15 Number Theory

15.8 Elliptic Curves (8 units)

Background material for this project is contained in the Part IB course, Groups, Rings and Modules, and the Part II course Number Theory. The Part II course Algebraic Geometry may be helpful but is not necessary.

For any field k, an equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with coefficients a_1, a_2, a_3, a_4, a_6 in k is said to define an *elliptic curve* E over k if the discriminant $\Delta(E)$, a certain polynomial in the coefficients (see Appendix), is nonzero in the field k. Sometimes the notation $[a_1, a_2, a_3, a_4, a_6]$ is used as a shorthand for the above elliptic curve. Geometrically, the condition $\Delta \neq 0 \in k$ ensures that at any solution (x, y) of the equation, written in the form $f(x, y) = 0$, there is a well-defined tangent line, meaning that $\partial f/\partial x$ and $\partial f/\partial y$ are not both 0 at the point (x, y). For any elliptic curve E, let $E(k)$ denote the set of solutions $[x, y, z]$ in the projective plane $\mathbb{P}^2(k)$ to the associated homogeneous equation

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$

(Here $\mathbb{P}^2(k)$ is the set of triples (x, y, z) of elements of the field k which are not all 0, modulo the equivalence relation that (x, y, z) is equivalent to (cx, cy, cz) for $c \neq 0$ in k.)

> **Question 1** Show that the set $E(k)$ is in one-to-one correspondence with the set of solutions of the original equation, taking $z = 1$, together with the one other point $[0, 1, 0]$.

The fundamental fact about elliptic curves is that the set $E(k)$ forms an abelian group in a natural way. The sum of two points $a, b \in E(k)$ is given by drawing the line through a and b, which will intersect $E \subset \mathbb{P}^2$ in exactly one other point c. The point c will have coefficients in k, and the group structure on $E(k)$ is defined by saying that $a + b + c = 0 \in E(k)$. (For a line which is tangent to E at one point a and intersects E at one other point c, we interpret the previous equation to mean that $2a + c = 0 \in E(k)$, because we think of the line as intersecting E with multiplicity 2 at the point a.) Also, the identity element $0 \in E(k)$ is the point $[0, 1, 0]$. See any of the references on elliptic curves for more details.

> **Question 2** Write a program which computes the order of the finite abelian group $E(\mathbb{F}_p)$ for an elliptic curve E over a finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, specified by the prime number p and the coefficients a_1, a_2, a_3, a_4, a_6. Your program should check that $\Delta(E) \neq 0 \in \mathbb{F}_p$, so that E actually is an elliptic curve over $\mathbb{F}_p$, and if so then it should output the order of $E(\mathbb{F}_p)$ and the number $t_p := p + 1 - |E(\mathbb{F}_p)|$. The reason for mentioning t_p is Hasse's theorem, which says that $|t_p| \leqslant 2\sqrt{p}$ for any elliptic curve E over $\mathbb{F}_p$.
>
> Later parts of the project will build upon this program, so it should be reasonably efficient: don't just search through all p^2 pairs $x, y \in \mathbb{F}_p$ to see if they satisfy the given cubic equation. (For a given $x \in \mathbb{F}_p$, at most how many y's in $\mathbb{F}_p$ can satisfy the given equation? Can you find exactly how many y's work for a given x, without actually finding them? The case $p = 2$ may have to be handled separately.) Discuss the complexity of the method used by your program.
>
> Try your program out on some elliptic curves over different fields $\mathbb{F}_p$.

Given an elliptic curve E over the rational numbers $\mathbb{Q}$, which we will assume is defined by integers a_1, a_2, a_3, a_4, a_6, we get a family of cubic curves over $\mathbb{F}_p$, as the prime number p varies, by reducing the coefficients a_i modulo p. The resulting cubic curve is actually an elliptic curve over $\mathbb{F}_p$ if and only if $\Delta(E) \not\equiv 0 (\text{mod } p)$; in that case, we say that E has good reduction at p, otherwise that E has bad reduction at p.

Question 3 Write a program which, given integers a_1, a_2, a_3, a_4, a_6, outputs the discriminant $\Delta(E) \in \mathbb{Z}$ and its prime factorization (if you are using MATLAB, then you may use the `factor` function). Then, given integers p_1 and p_2, the program should print a table showing the order of the group $E(\mathbb{F}_p)$ and the associated number t_p (as in Question 2) for all prime numbers p in the range $p_1 \leqslant p \leqslant p_2$. If E has bad reduction at a given prime number p, leave the entries for $|E(\mathbb{F}_p)|$ and t_p blank (or use asterisks).

Try your program on the following elliptic curves and the primes $p < 200$.

$$\begin{array}{ll} (a) & y^2 = x^3 + 7x^2 + 2x, \\ (b) & y^2 + xy + y = x^3 + x^2 - 5x - 7, \\ (c) & y^2 = x^3 - 14x^2 + 41x. \end{array}$$

Are the answers related in any way?

It is known that if (x_1, y_1) is a torsion point of $E(\mathbb{Q})$ (*i.e.* a point of finite order) then $4x_1$ and $8y_1$ are integers. For example the elliptic curve $y^2 + xy = x^3 + 4x + 1$ has torsion point $(-1/4, 1/8)$.

Question 4 By hand, find a nontrivial element of the group $E(\mathbb{Q})$ for the elliptic curve E over $\mathbb{Q}$ given by $y^2 + y = x^3 + x^2 + 2x + 4$ and find the subgroup of $E(\mathbb{Q})$ generated by your element. What does this suggest about the relation between the output of your program in Question 3 and the torsion subgroup of $E(\mathbb{Q})$? Can you prove anything in this direction?

Question 5 Write a program which, given an elliptic curve over $\mathbb{Q}$ as in Question 3, computes the numbers t_p for a given range of primes p and shows the distribution of the numbers $t_p/(2\sqrt{p})$, which should be in the interval $[-1, 1]$, in some understandable graphical form. Try it for a few elliptic curves over $\mathbb{Q}$, for a sufficiently large range of primes p to get a meaningful picture, and describe the resulting probability distributions on $[-1, 1]$.

Elliptic curves with 'complex multiplication', such as those of the form $y^2 = x^3 + bx$ or $y^2 = x^3 + c$, should behave quite differently from most elliptic curves: what do you find in these cases? On the basis of your graphs, is it likely than any of the elliptic curves in Question 3 have complex multiplication?

Programming note

If you use a computer algebra package (such as MAPLE), then you may find that some routines for elliptic curves are included in the package. In such cases, no credit will be given for using the packaged routines — you are expected to write and analyse your own programs. You may, however, use packaged routines for dealing with prime numbers.

Appendix

The formula for the discriminant of the elliptic curve $[a_1, a_2, a_3, a_4, a_6]$ uses the following auxiliary expressions:

$$\begin{array}{rcl} b_2 & = & a_1^2 + 4a_2 \\ b_4 & = & a_1a_3 + 2a_4 \\ b_6 & = & a_3^2 + 4a_6 \\ b_8 & = & a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2 \end{array}$$

Then the discriminant is

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6.$$

References

[1] D. Husemoller. *Elliptic curves*, Springer (1987).

[2] J. Silverman. *The arithmetic of elliptic curves*, Springer (1986).

[3] J. Silverman and J. Tate. *Rational points on elliptic curves*, Springer (1992).