β and γ and then noting $\alpha + \beta + \gamma = 0$ etc, and then explicitly checking that $(\alpha - \beta)^2(\beta - \gamma)^2(\gamma - \alpha)^2$ agrees with $4a^3 + 27b^2$ up to a minus sign (I think that the general rule is that discriminants are only defined up to sign).