

# Cryptography

## Lecture 23

# Announcements

- HW5 due on Wednesday, 4/24

# Agenda

- Last time:
  - Cyclic groups
- This time:
  - More on Cyclic Groups
  - Hard problems (Discrete log, Diffie-Hellman Problems—CDH, DDH)
  - Elliptic Curve Groups

# Cyclic Groups

For a finite group  $G$  of order  $m$  and  $g \in G$ , consider:

$$\langle g \rangle = \{g^0, g^1, \dots, g^{m-1}\}$$

$\langle g \rangle$  always forms a cyclic subgroup of  $G$ .

However, it is possible that there are repeats in the above list.

Thus  $\langle g \rangle$  may be a subgroup of order smaller than  $m$ .

If  $\langle g \rangle = G$ , then we say that  $G$  is a **cyclic group** and that  $g$  is a **generator** of  $G$ .

# Examples

Consider  $Z_{13}^*$ :

2 is a generator of  $Z_{13}^*$ :

$2^0$	1
$2^1$	2
$2^2$	4
$2^3$	8
$2^4$	$16 \rightarrow 3$
$2^5$	6
$2^6$	12
$2^7$	$24 \rightarrow 11$
$2^8$	$22 \rightarrow 9$
$2^9$	$18 \rightarrow 5$
$2^{10}$	10
$2^{11}$	$20 \rightarrow 7$
$2^{12}$	$14 \rightarrow 1$

order of 2 is 12

3 is not a generator of  $Z_{13}^*$ :

$3^0$	1
$3^1$	3
$3^2$	9
$3^3$	$27 \rightarrow 1$
$3^4$	3
$3^5$	9
$3^6$	$27 \rightarrow 1$
$3^7$	3
$3^8$	9
$3^9$	$27 \rightarrow 1$
$3^{10}$	3
$3^{11}$	9
$3^{12}$	$27 \rightarrow 1$

order of 3 is 3

# Definitions and Theorems

Definition: Let  $G$  be a finite group and  $g \in G$ . The order of  $g$  is the smallest positive integer  $i$  such that  $g^i = 1$ .

**Ex:** Consider  $Z_{13}^*$ . The order of 2 is 12. The order of 3 is 3.

Proposition 1: Let  $G$  be a finite group and  $g \in G$  an element of order  $i$ . Then for any integer  $x$ , we have  $g^x = g^{x \bmod i}$ .

Proposition 2: Let  $G$  be a finite group and  $g \in G$  an element of order  $i$ . Then  $g^x = g^y$  iff  $x \equiv y \pmod{i}$ .

$G$   
Cyclic group of order  $q$

generator

$$g$$
$$\boxed{(G, q, g)}$$

Adv

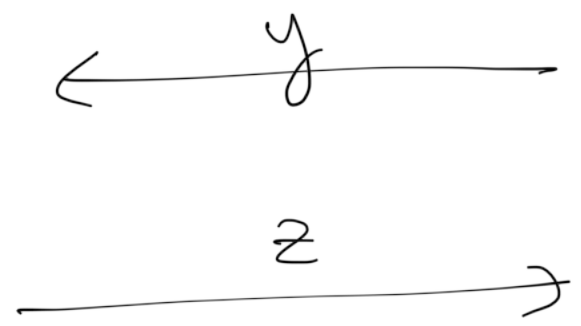
$$\{0, \dots, q-1\}$$

challenge  $\rightarrow$

$$x \in^R \mathbb{Z}_q$$

$$g^x = \boxed{y}$$

~~trying to compute~~  
 $\text{Dlog}_g(y)$



# More Theorems

Proposition 3: Let  $G$  be a finite group of order  $m$  and  $g \in G$  an element of order  $i$ . Then  $i \mid m$ .

Proof:

- We know by the generalized theorem of last class that  $g^m = 1 = g^0$ .
- By Proposition 2, we have that  $0 \equiv m \pmod{i}$
- By definition of modulus, this means that  $i \mid m$ .

Corollary: if  $G$  is a group of prime order  $p$ , then  $G$  is cyclic and all elements of  $G$  except the identity are generators of  $G$ .

Why does this follow from Proposition 3?

Theorem: If  $p$  is prime then  $\mathbb{Z}_p^*$  is a cyclic group of order  $p - 1$ .

Goal: Construct  
prime order  
cyclic group.



# Prime-Order Cyclic Groups

Consider  $Z_p^*$ , where  $p$  is a strong prime.

- Strong prime:  $p = 2q + 1$ , where  $q$  is also prime.
- Recall that  $Z_p^*$  is a cyclic group of order  $p - 1 = 2q$ .

*perfect squares*

The subgroup of quadratic residues in  $Z_p^*$  is a cyclic group of prime order  $q$ .

# Example of Prime-Order Cyclic Group

Consider  $Z_{11}^*$ .

Note that 11 is a strong prime, since  $11 = 2 \cdot 5 + 1$ .

$g = 2$  is a generator of  $Z_{11}^*$ :

$Z_p^*$

~~ECDH~~

$2^0$	1
$2^1$	2
$2^2$	4
$2^3$	8
$2^4$	16 → 5
$2^5$	10
$2^6$	20 → 9
$2^7$	18 → 7
$2^8$	14 → 3
$2^9$	6

The even powers of  $g$  are the “quadratic residues” (i.e. the perfect squares). Exactly half the elements of  $Z_p^*$  are quadratic residues.

Note that the even powers of  $g$  form a cyclic subgroup of order  $\frac{p-1}{2} = q$ .

inverse

Verify:

- closure (Multiplication translates into addition in the exponent. Addition of two even numbers mod  $p - 2$  gives an even number mod  $p - 1$ , since for prime  $p > 3$ ,  $p - 1$  is even.)
- Cyclic –any element is a generator. E.g. it is easy to see that all even powers of  $g$  can be generated by  $g^2$ .

# The Discrete Logarithm Problem

The discrete-log experiment  $DLog_{A,G}(n)$

1. Run  $G(1^n)$  to obtain  $(G, q, g)$  where  $G$  is a cyclic group of order  $q$  (with  $||q|| = n$ ) and  $g$  is a generator of  $G$ .
2. Choose a uniform  $h \in G$
3.  $A$  is given  $G, q, g, h$  and outputs  $x \in Z_q$
4. The output of the experiment is defined to be 1 if  $g^x = h$  and 0 otherwise.

Definition: We say that the DL problem is hard relative to  $G$  if for all ppt algorithms  $A$  there exists a negligible function  $neg$  such that

$$\Pr[DLog_{A,G}(n) = 1] \leq neg(n).$$

# The Diffie-Hellman Problems

Computational  
↓

Adv  $\boxed{G, q, g}$   
←  $h_1, h_2$

Chall  
 $x_1, x_2 \leftarrow \mathbb{Z}_q$

# The CDH Problem

public

$$z = g^{x_1 \cdot x_2} \xrightarrow{z}$$

$$h_1 = g^{x_1}, \quad h_2 = g^{x_2}$$

Given  $(G, q, g)$  and uniform  $h_1 = g^{x_1}, h_2 = g^{x_2}$ ,  
compute  $g^{x_1 \cdot x_2}$ .

$$\text{Dlog}_g(h_i) = x_i \quad \begin{pmatrix} h_1 \\ h_2 \end{pmatrix}^{x_1}$$

The CDH Assumption  $\rightarrow$  The Dlog assumption

If you can break  
Dlog

$\rightarrow$

You can break CDH

Decisional  
✓

# The DDH Problem

We say that the DDH problem is hard relative to  $G$  if for all ppt algorithms  $A$ , there exists a negligible function  $neg$  such that

$$|\Pr[A(G, q, g, g^x, g^y, g^z) = 1]$$

$$- \Pr[A(G, q, g, g^x, g^y, g^{xy}) = 1]| \leq neg(n).$$

Ideal

$$x, y, z \leftarrow \mathbb{Z}_q \quad (g^x, g^y, g^z)$$

Real

$$(g^x, g^y, g^{x \cdot y}) \quad x, y \leftarrow \mathbb{Z}_q$$

D

The DDH problem is not hard in  $\mathbb{Z}_p^*$

can modify this attack for any non-prime order group

Legendre Symbol

a poly-time algorithm to check

whether  $z \in \mathbb{Z}_p^*$  is a quadratic residue or not

quadratic residues are elements  $g^a$  where  $a$  is even.

$\text{Dlog}_g(z)$  is even or odd

$(g^x, g^y, g^z)$

vs

$(g^x, g^y, g^{x-y})$

any pattern	0	0	0	1	1	0	X
	0	0	1	1	0	1	X
	0	1	0				
			⋮				

\* Fill in details of distinguishing attack

# Relative Hardness of the Assumptions

Breaking DLog  $\rightarrow$  Breaking CDH  $\rightarrow$  Breaking DDH

DDH Assumption  $\rightarrow$  CDH Assumption  $\rightarrow$  DLog Assumption



## (Finite) Fields:

- A (finite) set of elements that can be viewed as a group with respect to two operations (denoted by addition and multiplication).
- The identity element for addition (0) is not required to have a multiplicative inverse.
- Example:  $\mathbb{Z}_p$ , for prime  $p$ :  $\{0, \dots, p-1\}$ 
  - $\mathbb{Z}_p$  is a group with respect to addition mod  $p$
  - $\mathbb{Z}_p^*$  (taking out 0) is a group with respect to multiplication mod  $p$
- We can now consider \*polynomials\* over  $\mathbb{Z}_p$  as polynomials consist of only multiplication and addition.

# Elliptic Curves over Finite Fields

- $Z_p$  is a finite field for prime  $p$ .
- Let  $p \geq 5$  be a prime
- Consider equation  $E$  in variables  $x, y$  of the form:

$$y^2 := x^3 + Ax + B \text{ mod } p$$

Where  $A, B$  are constants such that  $4A^3 + 27B^2 \neq 0$ .

(this ensures that  $x^3 + Ax + B \text{ mod } p$  has no repeated roots).

Let  $E(Z_p)$  denote the set of pairs  $(x, y) \in Z_p \times Z_p$  satisfying the above equation as well as a special value  $O$ .

$$E(Z_p) := \{(x, y) | x, y \in Z_p \text{ and } y^2 = x^3 + Ax + B \text{ mod } p\} \cup \{O\}$$

The elements  $E(Z_p)$  are called the points on the Elliptic Curve  $E$  and  $O$  is called the point at infinity.

# Elliptic Curves over Finite Fields

Example:

Quadratic Residues over  $Z_7$ .

$$0^2 = 0, 1^2 = 1, 2^2 = 4, 3^2 = 9 = 2, 4^2 = 16 = 2, 5^2 = 25 = 4, 6^2 = 36 = 1.$$

$f(x) := x^3 + 3x + 3$  and curve  $E: y^2 = f(x) \pmod{7}$ .

- Each value of  $x$  for which  $f(x)$  is a non-zero quadratic residue mod 7 yields 2 points on the curve
- Values of  $x$  for which  $f(x)$  is a non-quadratic residue are not on the curve.
- Values of  $x$  for which  $f(x) \equiv 0 \pmod{7}$  give one point on the curve.



# Elliptic Curves over Finite Fields

$f(0) \equiv 3 \pmod{7}$	a quadratic non-residue mod 7
$f(1) \equiv 0 \pmod{7}$	so we obtain the point $(1,0) \in E(\mathbb{Z}_7)$
$f(2) \equiv 3 \pmod{7}$	a quadratic non-residue mod 7
$f(3) \equiv 4 \pmod{7}$	a quadratic residue with roots 2,5. so we obtain the points $(3,2), (3,5) \in E(\mathbb{Z}_7)$
$f(4) \equiv 2 \pmod{7}$	a quadratic residue with roots 3,4. so we obtain the points $(4,3), (4,4) \in E(\mathbb{Z}_7)$
$f(5) \equiv 3 \pmod{7}$	a quadratic non-residue mod 7
$f(6) \equiv 6 \pmod{7}$	a quadratic non-residue mod 7

# Elliptic Curves over Finite Fields

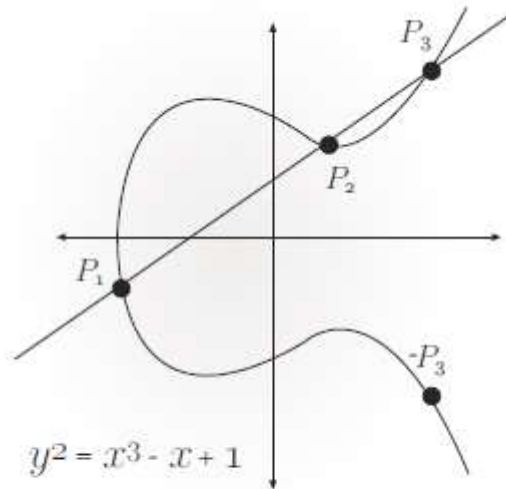


FIGURE 8.2: An elliptic curve over the reals.

Point at infinity:  $O$  sits at the top of the  $y$ -axis and lies on every vertical line.

Every line intersecting  $E(\mathbb{Z}_p)$  in 2 points, intersects it in exactly 3 points:

1. A point  $P$  is counted 2 times if line is tangent to the curve at  $P$ .
2. The point at infinity is also counted when the line is vertical.



# Addition over Elliptic Curves

Binary operation “addition” denoted by  $+$  on points of  $E(\mathbb{Z}_p)$ .

- The point  $O$  is defined to be an additive identity for all  $P \in E(\mathbb{Z}_p)$  we define  $P + O = O + P = P$ .
- For 2 points  $P_1, P_2 \neq O$  on  $E$ , we evaluate their sum  $P_1 + P_2$  by drawing the line through  $P_1, P_2$  (If  $P_1 = P_2$ , draw the line tangent to the curve at  $P_1$ ) and finding the 3<sup>rd</sup> point of intersection  $P_3$  of this line with  $E(\mathbb{Z}_p)$ .
- The 3<sup>rd</sup> point may be  $P_3 = O$  if the line is vertical.
- If  $P_3 = (x, y) \neq O$  then we define  $P_1 + P_2 = (x, -y)$ .
- If  $P_3 = O$  then we define  $P_1 + P_2 = O$ .



# Additive Inverse over Elliptic Curves

- If  $P = (x, y) \neq O$  is a point of  $E(\mathbb{Z}_p)$  then  $-P = (x, -y)$  which is clearly also a point on  $E(\mathbb{Z}_p)$ .
- The line through  $(x, y), (x, -y)$  is vertical and so addition implies that  $P + (-P) = O$ .
- Additionally,  $-O = O$ .

# Groups over Elliptic Curves

Proposition: Let  $p \geq 5$  be prime and let  $E$  be the elliptic curve given by  $y^2 = x^3 + Ax + B \pmod{p}$  where  $4A^3 + 27B^2 \neq 0 \pmod{p}$ .

Let  $P_1, P_2 \neq O$  be points on  $E$  with  $P_1 = (x_1, y_1)$  and  $P_2 = (x_2, y_2)$ .

1. If  $x_1 \neq x_2$  then  $P_1 + P_2 = (x_3, y_3)$  with  
$$x_3 = [m^2 - x_1 - x_2 \pmod{p}], y_3 = [m - (x_1 - x_3) - y_1 \pmod{p}]$$

Where  $m = \left[ \frac{y_2 - y_1}{x_2 - x_1} \pmod{p} \right]$ .

2. If  $x_1 = x_2$  but  $y_1 \neq y_2$  then  $P_1 = -P_2$  and so  $P_1 + P_2 = O$ .
3. If  $P_1 = P_2$  and  $y_1 = 0$  then  $P_1 + P_2 = 2P_1 = O$ .
4. If  $P_1 = P_2$  and  $y_1 \neq 0$  then  $P_1 + P_2 = 2P_1 = (x_3, y_3)$  with  
$$x_3 = [m^2 - 2x_1 \pmod{p}], y_3 = [m - (x_1 - x_3) - y_1 \pmod{p}]$$

Where  $m = \left[ \frac{3x_1^2 + A}{2y_1} \pmod{p} \right]$ .

The set  $E(\mathbb{Z}_p)$  along with the addition rule form an abelian group.

The elliptic curve group of  $E$ .

\*\*Difficult property to verify is associativity. Can check through tedious calculation.

# DDH over Elliptic Curves

DDH: Distinguish  $(aP, bP, abP)$  from  $(aP, bP, cP)$ .

# Size of Elliptic Curve Groups?

How large are EC groups *mod*  $p$ ?

Heuristic:  $y^2 = f(x)$  has 2 solutions whenever  $f(x)$  is a quadratic residue and 1 solution when  $f(x) = 0$ .

Since half the elements of  $Z_p^*$  are quadratic residues, expect  $\frac{2(p-1)}{2} + 1 = p$  points on curve. Including  $O$ , this gives  $p + 1$  points.

Theorem (Hasse bound): Let  $p$  be prime, and let  $E$  be an elliptic curve over  $Z_p$ . Then

$$p + 1 - 2\sqrt{p} \leq |E(Z_p)| \leq p + 1 + 2\sqrt{p}.$$

# Public Key Cryptography



# Key Agreement

The key-exchange experiment  $KE_{A,\Pi}^{eav}(n)$ :

1. Two parties holding  $1^n$  execute protocol  $\Pi$ . This results in a transcript *trans* containing all the messages sent by the parties, and a key  $k$  output by each of the parties.
2. A uniform bit  $b \in \{0,1\}$  is chosen. If  $b = 0$  set  $\hat{k} := k$ , and if  $b = 1$  then choose  $\hat{k} \in \{0,1\}^n$  uniformly at random.
3.  $A$  is given *trans* and  $\hat{k}$ , and outputs a bit  $b'$ .
4. The output of the experiment is defined to be 1 if  $b' = b$  and 0 otherwise.

Definition: A key-exchange protocol  $\Pi$  is secure in the presence of an eavesdropper if for all ppt adversaries  $A$  there is a negligible function  $neg$  such that

$$\Pr \left[ KE_{A,\Pi}^{eav}(n) = 1 \right] \leq \frac{1}{2} + neg(n).$$