Elliptic Curves

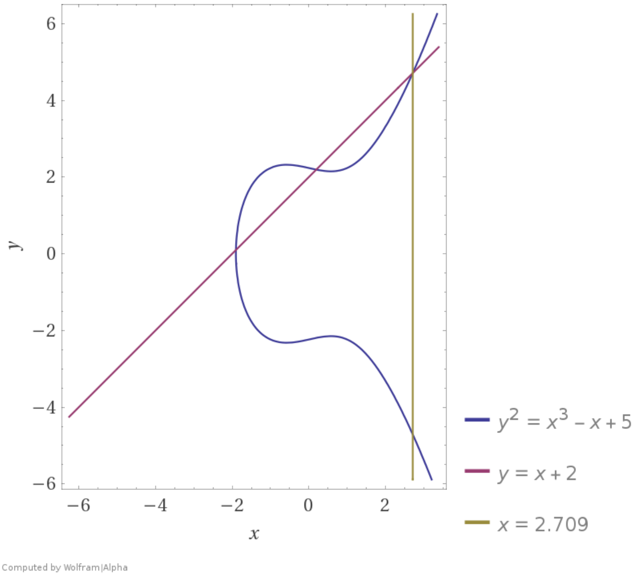
Jake Fisher and Davis Lister

May 16, 2018

Group Law for Elliptic Curves

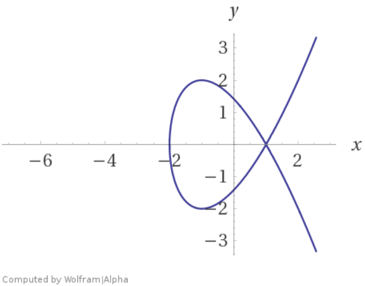
- Elliptic Curves are a group under the $+$ operation with the set $\{K \times K : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$ where $\mathcal{O}$ is the point at infinity and K is a field. We notate the set represented by an elliptic curve E over a field K, $E(K)$.
- Let us define the discriminant $\Delta = -16(4a^3 + 27b^2)$. If $\Delta = 0$ the group law does not hold.
- The $+$ operation is defined geometrically on two points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ 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 $(x, y)^{-1} = (x, -y)$.
- The $+$ operation is closed since each secant line will intersect the curve at exactly one other point. The definition of the operation does not discriminate between P_1 and P_2. Therefore, $(E(K), +)$ is an abelian group.

A Visualization of the + Operation over E(K)



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 elliptic curve S. 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.

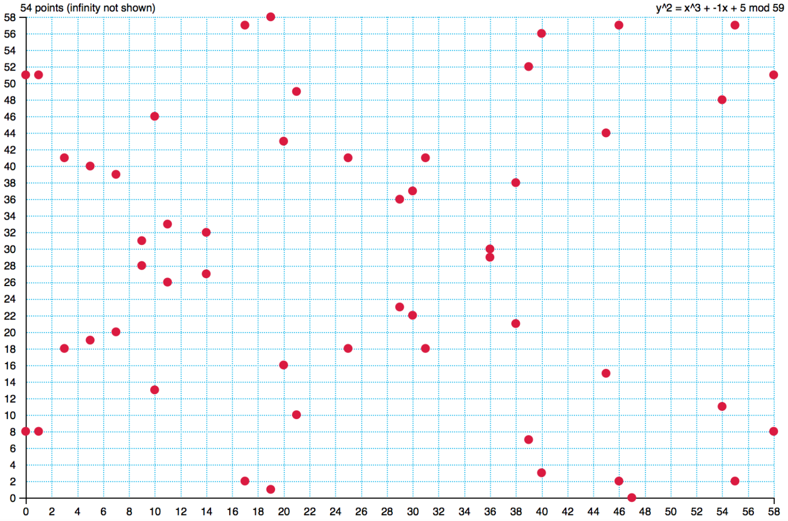
Pollard's p-1 Factoization

- 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 $m = \text{lcm}(1, 2, 3, \dots, B)$. 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.

Elliptic Curves over Finite Fields



Lenstra's Elliptic Curve Factorization

- Choose $N, B \in \mathbb{Z}^+$.
- Compute $m = \text{lcm}(1, 2, \ldots, B)$.
- Choose a random $a \in \mathbb{Z}/N\mathbb{Z}$ such that $4a^3 + 27 \in \mathbb{Z}/N\mathbb{Z}^*$. Thus, $P = (0, 1)$ is a point on the elliptic curve $y^2 = x^3 + ax + 14$ over $\mathbb{Z}/N\mathbb{Z}$.
- Attempt to compute mP using the $+$ operation for the group $(E(K), +)$. If at some point we cannot compute a sum of points because $\gcd(x_1 - x_2, N) \neq 1$ (where $x_1 - x_2$ is the denominator of the slope expression we compute in order to execute the $+$ operation), compute and return $\gcd(x_1 - x_2, N)$ if $\gcd(x_1 - x_2, N) \neq N$. If some point $kP = \mathcal{O}$ for $k \leq m$, terminate and output, "Fail." Additionally, if mP can be computed using the $+$ operation, output, "Fail."

Advantages of the Lenstra Method

- The advantage of the Lenstra method is that if the algorithm fails, we may choose a different elliptic curve and repeat the algorithm.
- We have more flexibility with our groups since we work with many different groups $E(\mathbb{Z}/N\mathbb{Z})$, which will have order $p + 1 \pm s$.
- In Pollard $p - 1$ we work with $\mathbb{Z}/N\mathbb{Z}^*$, which always has order $p - 1$.

An Example of the Lenstra Method

- Let us choose $N = 5959$ and $B = 8$.
- Therefore, $m = 840$ and our random $a = 6$, where $a \in \mathbb{Z} \mid 4a^3 + 27 \neq 0$.
- Note that $P = (0, 1)$ is on the elliptic curve $y^2 = x^3 + ax + 1$ over $\mathbb{Z}/N\mathbb{Z}$. We now attempt to compute mP.
- Observe that $60P = (649, 2654)$. Therefore $\lambda \equiv \frac{2653}{649} \mod 5959$. Since $649 \not\equiv 0 \mod 5959$, which would indicate that the next point were $\mathcal{O}$, we encounter a contradiction to the group law.
- Note that $(649, 2654)^{-1} = (649, -2654)$.
- Therefore, $p = \gcd(649, 5959)$ is a nontrivial factor of N, if $1 < p < N$.
- $\gcd(649, 5959) = 59 \implies 59$ is a nontrivial factor of 5959.

Elliptic Curve Cryptography

- The Diffie-Hellman key exchange can be implemented on an Elliptic Curve.
- Alice and Bob publicly agree on a prime p and an elliptic curve S over $\mathbb{Z}/p\mathbb{Z}$. They then agree on a point $P \in S(\mathbb{Z}/p\mathbb{Z})$.
- Alice chooses a private key m and sends Bob mP.
- Bob chooses a private key n and sends Alice nP.
- Alice and Bob both compute mnP, their shared secret key.

A Numerical Example of Diffie-Hellman Key Exchange with Elliptic Curves

- Alice and Bob publicly agree on $p = 571$ and the elliptic curve S given by $y^2 = x^3 - 12x + 5$. They then agree on $P = (16, 324)$.
- Alice privately computes and sends Bob $39P = (148, 387)$. Bob privately computes and sends $121P = (465, 556)$.
- Alice privately computes $39(465, 556) = (202, 445)$, and Bob privately computes $121(148, 387) = (202, 445)$.

Elliptic Curve Discrete Logarithm Problem

- The security of an elliptic-curve cryptosystem is dependent on the solution to the elliptic curve discrete logarithm problem.
- Let S be an elliptic curve over $\mathbb{Z}/p\mathbb{Z}$ and $P \in S(\mathbb{Z}/p\mathbb{Z})$.
- Given Q a multiple of P, we aim to find $n \in \mathbb{Z}$ such that $nP = Q$.
- The naive approach is to simply check each possible value of n until one arrives at the solution Q. However, the naive approach becomes computationally infeasible as p is sufficiently large.
- Currently, it appears that the discrete logarithm problem on $E(\mathbb{Z}/p\mathbb{Z})$ is more difficult than the discrete logarithm problem on $\mathbb{Z}/p\mathbb{Z}^*$.
- An elliptic curve cryptosystem can offer equivalent security to many cryptosystems currently in use with much smaller numbers, which allows for great gains in efficiency.

Why Should You Care?

- You probably shouldn't.
- But, if you want to...
- Elliptic curves are much more space-efficient than other methods – a 1024-bit RSA key is equivalent to a 163-bit ECC key in security.
- However, because it's not as well-established, it has other potential issues.

Dual_EC_DRBG

- Published first in 2006.
- It was pushed by NSA to be standardized, even going so far as to pay a security company $10 million to use it.
- Suspected to contain a backdoor.
- Removed by NIST in 2014.

Applications of Elliptic Curve Cryptography

- Presently, Bitcoin uses an elliptic curve digital signature algorithm to verify coin ownership.
- Google also utilizes elliptic curve public keys for encryption and verification.

Public Key Info	
Algorithm	Elliptic Curve Public Key (1.2.840.10045.2.1)
Parameters	Elliptic Curve secp256r1 (1.2.840.10045.3.1.7)
Public Key	65 bytes : 04 D1 E6 FF B3 77 D8 A6 ...
Key Size	256 bits
Key Usage	Encrypt, Verify, Derive
Signature	256 bytes : 21 BF D2 FF A4 E4 D4 02 ...