Elliptic Curves and Cryptography

Prof. Will Traves, USNA[1]

Many applications of mathematics depend on properties of smooth *degree-2* curves: for example, Galileo showed that planets move in elliptical orbits and modern car headlights are more efficient because they use parabolic reflectors (see Exercise 1). In the last 30 years smooth *degree-3* curves have been at the heart of significant theoretical and practical applications. Smooth degree-3 curves, known as elliptic curves, were used in Andrew Wiles's proof of Fermat's Last Theorem [11]. The points on elliptic curves form a group with a nice geometric description. Hendrick Lenstra [5] exploited this group structure to show that elliptic curves can be used to factor large numbers with a relatively small divisor. At one time this was thought to offer a serious challenge to RSA cryptography, which depends on the difficulty of factoring large numbers to secure communication. The Diffie-Helman protocol is another cryptographic scheme which is increasingly popular. While the Diffie-Helman protocol can be used with any group, recent implementations using elliptic curves seem to be very efficient. In this packet of course notes, we'll explore the mathematics underlying elliptic curves and their use in cryptography.

1 Elliptic Curves

The definition of an elliptic curve hides a lot of details:

An elliptic curve is a smooth degree-3 plane curve.

The first subtlety is that the curve lives in the *projective plane* rather than the usual xy-plane. In the projective plane $\mathbb{P}^2$ the points are tuples of ratios $(X : Y : Z) \neq (0 : 0 : 0)$ under the equivalence relation

$$(X : Y : Z) = (\lambda X : \lambda Y : \lambda Z) \text{ for } \lambda \neq 0.$$

A point $(X : Y : Z)$ with $Z \neq 0$ can be written in the form $(X/Z : Y/Z : 1)$ and corresponds to the point (x, y) with $x = X/Z$ and $y = Y/Z$ in two-space. Points $(X : Y : Z)$ with $Z = 0$ are said to be points "at infinity". Every curve defined by a polynomial equation in the usual plane can be extended to a curve in the projective plane. If $f(x, y) = 0$ is the equation of the curve in the xy-plane then we write $x = X/Z$ and $y = Y/Z$ and clear denominators by multiplying by $Z^{\deg(f)}$ to obtain an equation $F(X, Y, Z) = 0$ in the

[1]The development of these course notes was financially supported by the Defense Information Assurance Program funded by the National Security Agency.

variables of $\mathbb{P}^2$. The polynomial F is said to be homogenized since all its terms have the same degree. The value of the homogenized polynomial $F(X, Y, Z)$ at a point $(X : Y : Z)$ in projective space is not well-defined since $F(\lambda X, \lambda Y, \lambda Z) = \lambda^{\deg(F)} F(X, Y, Z)$ but it does make sense to talk about the collection $\mathbb{V}(F)$ of points $(X : Y : Z) \in \mathbb{P}^2$ where $F(X, Y, Z) = 0$. Note that if $(X : Y : Z) = (x : y : 1)$ then $F(X, Y, Z) = 0$ if and only if $f(x, y) = 0$, so $\mathbb{V}(F)$ contains points in $\mathbb{P}^2$ corresponding to the points on the original curve $f(x, y) = 0$ but $\mathbb{V}(F)$ also contains some points at infinity.

Example 1. Consider the line $y - x + 1 = 0$ in two-space. Its homogenization is $Y - X + Z = 0$. Every point (x, y) on the original line gives a point $(x : y : 1)$ on the homogenization. The homogenization also contains a point at infinity: when Z = 0 we see that the homogenization equation reduces to $Y - X = 0$, which determines a single point $(X : X : 0) = (1 : 1 : 0)$ in $\mathbb{P}^2$. That is,

$$\mathbb{V}(Y - X + Z) = \{(x : y : 1) \mid y - x + 1 = 0\} \cup \{(1 : 1 : 0)\}.$$

The line $y - x - 2 = 0$ has homogenization $Y - X - 2Z = 0$ and so if $Z = 0$ then we again get the point $(1 : 1 : 0)$ lying on the line at infinity.

In fact, all parallel lines intersect at the same point at infinity (see Exercise 2). So we think of the curve $Z = 0$ as defining the horizon, "at infinity". There is one point at infinity for each possible slope. It is much easier to describe the intersections of curves in projective space: for example, every pair of distinct lines meets in exactly one point, even if the lines are parallel. Étienne Bézout, working at the French Naval Academy, discovered a generalization of this result.

Figure 1: Parallel lines meet at infinity.

Theorem 2 (Bézout's Theorem)**.** *If two curves determined by homogeneous polynomials of degrees d_1 and d_2, respectively, do not share a common component, then they meet in precisely $d_1 d_2$ points in the projective plane if we count the points appropriately.*

The theorem requires that the two curves not share a common component, i.e. that the two defining polynomials do not share a common polynomial divisor. As well, we are instructed to count points appropriately. To do so we must allow complex coordinates, count points at infinity, and count points with multiplicity. To describe the computation of multiplicity rigorously requires advanced algebraic concepts, but we can get an accurate idea of how to count with multiplicity by looking at Figure 2.

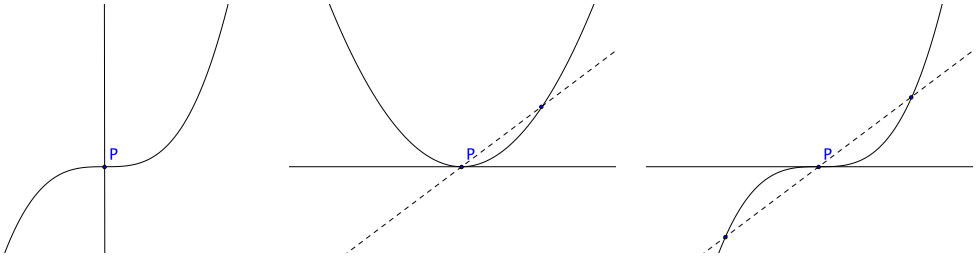

Figure 2: P is a point of multiplicity 1 (left), 2 (middle), 3 (right).

If a point P lies on two curves with distinct tangents at P then the point P counts with multiplicity one. If the tangent lines to the curves coincide at P then we move one of the curves slightly; the multiplicity at P is the number of points in the intersection that approach P as the moving curve approaches the original curve. In Figure 2 the moving curve is drawn with a dashed line and it approaches the horizontal line.

Let's return to our definition: an elliptic curve is a smooth *projective* plane curve of degree 3. That is, the curve is defined by an polynomial equation $F(X, Y, Z) = 0$ of degree 3. The curve is *smooth* if every point on the curve has a unique tangent line. We can find the tangent line using the gradient. If $P(X_0 : Y_0 : Z_0)$ is a point on the curve $F(X, Y, Z) = 0$ then P is a smooth point of the curve if

$$\nabla F(X_0, Y_0, Z_0) = \langle f_X(X_0, Y_0, Z_0), f_Y(X_0, Y_0, Z_0), f_Z(X_0, Y_0, Z_0)\rangle \neq \langle 0, 0, 0\rangle.$$

If P is a point on the curve that is not smooth we say that P is a singular point of the curve. The curve itself is said to be smooth if each of its points is smooth. If P is smooth point of the curve, then the tangent line at P is given by the equation

$$\nabla F(X_0, Y_0, Z_0) \cdot \langle X - X_0, Y - Y_0, Z - Z_0\rangle = 0.$$

Try Exercise 3 to get a feel for which cubic curves are smooth and which have singularities.

It turns out that each elliptic curve C has a point of inflection (see Exercise 4), a point where the curve C meets its tangent line in multiplicity three, as in the right diagram of Figure 2. Fix one such point of inflection and call it E. If P and Q are distinct points on the elliptic curve, then the line through P and Q is a degree 1 curve and by Bézout's Theorem it meets C in another point (PQ). Similarly, the line through E and (PQ) hits

the curve C in another point, which we denote $P+Q$. If two points in this process coincide then we replace the secant line through both points with the tangent line.

Theorem 3. *The points on the elliptic curve C form an Abelian group under the operation $+$ defined above. The identity element of the group is the point E.*

Proof. We leave it to the reader to check that the elliptic curve C is closed under the operation $+$, that the identity element is E, that the inverse of a point on C is again a point on C, and that $P+Q=Q+P$ (see Exercise 5).

It remains to check that the group law is associative. This follows from a nice result about cubics: if two cubic (degree-3) curves meet in 9 points, then any other cubic passing through 8 of them also passes through the ninth. This theorem can be proven using Bézout's Theorem; you might want to check out the proof given by Fields Medalist Terry Tao on his blog.[2] To show that $(P+Q)+R=P+(Q+R)$ it suffices to show that $R(P+Q)=P(Q+R)$ since then the line joining this point to E meets C for a third time in both $(P+Q)+R=P+(Q+R)$. We define three red lines and three blue lines as in Figure 3.

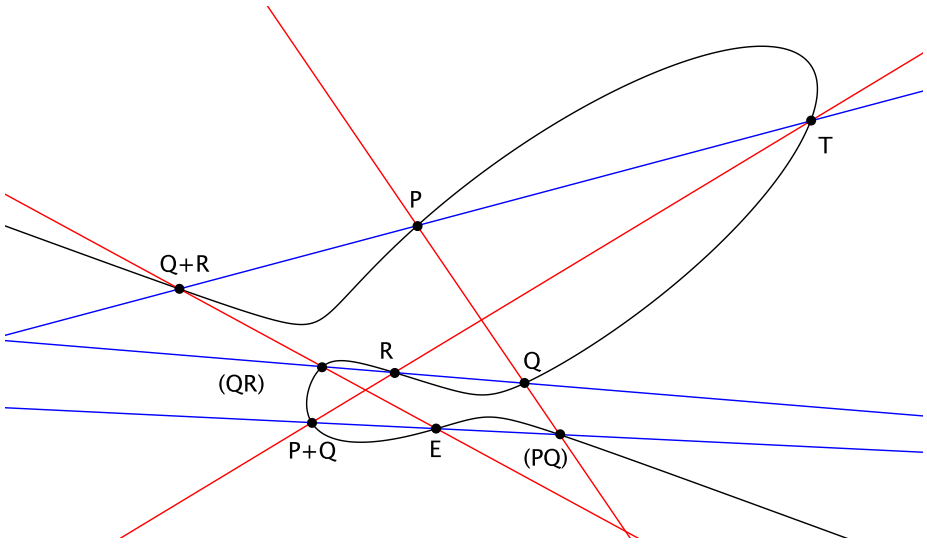

Figure 3: Six lines to show $R(P+Q)=P(Q+R)$.

Let the line through P and Q be colored red. It hits C at (PQ). Let the line through (PQ) and E be colored blue. It hits C at $P+Q$. Let the line through $P+Q$ and R be colored red. It hits C at $R(P+Q)$. Now let the line through Q and R be colored blue.

[2]See Tao's July 15, 2011 post at `terrytao.wordpress.com`.

It hits C at (QR). Let the line through (QR) and E be colored red. It hits C at $Q + R$. Let the line through $Q + R$ and P be colored blue. It hits C at $P(Q + R)$. Now consider the nine points P, Q, (PQ), E, $P + Q$, R, (QR), $Q + R$ and the intersection T of the red line joining $P + Q$ to R and the blue line joining $Q + R$ to P. All nine points lie on one of the three red lines and one of the three blue lines. The union of the blue lines forms a (degenerate) cubic curve, as does the union of the three red lines. Moreover, the elliptic curve C passes through the first 8 of the nine points, so C must also pass through T. It follows that $T = R(P + Q) = P(Q + R)$, as desired. □

Example 4. Consider the elliptic curve C, a portion of which is depicted in Figure 4, defined by

$$Y^2Z + YZ^2 - X^3 + XZ^2 = 0.$$

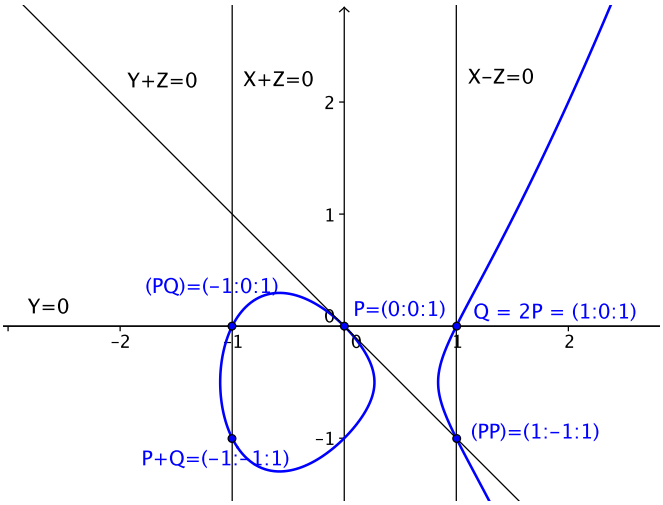

Figure 4: Addition on the elliptic curve $Y^2Z + YZ^2 - X^3 + XZ^2 = 0$.

The point $E(0 : 1 : 0)$ (not pictured) is an inflection point with tangent line $Z = 0$ and we use E as the identity of our group law. Let's add the points $P(0 : 0 : 1)$ and $Q(1 : 0 : 1)$ of C. The line through P and Q has equation $Y = 0$ and the third point of intersection of this line with C is $(PQ) = (-1 : 0 : 1)$. The line through (PQ) and E is $X + Z = 0$. Substituting $X = -Z$ into the equation for C we obtain

$$Y^2Z + YZ^2 = YZ(Y + Z) = 0.$$

The solutions $Y = 0$, $Z = 0$ and $Y + Z = 0$ correspond to $(PQ) = (-1 : 0 : 1)$, $E = (0 : 1 : 0)$ and $P + Q = (-1 : -1 : 1)$.

Let's also compute $2P$, where $P = (0 : 0 : 1)$. Here we need the tangent line to C at P, which is given by $X + Y = 0$. This hits C at a third point $(PP) = (1 : -1 : 1)$. The line through (PP) and E is $X - Z = 0$, which hits C in the third point $2P = (1 : 0 : 1)$.

Try Exercise 6 for some practice computing using the group law on an elliptic curve.

It is common to change coordinates so that the elliptic curve C is defined by an equation of the form

$$Y^2Z = X^3 + aXZ^2 + bZ^3$$

with identity $E(0 : 1 : 0)$. In this case we can write down the group law explicitly. Dehomogenize and suppose that $P(x_0 : y_0)$ and $Q(x_1 : y_1)$ are finite points on the elliptic curve with $x_0 \neq x_1$ (Question: If $x_0 = x_1$ then what is the sum of P and Q on C?). Then the line joining P and Q has equation $y - y_0 = m(x - x_0)$ where $m = (y_1 - y_0)/(x_1 - x_0)$. Substituting into the equation of the curve, we get

$$(y_0 + m(x - x_0))^2 = x^3 + ax + b,$$

a cubic in x. Expanding the cubic gives $x^3 - m^2x^2 + \cdots = 0$, which must factor as $(x - x_0)(x - x_1)(x - x_r) = 0$, where x_r is the x-coordinate of (PQ), the third point of intersection of the line with C. Expanding and equating coefficients of x^2 we see that $x_0 + x_1 + x_r = m^2$, or

$$x_r = m^2 - x_0 - x_1.$$

Plugging back into the equation of the line, we get that $y_r = y_0 + mx_r - mx_0$. Now the line through (PQ) and E is vertical so that the x-coordinate of $P + Q$ equals the x-coordinate of (PQ) and their y-coordinates differ by a factor of -1. So

$$P + Q = (x_2, y_2) = (m^2 - x_0 - x_1, -y_0 - mx_r + mx_0), \tag{1}$$

where $m = (y_1 - y_0)/(x_1 - x_0)$. These formulas hold even if the elliptic curve is defined over a finite ground field $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$. In that case we interpret the defining equation of C to hold modulo p and the variables X, Y and Z are only allowed to take values in $\mathbb{F}_p$. When $p \neq 2$ and $p \neq 3$ the same formulas for addition (and doubling, see Exercise 7) hold on the elliptic curve as long as everything is interpreted modulo the prime p (Question: Why make the assumptions $p \neq 2$ and $p \neq 3$?).

Example 5. Consider the elliptic curve C defined over $\mathbb{F}_{101} = \mathbb{Z}/101\mathbb{Z}$ by $Y^2Z = X^3 - 4Z^3$ with identity element $E(0 : 1 : 0)$. This means that the coordinates of each point are to

be taken as points in $\mathbb{F}_{101}$ and the equation defining the curve is understood to hold modulo 101. The points $P(3:15:1)$ and $Q(87:22:1)$ lie on C. Using Equation (1) and working modulo 101, we find that $m = (22-15)/(87-3) = 7/84 = 7(95) = 59$ and

$$P + Q = (58:73:1).$$

For more practice computing with elliptic curves, try Exercise 7.

2 Elliptic Curve Cryptography

Elliptic curves can be used to secure public communication using the Diffie-Helman protocol. Private key cryptography, in which both the sender and receiver share a special code, has been around for a long time, but private key cryptography is not well-suited to the world of digital communications. In the modern age we often need to communicate with people we've never met, and so we can't rely on a shared secret code. As well, we need to communicate with lots of people and sharing a secret code among so many people is likely to be insecure. Updating a widely shared secret code is also problematic. For all these reasons, public key cryptography is much better suited to communication in the digital age.

Public key cryptography does something that sounds impossible. It allows two people who have never met to communicate securely even if an eavesdropper can hear everything that they say! RSA cryptography is one type of public key cryptography; it uses the difficulty of factoring large numbers to guarantee that the communication is secure [2]. In contrast, the Diffie-Helman protocol uses the difficulty of finding discrete logarithms to secure communication.

The Diffie-Helman protocol works with an arbitrary group G and a fixed element $g \in G$. Suppose that Alice wants to send a message to Bob. They must first arrange to exchange some secret information using public communication. They do this as follows. First they agree on the group G and the element g. Then Alice picks an integer a and Bob picks an integer b. They keep these integers secret. Alice computes g^a (here we're writing out the group operation multiplicatively) and Bob computes g^b and they exchange this information. Alice gets $h = g^b$ from Bob and computes $h^a = g^{ab}$. Bob gets $k = g^a$ from Alice and computes $k^b = g^{ab}$. Now both Alice and Bob have g^{ab}. Of course, once they have a shared secret (like g^{ab}), Alice and Bob can use private key cryptography based on this secret to communicate securely. An eavesdropper would be able to obtain G, g, h, and k, but they would really need to get a or b to compute $g^{ab} = h^a = k^b$. That is, they'd need to compute $a = \log_g(g^a)$, given g^a. This is called the discrete log problem and it is thought to be very difficult if the size of the subgroup $\langle g \rangle$ is large enough and the group G doesn't possess some special structure.

Elliptic curve cryptography (ECC) essentially implements the Diffie-Helman protocol using an elliptic curve group defined over a finite ground field $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$. A base point P is chosen and P plays the role of the group element g in our description above. For various technical reasons, ECC is able to obtain the same security as the regular Diffie-Helman protocol using $G = \mathbb{F}_q$ where q is much larger than p. That is, ECC is able to guarantee strong security while using smaller field sizes. Using smaller field sizes is beneficial since it requires less storage and computations run much quicker if the field size is smaller too. In 2009, the National Security Agency endorsed ECC for both unclassified and classified communication.[3]

Example 6. Suppose that Alice and Bob agree to use the elliptic curve C defined over $\mathbb{F}_{101} = \mathbb{Z}/101\mathbb{Z}$ by $Y^2Z - X^3 + 4Z^3 = 0$ (and having identity element $E(0:1:0)$) and base point $P = (3:15:1)$. Alice chooses $a = 22$ and Bob chooses $b = 17$. Alice sends $22P = (61:63:1)$ to Bob and Bob sends $17P = (62:60:1)$ to Alice. Alice then computes $22(62:60:1) = (0:81:1)$ and Bob computes $17(61:63:1) = (0:81:1)$. Alice and Bob now share a secret, one that ought to be difficult for an eavesdropper to recover. However, the modulus $p = 101$ is too small to be secure since an eavesdropper could just compute all the multiples of P (which turns out to have order 102) and hence solve the discrete log problem, after which they can recover the secret point $(0:81:1)$. It is safer to use a much larger prime p (on the order of 300 digits) and correspondingly large values of a and b. Of course there are lots of primes of this size but actually finding one isn't so easy. Primality testing is a topic that would take us too far away from our narrative; an excellent source is Crandall and Pomerance [3]. For more practice with ECC, try Exercise 8.

3 Factoring with Elliptic Curves

The RSA public key cryptography protocol depends on the difficulty of factoring large numbers in order to secure communication. John Pollard [7] gave an algorithm that factors numbers with special structure reasonably quickly. Hendrick Lenstra [5] generalized Pollard's method, showing that large numbers with a relatively small divisor can be factored using elliptic curves.

Pollard's $p - 1$ algorithm is based on Fermat's Little Theorem, which is really just a corollary of the fact that the unit group of $\mathbb{F}_p$ has order $p - 1$ when p is a prime.

[3] See *The Case for Elliptic Curve Cryptography* on the NSA's website at `http://www.nsa.gov/business/programs/elliptic_curve.shtml`.

Theorem 7 (Fermat's Little Theorem)**.** *If a is a number relatively prime to the prime p then* $a^{p-1} \equiv 1 \mod p$.

Pollard realized that if n is a number with a prime factor p such that $p-1$ factors only into small primes then n can be factored as follows. First we set a bound B on the size of the primes that we are willing to allow in $p-1$. Then we compute

$$K = \prod_{q \text{ prime} \leq B} q^{\lfloor \log_q n \rfloor}.$$

If $p-1$ factors into primes less than or equal to B then $(p-1)|K$ (Question: Why?) and $K = (p-1)t$ for some integer t. Pick an integer a relatively prime to n (and hence to p). Then Fermat's Little Theorem shows that

$$a^K - 1 = a^{(p-1)t} - 1$$

is divisible by p and so n and $a^K - 1$ share a common factor (a multiple of p). It may turn out that this common factor is n itself, in which case we get no information and we should choose a different value of a, but it is more likely that $\gcd(a^K - 1, n) = p$. This greatest common divisor (gcd) can be computed quickly using the Euclidean algorithm (see Exercise 10). So we can use the Euclidean algorithm to obtain the first factor of n; if we are trying to break RSA, n is the product of two large primes and we can find the other factor of n by dividing by p. Unfortunately, if $p-1$ is not a product of small primes then our only recourse is to increase the bound B and do more work to try to factor n. There is no way to vary the group $\mathbb{F}_p$ that underlies Fermat's Little Theorem.

The Elliptic Curve Method (ECM) gets around this problem by working in the group of points of an elliptic curve defined over $\mathbb{F}_p$ rather than on the multiplicative group of $\mathbb{F}_p$. The benefit is that when the ECM fails, we can vary the elliptic curve and use the ECM again.

The ECM to factor n works as follows. First pick a point $P(x_0 : y_0 : 1)$ in projective space over $\mathbb{Z}/n\mathbb{Z}$. Then find an elliptic curve C with equation $Y^2Z = X^3 + aXZ^2 + bZ^3$ so that $P \in C$ (just pick a at random and set $b = y_0^2 - x_0^3 - ax_0$). Now pick a bound B and compute $B!P$, perhaps using the doubling method of Exercise 7. To add points on the elliptic curve we need to compute slopes (of secant or tangent lines) and these have the form u/v for some integers u and v. If v is relatively prime to n then we can compute $u/v \in \mathbb{Z}/n\mathbb{Z}$ but if v is not relatively prime to n then our addition formulas break down and the answer is not well-defined. And yet, in this moment of great despair, we realize that salvation is at hand: if v is not relatively prime to n then v and n share a common factor. That factor is unlikely to be n itself, so we've found a factor of n. In particular, if n were

an RSA number then we could break that instance of the RSA protocol. If we manage to compute $B!P$ without mishap, then we need to change our elliptic curve and try again.

The computations in the ECM can be understood as operating on several elliptic curves simultaneously. For instance, suppose that $n = pq$ is a product of two primes. Then $\mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})$. Moreover, the points on the elliptic curve C defined over $\mathbb{Z}/n\mathbb{Z}$ can be viewed as points on $C_p \times C_q$, where C_p (and C_q, respectively) is the elliptic curve with the same defining equation as C but interpreted over $\mathbb{Z}/p\mathbb{Z}$ (or $\mathbb{Z}/q\mathbb{Z}$, respectively) rather than $\mathbb{Z}/n\mathbb{Z}$. The elliptic curve addition on C breaks when the resulting point can be interpreted as (E, R) or (R, E) on $C_p \times C_q$, where E is the identity element at infinity and $R \neq E$. Now if $kP = E$ for some integer k then by Lagrange's Theorem k divides the order of the elliptic curve group. A celebrated theorem of Hasse shows that the number of points on an elliptic curve over $\mathbb{F}_p$ is randomly distributed between $p + 1 - 2\sqrt{p}$ and $p + 1 + 2\sqrt{p}$. So we expect C_p and C_q to have orders that are roughly equal to $p + 1$ and $q + 1$, respectively. Moreover, two such numbers are unlikely to share many factors. So if $kP = E$ on one of the two factors C_p or C_q, this is also unlikely to occur on the other factor. That is, if $kP = (R, E)$ then R is unlikely to be E and we'll obtain a factor of n.

Example 8. This example is taken from Trappe and Washington [10]. Suppose that we want to factor $n = 455839$. Let $P = (1 : 1 : 1)$ and choose the elliptic curve C to be defined by $Y^2Z = X^3 + 5XZ^2 - 5Z^3$ over $\mathbb{Z}/n\mathbb{Z}$. Let's try to compute $9!P$. At first we need to find $2P$ and so we compute the slope of the tangent line at P. The slope here is $(3X^2 + aZ^2)/(2YZ) = 8/2 = 4$ and so we have no trouble implementing the doubling algorithm to get $2P = (14 : -53 : 1)$. To compute $3!P = 3(2P)$ we first try to double $2P$. The slope of the tangent line is $(3(14^2) + 5)/(2(-53)) = -593/106 \mod n$ and 106 is invertible modulo n so again there is no problem computing $4P = (259851 : 116255 : 1)$. After this, one can compute $3!P = 6P = 4P + 2P$ without mishap. Continuing in this way we compute $4!P$, $5!P$, $6!P$ and $7!P$, but computing $8!P$ turns out to require that we invert $599 \mod 455839$ and since $599|455839$ out addition formulas break down. Fortunately, we win because we've managed to factor $n = 455839 = 599 \times 761$.

In our example, C_{599} has $640 = 2^7 \times 5$ points, while C_{761} has $777 = 3 \times 7 \times 37$ points. In fact, $\text{ord}_{C_{599}} P = 640$ and $\text{ord}_{C_{761}} P = 777$. Since $8!$ is a multiple of 640 but not a multiple of 777, we have $kP = E$ on C_{599} and not on C_{761}, so the addition formulas broke down at this point, giving the factorization of n.

Check out Exercise 11 to try your hand at factoring using the ECM.

4 Parting Comments and Further Reading

Elliptic curves take their name from elliptic functions. These are inverse functions to certain functions that appear when you try to compute the arclength of an ellipse. Elliptic functions are doubly periodic functions on the complex plane whose image turns out to be an elliptic curve. Roughly speaking, elliptic functions allow us to think of an elliptic curve as a parallelogram in which opposite edges are identified. The resulting object has 2 real dimensions (so it is sometimes called a Riemann surface) and 1 complex dimension (so it is also sometimes called a complex curve) and looks kind of like a donut. Mathematicians say that the resulting object has *genus* 1 since it has 1 hole. The study of Riemann surfaces sits at the intersection of analysis, algebra and topology and is an excellent introduction to advanced mathematics. A good reference is Miranda's book [6].

Elliptic curve cryptography (ECC) is an active area of current research. One worry for those using (ECC) – and other public-key cryptography protocols such as RSA – is that there are known attacks on ECC using quantum computers. There are currently no large-scale quantum computers but if one is ever built, we'll need to move to quantum resistant cryptographic schemes. Fortunately such schemes are already under development. A good reference for post-quantum cryptography is [1].

A good general reference on elliptic curves is Husemöller [4]. The book by Trappe and Washington [10] contains an accessible account of the use of elliptic curves in cryptography as well as a very readable introduction to the mathematics behind other cryptographic schemes. I'm generally a big fan of Simon Singh's books, and I can recommend his book on Fermat's Last Theorem [8] and his book on cryptography [9]; both contain a lot more background than you'll find in more specialized works, though the mathematical level is fairly low (which makes them easier to read but also might leave you wanting more details).

5 Exercises

1. (a) Imagine sunlight streaming across the xy-plane, with light particles moving parallel to the y-axis, approaching the x-axis from above. A mirrored barrier is fashioned in the shape of a smooth curve with equation $y = f(x)$. Light bounces off this curve so that the angle of incidence is equal to the angle of reflection (as measured against the tangent line to the curve), and all the reflected light passes through the point $(0, 1)$. Find the equation of the curve if the curve passes through the origin, i.e. $f(0) = 0$. [Hint: set up and solve an initial value problem.]
   (b) Of course, most mirrored barriers are not 2-dimensional. Explain how to make a surface so that light rays parallel to the y-axis, streaming toward the xz-plane from

"the right" all bounce off the surface and pass through the point $(0, 1, 0)$. This mathematical computation is the theoretical foundation for solar ovens – low technology ovens powered by the sun – and the large microphones seen on the sidelines of almost all professional football games.
(c) Instead of looking at light rays from the sun, we can consider a light source located at position $(0, 1, 0)$. Explain what happens to the light rays when they bounce off your reflecting surface. Why are these mirrored surfaces located at the back of most automobile headlights?

2. Show that parallel lines in $\mathbb{R}^2$ meet the line $Z = 0$ at infinity in a unique point and that this point depends on the slope of the parallel lines.

3. For each of the three curves below determine if any points on the curve are singular. Plot the curves and note the behavior of the curve near its singular points.
(a) $Y^2 - X^3 - X^2 = 0$
(b) $Y^2 - X^3 = 0$
(c) $Y^2 - X^3 + X = 0$.

4. Let C be a smooth curve defined by the homogeneous polynomial equation $F = 0$. Each inflection point P on C satisfies the Hessian condition: writing $X_1 = X$, $X_2 = Y$ and $X_3 = Z$, the evaluation of the determinant of the matrix $H(F) = (\partial^2 F/\partial X_i \partial X_j)$ at P equals zero.
(a) Find the points of inflection of the elliptic curve $Y^2Z + YZ^2 - X^3 + X^2Z = 0$.
(b) Show that a general elliptic curve has 9 points of inflection. [Hint: use Bézout's Theorem.]

5. Let C is an elliptic curve and let P and Q be points on C. Let E be an inflection point of C and let $+$ denote the associated addition law on the elliptic curve. In this exercise you will fill in the details of the proof that C is a group under the operation $+$ (the associativity of $+$ was established in the proof of Theorem 3).
(a) Show $P + Q$ is a point on C.
(b) Show that E is a the identity element for the operation $+$.
(c) Show that $-P$ is a point on the elliptic curve C and identify the point as a point of the form (AB) for suitable points A and B on C.
(d) Show that $P + Q = Q + P$ so that the elliptic curve group is Abelian.

6. Consider the curve C given by $Y^2Z + YZ^2 - X^3 + X^2Z = 0$ with identity element $E = (0 : 1 : 0)$. Find the multiples $2P$, $3P$, $4P$, and $5P$ of $P = (1 : 0 : 1)$. In particular, show that $5P = E$. That is, the subgroup of C generated by P is a *cyclic*

subgroup. Mordell conjectured (and Faltings proved) that the subgroup of rational points on an elliptic curve is finitely generated [4, Theorem 5.2]. Mazur described the possible finite subgroups of the rational points on an elliptic curve [4, Theorem 5.3].

7. (a) The same method that produced Equation (1) can be used to derive doubling formulas. Given an elliptic curve C defined by $Y^2Z = X^3 + aX + b$ and a finite point $P = (x_0, y_0)$ on C, find a formula for $2P = (x_1, y_1)$.
(b) Use your formula from part (a) to show that if $P = (3 : 15 : 1)$ is a point on the elliptic curve C defined over $\mathbb{F}_{101} = \mathbb{Z}/101\mathbb{Z}$ by $Y^2Z - X^3 + 4Z^3 = 0$ (and having identity element $E(0 : 1 : 0)$), then $2P = (14 : 66 : 1)$.
(c) In the set-up from part (b), check that $65P = (81 : 51 : 1)$ as follows. First write 65 in binary as $64 + 1$, i.e. 1000001. Then find $2P$, $4P, \ldots, 64P$ by repeated doubling. Finally, add $64P$ to P.

8. (a) Try writing a MATLAB program to add points on an elliptic curve $Y^2Z = X^3 + aXZ^2 + bZ^3$ modulo a prime p. Use Equation (1) or for a greater challenge, use the doubling procedure from the Exercise 7.
(b) Alice and Bob want to communicate using ECC with the elliptic curve $Y^2Z = X^3 + XZ^2 + 661Z^3$ modulo $p = 1000000007$. They use the $E(0 : 1 : 0)$ as their identity element and $P(4 : 27 : 1)$ as their base point. Alice picks $a = 2875$ and Bob picks $b = 3264$. Use your program[4] to check that Alice sends point $(625316551 : 876120926 : 1)$ to Bob and he replies with point $(797864344 : 881594541 : 1)$. Then find Alice and Bob's shared secret point.

9. Prove Fermat's Little Theorem, Theorem 7. That is, show that if a is an integer not divisible by the prime p then $a^{p-1} \equiv 1 \mod p$.

10. Euclid's algorithm gives a way to determine the greatest common divisor (gcd) of two numbers a and b. Euclid observed that if

$$a = qb + r$$

[4]If you didn't do part (a), you could use an online ECC calculator like the one found at `http://christelbach.com/ECCalculator.aspx`.

with $0 \leq r < b$ then $\gcd(a, b) = \gcd(b, r)$. So to compute $\gcd(a, b)$ we write

$$\begin{aligned} a &= qb + r, \\ b &= q_1 r + r_1, \\ r &= q_2 r_1 + r_2, \\ r_1 &= q_3 r_2 + r_3, \\ &\vdots \\ r_{k-1} &= q_{k+1} r_k + r_{k+1}, \end{aligned}$$

where each r_k satisfies $0 \leq r_k \leq r_{k-1}$. If $r_{k+1} = 0$ then

$$\gcd(a, b) = \gcd(b, r) = \gcd(r, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{k-1}, r_k) = r_k.$$

Use this algorithm to compute the gcd of 693 and 3213.

11. Try to factor the number $n = 131179$ using the Elliptic Curve Method. In particular, try to compute $6!P$ for $P = (1 : 1 : 1)$ on the elliptic curve C over $\mathbb{Z}/n\mathbb{Z}$ defined by the equation $Y^2Z = X^3 + 11XZ^2 - 11Z^3$.

References

[1] Daniel J. Bernstein. Introduction to post-quantum cryptography. In *Post-quantum cryptography*, pages 1–14. Springer, Berlin, 2009.

[2] S. C. Coutinho. *The mathematics of ciphers*. A K Peters Ltd., Natick, MA, 1999. Number theory and RSA cryptography, Translated and revised from the 1997 Portuguese original.

[3] Richard Crandall and Carl Pomerance. *Prime numbers*. Springer, New York, second edition, 2005. A computational perspective.

[4] Dale Husemöller. *Elliptic curves*, volume 111 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 2004. With appendices by Otto Forster, Ruth Lawrence and Stefan Theisen.

[5] H. W. Lenstra, Jr. Factoring integers with elliptic curves. *Ann. of Math. (2)*, 126(3):649–673, 1987.

[6] Rick Miranda. *Algebraic curves and Riemann surfaces*, volume 5 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 1995.

[7] J. M. Pollard. Theorems on factorization and primality testing. *Proc. Cambridge Philos. Soc.*, 76:521–528, 1974.

[8] Simon Singh. *Fermat's enigma*. Walker and Company, New York, 1997. The epic quest to solve the world's greatest mathematical problem, With a foreword by John Lynch.

[9] Simon Singh. *The Code Book*. Doubleday Books, New York, 1999. The Evolution of Secrecy from Mary, Queen of Scots to Quantum Cryptography.

[10] Wade Trappe and Lawrence C. Washington. *Introduction to cryptography with coding theory*. Pearson Prentice Hall, Upper Saddle River, NJ, second edition, 2006.

[11] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.