# Elliptic Curves

Sam Estep

November 26, 2017

## 1 Motivation

Elliptic curves have found widespread use in number theory and applications thereof, such as cryptography. In this paper we will first examine the basic theory of elliptic curves and then look specifically at how they can be used to construct cryptographic systems more efficient than their counterparts, and how they can be used to generate proofs for or against primality.

### 1.1 Cryptography

Cryptography is the most important current field of application for elliptic curves. In the most general terms, cryptography is the art of making it easy for parties to communicate with each other while simultaneously making it difficult for attackers to compromise this communication.

For a given cryptographic system, we can usually increase or decrease the key size to get more or less security, respectively. This change in key size will affect the time, memory, and power requirements of the system. In other words, these two requirements of ease for communicators and difficulty for attackers are inversely related in the context of a given system. The question then becomes, what is the ratio in this relation for different systems?

As it turns out, for a given level of security, elliptic curve cryptography works with keys an order of magnitude smaller than those required by other systems.[1] This reduced memory demand is accompanied by corresponding reductions in power and time demands. As a result, elliptic curve cryptography is slowly but surely becoming a staple in our everyday communication.

## 1.2 Primality

Up until the 1970s, number theory in general and prime numbers in specific were regarded as demonstrations of the part of mathematics that has no practical import. Some number theorists, such as Hardy, found a certain amount of satisfaction in the idea that their work would not be used for military purposes.[2] The invention of RSA and the ever-increasing usage of computers have brought a swift end to this notion.

In order to make use of the properties of prime numbers, we need to actually be working with prime numbers. In other words, given $n \in \mathbb{Z}^+$, we would like to have a method to determine whether or not $n$ is prime. If $n > 1$ is composite then there exist some $a, b \in \mathbb{Z}^+$ with $1 < a \leq b < n$ such that $ab = n$. If $a, b > \sqrt{n}$ then $ab > \sqrt{n} \cdot \sqrt{n} = n$ which is a contradiction, so since $a \leq b$ we know that $a \leq \sqrt{n}$. Thus the most naïve primality testing algorithm is to check all $m \in \mathbb{Z}^+$ with $1 < m \leq \sqrt{n}$; if $m \mid n$ for any such $m$ then $n$ is composite; otherwise $n$ is prime. This algorithm has time complexity $O(\sqrt{n})$, which is infeasibly slow when $n$ has many digits.

An algorithm was discovered in 2002 that can determine primality of $n$ in time proportional to a polynomial in the number of digits of $n$.[3] The most efficient version of this algorithm runs in $O(\log^6 n)$ time, which is decent, but even using the most efficient primality checking algorithms known, checking the primality of a large number can still take an inconvenient amount of time. If, say, we have a number that we know to be prime, we would like to be able to communicate this knowledge to someone else in a way that they can verify it efficiently without having to trust us; this is the concept of a primality certificate. For $p \in \mathbb{Z}^+$ prime, elliptic curves give us the most efficient known way to generate a certificate of size $O(\log^2 p)$ that takes $O(\log^4 p)$ time to check, which is considerably faster than starting from scratch.[4]

# 2 Group Theory

## 2.1 General Form

Let $F$ be a field. Given $A, B \in F$, an elliptic curve $E$ over $F$ is the graph of

$$y^2 = x^3 + Ax + B$$

for $x, y \in F$. For reasons discussed below, we also include a "point at infinity" $O \notin F \times F$ in the elliptic curve. This point $O$ can be thought of as the point at which distinct vertical lines in the $F \times F$ plane "meet". It can be formalized using projective space, but we will not explore that here.[5] To summarize,

$$E = \{O\} \cup \{(x,y) \in F \times F \mid y^2 = x^3 + Ax + B\}.$$

It can be helpful to consider $F = \mathbb{R}$ and think of elliptic curves geometrically.[6] Trying different values of $A$ and $B$ demonstrates that we can cause the curve to have either two components, such as for

$$(A,B) = (-1,0) \quad \Rightarrow \quad y^2 = x^3 - x,$$

or just one component, such as for

$$(A,B) = (-1,1) \quad \Rightarrow \quad y^2 = x^3 - x + 1.$$

In general, we can show that the discriminant

$$\Delta = -16(4a^3 + 27b^2)$$

is positive if the graph has two components and negative if the graph has one component. We would like to avoid cusps, self-intersections, and isolated points, so we will say that if $\Delta = 0$ then $E$ is not an elliptic curve. Algebraically, this means that the roots of $0 = x^3 + Ax + B$ are distinct, which follows even in $F \neq \mathbb{R}$ where geometric intuition breaks down.

## 2.2 Group Law

We will work toward an appropriate definition of $+ : E \times E \to E$ that makes $E$ into an additive abelian group. A first guess might be the operation defined by $F \oplus F$. However, as an example, if $F = \mathbb{Q}$ and $(A,B) = (-1,0)$ as in the example above, our equation is $y^2 = x^3 - x$, so $(1,0) \in E$, but

$$(0+0)^2 = 0 \neq 6 = (1+1)^3 - (1+1) \quad \Rightarrow \quad (1+1, 0+0) \notin E.$$

Thus $E - \{O\}$ may not be a subgroup of $F \oplus F$, so we need something else.

We will develop the group law from a geometric standpoint motivated by the $F = \mathbb{R}$ case, but we will show each step algebraically for an arbitrary $F$, assuming the characteristic of $F$ is not 2. It is possible to generalize to fields of characteristic 2, but we will ignore that case here.[5]

Given $P_1, P_2 \in E$, draw a line through $P_1$ and $P_2$. We will see that this line also intersects $E$ at a point $P_3'$. Then reflect $P_3'$ across the $x$-axis to obtain

$P_3$. We want to turn the somewhat vague geometric decree that $P_1+P_2 = P_3$ into an algebraic formulation of our group law.

If $O, P_1, P_2$ are all distinct then we can destructure them as $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$. If $x_1 \neq x_2$ then the nonvertical line through $P_1$ and $P_2$ is

$$y = m(x - x_1) + y_1 \quad \text{where} \quad m = (y_2 - y_1)(x_2 - x_1)^{-1}.$$

Substituting this $y$ into the elliptic curve equation yields

$$0 = x^3 + Ax + B - (m(x - x_1) + y_1)^2 = x^3 - m^2x^2 + \alpha x + \beta.$$

where $\alpha = A + 2m^2x_1 - 2my_1$ and $\beta = B - m^2x_1^2 + 2mx_1y_1 - y_1^2$. We know that $x_1$ is a solution to this equation and thus a factor of the polynomial, so the division algorithm yields

$$0 = x^3 - m^2x^2 + \alpha x + \beta = (x - x_1)(x^2 + (x_1 - m^2)x + \gamma)$$

where $\gamma = x_1(x_1 - m^2) + \alpha$. We also know that $x_2$ is a solution and $x_2 \neq x_1$, so applying the division algorithm a second time yields

$$0 = (x - x_1)(x^2 + (x_1 - m^2)x + \gamma) = (x - x_1)(x - x_2)(x - (m^2 - x_1 - x_2)).$$

Thus if we let $x_3 = m^2 - x_1 - x_2$ and $y_3' = m(x_3 - x_1) + y_1$ then we know $P_1$, $P_2$, and $(x_3, y_3')$ are all the points of intersection of the line and the curve. We reflect across the $x$-axis to obtain $y_3 = m(x_1 - x_3) - y_1$, let $P_3 = (x_3, y_3)$, and say $P_1 + P_2 = P_3$.

If $x_1 = x_2$ then the line through $P_1$ and $P_2$ is vertical, so it intersects $E$ at $O$. If you take the point at which vertical lines meet and reflect it across the $x$-axis, you still have the point at which vertical lines meet, so we say $P_1 + P_2 = O$.

If $O \neq P_1 = P_2$ then we can't take the secant line as above because $x_2 - x_1 = 0$ is not invertible. However, differentiating the elliptic curve equation gives us

$$2y\, dy = 3x^2\, dx + A\, dx \quad \Rightarrow \quad \frac{dy}{dx} = \frac{3x^2 + A}{2y},$$

suggesting that we can use this slope instead to obtain another point. We interpret $y_1 = 0$ as a vertical tangent line and say $P_1 + P_2 = O$ as above, so consider the case $y_1 \neq 0$ where we can define the nonvertical tangent line through $P_1 = P_2$ as

$$y = m(x - x_1) + y_1 \quad \text{where} \quad m = (3x_1^2 + A)(2y_1)^{-1};$$

again, we assume that $F$ is not characteristic 2. The same substitution as above, along with the knowledge that $x_1$ is a solution, yields

$$\begin{aligned} 0 &= x^3 + Ax + B - (m(x - x_1) + y_1)^2 \\ &= x^3 - m^2x^2 + \alpha x + \beta \\ &= (x - x_1)(x^2 + (x_1 - m^2)x + \gamma) \end{aligned}$$

with $\alpha, \beta, \gamma$ defined the same way with respect to $m$. Since

$$\begin{aligned} x_1^2 + (x_1 - m^2)x_1 + \gamma &= x_1^2 + (x_1 - m^2)x_1 + x_1(x_1 - m^2) + \alpha \\ &= x_1^2 + 2x_1(x_1 - m^2) + A + 2m^2x_1 - 2my_1 \\ &= 3x_1^2 + A - (3x_1^2 + A) \\ &= 0, \end{aligned}$$

we see that $x_1$ is also a solution to the quadratic, and thus a double root of the cubic, so we can factor it out again, yielding

$$x_3 = m^2 - x_1 - x_2 \quad \text{and} \quad y_3 = m(x_1 - x_3) - y_1$$

so we let $P_3 = (x_3, y_3)$ and say $P_1 + P_2 = P_3$.

If $P_2 = O$ then the line through $P_1$ and $O$ must be vertical, so it intersects $E$ at the reflection of $P_1$ across the $x$-axis. Reflecting across the $x$-axis again yields $P_1 + O = P_1$. Similarly $O + P_2 = P_2$, and we extend to $O + O = O$.

The symmetry in our geometric motivation and in these equations themselves makes it clear that this $+$ is commutative, that $O$ serves as an identity element, and that the reflection of a point across the $x$-axis serves as its additive inverse. We omit the proof here, but it can also be shown that this $+$ is associative, so $(E, +)$ is an abelian group.[5]

# 3 Discrete Logarithms

## 3.1 The Problem

Let $G$ be a multiplicative group. For $x \in G$ and $n \in \mathbb{Z}$, we use

$$x^n = \begin{cases} 1_G & \text{if } n = 0 \\ x^{n-1}x & \text{if } n > 0 \\ (x^{-1})^{-n} & \text{if } n < 0 \end{cases}$$

as our recursive definition of the $n$th power of $g$. Observing for $n > 0$ that

$$x^n = \begin{cases} (x^2)^{(n-1)/2}x & \text{if } n \text{ is odd} \\ (x^2)^{n/2} & \text{if } n \text{ is even} \end{cases}$$

leads us to an efficient algorithm for computing $x^n$.

If $n < 0$ then by definition $x^n = (x^{-1})^{-n}$, so let $x = x^{-1}$ and $n = -n$. If $n = 0$ then by definition $x^n = 1_G$, so return $1_G$. Otherwise, let $y = 1_G$. Clearly at this point $x^n = x^n y$, so if we keep $x^n y$ constant while changing our values of $x$, $n$, and $y$ then if we reduce $n$ to 1, we will have $xy$ equal to what we originally wanted to compute, so we can just return $xy$. Thus we will loop while $n > 1$. If $n$ is even then $x^n = (x^2)^{n/2}$, so let $x = x^2$ and $n = n/2$ and loop again. If $n$ is odd then $x^n y = (x^2)^{(n-1)/2}xy$, so let $y = xy$ and $x = x^2$ and $n = (n-1)/2$ and loop again. After the loop, we have $x^n = x^1 = x^0 x = x$, so return $xy$.

Using a binary representation of $n$, we can compute $n/2$ and $(n-1)/2$ very efficiently using simple bit operations. Each time we do this, we reduce the size of $n$ by at least one bit, so the number of steps in our loop will be less than or equal to the number of bits in $n$. At each step, we compute $x^2$ and possibly $xy$. If we can compute these operations in constant time then the algorithm has the very reasonable time complexity $O(\log n)$.

For $a, b \in G$ and $k \in \mathbb{Z}$, we say that $k$ is a discrete logarithm of $a$ to the base $b$ if $b^k = a$; we write $k = \log_b a$. While it is easy to compute $a$ given $b$ and $k$ using the algorithm described above, in general there is no efficient method known to compute $k$ given $a$ and $b$. Many cryptographic applications are based on the difficulty of this problem. The elliptic curves used in cryptography are used because they are not believed to be susceptible to some less general but more efficient methods for computing discrete logarithms.

## 3.2 Index Calculus

The index calculus algorithm can be used to find discrete logarithms in $\mathbb{Z}_q^*$ for $q$ prime, in subexponential time as opposed to other algorithms which work in more general groups but take exponential time.[7] It makes use of the notion of prime numbers, of which there is no analog in elliptic curve groups.

Let $g \in \mathbb{Z}_q^*$ be our base. We will assume that $g$ is a primitive root modulo $q$, which just means that $\langle g \rangle = \mathbb{Z}_q^*$. For $x \in \mathbb{Z}_q^*$ and $m, n \in \mathbb{Z}$ with $m = \log_g a$ and $n = \log_g a$, we have $g^m = g^n = a$, so $m \equiv n \pmod{|\mathbb{Z}_q^*|}$. We know $|\mathbb{Z}_q^*| = q - 1$, so $\log_g a$ can be thought of as a unique element of $\mathbb{Z}_{q-1}$.

For $x, y \in \mathbb{Z}_q^*$, if $m = \log_g x$ and $n = \log_g y$ then

$$b^m = x, \quad b^n = y \quad \Rightarrow \quad b^{m+n} = xy \quad \Rightarrow \quad m + n = \log_g xy;$$

in other words, $\log_g x + \log_g y = \log_g xy$. Thus if we can factor $x \in \mathbb{Z}_q^*$ into a product of things of which we know the discrete logarithms to the base $g$, then we can sum those to obtain the discrete logarithm of $x$.

We start by choosing a factor base $B \subseteq \mathbb{Z}_q^*$ of elements whose discrete logarithms we will compute first. A typical choice is

$$B = \{-1, \underbrace{2, 3, 5, 7, 11, \ldots, p_r}_{\text{the first } r \text{ primes}}\} \quad \Rightarrow \quad |B| = r + 1.$$

We know that each element in $B$ has a unique discrete logarithm in $\mathbb{Z}_{q-1}$. Let $k \in \mathbb{Z}^+$. If we can factor

$$g^k \bmod q = (-1)^{e_0} \cdot 2^{e_1} \cdot 3^{e_2} \cdots p_r^{e_r}$$

then we obtain a linear relation

$$k = e_0 \log_g(-1) + e_1 \log_g 2 + e_2 \log_g 3 + \cdots + e_r \log_g p_r$$

which we can write as a row matrix

$$\begin{bmatrix} e_0 & e_1 & e_2 & \cdots & e_r & \bar{k} \end{bmatrix} \in {\mathbb{Z}_{q-1}}^{1 \times (r+2)} \quad \text{where} \quad \bar{k} = k \bmod (q-1).$$

Thus we keep a list of the rows we've decided to keep so far, and try many $k$. If we can't factor $g^k \bmod q$ then we move on; otherwise we obtain a new row. We use Gaussian elimination with the rows we have so far to remove as many leading columns in the new row as we can. If the leading coefficient

$e_i$ in this reduced row is a unit in $\mathbb{Z}_{q-1}$ then we multiply by the row by $e_i^{-1}$, add it to our list of rows, and continue; otherwise we discard it and move on. We continue until we have an $(r+1) \times (r+2)$ matrix in row echelon form, which we can then easily convert to reduced row echelon form to obtain the discrete logarithms for all of $B$.

Now we compute $\log_g h$ for $h \in \mathbb{Z}_q^*$. Let $s \in \mathbb{Z}^+$. If we can factor

$$g^s h \bmod q = (-1)^{f_0} \cdot 2^{f_1} \cdot 3^{f_2} \cdots p_r^{f_r}$$

then

$$\log_g h = f_0 \log_g(-1) + f_1 \log_g 2 + f_2 \log_g 3 + \cdots + f_r \log_g p_r - s,$$

so once again we try many $s$ in parallel until we find something we can factor, and then we're done.

The index calculus tends to be much faster than other methods when it can be applied. However, it depends heavily on the structure of $\mathbb{Z}_q^*$ and there is no known adaptation of it that works for arbitrary elliptic curves, which makes the latter attractive for cryptography.

# 4 Applications

## 4.1 Cryptography

Cryptographic systems are traditionally explained in terms of actors Alice, Bob, and Eve with specific roles. Alice wants to send a message to Bob. Bob wants to know that the message is truly from Alice. Eve wants to read or spoof the message Alice is sending to Bob. The goal of the system is to facilitate Alice's goal and Bob's goal while hindering Eve's goal.

If Alice and Bob do not already have a physically secure channel which they can use to communicate with each other, then they must use a public channel and thus must encrypt their communication if they wish it to be private. If they both knew a shared secret key then they could use it in a symmetric encryption scheme such as AES. Diffie-Hellman key exchange allows Alice and Bob to agree on a secret key solely using communication over a public channel, without anyone else knowing what that secret key is.[8]

First Alice and Bob agree on an elliptic curve $E$ over a finite field $F$ such that the discrete logarithm is difficult in $E$. They also agree on some $P \in E$

such that $|\langle P\rangle|$ is large. There are methods to determine the orders of $E$ and $P$, but we do not discuss them here.[5]

Alice and Bob separately generate random integers $a$ and $b$, respectively. Alice computes $aP$ and sends it to Bob, and Bob computes $bP$ and sends it to Alice. These are just the $a$th and $b$th powers of $P$ expressed in additive notation, which is conventional for elliptic curve groups. Then Alice can compute $a(bP)$ and Bob can compute $b(aP)$, which are equal by properties of exponents, so they can use this shared point $abP \in E$ as their secret key.

Note that Eve observes $E$ and $P$ and $aP$ and $bP$. If Eve can solve the discrete logarithm problem in $E$ then she can compute $a$ or $b$ and thus $abP$, but the discrete logarithm problem is believed to be difficult over elliptic curves. It is not known if there is a way for an eavesdropper to compute $abP$ without solving the discrete logarithm problem.[5]

This algorithm is actually specifically the elliptic curve Diffie-Hellman key exchange algorithm. The original Diffie-Hellman key exchange algorithm uses $\mathbb{Z}_p^*$ for some prime $p$ instead of using an elliptic curve group, making it susceptible to attacks such as the index calculus. Indeed, in 2015 a vulnerability called Logjam was discovered, and the primary recommended defense against this vulnerability is to switch to elliptic-curve Diffie-Hellman.[9]

## 4.2 Primality

Let $n \in \mathbb{Z}^+$. If $n$ is prime then $\mathbb{Z}_n$ is a field, allowing us to pick $A, B \in \mathbb{Z}_n$ and define an elliptic curve $E$ by $y^2 = x^3 + Ax + B$. If $n$ is composite then we can still choose $A, B \in \mathbb{Z}_n$ and define

$$E = \{O\} \cup \{(x, y) \in \mathbb{Z}_n \times \mathbb{Z}_n \mid y^2 = x^3 + Ax + B\},$$

but the group law we defined above could fail because there may exist some $P_1 = (x_1, y_1) \in E$ and $P_2 = (x_2, y_2) \in E$ with $x_1 \neq x_2$ but $x_2 - x_1 \notin \mathbb{Z}_n^*$. However, if our goal is to generate a proof of the primality or compositeness of $n$, then we can simply insert an extra step into our procedure for adding points on $E$. We use the extended Euclidean algorithm to find modular inverses, so if any calculation turns up some $k \in \mathbb{Z}_n$ with $k \neq 0$ and $\gcd(n, k) \neq 1$, then the computed $\gcd(n, k)$ is a nontrivial factor of $n$, so we can return it immediately as a proof of compositeness.

We will make use of a proposition. Let $m \in \mathbb{Z}$. If there is a prime $q$ with $q \mid m$ and $q > (\sqrt[4]{n} + 1)^2$, and there is a point $P \in E$ such that $mP = O$, and $(m/q)P$ is well-defined and not equal to $O$, then $n$ is prime. We omit the proof of this proposition; it uses a theorem about $|E|$ assuming $E$ is a group, and some details regarding computation in $E$.[5]

The Goldwasser-Kilian algorithm works as follows.[5] First choose a random $P = (x, y) \in \mathbb{Z}_n \times \mathbb{Z}_n$. We can generate a curve that contains this point by choosing a random $A \in \mathbb{Z}_n$ and letting $B = y^2 - x^3 - Ax$. This defines an elliptic curve $E$ as discussed above. Assuming $n$ is prime, $E$ is a group, so we can apply an algorithm such as Schoof's algorithm to find $|E|$.[5] Again, if this point-counting algorithm fails, it will produce a nontrivial factor of $n$. If it returns a value $m \in \mathbb{N}$ then we proceed.

We try to factor $m = kq$ where $k \geq 2$ is a small integer and $q$ is a number that we believe to be prime. For instance, if we have applied some fast probabilistic primality test to $q$ which hasn't found it to be composite, then we will guess that it is prime and proceed. If we fail to find such a factorization, we start over with a different random point and curve. Now at this point, we have $m$ and $q$ with $q$ large enough to satisfy the proposition.

Then we calculate $mP$ and $(m/q)P = kP$. Assuming we don't find a nontrivial factor of $n$ in the process, we use these results to determine the primality of $n$. If $mP \neq O$ then $E$ is not a group, because if it were then we would have $m = |E|$ by Schoof's algorithm and thus $mP = O$ by Lagrange; thus $n$ is composite. If $kP = O$ then we start over. Otherwise, we have satisfied the conditions of the proposition, so we can return $(A, B, m, q, P)$ as a certificate that anyone can easily use to verify that $n$ is prime. The only thing remaining is the assumption that $q$ is prime. To determine this, we run the same algorithm recursively using $q$ as the parameter, and include the returned certificate in our certificate. The recursion stops when we reach a prime small enough to verify by other means.

# References

[1] Commercial National Security Algorithm Suite and Quantum Computing FAQ U.S. National Security Agency, January 2016.

[2] Hardy, Godfrey Harold (1940), *A Mathematician's Apology*, Cambridge University Press, ISBN 978-0-521-42706-7

[3] Agrawal, Manindra; Kayal, Neeraj; Saxena, Nitin (2004). "PRIMES is in P". *Annals of Mathematics.* **160** (2): 781–793. doi:10.4007/annals.2004.160.781. JSTOR 3597229.

[4] Goldwasser, Shafi, Kilian, Joe, *Almost All Primes Can Be Quickly Certified*, `http://www.iai.uni-bonn.de/~adrian/ecpp/p316-goldwasser.pdf`

[5] Lawrence Washington (2003). *Elliptic Curves: Number Theory and Cryptography.* Chapman & Hall/CRC. ISBN 1-58488-365-0.

[6] `https://www.desmos.com/calculator/ialhd71we3`

[7] L. Adleman, *A subexponential algorithm for the discrete logarithm problem with applications to cryptography*, In 20th Annual Symposium on Foundations of Computer Science, 1979

[8] Diffie, W.; Hellman, M. (1976). "New directions in cryptography". *IEEE Transactions on Information Theory.* **22** (6): 644–654. doi:10.1109/TIT.1976.1055638.

[9] "The Logjam Attack". *weakdh.org.* 2015-05-20.