CDH/DDH-Based Encryption

K&L Sections 8.3.1-8.3.3, 11.4.

Cyclic groups

- A finite group G of order q is cyclic if it has an element g of q. In this case, $G = \langle g \rangle = \{g^0, g^1, g^2, \ldots, g^{q-1}\}$; G is said to be generated by g, and g is a generator.
- In any group (not necessarily finite or cyclic), if g is an element of finite order q, then $\langle g \rangle = \{g^0, g^1, g^2, \ldots, g^{q-1}\}$ is a cyclic group of order q.
- Note: in general, $\langle g \rangle$ denotes the subgroup generated by g.
- Note: we implicitly assume multiplicative groups, and will write the identity of the group as 1.
- Recall: For any element $a \in G$, $a^m = a^{m \bmod |G|}$.

Discrete logarithm problem (DLP)

- Let G be a cyclic group of order q, and let g be any generator.
  So, $G = \langle g \rangle = \{g^0, g^1, g^2, \ldots, g^{q-1}\}$
- For any $h \in G$, there is a unique $x \in \mathbb{Z}_q$ such that $g^x = h$.
  This integer x is called the discrete logarithm (or index) of h with respect to base g. We write $\log_g h = x$.
- Standard logarithm rules still hold: $\log_g 1 = 0$,
  $\log_g (h_1 \cdot h_2) = (\log_g h_1 + \log_g h_2) \bmod q$, $\log_g h^k = (k \log_g h) \bmod q$.
- The DLP in G with base g is to compute $\log_g h$ for any $h \leftarrow_u G$.

DLP in $\mathbb{Z}_p^*$

- Theorem: If p is prime, then $\mathbb{Z}_p^*$ is a cyclic group of order $p-1$.
- Let g be any generator of $\mathbb{Z}_p^*$.
- $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\} = \{g^0, g^1, g^2, \ldots, g^{p-2}\}$.

  $\mathbb{Z}_{p-1} = \{0, 1, 2, \ldots, p-2\}$.
- DLP: given $g^x \in \mathbb{Z}_p^*$, compute x.
- There is a subexponential-time algorithm for DLP in $\mathbb{Z}_p^*$
  - Index Calculus, $O\left(2^{O\left(\sqrt{n \log n}\right)}\right)$, where $n = \log p$.

Frequently used groups

- $\mathbb{Z}_p^* = \{g^0,\ g^1,\ g^2,\ \ldots,\ g^{p-2}\}$,

  where p is a large prime, and g is a generator. //less secure//

- A subgroup of $\mathbb{Z}_p^*$ of prime order q,

$$G_q = \langle \alpha \rangle = \{\alpha^0,\ \alpha^1,\ \alpha^2,\ \ldots,\ \alpha^{q-1}\} \subset \mathbb{Z}_p^*,$$

  where $\alpha \in \mathbb{Z}_p^*$ is an element of prime order q (e.g. $\alpha = g^{(p-1)/q}$).

  - The Index Calculus doesn't work.

- Elliptic curves defined over finite fields. //increasingly popular//

- In these groups, there is no polynomial-time algorithm known for DLP.

Example 1

$G = \mathbb{Z}_{19}^{*} = \{1,\ 2,\ \ldots,\ 18\}.$

2 is a generator. $\mathbb{Z}_{19}^{*} = \langle 2 \rangle = \left\{2^0,\ 2^1,\ 2^2,\ \ldots,\ 2^{17}\right\}.$

$2^0 = 1,\ 2^1 = 2,\ 2^2 = 4,\ 2^3 = 8,\ 2^4 = 16,\ 2^5 = 13,$

$2^6 = 7,\ 2^7 = 14,\ \ldots$

$\log_2 7 = 6$

$\log_2 14 = 7$

$\log_2 12 = ?$

Example 2

$$G = \mathbb{Z}_{11}^{*} = \{1,\ 2,\ \ldots,\ 10\}.$$

$$G_5 = \langle 3 \rangle\ =\ \{1,\ 3,\ 9,\ 5,\ 4\}.$$

3 is a generator of G_5, but not a generator of Z_{11}^{*}.

$\log_3 5 = 3$

$\log_3 10 =$ not defined

Example 3

DLP in the additive group $\mathbb{Z}_N$.

Every $0 \neq g \in \mathbb{Z}_N$ coprime to N is a generator.

DLP: given $k \cdot g$, compute k.

RSA vs. Discrete Logarithm

- RSA is a one-way trapdoor function:

$$x \xrightarrow{\text{RSA}} x^e \qquad \text{(easy)}$$

$$x \xleftarrow{\text{RSA}^{-1}} x^e \qquad \text{(difficult)}$$

$$x \xleftarrow{\text{RSA}^{-1}} \left(x^e\right)^d \qquad (\,d \text{ is a trapdoor})$$

- Exponetiation is a one-way function without a trapdoor:

$$x \xrightarrow{\exp_g} g^x \qquad \text{(easy)}$$

$$x \xleftarrow{\log_g} g^x \qquad \text{(difficult)}$$

- An encryption scheme based on the difficulty of discrete log will not simply encrypt x as g^x.

Diffie-Hellman key agreement

- $G = \{g^0, g^1, g^2, \ldots, g^{q-1}\}$, a cyclic group of order q.

  $\mathbb{Z}_q = \{0, 1, 2, \ldots, q-1\}$.

- Alice and Bob wish to set up a secret key.
  1. They agree on (G, g, q).
  2. Alice $\to$ Bob: g^x, where $x \leftarrow_u \mathbb{Z}_q$.
  3. Alice $\leftarrow$ Bob: g^y, where $y \leftarrow_u \mathbb{Z}_q$.
  4. The agreed-on key: $g^{x \cdot y}$.

- Remark: in practice, (G, g, q) is standardized, and there is a mapping between bit strings and the elements of G.

Diffie-Hellman key agreement using $\mathbb{Z}_p^*$

- $\mathbb{Z}_p^* = \{g^0,\ g^1,\ g^2,\ \ldots,\ g^{p-2}\}$, p a large prime.

  $\mathbb{Z}_{p-1} = \{0,\ 1,\ 2,\ \ldots,\ p-2\}$.

- Alice and Bob wish to set up a secret key.
  1. Alice and Bob agree on a large prime p and a generator $g \in \mathbb{Z}_p^*$. (p, g, not secret)
  2. Alice $\to$ Bob: $g^x \bmod p$, where $x \leftarrow_u \mathbb{Z}_{p-1}$.
  3. Alice $\leftarrow$ Bob: $g^y \bmod p$, where $y \leftarrow_u \mathbb{Z}_{p-1}$.
  4. They agree on the key: $g^{xy} \bmod p$.

Diffie-Hellman problems

- $G = \{g^0, g^1, g^2, \ldots, g^{q-1}\}$, a cyclic group of order q.

  $Z_q = \{0, 1, 2, \ldots, q-1\}$.

- Computational Diffie-Hellman (CDH) Problem:

  given $g^x, g^y \in G$, where $x, y \leftarrow_u Z_q$, compute $g^{x \cdot y}$.

- Decisional Diffie-Hellman (DDH) Problem:

  given $g^x, g^y, h \in G$, where $x, y \leftarrow_u Z_q$, and

$$h = \begin{cases} g^{x \cdot y} & \text{with probability } 1/2 \\ \text{a random element in } G & \text{with probability } 1/2 \end{cases}$$

  determine if $h = g^{x \cdot y}$.

Relationships between DDH, CDH, DLP

- DDH $\leq$ CDH $\leq$ DLP.
- Open question: Is CDH $\geq$ DLP?
- There are example of groups (e.g., $\mathbb{Z}_p^*$) in which CDH and DLP are believed to be hard, but DDH is easy.

ElGamal encryption scheme

$$G = \{g^0,\ g^1,\ g^2,\ \ldots,\ g^{q-1}\},\quad \mathbb{Z}_q = \{0,\ 1,\ 2,\ \ldots,\ q-1\}.$$

- Keys: $sk = (G, g, q, x)$, $pk = (G, g, q, h)$ where $x \leftarrow \mathbb{Z}_q$, $h = g^x$.
- To encrypt a message $m \in G$:
  - Use Diffie-Hellman agreement to set up a "key" $k \in G$ by choosing $y \leftarrow_u \mathbb{Z}_q$ and computing $k := h^y$ $(= g^{x \cdot y})$.
  - Use k to encrypt m as $k \cdot m \in G$.
  - The ciphertext is $\langle g^y, k \cdot m \rangle = \langle g^y, h^y \cdot m \rangle$.
- Decryption: $Dec_{sk}(c_1,\ c_2) = c_2 \cdot c_1^{-x}$.

ElGamal encryption in $\mathbb{Z}_p^*$

1. Key generation (e.g. for Alice):
   - choose a large prime p and a generator $g \in \mathbb{Z}_p^*$,

     where $p-1$ has a large prime factor.
   - randomly choose a number $x \in \mathbb{Z}_{p-1}$ and compute $h = g^x$;
   - let $sk = (p, g, x)$ and $pk = (p, g, h)$.
2. Encryption: $Enc_{pk}(m) = (g^y,\ h^y \cdot m)$, where $m \in \mathbb{Z}_p^*$, $y \leftarrow_u \mathbb{Z}_{p-1}$.
3. Decryption: $D_{sk}(c_1, c_2) = c_2 \cdot c_1^{-x}$.
4. Remarks: Multiplications are done in $\mathbb{Z}_p^*$, *i.e.*, modulo p.

   The encryption scheme is randomized.

Security of ElGamal encryption

- Theorem: If the DDH problem is hard, then the ElGamal encryption scheme is CPA-secure.

- ElGamal encryption is homomorphic and thus not CCA-secure.

Homomorphism of ElGamal encryption

- A function $f : G \rightarrow G'$ is homomorphic if $f(xy) = f(x)f(y)$.
- ElGamal encryption is homomorphic, $E(mm') = E(m) \cdot E(m')$, in the following sense:

If $E(m) = \left(g^{y},\ mh^{y}\right)$ and $E(m') = \left(g^{y'},\ m'h^{y'}\right)$, then

$$E(m) \cdot E(m') = \left(g^{y},\ mh^{y}\right) \cdot \left(g^{y'},\ m'h^{y'}\right)$$

$$= \left(g^{y} g^{y'},\ mh^{y} m'h^{y'}\right)$$

$$= \left(g^{y+y'}, mm'h^{y+y'}\right)$$

is a valid encryption of mm'.

Elliptic Curve Cryptography

K&L Section 8.3.4

Field

- A field, denoted by $(F,\ +,\ \times)$, is a set F with two binary operations, $+$ and $\times$, such that
  1. $(F,+)$ is an abelian group (with identity 0).
  2. $(F\setminus\{0\},\times)$ is an abelian group (with identy 1).
  3. For all elements $a \in F$, $0\times a = a\times 0 = 0$.
  3. $\forall x, y, z \in F$, $x\times(y+z) = x\times y + x\times z$ (distributive).
- Example fields: $(\mathbb{Q},\ +,\ \times)$, $(\mathbb{R},\ +,\ \times)$, $(\mathbb{C},\ +,\ \times)$.
- $(\mathbb{Z},+,\times)$ is not a field, because $z^{-1} \notin \mathbb{Z}$ (except for $z=1$).
- For any prime p, $(\mathbb{Z}_p,\ +,\ \times)$ is a field, denoted as F_p.

The equation of an elliptic curve

- An elliptic curve is a curve given by

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

- It is required that the discriminant $\Delta = 4a^3 + 27b^2 \neq 0$. When $\Delta \neq 0$, the polynomial $x^3 + ax + b = 0$ has distinct roots, and the curve is said to be nonsingular.
- For reasons to be explained later, we introduce an additional point, O, called the point at infinity, so the elliptic curve is the set

$$E = \left\{(x, y) : y^2 = x^3 + ax + b\right\} \cup \left\{O\right\}$$

- We are often interested in points on the curve of specific coordinates:

$$E(\mathbb{Z}) = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} :\ y^2 = x^3 + ax + b\} \cup \{O\}$$

$$E(\mathbb{Q}) = \{(x, y) \in \mathbb{Q} \times \mathbb{Q} :\ y^2 = x^3 + ax + b\} \cup \{O\}$$

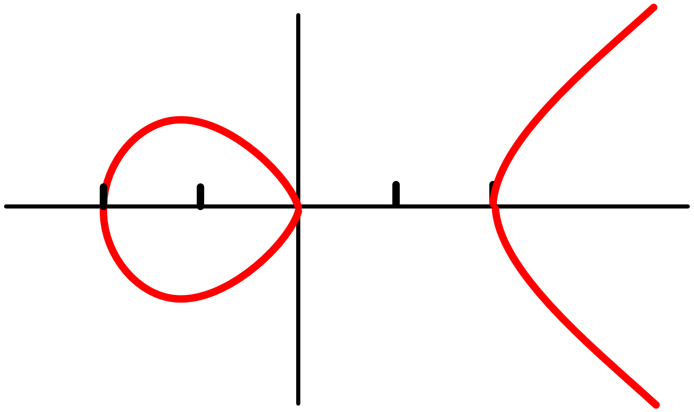
$$E(\mathbb{R}) = \{(x, y) \in \mathbb{R} \times \mathbb{R} :\ y^2 = x^3 + ax + b\} \cup \{O\}$$

$$E(\mathbb{C}) = \{(x, y) \in \mathbb{C} \times \mathbb{C} :\ y^2 = x^3 + ax + b\} \cup \{O\}$$

$$E(F_p) = \{(x, y) \in F_p \times F_p :\ y^2 = x^3 + ax + b\} \cup \{O\}$$

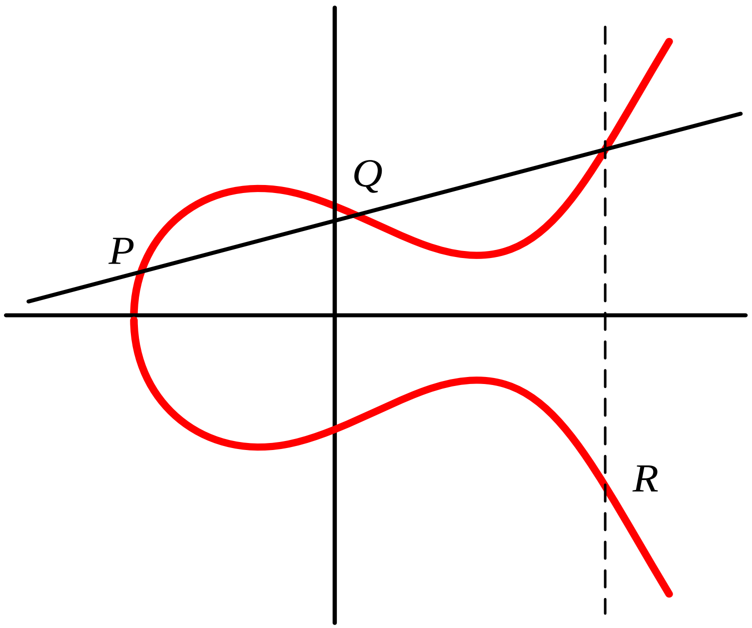
Example:

$$E: y^2 = x^3 - 4x \qquad (x,\ y \in \mathbb{R})$$



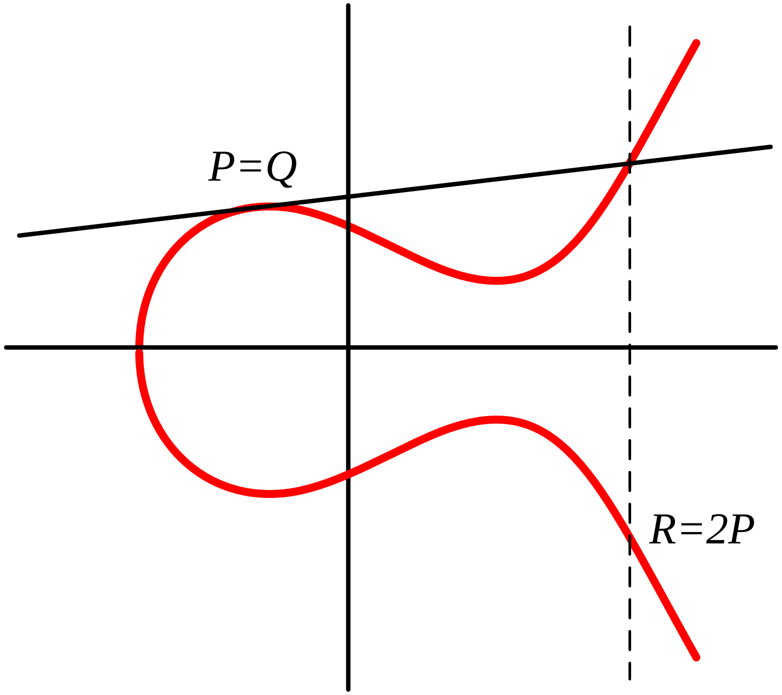
Making an elliptic curve into a group

- Amazing fact: we can use geometry to make the points of an elliptic curve into a group.
- Suppose $P \neq Q$. Then define $P + Q = R$.

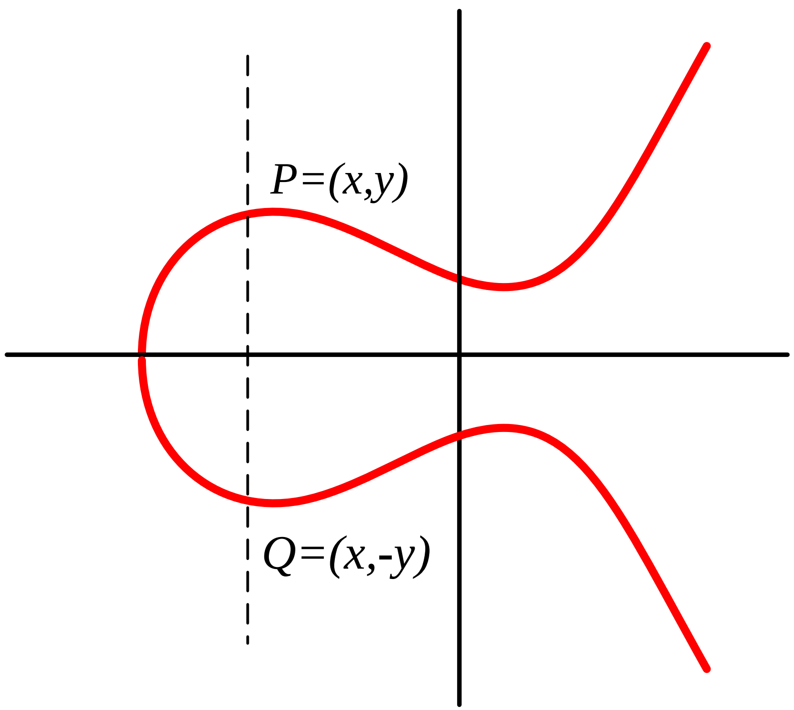


- Suppose $P = Q$.

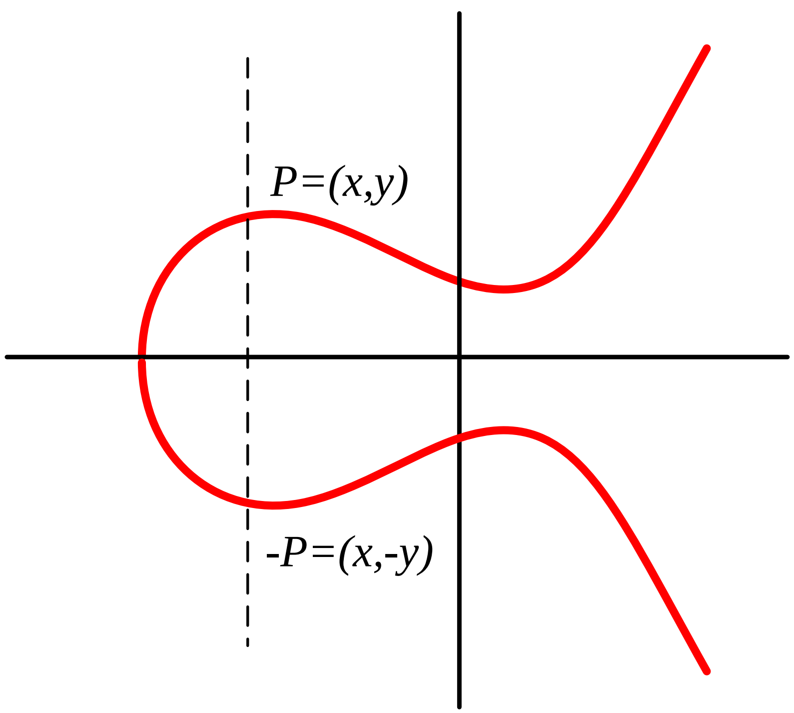
  Then define $P + Q = 2P = R$.



- What if $P=(x,y),\ Q=(x,-y),$ so that $\overleftrightarrow{PQ}$ is vertical? In this case, we define $P+Q=O.$
- This is why we added the extra point O into the curve.



- Now having defined $P+Q$ for $P,\ Q \neq O,$ we still need to define $P+O.$
- Let O play the role of identity, and define $P+O=O+P=P.$
- Now every point $P=(x,y)$ has an inverse: $-P=(x,-y).$



Theorem. The addition law on E has these properties:

1. $P+O=O+P=P$ for all $P \in E$.
2. $P+(-P)=O$ for all $P \in E$.
3. $P+(Q+R)=(P+Q)+R$ for all $P,Q,R \in E$.
4. $P+Q=Q+P$ for all $P,Q \in E$.

- That is, $(E(\mathbb{R}),+)$ forms an abelian group.
- All of these properties are trivial to check except the associative law (3), which can be verified by a lengthy computation using explicit formulas, or by using more advanced algebraic or analytic methods.

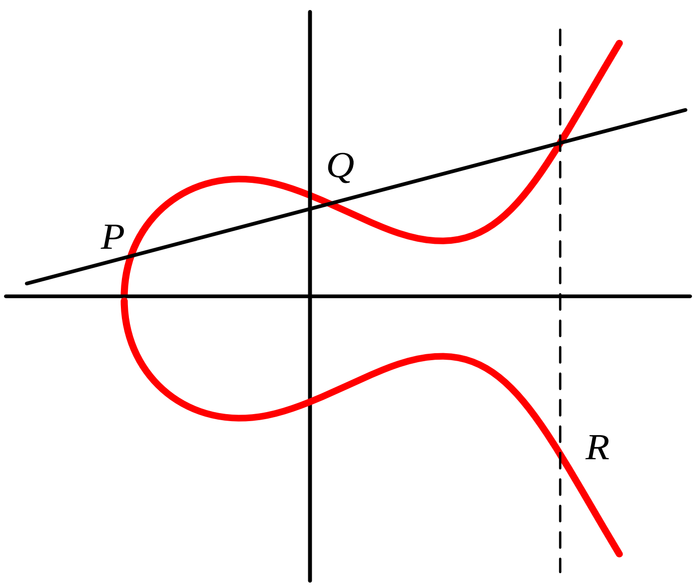
Formulas for Addition on E

- $P=(x_1,y_1),\ Q=(x_2,y_2),\ P\neq Q.\quad R=P+Q=(x_3,y_3).$
- The curve $E:\quad y^2=x^3+ax+b.$
- The line $\overleftrightarrow{PQ}:\quad y=\lambda x+\nu,$ where

$$\lambda=\frac{y_1-y_2}{x_1-x_2}\ \text{ and }\ \nu=y_1-\lambda x_1.$$

- $x_3=\lambda^2-x_1-x_2$

  $y_3=(x_1-x_3)\lambda-y_1$

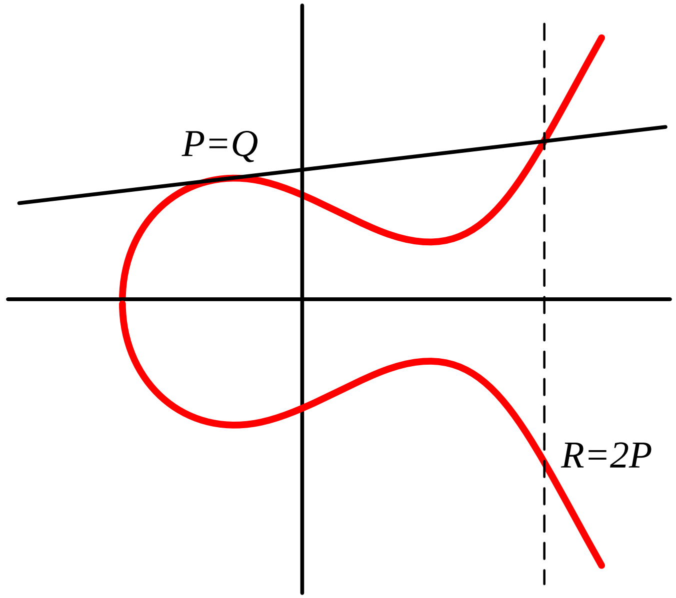


- If $P = Q = (x_1, y_1)$, with $y_1 \neq 0$, and $R = P + Q = 2P = (x_3, y_3)$, then

$$\lambda = \frac{3x_1^{\ 2} + a}{2y_1}$$

$$x_3 = \lambda^2 - 2x_1$$

$$y_3 = (x_1 - x_3)\lambda - y_1$$



An important fact

- $E: \ y^2 = x^3 + ax + b.$
- If a and b are in a field K and if P and Q have coordinates in K, then $P+Q$ and $2P$ as computed by the formulas also have coordinates in K, or equal O.
- Thus, we can use the same addition laws to make the points of an elliptic curve over a finite field F_p into a group, even though the addition laws will no longer have the geometric interpretations.

Theorem (Poincare, $\approx$1900)

Let K be a field, and suppose that an elliptic curve E is given by an equation of the form

$$E:\ y^2 = x^3 + ax + b \text{ with } a, b \in K.$$

Let $E(K)$ denote the set of points of E with coordinates in K, plus O,

$$E(K) = \{(x,y) \in E:\ x, y \in K\} \cup \{O\}.$$

Then $E(K)$ is a group.

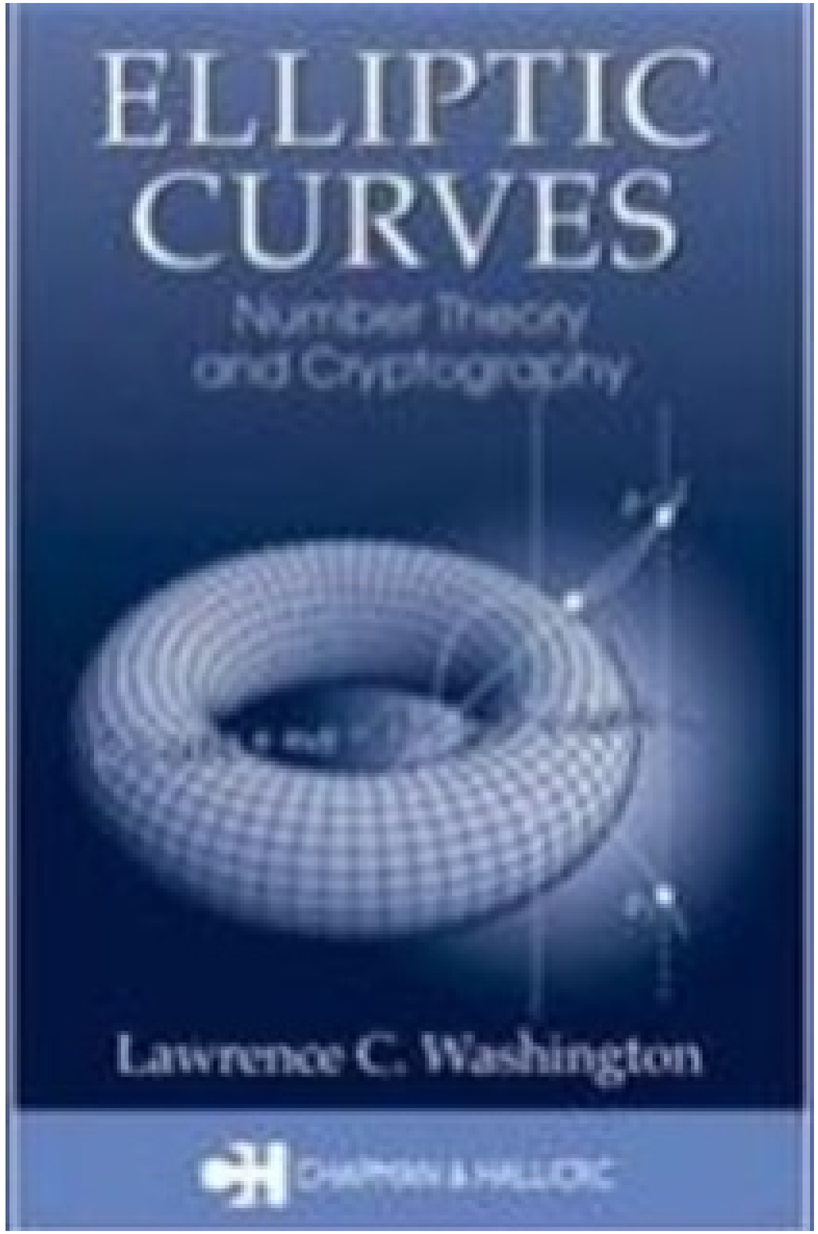
What does $E(C)$ look like?

$$E: y^2 = x^3 + ax + b \text{ with } a, b \in R.$$

Let $E(\mathbb{C})$ denote the set of points of E with coordinates in C, plus O,

$$E(\mathbb{C}) = \left\{(x, y) \in C \times C : y^2 = x^3 + ax + b\right\} \cup \left\{O\right\}$$

An amazing fact: $E(\mathbb{C})$ is isomorphic to a torus.


ELLIPTIC
CURVES
Number Theory
and Cryptography
Lawrence C. Washington
CHAPMAN & HALL/CRC

Elliptic curves defined over F_p

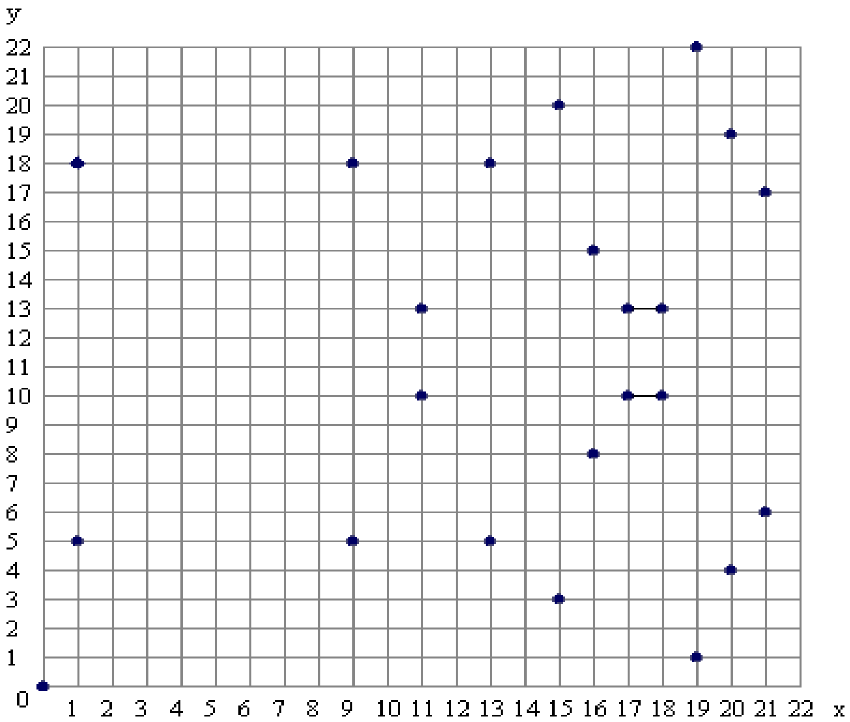
Equation: $y^2 = x^3 + ax + b$ over F_p

where $p > 3,\ a, b \in F_p,\ \ 4a^3 + 27b^2 \neq 0 \pmod{p}$.

$$E = \left\{ (x, y) \in F_p \times F_p :\ y^2 = x^3 + ax + b \right\} \cup \{O\}$$

Example:

$E:\ y^2 = x^3 + x$ over F_{23}



Elliptic curve equation: $y^2 = x^3 + x$ over F_{23}

Example

$E : y^2 = x^3 + x + 6$ over F_{11}

To find all points (x, y) of E, for each $x \in F_{11}$, compute $z = x^3 + x + 6 \bmod 11$ and determine whether z is a quadratic residue.

If so, solve $y^2 = z$ in F_{11}.

$|E(F_{11})| = 13.$

x	$x^3 + x + 6$	quad res?	y
0	6	*no*	
1	8	*no*	
2	5	*yes*	4,7
3	3	*yes*	5,6
4	8	*no*	
5	4	*yes*	2,9
6	8	*no*	
7	4	*yes*	2,9
8	9	*yes*	3,8
9	7	*no*	
10	4	*yes*	2,9

Example (continued)

There are 13 points in the group.

So, it is cyclic and any point other O is a generator.

Let $\alpha = (2,7)$. We can compute $2\alpha = (x_2, y_2)$ as follows.

$$\lambda = \frac{3{x_1}^2 + a}{2y_1} = \frac{3(2)^2 + 1}{2 \times 7} = \frac{13}{14} = 2 \times 3^{-1} = 2 \times 4 = 8 \ (\text{mod} 11)$$

$$x_2 = \lambda^2 - 2x_1 = (8)^2 - 2 \times (2) = 5 \ \ (\text{mod} 11)$$

$$y_2 = (x_1 - x_2)\lambda - y_1 = (2 - 5) \times 8 - 7 = 2 \ (\text{mod} 11)$$

$$2\alpha = (5,2)$$

Example (continued)

Let $3\alpha = (x_3, y_3)$. Then,

$$\lambda \;=\; \frac{y_2 - y_1}{x_2 - x_1} = \frac{2-7}{5-2} = 2 \pmod{11}$$

$$x_3 \;=\; \lambda^2 - x_1 - x_2 = 2^2 - 2 - 5 = 8 \pmod{11}$$

$$y_3 \;=\; (x_1 - x_3)\lambda - y_1 = (2-8)\times 2 - 7 = 3 \pmod{11}$$

$\alpha = (2,7)$	$2\alpha = (5,2)$	$3\alpha = (8,3)$
$4\alpha = (10,2)$	$5\alpha = (3,6)$	$6\alpha = (7,9)$
$7\alpha = (7,2)$	$8\alpha = (3,5)$	$9\alpha = (10,9)$
$10\alpha = (8,8)$	$11\alpha = (5,9)$	$12\alpha = (2,4)$

$$13\alpha = \alpha + 12\alpha = 2\alpha + 11\alpha = 3\alpha + 10\alpha = \cdots = ?$$

Point Counting

- Determining $|E(F_p)|$ is an important problem, called point counting.
- Hasse's Theorem:

$$p+1-2\sqrt{p} \le |E(F_p)| \le p+1+2\sqrt{p}.$$

- There are polynomial time algorithms that precisely determine $|E(F_p)|$.
- In practice, $E(F_p)$ of prime order q is used.

DLP in $\langle g \rangle$ - reviewed

- Let $\langle g \rangle = \{ g^0, g^1, g^2, \ldots, g^{q-1} \}$ be a group of order q.
- DLP in $\langle g \rangle$: given an element $h \in \langle g \rangle$, find the unique exponent $x \in \mathbb{Z}_q$ such that $g^x = h$.

Elliptic Curve Discrete Logarithm Problem

- Consider an elliptic curve group $E(F_p)$.
- Let $G \in E(F_p)$ be a point of large prime order q.
- $\langle G \rangle = \{0G,\ 1G,\ 2G,\ \ldots,\ (q-1)G\}$ is a subgroup of $E(F_p)$.
- ECDLP: given a point $H \in \langle G \rangle$, find the unique multiplier $x \in \mathbb{Z}_q$ such that $xG = H$.

Diffie-Hellman key agreement

$$\text{Alice} \xrightarrow{g^a} \text{Bob}$$

$$\text{Alice} \xleftarrow{g^b} \text{Bob}$$

Agreed key: g^{ab}

Elliptic Curve Diffie-Hellman

$$\text{Alice} \xrightarrow{aG} \text{Bob}$$

$$\text{Alice} \xleftarrow{bG} \text{Bob}$$

Agreed key: abG

Elliptic Curve Diffie-Hellman key agreement

- Alice and Bob wish to agree on a secret key.
  1. Alice and Bob agree on an elliptic curve $E(F_p)$ and a point G on the curve of large prime order q.
  2. Alice $\rightarrow$ Bob: aG, where $a \leftarrow_u Z_q$.
  3. Alice $\leftarrow$ Bob: bG, where b $\leftarrow_u Z_q$.
  4. They agree on the key abG, which is a point on $E(F_p)$.

- They can now use $x(abG)$, the x-coordinate of abG, as a secret key for, for example, a symmetric encryption scheme.

Key lengths recommended by NIST

Effective Key Length	RSA	Discrete Logarithm	
	Modulus Length	Order-q Subgroup of $\mathbb{Z}_p^*$	Elliptic-Curve Group Order q
112	2048	p: 2048, q: 224	224
128	3072	p: 3072, q: 256	256
192	7680	p: 7680, q: 384	384
256	15360	p: 15360, q: 512	512

Effective key length n: brute-force search against an n-bit symmetric key encryption scheme