Course 428

Elliptic Curves III

Dr Timothy Murphy

EELT1 Thursday, 2 May 2002 16:15–17:15

Attempt 3 questions. (If you attempt more, only the best 3 will be counted.) All questions carry the same number of marks.

1. State (without proof) Hasse's Theorem on the number of points on an elliptic curve over a finite field.

   Show that the curve
   $$\mathscr{E}(\mathbb{F}_8) : y^2 + y = x^3$$
   is elliptic, and find the number of points on it.

   Answer:

   (a) Hasse's Theorem states that the number N of points on an elliptic curve $\mathscr{E}(\mathbb{F}_q)$ over the finite filed $\mathbb{F}_q$ satisfies
   $$|N - (q + 1)| \leq 2\sqrt{q}.$$

   (b) In homogeneous coordinates the equation takes the form
   $$F(X, Y, Z) = Y^2Z + YZ^2 + X^3 = 0$$
   (using the fact that the field is of characteristic 2). Thus
   $$\frac{\partial F}{\partial X} = X^2,$$
   $$\frac{\partial F}{\partial Y} = Z^2,$$
   $$\frac{\partial F}{\partial Z} = Y^2.$$
   Thus at a singular point $X = Y = Z = 0$, which is impossible.

(c) *The polynomial*
$$p(x) = x^3 + x + 1$$
is irreducible over $\mathbb{F}_2$*, since* $p(0) \neq 0,\ p(1) \neq 0$*. Thus*
$$F_8 = F_2[x]/(p(x)).$$
Let $\alpha = x \bmod p(x)$*. Then the elements of* F_8 *are*
$$c_0 + c_1\alpha + c_2\alpha^2,$$
where $c_0, c_1, c_2 \in \{0, 1\}$*; and*
$$\alpha^3 = \alpha + 1.$$
Since $|F_8^\times| = 7$ *there are no elements of order 3 in* $\mathbb{F}_8^\times$*. Thus the homomorphism*
$$x \mapsto x^3 : \mathbb{F}_8^\times \to \mathbb{F}_8^\times$$
has trivial kernel, and so is an isomorphism. In other words, each element of $\mathbb{F}_8^\times$ *has a unique cube-root; and this is evidently true of the element 0 too.*

It follows that for each choice of y *we can find just one* x *with* $x^3 = y^2 + y$*. Thus there are 8 points on the affine curve; and so, on adding the point* $O = [0, 1, 0]$,
$$|\mathscr{E}(\mathbb{F}_8)| = 9.$$

2. Show that there are no rational numbers x, y such that
$$y^2 = x^4 + 2.$$

Answer: *To bring this hyper-elliptic equation to elliptic form we re-write it as*
$$(y - x^2)(y + x^2) = 2.$$
Now set
$$s = y + x^2.$$
Then
$$y - x^2 = \frac{2}{s}.$$
Thus
$$2x^2 = s - \frac{2}{s}.$$
Multiplying across by s^2,
$$2s^2x^2 = s^3 - 2s.$$

Setting $sx = t$,
$$2t^2 = s^3 - 2s.$$

Explicitly,
$$(s,t) = (y + x^2, xy + x^3),$$
while the inverse map is
$$(x,y) = (t/2, s - t^2/4).$$

Now set $x = s/2,\ y = t/4$. *We obtain the elliptic curve*
$$\mathscr{E}(\mathbb{Q}) : y^2 = x^3 - 8x.$$

The associated elliptic curve is
$$\mathscr{E}_1(\mathbb{Q}) : y^2 = x^3 + 32x.$$

Since $\mathscr{E}$ *has just one point of order 2, while* $b_1 = 32$ *is not a perfect square, the rank* r *of* $\mathscr{E}$ *is given by*
$$2^{r+1} = \frac{|\operatorname{im}\chi| \cdot |\operatorname{im}\chi_1|}{2},$$
where
$$\chi : \mathscr{E} \to \mathbb{Q}^\times \to \mathbb{Q}^{\times 2}, \quad \chi : \mathscr{E}_1 \to \mathbb{Q}^\times \to \mathbb{Q}^{\times 2}$$
are the auxiliary homomorphisms.

We have
$$\operatorname{im}\chi \subset \{\pm 1, \pm 2\}, \quad \operatorname{im}\chi_1 \subset \{\pm 1, \pm 2\}.$$

Since $\chi(0,0) = -8 \sim -2$,
$$\operatorname{im}\chi = \{1, -2\} \text{ or } \{\pm 1, \pm 2\}.$$

Recall that $d \in \operatorname{im}\chi$ *if and only if the equation*
$$du^4 + d't^4 = v^2,$$
where $d' = b/d$, *has an integral solution with* $\gcd(u,t) = 1 = \gcd(v,t)$. *Taking* $d = -1$ *we have* $d = 8$ *and the equation is*
$$-u^4 + 8t^4 = v^2.$$

If v *is odd then so is* u. *But then* $u^4 \equiv 1 \bmod 4$ *and* $v^2 \equiv 1 \bmod 4$, *which is a contradiction.*

Hence v is even, and so u is even. But then

$$\begin{aligned} 2 \mid u &\implies 16 \mid u^4 \\ &\implies 8 \mid v^2 \\ &\implies 4 \mid v \\ &\implies 16 \mid v^2 \\ &\implies 2 \mid t, \end{aligned}$$

contradicting the assumption that $\gcd(t, u) = 1$.

It follows that

$$\operatorname{im} \chi = \{1, -2\}.$$

For $\operatorname{im} \chi_1$ *we note that* $d < 0 \implies d' = 32/d < 0$, *in which case* $u = t = v = 0$, *which is absurd. On the other hand,* $\chi_1(0, 0) = 2$. *Thus*

$$\operatorname{im} \chi_1 = \{1, 2\}.$$

We conclude that $r = 0$, ie the group on the curve is finite.

To find the points of finite order, we recall that if $\chi(x, y) = (x_1, y_1)$ *then*

$$x_1 = \frac{x^2 - 8}{x}.$$

But if $P = (x, y)$ is of finite order then so is (x_1, y_1). Hence

$$x, x_1 \in \mathbb{Z}.$$

Thus $x \in \{\pm 1, \pm 2, \pm 4, \pm 8\}$. But it is a trivial matter to verify that none of these make $x^3 - 8x$ a perfect square. Thus $\mathcal{E}$ contains only the point $(0, 0)$.

But no point (x, y) on the original curve gives rise to this point. (More precisely, the point $(0, 0$ on $\mathcal{E}$ corresponds to a point on the line at infinity on the original curve.) We conclude that the original equation has no rational solution.

3. Show that a non-singular cubic Γ over the field k can be brought to Weierstrassian form if and only if there is a point $P \in \Gamma$ defined over k.

   Bring the curve
   $$X^3 + Y^3 + Z^3 = XYZ$$
   to Weierstrassian form.

   Show that the cubic
   $$X^3 + 2Y^3 + 4Z^3 = 0$$
   is non-singular, but has no rational point.

   Answer:

(a) *Let P be a rational point on Γ.*

If P is a point of inflexion then we can bring P to the point $[0,1,0]$ and the tangent at P to the line $Z = 0$ by a projective transformation.

Since the line $Z = 0$ meets Γ where $X^3 = 0$ it follows that the coefficients of Y^3, XY^2, X^2Y all vanish. Thus Γ takes the form

$$F(X,Y,Z) = AY^2Z + BXYZ + CYZ^2 + DX^3 + EX^2Z + FXZ^2 + GZ^3 = 0.$$

If $D = 0$ then Z is a factor, so the curve is degenerate and therefore singular.

If $A = 0$ then

$$\partial F/\partial X = \partial F/\partial Y = \partial F/\partial Z = 0$$

at $P = [0,1,0]$, so again the curve is singular.

Thus the curve takes the inhomogeneous form

$$y^2 + axy + by = cx^3 + dx^2 + ex + f,$$

with $c \neq 0$. But now the transformation $x' = cx,\ y' = xy$ makes the coefficients of y^2 and x^3 equal, bringing the curve to Weierstrassian form.

Suppose now that P is not a flex. Let the tangent at P meet the curve again at Q, and let the tangent at Q meet the curve again at R. We may suppose that Q is not a flex, so that P, Q, R are non-collinear and can be brought by a projective transformation to the points $[1,0,0], [0,1,0], [0,0,1]$.

Since the curve goes through these three points, the coefficients of X^3, Y^3, Z^3 all vanish. Since the tangent at $[1,0,0]$ is $Z = 0$, the coefficient of X^2Y vanishes; and since the tangent at $[0,1,0]$ is $X = 0$, the coefficient of Y^2Z vanishes. Thus the curve takes the form

$$aXY^2 + bXYZ + cYZ^2 = dX^2Z + eXZ^2,$$

or in inhomogeneous form,

$$axy^2 + bxy + cy = dx^2 + ex.$$

Multiplying by x, and setting $xy = y'$,

$$ay'^2 + bxy' + cy' = dx^3 + ex^2.$$

The transformation $(x, y') = (x, xy)$ is birational, with inverse $(x, y) = (x, y'/x)$.

As above, the curve is singular if $a = 0$ or $d = 0$; and the transformation $y'' = \lambda y',\ x'' = \lambda x$ with $\lambda = a/d$ brings the curve to Weierstrassian form.

(b) *If*

$$F(X,Y,Z) = X^3 + Y^3 + Z^3 + XYZ$$

then

$$\begin{aligned}\frac{\partial F}{\partial X} &= 3X^2 + YZ,\\ \frac{\partial F}{\partial Y} &= 3Y^2 + XZ,\\ \frac{\partial F}{\partial Z} &= 3Z^2 + XY.\end{aligned}$$

At a singular point,

$$\begin{aligned}3X^2 = -YZ,\ 3Y^2 = -XZ,\ 3Z^2 = -XY &\implies 27X^2Y^2Z^2 = -X^2Y^2Z^2\\ &\implies XYZ = 0\\ &\implies X = Y = Z = 0.\end{aligned}$$

Thus the curve is non-singular.
Let $P = [1, -1, 0]$. *The tangent at* P *is*

$$3X + 3Y - Z = 0.$$

This meets the curve again where

$$(X^3 + Y^3) + 27(X+Y)^3 + 3XY(X+Y) = 0,$$

ie

$$(X+Y)\left[(X^2 - XY + Y^2) + 3XY + 27(X+Y)^2\right]$$

ie

$$28(X+Y)^3.$$

Thus the tangent meets the curve three times at P, *ie* P *is a point of inflexion.*
Hence we can bring the curve to Weierstrassian form by a projective transformation taking the point $[1, -1, 0]$ *to* $[0, 1, 0]$ *and the line* $3X + 3Y - Z = 0$ *to* $Z = 0$. *A suitable transformation is*

$$X' = X + Y,\ Y' = Y,\ Z' = Z - 3(X+Y),$$

or inversely,

$$X = X' - Y',\ Y = Y',\ Z = 3X' + Z'.$$

The equation becomes

$$(X' - Y')^3 + Y'^3 + (3X' + Z')^3 + (X' - Y')Y'(3X' + Z') = 0,$$

ie

$$28X'^3 + 27X'^2Z' + 9X'Z'^2 + Z'^3 + X'Y'Z' - Y'^2Z' = 0,$$

or in affine coordinates

$$y'^2 - x'y' = 28x'^3 + 27x'^2 + 9x' + 1.$$

The transformation

$$x' = x/28, \ y' = y/28$$

brings this to Weierstrassian form

$$y^2 - xy = x^3 + 27x^2 + 9 \cdot 28x + 28^2.$$

(c) *Suppose* X, Y, Z *(not all 0) satisfy*

$$X^3 + 2Y^3 + 4Z^3 = 0$$

We may suppose without loss of generality that $\gcd(X.Y.Z) = 1$. *Evidently* $2 \mid X$, *say* $X = 2X'$. *Then*

$$8X'^3 + 2Y^3 + 4Z^3 = 0,$$

ie

$$4X'^3 + Y^3 + 2Z^3 = 0.$$

Now $2 \mid Y$, *say* $Y = 2Y'$; *and*

$$4X'^3 + 8Y'^3 + 2Z^3 = 0,$$

ie

$$2X'^3 + 4Y'^3 + Z^3 = 0.$$

But now $2 \mid Z$, *contradicting our assumption that* $\gcd(X, Y, Z) = 1$.

4. Outline Pollard's $p - 1$ method for factorizing large numbers, and Lenstra's Elliptic Curve development of this.

   What advantage does Lenstra's method possess?

   Answer:

Pollard's $p-1$ method *Suppose n is a large composite number. (It is easy to establish that n is composite, by the Miller-Rabin algorithm.) Let p be a prime factor of n.*

Recall that a number m is said to be b-smooth, where b is a relatively small number, if every for every prime factor q of m the highest power of q dividing m is $\leq b$:

$$q^e \mid m \implies q^e \leq b.$$

This is the same as saying that

$$m \mid k,$$

where

$$k = k(b) = \prod_{p \leq b} p^{e(p)},$$

where $e(p)$ is the exponent of the highest power of p such that

$$p^{e(p)} \leq b.$$

Now suppose that $p-1$ is b-small. Then

$$p - 1 \mid k.$$

By Fermat's Little Theorem, if a is coprime to p then

$$a^{p-1} \equiv 1 \bmod p.$$

Hence

$$a^k \equiv 1 \bmod p,$$

ie

$$p \mid a^k - 1,$$

and so

$$d = \gcd(a^k - 1, n) > 1.$$

It is improbable that $d = n$; so d gives a proper factor of n.

To summarise, we choose a small number a, compute $a^k \bmod n$ (working throughout $\bmod n$) and then calculate $d = \gcd(a^k - 1, n)$.

Lenstra's elliptic curve method *Suppose as before that n is a large composite integer, and that p is a prime factor of n.*

Let

$$\mathscr{E}(\mathbb{Q}) : y^2 = x^3 + bx + c \quad (b, c \in \mathbb{Z})$$

be an elliptic curve; and let $\mathscr{E}(\mathbb{F}_p)$ be the reduction of $\mathscr{E}$ $\bmod p$.
We may suppose that the reduction is good, ie $\mathscr{E}(\mathbb{F}_p)$ is an elliptic curve. For if it is not then

$$p \mid \Delta = -(4b^3 + 27c^2)$$

and so

$$d = \gcd(\Delta, n) > 1$$

will almost certainly provide a proper factor of n.
Let the order of the group $\mathscr{E}(\mathbb{F}_p)$ be N. By Hasse's Theorem, N is roughly equal to p; more precisely,

$$|N - (p+1)| \leq 2\sqrt{p}.$$

Now suppose N is b-small. Then

$$N \mid k$$

as in Pollard's method.
Let us choose a point

$$P = [X, Y, Z] \quad (X, Y, Z \in \mathbb{Z})$$

on $\mathscr{E}(\mathbb{Q})$; and set

$$rP = [X_r, Y_r, Z_r]$$

for $r \in \mathbb{N}$.
Let P_p denote the reduction of P $\bmod p$. *By Lagrange's Theorem,*

$$NP_p = 0,$$

and so

$$kP_p = 0,$$

ie

$$kP_p = [0, 1, 0].$$

Thus

$$Z_k \equiv 0 \bmod p.$$

Hence

$$d = \gcd(Z_k, n) > 1;$$

and we may expect d to be a proper factor of n.
Note that we can compute the coordinates of rP as polynomials (with integer coefficients) in X, Y, Z. In effect if

$$P_1 = [X_1, Y_1, Z_1], \; P_2 = [X_2, Y_2, Z_2]$$

and

$$P_3 = P_1 + P_2 = [X_3, Y_3, Z_3]$$

then

$$X_3, Y_3, Z_3 \in \mathbb{Z}[X_1, Y_1, Z_1, X_2, Y_2, Z_2].$$

Note that we can work throughout $\bmod n$*. Thus the computation of* $kP \bmod n$ *requires approximately* $\log k$ *additions and doublings of points* $\bmod n$*.*

Note too that it is simplest to choose the point $P = [X, Y, Z]$ *and then find an elliptic curve* $y^2 = x^3 + bx + c$ *containing this point.*

Comparison *We can choose many different elliptic curves* $y^2 = x^3 + bx + c$*. We may expect that as the curve varies the order* N *of the reduced curve will be randomly distributed over the range* $(p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p})$ *allowed by Hasse's Theorem.*

Thus there is a far greater chance of finding a curve with b-small order N *than there is with Pollard's method which relies on the single number* $p - 1$ *being b-small.*