Elliptic Curves (for use in Cryptography)

Most Public Key Cryptography schemes involve the use of groups, in some way shape or form, as previously discussed. In RSA, the members of our group are integers relatively prime to the public key n, and the operation used is modular exponentiation. While this works, the computation required to get the desired security is quite a bit, rendering RSA to be fairly slow compared to private key schemes. A public key scheme that is faster than RSA is desirable for this reason.

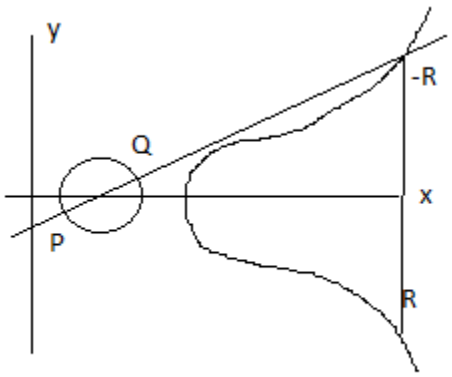
Elliptic Curves (real-valued) are studied in Group Theory as well. The general form of the equation of an elliptic curve is:

$$y^2 = x^3 + ax + b$$

The idea is that the LHS is simply y^2 (so for any x value making the RHS positive, there are two matching y values) while the RHS is a cubic equation in x. It turns out that any general cubic can be transformed into another cubic without the quadratic term that has roots related to the original. (This is a neat exercise by itself. Think about rewriting the cubic $x^3 + cx^2 + dx + e$ by making a variable substitution for x so that after the substitution, there is no quadratic term.)

The key operation we will describe for these curves is addition, an operation which is definitely not intuitive. Given two points P and Q on a Elliptic Curve, if we draw a line through those two points, the line will usually intersect in a third point. We will define this point as -R. To negate a point, simply reflect it over the x-axis. (Thus, for a given point, its negative point has the same x coordinate and opposite y coordinate. For example, on the elliptic curve $y^2 = x^3 + 2x + 1$, the negative of the point (1, 2) is (1, -2).)

We define the sum of P + Q equal to R, using the definition above. Here is an illustration on a typical looking elliptic curve:



We can define multiplication as repeated addition of a point. (Note: adding a point to itself is slightly different than the illustration above.) Just like the discrete log problem, it's relatively easy for us to add a point P to itself k times to calculate kP, but given kP and P, it's difficult to figure out the value of k.

In cryptography, we'll use integer versions of elliptic curves by adding a prime number modulus. Thus, an elliptic curve used for cryptography will create a group of points of the form (x, y), where both x and y are integers mod p that satisfy the equation:

$$y^2 \equiv (x^3 + ax + b) \bmod p$$

where a and b are valid integers mod p. Let $E_p(a, b)$ refer to the Elliptic Curve with the equation above. Thus, $E_{23}(1, 1)$ is the Elliptic Curve with the equation $y^2 \equiv (x^3 + x + 1) \bmod 23$.

It turns out that in order for this equation to produce a valid set of points that form a group under point addition, it's necessary that $4a^3 + 27b^2 \not\equiv 0 \pmod p$.

Each ordered pair of integers (x, y) with $0 \leq x, y < p$ that satisfy the equation above are the points for the Elliptic Curve. In addition, we have a special point, O, called the origin, that is part of the curve. This point does not have coordinates, per se.

Here are the rules for addition:

1. For each point P on the curve, P + O = P

2. For each point P = (x, y), -P = (x, -y). Under mod, this means -P = (x, p-y) and P + (-P) = O.

3. Let $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$. Define R = P + Q, where $R = (x_R, y_R)$. We can calculate R as follows:

First calculate lambda, which is a roughly translates to slope:

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P} \; mod \; p, \text{ if } P \neq Q$$

$$\lambda = \frac{3x_P^2 + a}{2y_P} \; mod \; p, \text{ if } P = Q$$

Then, we can calculate the necessary x and y coordinates (in that order), as follows:

$$x_R = \left(\lambda^2 - x_P - x_Q\right) mod \; p$$

$$y_R = (\lambda(x_P - x_R) - y_P) \; mod \; p$$

Example of Adding P + Q

For this example, we'll use the Elliptic Curve $E_{23}(1, 1)$, which uses the equation $y^2 \equiv (x^3 + x + 1) \bmod 23$. Two points on this curve are P = (3, 10) and Q = (9, 7). We will calculate R = P + Q.

First we must calculate lambda:

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P} \; mod \; p = \frac{7 - 10}{9 - 3} = \frac{-3}{6} = (-3)(6^{-1}) = (-3)(3^{-1}2^{-1}) = -2^{-1} \; (mod \; 23)$$

Note that effectively, we can "cancel" a common factor in the numerator and denominator even though we are working under mod, because we can rewrite the denominator as a product of modular inverses. In the end though, once we cancel items, we are typically still left with a modular inverse calculation to make, since we aren't allowed fractions.

We can either run the Extended Euclidean Algorithm to find $2^{-1} \bmod 23$, or eyeball that 2 x 12 = 24 = 1 (mod 23). It follows that:

$$\lambda = -2^{-1} \equiv -12 \equiv 11 \; (mod \; 23)$$

Next, let's solve for x_R:

$$x_R = \left(\lambda^2 - x_P - x_Q\right) mod \; p = (11^2 - 3 - 9) = 109 \equiv 17 \; (mod \; 23)$$

Finally, let's solve for y_R:

$$y_R = (\lambda(x_P - x_R) - y_P) \; mod \; p = (11(3 - 17) - 10) \equiv (11 \times 9 - 10) \equiv 89 \equiv 20 \; (mod \; 23)$$

It follows that (3, 10) + (9, 7) = (17, 20).

Example of Adding 2P

Use the same curve and the point P = (3, 10). Let's calculate R = 2P. We still have to find lambda:

$$\lambda = \frac{3x_P^2 + a}{2y_P} \; mod \; p = \frac{3(3)^3 + 1}{2(10)} = \frac{28}{20} = \frac{7}{5} = 7(5^{-1}) \; mod \; 23$$

Let's use the Extended Euclidean Algorithm to determine $5^{-1} \bmod 23$. Note that since we've established that we can "cancel" in fractions, I have done so above, directly just canceling until the resulting fraction is in lowest terms. (Also, you'll notice that an alternate path would have been to reduce 28 to 5 and rewrite the fraction as ¼, which is just $4^{-1} \bmod 23$. Both will lead to the correct answer for lambda.

23 = 4 x 5 + 3
5 = 1 x 3 + 2
3 = 1 x 2 + 1
3 – 2 = 1

3 – (5 – 3) = 1
2 x 3 – 1 x 5 = 1
2(23 – 4 x 5) = 1
2 x 23 – 9 x 5 = 1
5^{-1} = -9 mod 23

Now, solving for lambda: $\lambda = 7(5^{-1}) \equiv 7(-9) \equiv -63 \equiv 6\ mod\ 23$.

Now, solve for x_R:

$$x_R = \left(\lambda^2 - x_P - x_Q\right) mod\ p = (6^2 - 3 - 3) = 30 \equiv 7\ (mod\ 23)$$

Finally, let's solve for y_R:

$$y_R = (\lambda(x_P - x_R) - y_P)\ mod\ p = (6(3 - 7) - 10) = -24 - 10 = -34 = 12\ (mod\ 23)$$

This means that 2 x (3, 10) = (7, 12)