Introduction to Groups and Elliptic Curves

Tim Carstens\textsuperscript{1}  Kevin Wilson\textsuperscript{2}

\textsuperscript{1}University of Utah
Department of Mathematics

\textsuperscript{2}Princeton University
Department of Mathematics

Toorcamp
July 2009
1 Basic Group Theory
2 Basic Cryptography
3 Where do groups come in?
4 Elliptic Curves
5 Factorization
6 Identity-Based Encryption
7 The Technicalities
Examples

What do these things have in common?

- The integers: \( \ldots, -2, -1, 0, 1, 2, \ldots \)
- The integers mod 5: 0, 1, 2, 3, 4
- The real numbers: \( \pi, \frac{4}{3}, 7, \ldots \)
- Invertible matrices
- Permutations of sets
The answer: They form a group.

Definition

A **group** $G$ is a set along with a binary operator $m : G \times G \rightarrow G$ (multiplication) and a unary operator $i : G \rightarrow G$ (inversion) and a distinguished element $e \in G$ (the identity) such that for all $g, h, k \in G$

- **Inverse Law** $m(g, i(g)) = m(i(g), g) = e$
- **Identity Law** $m(g, e) = m(e, g) = g$
- **Associativity** $m(g, m(h, k)) = m(m(g, h), k)$

A group is called **abelian** provided that $m(g, h) = m(h, g)$ for all $g, h \in G$. 
Example: Integers

The integers form a group under addition:

\[ 2 + 5 = 7 \]

<table>
<thead>
<tr>
<th>Inversion</th>
<th>Identity</th>
<th>Abelian</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 0 = 7 + (-7) )</td>
<td>( 7 = 0 + 7 )</td>
<td>( 7 = 3 + 4 )</td>
</tr>
<tr>
<td>( 0 = (-7) + 7 )</td>
<td>( 7 = 7 + 0 )</td>
<td>( 7 = 4 + 3 )</td>
</tr>
</tbody>
</table>

**Associativity**

\[ 7 = 3 + 4 = (1 + 2) + 4 \]
\[ 7 = 1 + 6 = 1 + (2 + 4) \]
Example: Modular Arithmetic

The integers mod $N$ for any $N \in \mathbb{Z}_{>0}$ form a group:

\[ 6 + 13 \equiv 4 \pmod{5} \]

<table>
<thead>
<tr>
<th>Inversion</th>
<th>Identity</th>
<th>Abelian</th>
</tr>
</thead>
<tbody>
<tr>
<td>$0 \equiv 1 + 4$</td>
<td>$3 \equiv 0 + 3$</td>
<td>$2 \equiv 1 + 6$</td>
</tr>
<tr>
<td>$0 \equiv 4 + 1$</td>
<td>$3 \equiv 3 + 0$</td>
<td>$2 \equiv 6 + 1$</td>
</tr>
</tbody>
</table>

**Associativity**

\[ 2 \equiv 3 + 4 \equiv (1 + 2) + 4 \]
\[ 2 \equiv 1 + 1 \equiv 1 + (2 + 4) \]
Example: Fractions

The rational numbers (minus 0) form a group under multiplication:

\[
\frac{2}{5} \cdot \frac{7}{3} = \frac{14}{15}
\]

**Inversion**

\[
1 = \frac{2}{3} \cdot \frac{3}{2}
\]

**Identity**

\[
5 = 5 \cdot 1
\]

**Abelian**

\[
5 = \frac{5}{2} \cdot 2
\]

**Associativity**

\[
24 = 2 \cdot 12 = 2 \cdot (3 \cdot 4)
\]
\[
24 = 6 \cdot 4 = (2 \cdot 3) \cdot 4
\]
Example: Finite Fields

A more exotic example is the set \((\mathbb{Z}/p\mathbb{Z})^\times = (\mathbb{Z}/p\mathbb{Z}) - \{0\}\) with the obvious multiplication.

This obviously satisfies every group axiom except inversion.

To find the inverse of \(0 < a < p\), use Euclid’s algorithm to find \(x, y \in \mathbb{Z}\) such that \(ax + py = 1 = \gcd(a, p)\). Then

\[
ax + py \equiv ax \equiv 1 \mod p
\]

It is crucial here that \(p\) is a prime. (Why?)
Example: Matrices

Invertible matrices (det ≠ 0) form a group under multiplication. This group is not abelian:

\[
\begin{bmatrix}
1 & 1 \\
0 & 1 \\
\end{bmatrix}
\begin{bmatrix}
2 & 0 \\
0 & 5 \\
\end{bmatrix}
= 
\begin{bmatrix}
2 & 5 \\
0 & 5 \\
\end{bmatrix}
\]

\[
\begin{bmatrix}
2 & 0 \\
0 & 5 \\
\end{bmatrix}
\begin{bmatrix}
1 & 1 \\
0 & 1 \\
\end{bmatrix}
= 
\begin{bmatrix}
2 & 2 \\
0 & 5 \\
\end{bmatrix}
\]
Our examples of groups all use the $+$ and the $\cdot$ sign for the binary operation $m$.

When working with an abstract group, mathematicians usually use the $\cdot$ sign, with the usual convention of dropping it.

However, for an abstract group, the following three expressions mean the same thing:

$$m(g, h) \quad g \cdot h \quad gh \quad g + h$$
Algebra is one of the major methods by which mathematical results are proved.

Groups are an integral part of this formalism.

They come in many flavors: finite, Lie, algebraic, . . .

Many classes of groups (e.g., finite groups) have been enumerated.
Importance to Computer Science

- Fourier transforms are maps between two groups
  - $\mathbb{R}$ (frequency space) $\rightarrow \mathbb{R}$ (phase space)
  - $(\mathbb{Z}/2\mathbb{Z})^N \rightarrow (\mathbb{Z}/2\mathbb{Z})^N$ (fast multiplication)
  - $S^1$ (the circle) $\rightarrow \mathbb{Z}$

- Linked lists form an almost-group (inverses don’t work)

- Cryptography
Basic Group Theory

Basic Cryptography

Where do groups come in?

Elliptic Curves

Factorization

Identity-Based Encryption

The Technicalities
How to Encrypt

Public Key → One Way Fn → Cipher Text

Plain Text → One Way Fn → Cipher Text
How to Decrypt

Private Key → Inverse Fn → Plain Text

Cipher Text → Private Key

Groups and Curves
Toorcamp '09
Tim Carstens, Kevin Wilson

Basic Group Theory
Basic Cryptography
Where do groups come in?
Elliptic Curves
Factorization
Identity-Based Encryption
The Technicalities
A function is essentially a look up table

<table>
<thead>
<tr>
<th>Plaintext</th>
<th>$x$</th>
<th>$f(x)$</th>
<th>Ciphertext</th>
</tr>
</thead>
<tbody>
<tr>
<td>$11432$</td>
<td>$2$</td>
<td>$0$</td>
<td>$44210$</td>
</tr>
<tr>
<td>$0$</td>
<td></td>
<td>$3$</td>
<td></td>
</tr>
<tr>
<td>$1$</td>
<td></td>
<td>$4$</td>
<td></td>
</tr>
<tr>
<td>$3$</td>
<td></td>
<td>$1$</td>
<td></td>
</tr>
<tr>
<td>$4$</td>
<td></td>
<td>$2$</td>
<td></td>
</tr>
</tbody>
</table>
Problems with look ups

- Only handle finite lists
- Hard to store
- Unwieldy to search
- For security, if look up table is compromised, the system is compromised.
An Alternative Approach

Instead of having a look-up, we can define a function based on a computable group structure:

\[
\begin{array}{|c|c|}
\hline
x & f(x) \\
\hline
0 & 3 \\
1 & 4 \\
2 & 0 \\
3 & 1 \\
4 & 2 \\
\hline
\end{array}
\]

\[
f : \mathbb{Z}/5\mathbb{Z} \rightarrow \mathbb{Z}/5\mathbb{Z}
\]

\[
f(x) = (x + 3) \% 5
\]
This kind of cipher (add $m \mod n$) is called a \textit{Caesar cipher}.

Statistically cracked around 1935 by Freedman.

One of the first appearances of information theory and modern notions of security.
One-way functions

In cryptography, the function from plaintext to ciphertext should be:

- Easy to calculate
- Hard to invert (without additional secret: the key)

This is a one-way function.
Famous one-way functions

- Hash functions (SHA, MD5, ...)
  - Hash functions (at least these) tend to compress their input.
  - Cryptographic one-way functions should be invertible
- Multiplication of integers
  - This is invertible and used in RSA.
- Discrete log
1. Basic Group Theory
2. Basic Cryptography
3. Where do groups come in?
4. Elliptic Curves
5. Factorization
6. Identity-Based Encryption
7. The Technicalities
ElGamal: Discrete log in action

Suppose Bob wants to send a message \( m \in \mathbb{Z}/N\mathbb{Z} \) to Alice.

- Alice and Bob agree on \( 1 \in \mathbb{Z}/N\mathbb{Z} \)
- Alice chooses a random number \( k \in \{0, 1, \ldots, N - 1\} \)
- Alice sends Bob \( p = 1 \cdot k \mod N \) (public key)
- Bob chooses a random number \( \ell \in \{0, 1, \ldots, N - 1\} \)
- Bob computes \( s = p \cdot \ell \mod N \)
- Bob sends \((m + s, 1 \cdot \ell)\) to Alice
- Alice gets \( m \) by computing \((m + s) - (1 \cdot \ell \cdot k) = m\)
Example

\[ N = 12 \]

- Alice chooses \( k = 2 \)
- Alice sends Bob \( p = 2 \)
- Bob chooses \( \ell = 6 \)
- Bob computes \( s = 2 \cdot 6 \% 12 = 0 \)
- To send the message \( m = 9 \), Bob sends \((9, 6)\)
- Alice recovers \( m \) by computing \( 9 - 6 \cdot 2 \equiv 9 \mod 12 \).
Ups and Downs

Good things:
- It works
- It’s fast
- Public/Private key infrastructure

Bad things:
- It is *not* secure!
How to fix

The problem is one of representation:

- Private key is $k$.
- $1 \cdot k = k$, so there is no obfuscation.
A Different Representation

Let \( q \) be a prime number. Then \( (\mathbb{Z}/q\mathbb{Z})^\times \) is a group under multiplication.

\[
\begin{array}{c|cccccc}
\times & 1 & 2 & 3 & 4 & 5 & 6 \\
\hline
1 & 1 & 2 & 3 & 4 & 5 & 6 \\
2 & 2 & 4 & 6 & 1 & 3 & 5 \\
3 & 3 & 6 & 2 & 5 & 1 & 4 \\
4 & 4 & 1 & 5 & 2 & 6 & 3 \\
5 & 5 & 3 & 1 & 6 & 4 & 2 \\
6 & 6 & 5 & 4 & 3 & 2 & 1 \\
\end{array}
\]

Note: For every \( n \in \{1, 2, 3, 4, 5, 6\} \) there is some \( m \in \{1, 2, 3, 4, 5, 6\} \) such that \( n = 3^m \). We write \( m = \log_3(n) \).
Cyclic groups

Definition
A group $G$ is called cyclic provided that there exists $\omega \in G$ such that for every $g \in G$ there exists $n \in \mathbb{Z}$ such that $g = \omega^n$.

- All cyclic groups look like $\mathbb{Z}$ or $\mathbb{Z}/N\mathbb{Z}$ for some $N$.
- If we represented our group this way, finding discrete logs is not hard.
- So we must disguise the group so that multiplication is still easy but finding logs is hard.
Suppose Bob wants to send a message $m \in (\mathbb{Z}/q\mathbb{Z})^\times$ to Alice.

- Alice and Bob agree on $\omega \in (\mathbb{Z}/q\mathbb{Z})^\times$ such that for all $n \in (\mathbb{Z}/q\mathbb{Z})^\times$ there exists $m \in \{0, \ldots, q - 1\}$ such that $n = \omega^m$ (these always exist).
- Alice chooses a random number $k \in \{0, 1, \ldots, q - 1\}$
- Alice sends Bob $p = \omega^k \% q$ (public key)
- Bob chooses a random number $\ell \in \{0, 1, \ldots, q - 1\}$
- Bob computes $s = p^\ell \% q$, $c = m^s$, $d = \omega^\ell$
- Bob sends $(c, d)$ to Alice
- Alice gets $m$ by computing $(c(d^k))^{-1} \mod q$
Example: Redux

\[ q = 7 \quad \omega = 3 \]

- Alice chooses \( k = 5 \)
- Alice sends Bob \( p = 3^5 \% 7 = 5 \)
- Bob chooses \( \ell = 2 \)
- To send the message \( m = 4 \), Bob computes
  - \( s = 5^2 \% 7 = 4 \)
  - \( c = 4^4 \% 7 = 4 \)
  - \( d = 3^2 \% 7 = 2 \)
- Bob sends \((c, d) = (4, 2)\) to Alice
- Alice recovers \( m \) by computing \((4(2^5))^{-1} = 2^{-1} = 4\).
Ups and Downs: Redux

Good things:
- It works
- It’s fast
- Public/Private key infrastructure
- Generally considered secure (for huge q).
Where are the groups?

Discrete Log is a problem about *groups*:

**Definition (Discrete Log Problem)**

Let $G$ be a finite cyclic group and let $\omega$ be a generator. Given $g \in G$ the *discrete log problem* is the problem of finding $n \in \mathbb{Z}$ such that $\omega^n = g$.

- We rig group multiplication (aided by repeated squaring) to be easy.
- Abstractly, the discrete log problem is hard.
- Concretely, we’ve seen that “hard” can depend on the representation of the group.
Basic Group Theory

Basic Cryptography

Where do groups come in?

Elliptic Curves

Factorization

Identity-Based Encryption

The Technicalities
We’ve seen one way of representing certain cyclic groups: $(\mathbb{Z}/q\mathbb{Z})^\times$ for $q$ prime.

- The $q$ needed for cryptographic purposes must be huge.
- Consequently, computation is slow and storage is an issue.
- There is no way known to find a generator.
- Unknown whether you can expect to find one quickly.
Elliptic curves offer one (perhaps the best current) solution.

- Elliptic curves are geometric objects that admit a group structure.
- They are almost as ubiquitous in mathematics as groups are.
Really though, What *is* an elliptic curve?

For our purposes, an elliptic curve is the graph of an equation:

\[ y^2 = x^3 + ax + b \]

which doesn’t have any kinks.

**Good Example**

\[ y^2 = x^3 - x \]

**Bad Example**

\[ y^2 = x^3 - \frac{1}{3}x + \frac{2}{27} \]
Group Law

Note that (almost) every line through two points of an elliptic curve intersects the curve in a (unique!) third point.

This observation is actually a very general fact which we will discuss later.
Step 1: Given two points $P, Q \in E$, draw the line between them.
Group Law

- Step 1: Given two points $P, Q \in E$, draw the line between them.
- Step 2: If $R$ is the third point on the line $PQ \cap E$, then draw the vertical line through $R$. 

![Diagram of Group Law](image)
Group Law

- Step 1: Given two points $P, Q \in E$, draw the line between them.
- Step 2: If $R$ is the third point on the line $\overline{PQ} \cap E$, then draw the vertical line through $R$.
- Step 3: Say $P + Q$ is the unique other point on this vertical line.
This description of the group law can be summed up as follows:

**Theorem**

Let $E$ be an elliptic curve. The group law on $E$ is determined by a choice $I \in E$ of an identity point and declaring that if three points of $P, Q, R \in E$ lie on the same line (counted with multiplicity) then

$$P + Q + R = I.$$
Group Law: Identity

- We will always choose the “point at infinity” as the identity of the elliptic curve.
- For our purposes, a line through the point at infinity is a vertical line.
- Going through the motions, we see this is actually an identity!
Given $P \in E$, $-P$ is the other point on the vertical line through $P$:

$$P + Q + I = I \iff P = -Q$$
When we say “draw the line between a point and itself” we mean “draw the line tangent to the curve at that point.”
Group Law: Explicitly

\[ E = \{ y^2 = x^3 + ax + b \} \quad P = (x_P, y_P) \quad Q = (x_Q, y_Q) \]

Then \( R = (x_R, y_R) \) is given by:

\[
\begin{align*}
    x_P &\neq x_Q & P &= Q & P &= -Q \\
    s &= (y_Q - y_P)/(x_Q - x_P) & s &= (3x_P^2 + a)/(2y_P) \\
    x_R &= s^2 - x_P - x_Q & x_R &= s^2 - 2x_P & x_R &= \infty \\
    -y_R &= y_P + s(x_R - x_P) & -y_R &= y_P + s(x_R - x_P) & y_R &= \infty 
\end{align*}
\]
Why Do Mathematicians Care?

- Like groups, elliptic curves are one of the most important objects in mathematics.
- Where they show up:
  - Finding the circumference of an ellipse
  - Doubly-periodic functions on $\mathbb{C}$
  - Fermat’s Last Theorem
  - Modular forms
  - Representation theory
  - The list goes on and on and on...
Why Do You Care?

- We will soon see that with a few modifications, it is easy to find a point on an elliptic curve of large finite order, i.e., a point \( P \in E \) such that \( NP = I \) for some large \( N \) and for no \( 0 < n < N \).
- Computation on elliptic curves is neither too quick nor too slow.
- To our knowledge, there are no known attacks on the general elliptic curve discrete log problem.
Implementing ElGamal

Recall the definition of the discrete log problem:

**Definition (Discrete Log Problem)**

Let \( G \) be a finite cyclic group and let \( \omega \) be a generator. Given \( g \in G \) the *discrete log problem* is the problem of finding \( n \in \mathbb{Z} \) such that \( \omega^n = g \).

By definition, any point \( P \in E \) generates a cyclic group. But over \( \mathbb{C} \), it is very hard to find a point of *finite order*!
Implementing ElGamal

One way of fixing the problem is to turn $E$ into a (large) finite group (where it is easy to find points of large order).

To do this, we need there to be a finite number of solutions of the equation

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

This is (provably!) impossible over $\mathbb{C}$. But what about something else?
Implementing ElGamal

In the previous slides, the only thing special about \( \mathbb{C} \) and \( \mathbb{R} \) is that they are fields:

**Definition**

A **field** is a quintuple \((F, +, \cdot, 0, 1)\) such that

- \((F, +)\) is an abelian group with identity 0
- \((F^\times = F - \{0\}, \cdot)\) is an abelian group with identity 1
- Distributive Law: \(a(b + c) = ab + ac\)
Let \( p \) be a prime number. We have already seen:

- \( \mathbb{Z}/p\mathbb{Z} \) is a group under addition.
- \( (\mathbb{Z}/p\mathbb{Z})^\times \) is a group under multiplication.
- The distributive law holds.

That is, \( \mathbb{Z}/p\mathbb{Z} \) is a field with its natural operations.
Potential Problems

The explicit group law we wrote down still makes sense over \( \mathbb{Z}/p\mathbb{Z} \)! Thus, \( E \) is a group.

Later we will see that elliptic curves live in what mathematicians call the *projective plane*.

The projective plane over \( \mathbb{Z}/p\mathbb{Z} \) has \( p^2 + p + 1 \) points. Therefore, and elliptic curve over \( \mathbb{Z}/p\mathbb{Z} \) has at most \( p^2 + p + 1 \) points.

That is, an elliptic curve over \( \mathbb{Z}/p\mathbb{Z} \) is a *finite group*!
Recall that one problem with using \((\mathbb{Z}/p\mathbb{Z})^\times\) as a group for ElGamal was that it was hard to find a generator. Why is \(E\) better?

- \(E\) is usually not cyclic, but “most” points have near-maximal order.
- Indeed, Schoof’s algorithm for counting \(|E|\) amounts to choosing a random point and powering it.
- This allows us to use the discrete log problem for cryptographic purposes.
Problems with elliptic curves

- Computations can be unwieldy in small devices
- There are cracks for certain classes of elliptic curves
- Elliptic curves have a huge amount of structure (it’s why they are such rich mathematical objects). So it seems likely that somebody will figure out some general crack eventually (but not in the near future).
Why Elliptic Curves?

They fit the bill!

- The group law is easy to calculate.
- In the general case, there is no known way to exploit the structure of the elliptic curve to speed up the discrete log calculation.
- Being well-studied mathematical objects, we have many examples of cryptological strength.
Basic Group Theory

Basic Cryptography

Where do groups come in?

Elliptic Curves

Factorization

Identity-Based Encryption

The Technicalities
Let

\[ E = \{ y^2 = x^3 + ax + b \} \]

be an elliptic curve over \( \mathbb{Z}/n\mathbb{Z} \). If \( n \) is composite, the elliptic curve fails to have a group structure since \( k \mid n \) implies \( \frac{1}{k} \) does not exist mod \( n \).

The basic idea:

*To factor \( n \), pick a random point \( P \) on the curve and compute

\[ k \cdot P = P + \cdots + P. \]

*If the process breaks along the way, it is because we lucked into a factor of \( n \).*
Why should this work?

- Adding points requires us to invert some numbers modulo $n$.
- $m$ is invertible mod $n$ if and only if $\gcd(m, n) = 1$.
- In the course of computing $k \cdot P$, we wind up computing $\gcd(m, n)$ for several choices of $m$. 
An example (Trappe and Washington)

Factor $n = 455839$ using the curve $y^2 = x^3 + 5x - 5$ with the point $P = (1, 1)$ by computing $(10!)P$. 

Along the way, we are able to compute $2P$, $(3!)P$, $(4!)P$, and so forth. But to compute $(8!)P$ we must invert 599 modulo $n$. We find that 

$$\text{gcd}(599, n) = 599 \neq 1$$

In fact $n = 599 \cdot 761$. 
1. Basic Group Theory
2. Basic Cryptography
3. Where do groups come in?
4. Elliptic Curves
5. Factorization
6. Identity-Based Encryption
7. The Technicalities
One major problem of public key crypto is key management:

- Recipients must have a public key *before* they can receive encrypted messages
- Usually hard to recover keys if lost
- Obtaining a user’s public key can be logistically difficult
- Can’t anticipate a user’s future public key
Identity-Based Cryptography

In 1984, Shamir posed the problem of developing a cryptographic system where keys are a function of a user’s “identity” (e.g., email address, SSN, phone, . . .).

He implemented a very basic scheme, which was tossed on the dust pile of history.

In 2001, Boneh and Franklin proposed a workable identity-based scheme. We will describe this.
Outline

As before:

- Alice is receiving a message.
- Bob is sending a message.
- Tom is a trusted third-party.

We need some mathy objects:

- A cyclic group $G$ of prime order $q$.
- A \textit{bilinear pairing} $e : G \times G \rightarrow \mathbb{Z}/q\mathbb{Z}$.
Definition

A \emph{bilinear pairing} \( e : G \times G \to H \) is a function of two arguments which satisfies the following conditions:

- \( e(P + P', Q) = e(P, Q)e(P', Q) \)
- \( e(P, Q + Q') = e(P, Q)e(P, Q') \)

In particular, \( e(aP, bQ) = e(P, Q)^{ab} \).

The easiest example to think of is the dot product on \( \mathbb{R}^2 \):
\[ e((x_1, y_1), (x_2, y_2)) = x_1x_2 + y_1y_2. \]
The Scheme

Public knowledge:

1. Tom publishes a generator \( \omega \in G \).
2. Tom chooses a random number \( s \in \{1, 2, \ldots, q - 1\} \).
3. Tom publishes Global = \( \omega^s \).
4. Tom does not publish the “master key” \( s \).

Alice gets her keys:

1. Alice’s public key is some function of her email: \( Alice \in G \)
2. Alice asks Tom for her private key.
3. Tom sends back Private = \( Alice^s \).
The Scheme: Continued

Bob sends a message $m \in \mathbb{Z}/q\mathbb{Z}$:

1. Bob computes $Alice \in G$.
2. Bob chooses a random $r \in \{1, 2, \ldots, q - 1\}$.
3. Bob sends a pair of data $(\omega^r, m \cdot e(Alice, Global))$.

Alice decrypts:

1. Alice receives $(u, v)$ from Bob.
2. Alice computes $v \cdot e(Private, u)^{-1}$.

$$e(Private, u) = e(Alice^s, \omega^r) = e(Alice, \omega)^{sr} = e(Alice, Global)^r$$
Where do groups come in?

Elliptic Curves

Factorization

Identity-Based Encryption

The Technicalities
Some Notes

The Good:

- Recipients can get their public keys *after* receiving messages.
- Keys are a function of the identity of user, so they are easily recoverable.
- Senders can encrypt without asking anyone for a key.
- You can “encrypt for the future”, provided you trust Tom.

The Bad:

- Pairings can be slow to compute.
- Tom!
  - All users must rely on Tom for their keys.
  - If you know s, you can read all traffic.
Among other useful features, elliptic curves come naturally equipped with (lots of) bilinear pairings: the *Weil pairing*. The description of this pairing is entirely abstract, though it is eminently computable.

We won’t define it, as doing so would require words like “Riemann-Roch”, “genus”, “divisor”, “degree zero”, . . . to be introduced. This is more than many mathematicians would ever want to know.
1. Basic Group Theory
2. Basic Cryptography
3. Where do groups come in?
4. Elliptic Curves
5. Factorization
6. Identity-Based Encryption
7. The Technicalities
The Group Law Makes Sense?

We made the following vague claim:

**Claim**

Every line intersects an elliptic curve in precisely three points.

This claim is patently false as it stands. However, with a little change of perspective, the following fact is true:

**Theorem (Bézout)**

A degree $d$ and degree $e$ curve in $\mathbb{P}_C^2$ intersect in precisely $de$ points (counted with multiplicity).

In this section, we attempt to explain these words.
Projective Space

In $\mathbb{R}^2$, two distinct lines either intersect in a single point or are parallel.

Projective 2-space $\mathbb{P}_\mathbb{R}^2$ is $\mathbb{R}^2$ with the added condition that two parallel lines with slope $m$ “intersect at infinity” with slope $m$.

We can do the same thing for $\mathbb{C}$. 
A point \( P \in \mathbb{P}^n_{\mathbb{C}} \) is an \((n + 1)\)-tuple \([z_0 : z_1 : \cdots : z_n]\).

- We do not allow \( z_0 = z_1 = \cdots = z_n = 0 \).
- We say \([z_0 : \cdots : z_n] = [w_0 : \cdots : w_n]\) provided that there is some \( \lambda \in \mathbb{C}^\times \) such that \( z_i = \lambda w_i \) for all \( i \).

An example of this last condition:

\[
[0 : 1 : 0] = [0 : 10 : 0] \quad [1 : 2 : 3] = [3 : 6 : 9]
\]
What Does a Line Look Like?

- In $\mathbb{C}^2$ a line is the graph of a function $ax + by + c = 0$.
- In $\mathbb{P}^2_{\mathbb{C}}$, a line is the graph of a function $ax + by + cz = 0$.
- If $z = 1$ we recover the original equation.
- If $z = 0$:
  - $b = 0$ is a vertical line; $[0 : 1 : 0]$ on line.
  - $b \neq 0$ is any other line; $[1 : m : 0]$ on line where $m$ is the slope of the line.
  - These are called the points at $\infty$. 
Let $ax + by + cz = 0$ and $Ax + By + Cz = 0$ be two lines.

**Lemma**

There is a unique point $[X : Y : Z] \in \mathbb{P}_C^2$ such that $aX + bY + cZ = AX + BY + CZ = 0$.

**Proof.**

If $ax + by + c = 0$ and $Ax + By + C = 0$ intersect in $\mathbb{C}^2$ (i.e., $z = 1$), then the lines have different slopes and the previous slide says they don’t intersect at $\infty$.

If $ax + by + c = 0$ and $Ax + By + C = 0$ do *not* intersect in $\mathbb{C}^2$, then they have the same slope, so they intersect at $\infty$.  \[\Box\]
Over a finite field, we can define projective space exactly the same way: $\mathbb{P}^2_{\mathbb{Z}/p\mathbb{Z}}$ consists of triples $[x : y : z]$.

- We do not allow $x = y = z = 0$.
- We say $[x : y : z] = [X : Y : Z]$ if and only if there exists $\lambda \in (\mathbb{Z}/p\mathbb{Z})^\times$ such that $x = \lambda X$, $y = \lambda Y$, $z = \lambda Z$.

Note that we can only look at the zero sets of homogeneous polynomials. (Why?)
Finite Fields and Elliptic Curves

We say an elliptic curve $E$ is the set of $[x : y : z] \in \mathbb{P}^2_{\mathbb{Z}/p\mathbb{Z}}$ such that

$$y^2z = x^3 + axz^2 + bz^3.$$ 

Note that this is a homogeneneous polynomial, so the set of points satisfying this equation makes sense.
Finite Fields and Elliptic Curves

Why is this method important?

- Unlike arithmetic over $\mathbb{C}$ and $\mathbb{R}$, computers are very good at modular arithmetic.
- The number of points in $\mathbb{P}^2_{\mathbb{Z}/p\mathbb{Z}}$ is finite (it is $p^2 + p + 1$)
- As $E \subseteq \mathbb{P}^2_{\mathbb{Z}/p\mathbb{Z}}$, we know $E$ must be a finite group. Thus, every point generates a finite cyclic group, which is what we need for the discrete log problem.
Variety and Degree

How do you generalize the notion of line to curve?

Definition

A (projective) variety is a subset of projective space cut out by a homogeneous polynomial equation. We say the degree of the variety is the degree of the defining polynomial.
An elliptic curve looks like $y^2z = x^3 + axz^2 + bz^3$ with $a^3 + 108b^2 \neq 0$. It is degree 3.

If $z = 0$ then we find $x^3 = 0$ so the only point at $\infty$ is $[0 : 1 : 0]$.

Recall: For our elliptic curve, we said the “line through $\infty$ and a point” was vertical. Why is that?
A Calculation

Let \([X : Y : 1] \in \mathbb{P}^2\) (e.g., a non-infinite point on an elliptic curve).

Suppose \(Ax + By + Cz = 0\) is a line in \(\mathbb{P}^2\) hitting \([0 : 1 : 0]\) and \([X : Y : Z]\).

- \(A \cdot 0 + B \cdot 1 + C \cdot 0 = 0 \Rightarrow B = 0\)
- So \(AX + C = 0\).
  - \(X = 0 \Rightarrow C = 0 \Rightarrow A = 1.\)
  - \(X \neq 0 \Rightarrow AC \neq 0 \Rightarrow A = 1.\)

In both cases, the line through these points is the \textit{vertical line} \(x = X.\)
Multiplicity

Multiplicity measures “how tangent” one variety is to another.
For our purposes, Bézout’s Theorem says that any line intersects an elliptic curve in precisely three points.

In this picture, we have $y^3 = y^2 + xy + x$ (degree 3) and $10x^2 + y^2 = 4$ (degree 2). There are $6 = 2 \cdot 3$ intersection points.
Group Law in Projective Coordinates

\[ E = \{ y^2z = x^3 + fx + g \} \]

\[ P = [X_P : Y_P : Z_P] \quad Q = [X_Q : Y_Q : Z_Q] \]

Anything but doubling:

\[ A = Y_Q Z_P - Y_P Z_Q \quad B = X_Q Z_P - X_P Z_Q \]

\[ C = A^2 Z_P Z_Q - B^3 - 2B^2 X_P Z_Q \]

\[ X = BC \quad Y = A (B^2 X_P Z_Q - C) - B^3 Y_P Z_Q \quad Z = B^3 Z_P Z_Q \]

Doubling:

\[ A = fZ_P^2 + 3Z_P^2 \quad B = Y_P Z_P \quad C = X_P Y_P B \quad D = A^2 - 8C \]

\[ X = 2BD \quad Y = A (4C - D) - 8Y_P^2 B^2 \quad Z = 8B^3 \]