Elliptic curves
Definition of a finite group

(G,*) is a \textbf{finite group} if:

1. G is a finite set.
2. For each \(a\) and \(b\) in G, also \(a*b\) is in G.
3. There is an \(e\) in G such that for all \(a\) in G,
   \[a*e = e*a = a.\]
4. For each \(a\) in G there is a \(b\) in G with
   \[a*b = b*a = e.\]
5. For all \(a, b\) and \(c\) in G, \((a*b)*c = a*(b*c)\).

The element \(e\) in 3 above is the \underline{identity} element of the group \((G,*)\).
Order of a group

The number of elements of a finite group \((G, \ast)\) is denoted by the symbol \(|G|\), and is said to be the order of the group.

For a finite group \((G, \ast)\) it can be computationally difficult to compute the order, \(|G|\), of the group.
Subgroup

Let \((G, \ast)\) be a group. If \(H\) is a subset of \(G\) and \((H, \ast)\) is also a group, then \((H, \ast)\) is said to be a **subgroup** of \((G, \ast)\).

**Theorem:** If \((H, \ast)\) is a finite group and if \(H\) is a subset of \(G\) such that
- \(H\) is nonempty and
- for any \(a\) and \(b\) in \(H\), also \(a \ast b\) is in \(H\).

Then \((H, \ast)\) is a subgroup of \((G, \ast)\).

**Theorem** (Lagrange): If \((G, \ast)\) is a finite group and if \((H, \ast)\) is a subgroup of \((G, \ast)\), then \(|H|\) is a factor of \(|G|\).
Abelian group and cyclic group

\((G,\ast)\) is an **Abelian group** if it is a group and for each \(a\) and \(b\) in \(G\), \(a \ast b = b \ast a\).

If it exists, the least \(n\) such that \(a^n = e\) is called the **order of \(a\) in \(G\)**.

For an element \(a\) of order \(n\) of the finite group \((G,\ast)\), let \(<a>\) denote the set \(\{a^i : i=0,1,2,\ldots,n-1\}\).

Then \(<a>\) is a subgroup of \(G\), generated by the element \(a\) of \(G\), and is said to be the **cyclic subgroup** of \(G\) generated by \(a\). The element \(a\) is called a **generator** of \(<a>\).
Finite fields

\((F,+,*\)) is a **field** if:

- \((F,+\)) is an abelian group with (additive) identity denoted by 0.
- \((F\{0\},*\)) is an abelian group with (multiplicative) identity denoted by 1.
- The distributive law holds

**Theorem.** There exists a finite field \(F\) of order \(q\) iff \(q=p^m\) where \(p\) is prime and \(m\) is positive integer.

The prime \(p\) is called a **characteristic** of \(F\).

If \(m=1\), \(F\) is called a **prime field**. If \(m>1\), then \(F\) is called an **extension field**.
Mod and reduction mod

**Modulo operation:**

\[ a \mod p \equiv b \text{ if } p \mid (b-a). \]

\[ z_p = \{0, 1, 2, \ldots, p-1\}. \]

**Reduction modulo p:**

\[ a \mod p = r \text{ where } r \in [0, p-1] \text{ is the remainder obtained upon dividing } a \text{ by } p. \]
Prime fields

Addition: If $a, b \in \mathbb{Z}_p$, then
$$a +_p b = r \text{ in } \mathbb{Z}_p$$
where $r \in [0, p-1]$ is the remainder when the integer $a+b$ is divided by $p$.

Multiplication: If $a, b \in \mathbb{Z}_p$, then
$$a \circ_p b = r \text{ in } \mathbb{Z}_p$$
where $r \in [0, p-1]$ is the remainder when the integer $a \cdot b$ is divided by $p$.

Prime field:
$$\mathbb{F}_p = (\mathbb{Z}_p, +_p, \circ_p)$$
The finite field $F_{2^m}$

$$F_{2^m} = \{ a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \cdots + a_2x^2 + a_1x + a_0 : a_i \in \{0,1\} \}$$

- **Addition in $F_{2^m}$**: Usual addition of polynomials, with coefficients in $F_{2^m}$: Arithmetic performed modulo 2.
- **Multiplication in $F_{2^m}$**: Usual multiplication of polynomials and then division by a fixed irreducible polynomial $f(x)$ of degree $m$. 
Further readings

Fast algorithms for performing the reduction modulo operation and modular multiplication:

- Barrett reduction algorithm\(^1\)
- Montgomery multiplication algorithm\(^1\)

NIST primes

The following primes are the NIST standards for EC over prime fields:

• $p_{192} = 2^{192} - 2^{64} - 1$
• $p_{224} = 2^{224} - 2^{96} + 1$
• $p_{256} = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$
• $p_{384} = 2^{384} + 2^{128} + 2^{96} + 2^{32} - 1$
• $p_{521} = 2^{521} - 1$
An elliptic curve $E$ over a field $K$ is defined by an equation

$$E: y^2 + Axy + By = x^3 + Cx^2 + Dx + F$$

where $A,B,C,D,F \in K$. 
Isomorphic Elliptic curves

Two elliptic curves

\[ E_1: y^2 + A_1xy + B_1y = x^3 + C_1x^2 + D_1x + F_1 \]
\[ E_2: y^2 + A_2xy + B_2y = x^3 + C_2x^2 + D_2x + F_2 \]

are isomorphic if there exist \( u, r, s, t \in K \) such that the change of the variables

\( (x,y) \rightarrow (u^2x + r, u^3y + u^2sx + t) \)

transforms equation \( E_1 \) into equation \( E_2 \).
Isomorphic EC

The following change of the variables

\((x, y) \rightarrow \left( \frac{x-3A^2-12C}{36}, \frac{y-3Ax}{216} - \frac{A^3-4AC-12B}{24} \right)\)

transforms the elliptic curve

\(E: y^2 + Ay + B = x^3 + Cx^2 + Dx + F\)

into an elliptic curve

\(y^2 = x^3 + ax + b\)

where \(a, b \in K\) and \(K\) is a field with characteristic \(\neq 2,3\).
Further readings

• Isomorphic elliptic curves over fields with characteristic 2.

• Isomorphic elliptic curves over fields with characteristic 3.

The elliptic curve \( y^2 = x^3 + Ax + B \)

\[ E(A,B) = \{ (x, y) : y^2 = x^3 + Ax + B \} \cup \{ \text{Id} \} \]

where \( A, B \in K \) such that \( 4A^3 + 27B^2 \neq 0 \).

and \( K \) is a finite field.

\( \text{Id} \) – “point at infinity”

Geometric \textbf{model} of Elliptic curve \( y^2 = x^3 + Ax + B \).
The group law in $y^2 = x^3 + Ax + B$

Adding points

$P \oplus Q = R \quad \text{or just} \quad P + Q = R$
The group law in $y^2 = x^3 + Ax + B$

Adding points

Problem: The vertical line through $P$ and $Q$ does not intersect $E(A,B)$ in a third point!

Solution: $P \oplus Q = \text{Id}$ or just $P + Q = \text{Id}$
The group law in $y^2 = x^3 + Ax + B$

Adding points to itself

$P \oplus P$ or just $2P$
The algebra of elliptic curves

The addition law on $E(A,B)$ has the following properties:

- $P \oplus \text{Id} = \text{Id} \oplus P = P$ for all $P$ in $E(A,B)$.
- $P \oplus (-P) = \text{Id}$ for all $P$ in $E(A,B)$.
- $P \oplus (Q \oplus R) = (P \oplus Q) \oplus R$ for all $P$, $Q$, $R$ in $E(A,B)$.
- $P \oplus Q = Q \oplus P$ for all $P$, $Q$ in $E(A,B)$. 
Theorem \((E(A,B), \oplus)\) is an Abelian group.

**Note:** For the generalized Weierstess equation this is no longer true.
Formulas for addition on $E(A,B)$

Case 1: Let $P(x_1,y_1)$ and $Q(x_2,y_2)$ be two distinct points on $E(A,B)$ with $x_1 \neq x_2$

Let the line connecting $P$ and $Q$ be

$$L: y = y_1 + m(x-x_1)$$

Then the slope of $L$ is given by

$$m = \frac{y_2 - y_1}{x_2 - x_1}$$

$$P+Q = (m^2-x_1-x_2, -y_1+m(x_1-x_3))$$
Formulas for addition on \(E(A,B)\)

Case 2: Let \(P(x_1,y_1)\) and \(Q(x_2,y_2)\) be two distinct points on \(E(A,B)\) with \(x_1=x_2\).

Then \(P + Q = Q + P = \text{Id.}\)
Formulas for addition on $E(A,B)$

**Case 3:** Let $P(x_1,y_1) = Q(x_2,y_2)$ and $y_1 \neq 0$.

The slope of the tangent line can be found by implicitly differentiating the equation

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

and substituting in the coordinates of $P$:

$$m = \frac{3x_1^2 + A}{2y_1}$$

Then $P + P = 2P = (m^2-2x_1,-y_1+m(x_1-m^2+2x_1))$. 
Formulas for addition in $E(A,B)$

Case 4:

Let $P(x_1, y_1) = Q(x_2, y_2)$ and $y_1 = 0$. Then $P + Q = 2P = \text{Id.}$
Computing multiples of a point

Double-and-Add method:
Write
\[ k = k_0 + k_1 \cdot 2 + k_2 \cdot 2^2 + \ldots + k_n \cdot 2^n \]
with \( k_0, k_1, k_2, \ldots, k_n \) in \( \{0, 1\} \).
Then,
\[ kP = k_0 P + k_1 \cdot 2P + k_2 \cdot 2^2P + \ldots + k_n \cdot 2^n P \]
where \( 2^n \ P = 2 \cdot 2 \cdot 2 \cdot \ldots \cdot 2P \) requires only \( n \) doublings.
Order of $E(A,B,p)$

It is clear that $\#E(A,B,p) \in [1, 2p+1]$. The following theorem gives better bounds for $\#E(A,B,p)$.

**Theorem** (Hasse, 1922): For $p \geq 3$ prime,

$$p + 1 - 2\sqrt{p} \leq \#E(A,B,p) \leq p + 1 + 2\sqrt{p}.$$ 

Alternate formulation of Hasse’s theorem:

$$\#E(A,B,p) = p + 1 - t$$

where $|t| \leq 2\sqrt{p}$

**Remark:** $t$ is called the trace of $E(A,B,p)$. 
Order of $E(F_q)$

**Theorem.** Let $q=p^n$ be a power of a prime $p$ and $N=q+1-t$. There is an elliptic curve over $F_q$ with order $N$ iff $|t| \leq 2\sqrt{q}$ and $t$ satisfies one of the following:

- gcd$(t,p)=1$
- $n$ is even and $t=2\sqrt{q}$ or $t=-2\sqrt{q}$
- $n$ is even, $p\not\equiv 1 \pmod{3}$ and $t=\sqrt{q}$ or $t=-\sqrt{q}$
- $n$ is odd, $p=2$ or $3$ and $t=p^{(n+1)/2}$ or $t=-p^{(n+1)/2}$
- $n$ is even, $p\not\equiv 1 \pmod{4}$ and $t=0$
- $n$ is odd and $t=0$. 
Determining the order of $E(F_{q^n})$

**Theorem.** Let $\#E(F_q) = q+1-a$ and let $q+1-a = (x-u)(x-v)$. Then

$E(F_{q^n}) = q^n + 1 - (u^n + v^n)$ for all $n \geq 1$. 
Determining the order of $E(F_{q^n})$

Legendre symbol:

$$\text{legendre}(x, F_q) = \begin{cases} 
1 & \text{if } t^2 = x \text{ has a solution in } F_q \\
-1 & \text{if } t^2 = x \text{ has no solution in } F_q \\
0 & \text{if } x = 0
\end{cases}$$

Theorem. Let $E$ be an elliptic curve defined by $y^2 = x^3 + ax + b$ over $F_{q^n}$. Then
Def. An elliptic curve E defined over a field \( \mathbb{F}_q \) of characteristic p is called a supersingular if \( p \mid t \), where t is the trace. If p does not divide t, then E is non-supersingular.
Supersingular EC group

**Theorem:** Let $p > 3$ be a prime number.

[1] If $B=0$ and $p \mod 4 = 3$ then

$$\#E(A,B,p) = p+1$$

[2] If $A=0$ and $p \mod 3 = 2$ then

$$\#E(A,B,p) = p+1$$


Anomalous curves

**Def.** If the order $\#E(F_q)$ is equal to the characteristic $p$ of $F_q$, the elliptic curve is called an **anomalous** curve.

**Note:** The anomalous curves are not secure for use in ECC.
Elliptic Curve Cryptography - advantages

• Computationally efficient public key cryptosystem

• Memory and power savings

• Highest security
“Elliptic Curve Cryptography provides greater security and more efficient performance than the first generation public key techniques (RSA and Diffie-Hellman) now in use. As vendors look to upgrade their Systems they should seriously consider the elliptic curve alternative for the computational and bandwidth advantages they offer at comparable security.”

“The majority of public key systems in use today use 1024-bit parameters for RSA and Diffie-Hellman. The US National Institute for Standards and Technology has recommended that these 1024-bit systems are sufficient for use until 2010. After that, NIST recommends that they be upgraded to something providing more security.”
## NIST Recommended Key Sizes

<table>
<thead>
<tr>
<th>Symmetric Key Size (bits)</th>
<th>RSA and Diffie-Hellman Key Size (bits)</th>
<th>Elliptic Curve Key Size (bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>1024</td>
<td>160</td>
</tr>
<tr>
<td>112</td>
<td>2048</td>
<td>224</td>
</tr>
<tr>
<td>128</td>
<td>3072</td>
<td>256</td>
</tr>
<tr>
<td>192</td>
<td>7680</td>
<td>384</td>
</tr>
<tr>
<td>256</td>
<td>15360</td>
<td>521</td>
</tr>
</tbody>
</table>