Elliptic Curves

Jake Fisher and Davis Lister

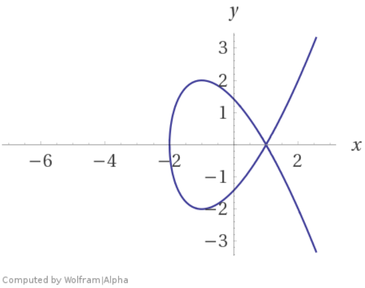
May 1, 2018

Group Law for Elliptic Curves

- Elliptic Curves are a group under the $+$ operation with the set $\{K \times K : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$ where $\mathcal{O}$ is the point at infinity and K is a field. We notate the set of elliptic curves over a field K, $(E(K))$.
- Let us define the discriminant $\Delta = -16(4a^3 + 27b^2)$. If $\Delta = 0$ the group law does not hold.
- The $+$ operation is defined geometrically on two points (x_1, y_1) and (x_2, y_2) thus: draw the secant line and find the third point where it intersects the curve (x', y'), which can include $\mathcal{O}$, finally find $(x', -y')$, the resulting point.
- Under the $+$ operation $\mathcal{O}$ is the identity and $(x, y)^{-1} = (x, -y)$.
- All computations are done over the set $\mathbb{Z}/n\mathbb{Z}$ in cryptographic and integer factorization applications.

More on the Discriminant

- The condition we impose on the discriminant is the is motivated by the need to have a tangent line be well defined at all points on the curve $S \in (E(K))$. If the tangent line is not defined at a point $P_0 = (x_0, y_0)$, then S is singular.
- If S is singular, then $P_0 + P_0$ is not well-defined, which breaks the group law.
- Geometrically, a singularity is a cusp or self-intersection.



Definition of B-power smooth

- Let B be a positive integer. The prime factorization of an integer $n = \prod p_i^{e_i}$. If $\forall i \; p_i^{e_i} \leq B$, n is B-power smooth.
- For instance, 60 is 5-power smooth but 150 is 25-power smooth.

Pollard's p-1 Factoization

- We wish to find a nontrivial factor of a large positive integer N using the Pollard p-1 method.
- Let us choose a positive integer B. Suppose that there is a prime factor p of N such that $p-1$ is B-power smooth.
- Let us choose $a > 1$ such that p does not divide a. Often we will choose $a = 2$ for convenience.
- By Fermat's Little Theorem $a^{p-1} \equiv 1 \mod p$.
- Let $m = \operatorname{lcm}(1, 2, 3, \dots, B)$. Since $p-1$ is B-power smooth, $p-1 \mid m \implies p \mid \gcd(a^m - 1, N) > 1$.
- If $\gcd(a^m - 1, N) < N$, then $\gcd(a^m - 1, N)$ is a nontrivial factor of N.
- The algorithm becomes more transparent if we consider $m = k(p-1)$, where $k \in \mathbb{Z}$.

Factoring Magic!

- An example of integer factorization using Pollard's p-1 method.
- Let $N = 5917$ and let $B = 5$. $m = \text{lcm}(1, 2, 3, 4, 5) = 60$.
- Note that $2^{60} - 1 = 3416 \mod 5917$, and $\gcd(2^{60} - 1, 5917) = \gcd(3416, 5917) = 61$.
- 61 is a factor of 5917!
- But if $p - 1$ and $q - 1$ (where $pq = N$) are not B-power smooth, Pollard p-1 does not work.
- The issue is that $(\mathbb{Z}/p\mathbb{Z})^*$ has order p-1.
- Additionally, if $p - 1$ is the product of many small primes, then the algorithm will return N.

Lenstra's Elliptic Curve Factorization

-