COMPUTATIONAL NUMBER THEORY
\( \mathbb{Z} = \{ \ldots, -2, -1, 0, 1, 2, \ldots \} \)

\( \mathbb{N} = \{ 0, 1, 2, \ldots \} \)

\( \mathbb{Z}_+ = \{ 1, 2, 3, \ldots \} \)

d divides \( a \) means \( d \) divides \( a \)

Example: \( 2 \mid 4 \).

For \( a, N \in \mathbb{Z} \) let \( \gcd(a, N) \) be the largest \( d \in \mathbb{Z}_+ \) such that \( d \mid a \) and \( d \mid N \).

Example: \( \gcd(30, 70) = \)
\[ \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} \]

\[ \mathbb{N} = \{0, 1, 2, \ldots\} \]

\[ \mathbb{Z}_+ = \{1, 2, 3, \ldots\} \]

\(d | a\) means \(d\) divides \(a\)

Example: \(2 | 4\).

For \(a, N \in \mathbb{Z}\) let \(\gcd(a, N)\) be the largest \(d \in \mathbb{Z}_+\) such that \(d | a\) and \(d | N\).

Example: \(\gcd(30, 70) = 10\).
Integers mod $N$

For $N \in \mathbb{Z}_+$, let

- $\mathbb{Z}_N = \{0, 1, \ldots, N - 1\}$
- $\mathbb{Z}_N^* = \{a \in \mathbb{Z}_N : \gcd(a, N) = 1\}$
- $\varphi(N) = |\mathbb{Z}_N^*|$

Example: $N = 12$

- $\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$
- $\mathbb{Z}_{12}^* =$
Integers mod $N$

For $N \in \mathbb{Z}_+$, let

- $\mathbb{Z}_N = \{0, 1, \ldots, N - 1\}$
- $\mathbb{Z}_N^* = \{a \in \mathbb{Z}_N : \gcd(a, N) = 1\}$
- $\varphi(N) = |\mathbb{Z}_N^*|$

Example: $N = 12$

- $\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$
- $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$
- $\varphi(12) = \frac{3}{70}$
Integers mod $N$

For $N \in \mathbb{Z}_+$, let

- $\mathbb{Z}_N = \{0, 1, \ldots, N - 1\}$
- $\mathbb{Z}_N^* = \{a \in \mathbb{Z}_N : \gcd(a, N) = 1\}$
- $\varphi(N) = |\mathbb{Z}_N^*|$

**Example:** $N = 12$

- $\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$
- $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$
- $\varphi(12) = 4$
**Fact:** For any \( a, N \in \mathbb{Z} \) with \( N > 0 \) there exist unique \( q, r \in \mathbb{N} \) such that

- \( a = Nq + r \)
- \( 0 \leq r < N \)

Refer to \( q \) as the **quotient** and \( r \) as the **remainder**. Then

\[
a \mod N = r \in \mathbb{Z}_N
\]

is the remainder when \( a \) is divided by \( N \).

**Def:** \( a \equiv b \pmod{N} \) iff \((a \mod N) = (b \mod N)\).

**Examples:**

- If \( a = 17 \) and \( N = 3 \) then the quotient and remainder are \( q = ? \) and \( r = ? \).
Division and mod

Fact: For any $a, N \in \mathbb{Z}$ with $N > 0$ there exist unique $q, r \in \mathbb{N}$ such that

- $a = Nq + r$
- $0 \leq r < N$

Refer to $q$ as the quotient and $r$ as the remainder. Then

$$a \mod N = r \in \mathbb{Z}_N$$

is the remainder when $a$ is divided by $N$.

Def: $a \equiv b \pmod{N}$ iff $(a \mod N) = (b \mod N)$.

Examples:

- If $a = 17$ and $N = 3$ then the quotient and remainder are $q = 5$ and $r = 2$
**Fact:** For any $a, N \in \mathbb{Z}$ with $N > 0$ there exist unique $q, r \in \mathbb{N}$ such that

- $a = Nq + r$
- $0 \leq r < N$

Refer to $q$ as the **quotient** and $r$ as the **remainder.** Then

$$a \mod N = r \in \mathbb{Z}_N$$

is the remainder when $a$ is divided by $N$.

**Def:** $a \equiv b \pmod{N}$ iff $(a \mod N) = (b \mod N)$.

**Examples:**
- If $a = 17$ and $N = 3$ then the quotient and remainder are $q = 5$ and $r = 2$
- $17 \mod 3 =$
**Fact:** For any $a, N \in \mathbb{Z}$ with $N > 0$ there exist unique $q, r \in \mathbb{N}$ such that

- $a = Nq + r$
- $0 \leq r < N$

Refer to $q$ as the quotient and $r$ as the remainder. Then

$$a \mod N = r \in \mathbb{Z}_N$$

is the remainder when $a$ is divided by $N$.

**Def:** $a \equiv b \pmod{N}$ iff $(a \mod N) = (b \mod N)$.

**Examples:**

- If $a = 17$ and $N = 3$ then the quotient and remainder are $q = 5$ and $r = 2$
- $17 \mod 3 = 2$
- $17 \equiv 14 \pmod{3}$
Division and mod

**Fact:** For any $a, N \in \mathbb{Z}$ with $N > 0$ there exist unique $q, r \in \mathbb{N}$ such that

- $a = Nq + r$
- $0 \leq r < N$

Refer to $q$ as the quotient and $r$ as the remainder. Then

$$a \mod N = r \in \mathbb{Z}_N$$

is the remainder when $a$ is divided by $N$.

**Def:** $a \equiv b \pmod{N}$ iff $(a \mod N) = (b \mod N)$.

**Examples:**

- If $a = 17$ and $N = 3$ then the quotient and remainder are $q = 5$ and $r = 2$
- $17 \mod 3 = 2$
- $17 \equiv 14 \pmod{3}$ because $17 \mod 3 = 14 \mod 3 = 2$
Groups

Let $G$ be a non-empty set, and let $\cdot$ be a binary operation on $G$. This means that for every two points $a, b \in G$, a value $a \cdot b$ is defined.

Examples:

- $G = \mathbb{Z}_{12}$ and “$\cdot$” is addition modulo 12, meaning
  \[ a \cdot b = (a + b) \mod 12 \]
- $G = \mathbb{Z}_{12}^*$ and “$\cdot$” is multiplication modulo 12, meaning
  \[ a \cdot b = ab \mod 12 \]
Let $G$ be a non-empty set, and let $\cdot$ be a binary operation on $G$. This means that for every two points $a, b \in G$, a value $a \cdot b$ is defined.

We say that $G$ is a **group** if it has the following properties:

1. **Closure:** For every $a, b \in G$ it is the case that $a \cdot b$ is also in $G$.

2. **Associativity:** For every $a, b, c \in G$ it is the case that $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

3. **Identity:** There exists an element $1 \in G$ such that $a \cdot 1 = 1 \cdot a = a$ for all $a \in G$.

4. **Invertibility:** For every $a \in G$ there exists a unique $b \in G$ such that $a \cdot b = b \cdot a = 1$.

The element $b$ in the invertibility condition is referred to as the inverse of the element $a$, and is denoted $a^{-1}$. 
**Fact:** Let $N \in \mathbb{Z}_+$. Then $\mathbb{Z}_N$ is a group under addition modulo $N$.

Addition modulo $N$: $a, b \mapsto a + b \mod N$
**Fact:** Let $N \in \mathbb{Z}_+$. Then $\mathbb{Z}_N$ is a group under addition modulo $N$.

**Example:** Let $N = 12$, so $\mathbb{Z}_N = \mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$
Fact: Let $N \in \mathbb{Z}_+$. Then $\mathbb{Z}_N$ is a group under addition modulo $N$.

Example: Let $N = 12$, so $\mathbb{Z}_N = \mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

Closure: $a, b \in \mathbb{Z}_N \Rightarrow a + b \mod N \in \mathbb{Z}_N$.

Check: $9 + 7 \mod 12 = 16 \mod 12 = 4 \in \mathbb{Z}_{12}$
**Fact:** Let \( N \in \mathbb{Z}_+ \). Then \( \mathbb{Z}_N \) is a group under addition modulo \( N \).

**Example:** Let \( N = 12 \), so \( \mathbb{Z}_N = \mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\} \)

**Associative:**
\[
((a + b \text{ mod } N) + c) \text{ mod } N = (a + (b + c \text{ mod } N)) \text{ mod } N
\]

**Check:**
\[
(9 + 7 \text{ mod } 12) + 10 \text{ mod } 12 = (16 \text{ mod } 12) + 10 \text{ mod } 12 = 4 + 10 \text{ mod } 12 = 2
\]
\[
9 + (7 + 10 \text{ mod } 12) \text{ mod } 12 = 9 + (17 \text{ mod } 12) \text{ mod } 12 = 9 + 5 \text{ mod } 12 = 2
\]
Zₙ under MOD-ADD

**Fact:** Let \( N \in \mathbb{Z}_+ \). Then \( \mathbb{Z}_N \) is a group under addition modulo \( N \).

**Example:** Let \( N = 12 \), so \( \mathbb{Z}_N = \mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\} \)

**Identity:** 0 is the identity element because \( a + 0 \equiv 0 + a \equiv a \) (mod \( N \)) for every \( a \).
Fact: Let $N \in \mathbb{Z}_+$. Then $\mathbb{Z}_N$ is a group under addition modulo $N$.

Example: Let $N = 12$, so $\mathbb{Z}_N = \mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

Inverse: $\forall a \in \mathbb{Z}_N \exists a^{-1} \in \mathbb{Z}_N^*$ such that $a + a^{-1} \mod N = 0$.

Check: $9^{-1}$ is the $x \in \mathbb{Z}_{12}$ satisfying

$$9 + x \equiv 0 \pmod{12}$$

so $x =$
Fact: Let $N \in \mathbb{Z}_+$. Then $\mathbb{Z}_N$ is a group under addition modulo $N$.

Example: Let $N = 12$, so $\mathbb{Z}_N = \mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

Inverse: $\forall a \in \mathbb{Z}_N \quad \exists a^{-1} \in \mathbb{Z}_{N}^*$ such that $a + a^{-1} \mod N = 0$.

Check: $9^{-1}$ is the $x \in \mathbb{Z}_{12}$ satisfying

$$9 + x \equiv 0 \pmod{12}$$

so $x = 3$
Fact: Let $N \in \mathbb{Z}_+$. Then $\mathbb{Z}_N^*$ is a group under multiplication modulo $N$.

Multiplication modulo $N$: $a, b \mapsto ab \mod N$

Example: Let $N = 12$, so $\mathbb{Z}_N^* = \mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$
Fact: Let $N \in \mathbb{Z}_+$. Then $\mathbb{Z}_N^*$ is a group under multiplication modulo $N$.

Example: Let $N = 12$, so $\mathbb{Z}_N^* = \mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$

Closure: $a, b \in \mathbb{Z}_N^* \Rightarrow ab \pmod{N} \in \mathbb{Z}_N^*$. That is

$$\gcd(a, N) = \gcd(b, N) = 1 \Rightarrow \gcd(ab \pmod{N}, N) = 1$$

Check: $5 \cdot 7 \pmod{12} = 35 \pmod{12} = 11 \in \mathbb{Z}_{12}^*$

If $a, b \in \mathbb{Z}_{12}^*$, $ab \pmod{12}$ can never be 3!
**Fact:** Let $N \in \mathbb{Z}_+$. Then $\mathbb{Z}_N^*$ is a group under multiplication modulo $N$.

**Example:** Let $N = 12$, so $\mathbb{Z}_N^* = \mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$

**Associative:** $((ab \mod N)c) \mod N = (a(bc \mod N)) \mod N$

**Check:**

$$(5 \cdot 7 \mod 12) \cdot 11 \mod 12 = (35 \mod 12) \cdot 11 \mod 12$$

$$= 11 \cdot 11 \mod 12 = 1$$

$$5 \cdot (7 \cdot 11 \mod 12) \mod 12 = 5 \cdot (77 \mod 12) \mod 12$$

$$= 5 \cdot 5 \mod 12 = 1$$
Fact: Let $N \in \mathbb{Z}_+$. Then $\mathbb{Z}_N^*$ is a group under multiplication modulo $N$.

Example: Let $N = 12$, so $\mathbb{Z}_N^* = \mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$

Identity: 1 is the identity element because $a \cdot 1 \equiv 1 \cdot a \equiv a \pmod{N}$ for all $a$. 
Fact: Let $N \in \mathbb{Z}_+$. Then $\mathbb{Z}_N^*$ is a group under multiplication modulo $N$.

Example: Let $N = 12$, so $\mathbb{Z}_N^* = \mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$

Inverse: $\forall a \in \mathbb{Z}_N^* \exists a^{-1} \in \mathbb{Z}_N^*$ such that $a \cdot a^{-1} \mod N = 1$.

Check: $5^{-1}$ is the $x \in \mathbb{Z}_{12}^*$ satisfying $5x \equiv 1 \pmod{12}$

so $x =$
**Z\_N^\ast** under MOD-MULT

**Fact:** Let \( N \in \mathbb{Z}_+ \). Then \( \mathbb{Z}_N^\ast \) is a group under multiplication modulo \( N \).

**Example:** Let \( N = 12 \), so \( \mathbb{Z}_N^\ast = \mathbb{Z}_{12}^\ast = \{1, 5, 7, 11\} \)

**Inverse:** \( \forall a \in \mathbb{Z}_N^\ast \exists a^{-1} \in \mathbb{Z}_N^\ast \) such that \( a \cdot a^{-1} \mod N = 1 \).

**Check:** \( 5^{-1} \) is the \( x \) satisfying

\[
5x \equiv 1 \pmod{12}
\]

so \( x = 5 \)
Computational Shortcuts

What is $5 \cdot 8 \cdot 10 \cdot 16 \mod 21$?
Computational Shortcuts

What is $5 \cdot 8 \cdot 10 \cdot 16 \mod 21$?

**Slow way:** First compute

$$5 \cdot 8 \cdot 10 \cdot 16 = 40 \cdot 10 \cdot 16 = 400 \cdot 16 = 6400$$

and then compute $6400 \mod 21 =$
What is $5 \cdot 8 \cdot 10 \cdot 16 \mod 21$?

**Slow way:** First compute

$$5 \cdot 8 \cdot 10 \cdot 16 = 40 \cdot 10 \cdot 16 = 400 \cdot 16 = 6400$$

and then compute $6400 \mod 21 = 16$

**Fast way:**
- $5 \cdot 8 \mod 21 = 40 \mod 21 = 19$
- $19 \cdot 10 \mod 21 = 190 \mod 21 = 1$
- $1 \cdot 16 \mod 21 = 16$
Let $G$ be a group and $a \in G$. We let $a^0 = 1$ be the identity element and for $n \geq 1$, we let

$$a^n = a \cdot a \cdots a.$$ 

Also we let

$$a^{-n} = a^{-1} \cdot a^{-1} \cdots a^{-1}.$$ 

This ensures that for all $i, j \in \mathbb{Z}$,

- $a^{i+j} = a^i \cdot a^j$
- $a^{ij} = (a^i)^j = (a^j)^i$
- $a^{-i} = (a^i)^{-1} = (a^{-1})^i$

Meaning we can manipulate exponents “as usual”.
Examples

Let $N = 14$ and $G = \mathbb{Z}_N^*$. Then modulo $N$ we have

$$5^3 =$$
Examples

Let $N = 14$ and $G = \mathbb{Z}_N^*$. Then modulo $N$ we have

$$5^3 = 5 \cdot 5 \cdot 5$$
Examples

Let $N = 14$ and $G = \mathbb{Z}_N^*$. Then modulo $N$ we have

$$5^3 = 5 \cdot 5 \cdot 5 \equiv 25 \cdot 5 \equiv 11 \cdot 5 \equiv 55 \equiv 13$$

and

$$5^{-3} =$$
Examples

Let $N = 14$ and $G = \mathbb{Z}_N^*$. Then modulo $N$ we have

$$5^3 = 5 \cdot 5 \cdot 5 \equiv 25 \cdot 5 \equiv 11 \cdot 5 \equiv 55 \equiv 13$$

and

$$5^{-3} = 5^{-1} \cdot 5^{-1} \cdot 5^{-1}$$
Let $N = 14$ and $G = \mathbb{Z}_N^*$. Then modulo $N$ we have

$$5^3 = 5 \cdot 5 \cdot 5 \equiv 25 \cdot 5 \equiv 11 \cdot 5 \equiv 55 \equiv 13$$

and

$$5^{-3} = 5^{-1} \cdot 5^{-1} \cdot 5^{-1} \equiv 3 \cdot 3 \cdot 3$$
Examples

Let $N = 14$ and $G = \mathbb{Z}_{N}^{*}$. Then modulo $N$ we have

$$5^{3} = 5 \cdot 5 \cdot 5 \equiv 25 \cdot 5 \equiv 11 \cdot 5 \equiv 55 \equiv 13$$

and

$$5^{-3} = 5^{-1} \cdot 5^{-1} \cdot 5^{-1} \equiv 3 \cdot 3 \cdot 3 \equiv 27 \equiv 13$$
The order of a group $G$ is its size $|G|$, meaning the number of elements in it.

Example: The order of $\mathbb{Z}_{21}^*$ is
The **order** of a group $G$ is its size $|G|$, meaning the number of elements in it.

**Example:** The order of $\mathbb{Z}_{21}^*$ is 12 because

$$\mathbb{Z}_{21}^* = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$$

**Fact:** Let $G$ be a group of order $m$ and $a \in G$. Then, $a^m = 1$.

**Examples:** Modulo 21 we have

- $5^{12} \equiv (5^3)^4 \equiv 20^4 \equiv (-1)^4 \equiv 1$
- $8^{12} \equiv (8^2)^6 \equiv (1)^6 \equiv 1$
Corollary: Let $G$ be a group of order $m$ and $a \in G$. Then for any $i \in \mathbb{Z}$,

$$a^i = a^i \mod m.$$ 

Example: What is $5^{74} \mod 21$?
**Corollary:** Let $G$ be a group of order $m$ and $a \in G$. Then for any $i \in \mathbb{Z}$,

$$a^i = a^{i \mod m}.$$ 

**Example:** What is $5^{74} \mod 21$?

**Solution:** Let $G = \mathbb{Z}_{21}^*$ and $a = 5$. Then, $m = 12$, so

$$5^{74} \mod 21 = 5^{74 \mod 12} \mod 21 = 5^2 \mod 21 = 4.$$
In an algorithms course, the cost of arithmetic is often assumed to be $O(1)$, because numbers are small. In cryptography numbers are very, very BIG!

Typical sizes are $2^{512}$, $2^{1024}$, $2^{2048}$.

Numbers are provided to algorithms in binary. The length of $a$, denoted $|a|$, is the number of bits in the binary encoding of $a$.

**Example:** $|7| = 3$ because 7 is 111 in binary.

Running time is measured as a function of the lengths of the inputs.
Addition

\[(a, b) \mapsto a + b\]

\[
\begin{array}{cccccc}
1 & 0 & 1 & 1 & 0 & 1 \\
+ & 1 & 0 & 1 & 1 & 1 \\
\hline
1 & 1 & 1 & 0 & 0 & 0 \\
\end{array}
\]

By the usual “carry” algorithm, we can compute \(a + b\) in time \(O(|a| + |b|)\).

Addition is linear time.
Multiplication

\[(a, b) \mapsto ab\]

\[
\begin{array}{cccccc}
1 & 0 & 1 & 1 & 1 & 0 \\
\times & & & & & \\
1 & 0 & 1 & & & 1 \\
\hline
1 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
+ & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
\hline
1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\
\end{array}
\]

By the usual algorithm, we can compute \(ab\) in time \(O(|a| \cdot |b|)\).

Multiplication is \textit{quadratic} time.
Integer Division

\(\text{INT-DIV}(a, N)\) returns \((q, r)\) such that

- \(a = qN + r\)
- \(0 \leq r < N\)

**Example:** \(\text{INT-DIV}(17, 3) = (5, 2)\)

By the usual algorithm, we can compute \(\text{INT-DIV}(a, N)\) in time \(O(|a| \cdot |N|)\).

Integer division is **quadratic** time.
(a, N) ↦ a \mod N

But

(q, r) \leftarrow \text{INT-DIV}(a, N)
return r

computes a \mod N, so again the time needed is \(O(|a| \cdot |N|)\).

Mod is \textit{quadratic} time.
About gcd

**Fact:** If $a, N \in \mathbb{Z}$ and $(a, N) \neq (0, 0)$ then $\gcd(a, N)$ is the smallest positive integer in the set

$$\{a \cdot a' + N \cdot N' : a', N' \in \mathbb{Z}\}$$

**Corollary:** If $d = \gcd(a, N)$ then there are “weights” $a', N' \in \mathbb{Z}$ such that

$$d = a \cdot a' + N \cdot N'$$

**Example:** $\gcd(20, 12) = 4$ and $4 = 20 \cdot a' + 12 \cdot N'$ for

- $a' =$
- $N' =$
About gcd

**Fact:** If \( a, N \in \mathbb{Z} \) and \((a, N) \neq (0, 0)\) then \( \gcd(a, N) \) is the smallest positive integer in the set

\[
\{ a \cdot a' + N \cdot N' : a', N' \in \mathbb{Z} \}
\]

**Corollary:** If \( d = \gcd(a, N) \) then there are “weights” \( a', N' \in \mathbb{Z} \) such that

\[
d = a \cdot a' + N \cdot N'
\]

**Example:** \( \gcd(20, 12) = 4 \) and \( 4 = 20 \cdot a' + 12 \cdot N' \) for
- \( a' = 2 \)
- \( N' = -3 \)
Extended gcd

\[ \text{EXT-GCD}(a, N) \leftrightarrow (d, a', N') \] such that

\[ d = \gcd(a, N) = a \cdot a' + N \cdot N'. \]

**Lemma:** Let \((q, r) = \text{INT-DIV}(a, N)\). Then, \(\gcd(a, N) = \gcd(N, r)\).

**Example:** \(\text{INT-DIV}(17, 3) = (5, 2)\) so \(\gcd(17, 3) = \gcd(3, 2)\).
Extended gcd

\[ \text{EXT-GCD}(a, N) \rightarrow (d, a', N') \] such that

\[ d = \gcd(a, N) = a \cdot a' + N \cdot N'. \]

**Lemma:** Let \( (q, r) = \text{INT-DIV}(a, N) \). Then, \( \gcd(a, N) = \gcd(N, r) \)

**Alg**

\begin{align*}
\text{EXT-GCD}(a, N) & \quad // (a, N) \neq (0, 0) \\
\text{if } N = 0 & \text{ then return } (a, 1, 0) \\
\text{else} & \\
(q, r) & \leftarrow \text{INT-DIV}(a, N) \\
(d, x, y) & \leftarrow \text{EXT-GCD}(N, r) \\
a' & \leftarrow \square; \ N' \leftarrow \square \\
\text{return } (d, a', N')
\end{align*}
Extended gcd

We know that $a = qN + r$ with $0 \leq r < N$ and we have $d, x, y$ satisfying

$$d = \gcd(N, r) = Nx + ry$$

Then

$$d = Nx + ry$$
$$= Nx + (a - qN)y$$
$$= ay + N(x - qy)$$

so $d = \gcd(a, N) = a \cdot a' + N \cdot N'$ with $a' = y$ and $N' = x - qy$. 
**Algorithm EXT-GCD**($a, N$)  // ($a, N) \neq (0, 0)$

if $N = 0$ then return ($a, 1, 0$)
else
  ($q, r) \leftarrow \text{INT-DIV}(a, N)$
  ($d, x, y) \leftarrow \text{EXT-GCD}(N, r)$
  $a' \leftarrow y$;  $N' \leftarrow x - qy$
return ($d, a', N'$)

Running time analysis is non-trivial (worst case is Fibonacci numbers) and shows that the time is $\mathcal{O}(|a| \cdot |N|)$.

So the extended gcd can be computed in **quadratic** time.
For \( a, N \) such that \( \gcd(a, N) = 1 \), we want to compute \( a^{-1} \mod N \), meaning the unique \( a' \in \mathbb{Z}_N^* \) satisfying \( aa' \equiv 1 \pmod{N} \).

But if we let \((d, a', N') \leftarrow \text{EXT-GCD}(a, N)\) then

\[
d = 1 = \gcd(a, N) = a \cdot a' + N \cdot N'
\]

But \( N \cdot N' \equiv 0 \pmod{N} \) so \( aa' \equiv 1 \pmod{N} \)

**Alg** \textbf{MOD-INV}(a, N)

\((d, a', N') \leftarrow \text{EXT-GCD}(a, N)\)

return \( a' \mod N \)

Modular inverse can be computed in \textit{quadratic} time.
Let $G$ be a group and $a \in G$. For $n \in \mathbb{N}$, we want to compute $a^n \in G$.

We know that

$$a^n = a \cdot a \cdots a$$

Consider:

\[
y \leftarrow 1 \\
\text{for } i = 1, \ldots, n \text{ do } y \leftarrow y \cdot a \\
\text{return } y
\]

**Question:** Is this a good algorithm?
Let $G$ be a group and $a \in G$. For $n \in \mathbb{N}$, we want to compute $a^n \in G$.

We know that

$$a^n = \underbrace{a \cdot a \cdots a}_n$$

Consider:

$$y \leftarrow 1$$
for $i = 1, \ldots, n$ do $y \leftarrow y \cdot a$
return $y$

**Question:** Is this a good algorithm?

**Answer:** It is correct but VERY SLOW. The number of group operations is

$$\mathcal{O}(n) = \mathcal{O}(2^{|n|})$$

so it is exponential time. For $n \approx 2^{512}$ it is prohibitively expensive.
We can compute

\[ a \rightarrow a^2 \rightarrow a^4 \rightarrow a^8 \rightarrow a^{16} \rightarrow a^{32} \]

in just 5 steps by repeated squaring. So we can compute \( a^n \) in \( i \) steps when \( n = 2^i \).

But what if \( n \) is not a power of 2?
Suppose the binary length of $n$ is 5, meaning the binary representation of $n$ has the form $b_4 b_3 b_2 b_1 b_0$. Then

\[ n = 2^4 b_4 + 2^3 b_3 + 2^2 b_2 + 2^1 b_1 + 2^0 b_0 \]
\[ = 16b_4 + 8b_3 + 4b_2 + 2b_1 + b_0 . \]

We want to compute $a^n$. Our exponentiation algorithm will proceed to compute the values $y_5, y_4, y_3, y_2, y_1, y_0$ in turn, as follows:

\[
\begin{align*}
    y_5 &= 1 \\
    y_4 &= y_5^2 \cdot a^{b_4} = a^{b_4} \\
    y_3 &= y_4^2 \cdot a^{b_3} = a^{2b_4+b_3} \\
    y_2 &= y_3^2 \cdot a^{b_2} = a^{4b_4+2b_3+b_2} \\
    y_1 &= y_2^2 \cdot a^{b_1} = a^{8b_4+4b_3+2b_2+b_1} \\
    y_0 &= y_1^2 \cdot a^{b_0} = a^{16b_4+8b_3+4b_2+2b_1+b_0} .
\end{align*}
\]
Fast Exponentiation Algorithm

Let \( \text{bin}(n) = b_{k-1} \ldots b_0 \) be the binary representation of \( n \), meaning

\[
n = \sum_{i=0}^{k-1} b_i 2^i
\]

**Alg** \( \text{EXP}_G(a, n) \) // \( a \in G, n \geq 1 \)

\[
\quad b_{k-1} \ldots b_0 \leftarrow \text{bin}(n)
\]

\[
\quad y \leftarrow 1
\]

\[
\text{for } i = k - 1 \text{ downto } 0 \text{ do } y \leftarrow y^2 \cdot a^{b_i}
\]

\[
\text{return } y
\]

The running time is \( \mathcal{O}(|n|) \) group operations.

MOD-EXP(\( a, n, N \)) returns \( a^n \mod N \) in time \( \mathcal{O}(|n| \cdot |N|^2) \), meaning is cubic time.
<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Input</th>
<th>Output</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>INT-DIV</td>
<td>$a, N$</td>
<td>$q, r$</td>
<td>quadratic</td>
</tr>
<tr>
<td>MOD</td>
<td>$a, N$</td>
<td>$a \mod N$</td>
<td>quadratic</td>
</tr>
<tr>
<td>EXT-GCD</td>
<td>$a, N$</td>
<td>$(d, a', N')$</td>
<td>quadratic</td>
</tr>
<tr>
<td>MOD-ADD</td>
<td>$a, b, N$</td>
<td>$a + b \mod N$</td>
<td>linear</td>
</tr>
<tr>
<td>MOD-MULT</td>
<td>$a, b, N$</td>
<td>$ab \mod N$</td>
<td>quadratic</td>
</tr>
<tr>
<td>MOD-INV</td>
<td>$a, N$</td>
<td>$a^{-1} \mod N$</td>
<td>quadratic</td>
</tr>
<tr>
<td>MOD-EXP</td>
<td>$a, n, N$</td>
<td>$a^n \mod N$</td>
<td>cubic</td>
</tr>
<tr>
<td>EXP&lt;sub&gt;G&lt;/sub&gt;</td>
<td>$a, n$</td>
<td>$a^n \in G$</td>
<td>$O(</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Definition: Let $G$ be a group and $S \subseteq G$. Then $S$ is called a subgroup of $G$ if $S$ is itself a group under $G$’s operation.

Example: Let $G = \mathbb{Z}_{11}^*$ and $S = \{1, 2, 3\}$. Then $S$ is not a subgroup because

- $2 \cdot 3 \mod 11 = 6 \notin S$, violating Closure.
- $3^{-1} \mod 11 = 4 \notin S$, violating Inverse.

But $\{1, 3, 4, 5, 9\}$ is a subgroup, as you can check.
Let $G$ be a (finite) group.

**Definition:** The order of $g \in G$, denoted $o(g)$, is the smallest integer $n \geq 1$ such that $g^n = 1$. 
Order determinations

Let \( G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} \).

<table>
<thead>
<tr>
<th>( i \mod 11 )</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 2^i \mod 11 )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Let $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

<table>
<thead>
<tr>
<th>$i$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^i \mod 11$</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Order determinations

Let $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. 

<table>
<thead>
<tr>
<th>$i$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^i \mod 11$</td>
<td>1</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Let $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

<table>
<thead>
<tr>
<th>$i$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^i \mod 11$</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Let $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. 

<table>
<thead>
<tr>
<th>$i$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^i \mod 11$</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Let \( G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} \).

<table>
<thead>
<tr>
<th>( i )</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 2^i \mod 11 )</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Let $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. 

<table>
<thead>
<tr>
<th>$i$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^i \mod 11$</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


Let $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

<table>
<thead>
<tr>
<th>$i$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^i \mod 11$</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Let $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. 

<table>
<thead>
<tr>
<th>$i$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^i \mod 11$</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>9</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Order determinations

Let $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

<table>
<thead>
<tr>
<th>$i$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^i \mod 11$</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Let $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

\[
\begin{array}{c|cccccccccc}
  i & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\
  \hline 
  2^i \pmod{11} & 1 & 2 & 4 & 8 & 5 & 10 & 9 & 7 & 3 & 6
\end{array}
\]
Let $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

<table>
<thead>
<tr>
<th>$i$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^i \mod 11$</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>$5^i \mod 11$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Let $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

<table>
<thead>
<tr>
<th>$i$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^i \mod 11$</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>$5^i \mod 11$</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Order determinations
Let $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

<table>
<thead>
<tr>
<th>$i$ mod 11</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^i$ mod 11</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>$5^i$ mod 11</td>
<td>1</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Order determinations

Let $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

<table>
<thead>
<tr>
<th>$i$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^i \mod 11$</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>$5^i \mod 11$</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Let \( G = \mathbb{Z}^*_{11} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} \).

<table>
<thead>
<tr>
<th>( i )</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 2^i \mod 11 )</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>( 5^i \mod 11 )</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Let \( G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}. \)

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 2^i \mod 11 )</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>( 5^i \mod 11 )</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Let $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

<table>
<thead>
<tr>
<th>$i$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^i \mod 11$</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>$5^i \mod 11$</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>9</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Let $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

<table>
<thead>
<tr>
<th>$i$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^i \mod 11$</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>$5^i \mod 11$</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>9</td>
<td>1</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Let $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. 

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^i \mod 11$</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>$5^i \mod 11$</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>9</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Let $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

<table>
<thead>
<tr>
<th>$i$ mod 11</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^i$ mod 11</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>$5^i$ mod 11</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>9</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Let $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

<table>
<thead>
<tr>
<th></th>
<th>$i$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^i \mod 11$</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>6</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>$5^i \mod 11$</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>9</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>9</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Let $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

<table>
<thead>
<tr>
<th>$i$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^i \mod 11$</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>$5^i \mod 11$</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>9</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>9</td>
<td>1</td>
</tr>
</tbody>
</table>
Order determinations

Let $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

<table>
<thead>
<tr>
<th>$i$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^i \mod 11$</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>$5^i \mod 11$</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>9</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>9</td>
<td>1</td>
</tr>
</tbody>
</table>

The order $o(a)$ of $a$ is the smallest $n \geq 1$ such that $a^n = 1$. So

- $o(2) =$
Let $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. 

<table>
<thead>
<tr>
<th>$i$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^i \mod 11$</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>$5^i \mod 11$</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>9</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>9</td>
<td>1</td>
</tr>
</tbody>
</table>

The order $o(a)$ of $a$ is the smallest $n \geq 1$ such that $a^n = 1$. So

- $o(2) = 10$
Order determinations

Let \( G = \mathbb{Z}_{11}^{*} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} \).

<table>
<thead>
<tr>
<th>( i )</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 2^i \mod 11 )</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>( 5^i \mod 11 )</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>9</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>9</td>
<td>1</td>
</tr>
</tbody>
</table>

The order \( o(a) \) of \( a \) is the smallest \( n \geq 1 \) such that \( a^n = 1 \). So
- \( o(2) = 10 \)
- \( o(5) = \)
Let $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^i \mod 11$</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>$5^i \mod 11$</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>9</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>9</td>
<td>1</td>
</tr>
</tbody>
</table>

The order $o(a)$ of $a$ is the smallest $n \geq 1$ such that $a^n = 1$. So

- $o(2) = 10$
- $o(5) = 5$
Definition: For $g \in G$ we let

$$\langle g \rangle = \{ g^0, g^1, \ldots, g^{o(g) - 1} \}.$$ 

This is a subgroup of $G$ and its order (that is, its size) is the order $o(g)$ of $G$. 

Subgroup generated by $g \in G$
Fact: The order $|S|$ of a subgroup $S$ always divides the order $|G|$ of the group $G$.

Fact: The order $o(g)$ of $g \in G$ always divides $|G|$.

Example: If $G = \mathbb{Z}_{11}^*$ then

- $|G| =$
Fact: The order $|S|$ of a subgroup $S$ always divides the order $|G|$ of the group $G$.

Fact: The order $o(g)$ of $g \in G$ always divides $|G|$.

Example: If $G = \mathbb{Z}_{11}^*$ then

- $|G| = 10$
- $o(2) = 10$ which divides 10
- $o(5) = 5$ which divides 10
Let $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

\[
\begin{array}{c|cccccccccc}
  i & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\
  \hline
  2 \mod 11 & 1 & 2 & 4 & 8 & 5 & 10 & 9 & 7 & 3 & 6 & 1 \\
  5 \mod 11 & 1 & 5 & 3 & 4 & 9 & 1 & 5 & 3 & 4 & 9 & 1 \\
\end{array}
\]

so

\[
\langle 2 \rangle = \\
\langle 5 \rangle = 
\]
Subgroups generated by a group element

Let $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

<table>
<thead>
<tr>
<th>$i$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^i \mod 11$</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>$5^i \mod 11$</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>9</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>9</td>
<td>1</td>
</tr>
</tbody>
</table>

so

$$\langle 2 \rangle = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

$$\langle 5 \rangle =$$
Subgroups generated by a group element

Let \( G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} \).

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 2' \mod 11 )</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>( 5' \mod 11 )</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>9</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>9</td>
<td>1</td>
</tr>
</tbody>
</table>

so

\[
\langle 2 \rangle = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}
\]

\[
\langle 5 \rangle = \{1, 3, 4, 5, 9\}
\]
Generators

Definition: \( g \in G \) is a generator (or primitive element) if \( \langle g \rangle = G \).

Fact: \( g \in G \) is a generator iff \( o(g) = |G| \).

Definition: \( G \) is cyclic if it has a generator.
Generators

Let $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^i \mod 11$</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>$5^i \mod 11$</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>9</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>9</td>
<td>1</td>
</tr>
</tbody>
</table>

so

\[
\langle 2 \rangle = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}
\]
\[
\langle 5 \rangle = \{1, 3, 4, 5, 9\}
\]
Generators

Let $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

<table>
<thead>
<tr>
<th>$i$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^i \mod 11$</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>$5^i \mod 11$</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>9</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>9</td>
<td>1</td>
</tr>
</tbody>
</table>

so

\[
\langle 2 \rangle = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}
\]

\[
\langle 5 \rangle = \{1, 3, 4, 5, 9\}
\]

- Is 2 a generator?
Generators

Let $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

<table>
<thead>
<tr>
<th>$i$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^i \mod 11$</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>$5^i \mod 11$</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>9</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>9</td>
<td>1</td>
</tr>
</tbody>
</table>

so

\[ \langle 2 \rangle = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} \]
\[ \langle 5 \rangle = \{1, 3, 4, 5, 9\} \]

- Is 2 a generator?
  YES because $\langle 2 \rangle = \mathbb{Z}_{11}^*$. 
Generators

Let \( G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} \).

<table>
<thead>
<tr>
<th>( i )</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 2^i \mod 11 )</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>( 5^i \mod 11 )</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>9</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>9</td>
<td>1</td>
</tr>
</tbody>
</table>

so

\[
\langle 2 \rangle = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}
\]

\[
\langle 5 \rangle = \{1, 3, 4, 5, 9\}
\]

• Is 2 a generator?
  YES because \( \langle 2 \rangle = \mathbb{Z}_{11}^* \).

• Is 5 a generator?
Generators

Let $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

<table>
<thead>
<tr>
<th>$i$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^i \mod 11$</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>$5^i \mod 11$</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>9</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>9</td>
<td>1</td>
</tr>
</tbody>
</table>

so

$\langle 2 \rangle = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

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

- Is 2 a generator?
  YES because $\langle 2 \rangle = \mathbb{Z}_{11}^*$.
- Is 5 a generator?
  NO because $\langle 5 \rangle \neq \mathbb{Z}_{11}^*$. 
Generators

Let \( G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} \).

<table>
<thead>
<tr>
<th>( i )</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 2^i \mod 11 )</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>( 5^i \mod 11 )</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>9</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>9</td>
<td>1</td>
</tr>
</tbody>
</table>

so

\[
\langle 2 \rangle = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}
\]

\[
\langle 5 \rangle = \{1, 3, 4, 5, 9\}
\]

- Is 2 a generator?
  YES because \( \langle 2 \rangle = \mathbb{Z}_{11}^* \).

- Is 5 a generator?
  NO because \( \langle 5 \rangle \neq \mathbb{Z}_{11}^* \).

- Is \( \mathbb{Z}_{11}^* \) cyclic?

Generators

Let $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

<table>
<thead>
<tr>
<th>$i$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^i \mod 11$</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>$5^i \mod 11$</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>9</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>9</td>
<td>1</td>
</tr>
</tbody>
</table>

so

\[
\langle 2 \rangle = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}
\]

\[
\langle 5 \rangle = \{1, 3, 4, 5, 9\}
\]

- Is 2 a generator?
  YES because $\langle 2 \rangle = \mathbb{Z}_{11}^*$.

- Is 5 a generator?
  NO because $\langle 5 \rangle \neq \mathbb{Z}_{11}^*$.

- Is $\mathbb{Z}_{11}^*$ cyclic?
  YES because it has a generator
Discrete Log

If $G = \langle g \rangle$ is cyclic then for every $a \in G$ there is a unique exponent $i \in \{0, \ldots, |G| - 1\}$ such that $g^i = a$. We call $i$ the discrete logarithm of $a$ to base $g$ and denote it by

$$\text{DLog}_{G,g}(a)$$

The discrete log function is the inverse of the exponentiation function.
Let $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. We know that 2 is a generator, so $\text{DLog}_{G, 2}(a)$ is the exponent $i \in \{0, \ldots, 9\}$ such that $2^i \equiv a \pmod{11}$.

<table>
<thead>
<tr>
<th>$i$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^i \mod 11$</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$a$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{DLog}_{G, 2}(a)$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Let $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. We know that 2 is a generator, so $\text{DLog}_{G,2}(a)$ is the exponent $i \in \{0, \ldots, 9\}$ such that $2^i \equiv a \pmod{11}$.

<table>
<thead>
<tr>
<th>$i$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^i \mod 11$</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$a$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{DLog}_{G,2}(a)$</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Let $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. We know that 2 is a generator, so $D\text{Log}_{G,2}(a)$ is the exponent $i \in \{0, \ldots, 9\}$ such that $2^i \equiv a \pmod{11}$.

<table>
<thead>
<tr>
<th>$i$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^i \mod 11$</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$a$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$D\text{Log}_{G,2}(a)$</td>
<td>0</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Let $G = \mathbb{Z}^*_{11} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. We know that 2 is a generator, so $\text{DLog}_{G,2}(a)$ is the exponent $i \in \{0, \ldots, 9\}$ such that $2^i \equiv a \pmod{11}$.

<table>
<thead>
<tr>
<th>$i$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^i \pmod{11}$</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$a$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{DLog}_{G,2}(a)$</td>
<td>0</td>
<td>1</td>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Let $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. We know that 2 is a generator, so $D\text{Log}_{G,2}(a)$ is the exponent $i \in \{0, \ldots, 9\}$ such that $2^i \equiv a \pmod{11}$.

\[
\begin{array}{cccccccccc}
  i & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
 2^i \pmod{11} & 1 & 2 & 4 & 8 & 5 & 10 & 9 & 7 & 3 & 6 \\
\end{array}
\]

\[
\begin{array}{cccccccccc}
a & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\
D\text{Log}_{G,2}(a) & 0 & 1 & 8 & 2 & & & & & & \\
\end{array}
\]
Let $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. We know that 2 is a generator, so $D\log_{G,2}(a)$ is the exponent $i \in \{0, \ldots, 9\}$ such that $2^i \equiv a \pmod{11}$.

<table>
<thead>
<tr>
<th>$i$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^i \mod 11$</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$a$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$D\log_{G,2}(a)$</td>
<td>0</td>
<td>1</td>
<td>8</td>
<td>2</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Let $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. We know that 2 is a generator, so $D\text{Log}_{G,2}(a)$ is the exponent $i \in \{0, \ldots, 9\}$ such that $2^i \equiv a \pmod{11}$.

<table>
<thead>
<tr>
<th>$i$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^i \mod 11$</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$a$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$D\text{Log}_{G,2}(a)$</td>
<td>0</td>
<td>1</td>
<td>8</td>
<td>2</td>
<td>4</td>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Let $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. We know that 2 is a generator, so $\text{DLog}_{G, 2}(a)$ is the exponent $i \in \{0, \ldots, 9\}$ such that $2^i \equiv a \pmod{11}$.

\[
\begin{array}{cccccccccccc}
  i & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
 2^i \mod 11 & 1 & 2 & 4 & 8 & 5 & 10 & 9 & 7 & 3 & 6 \\
\end{array}
\]

\[
\begin{array}{cccccccccccc}
  a & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\
  \text{DLog}_{G, 2}(a) & 0 & 1 & 8 & 2 & 4 & 9 & 7 & & & \\
\end{array}
\]
Let $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. We know that 2 is a generator, so $\text{DLog}_{G, 2}(a)$ is the exponent $i \in \{0, \ldots, 9\}$ such that $2^i \equiv a \pmod{11}$.

<table>
<thead>
<tr>
<th>$i$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^i \mod 11$</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$a$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{DLog}_{G, 2}(a)$</td>
<td>0</td>
<td>1</td>
<td>8</td>
<td>2</td>
<td>4</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Let $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. We know that 2 is a generator, so $D\text{Log}_{G,2}(a)$ is the exponent $i \in \{0, \ldots, 9\}$ such that $2^i \equiv a \pmod{11}$.

<table>
<thead>
<tr>
<th>$i$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^i \pmod{11}$</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$a$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$D\text{Log}_{G,2}(a)$</td>
<td>0</td>
<td>1</td>
<td>8</td>
<td>2</td>
<td>4</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>6</td>
<td></td>
</tr>
</tbody>
</table>
Let $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. We know that 2 is a generator, so $\text{DLog}_{G,2}(a)$ is the exponent $i \in \{0, \ldots, 9\}$ such that $2^i \equiv a \pmod{11}$.

<table>
<thead>
<tr>
<th>$i$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^i \pmod{11}$</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$a$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{DLog}_{G,2}(a)$</td>
<td>0</td>
<td>1</td>
<td>8</td>
<td>2</td>
<td>4</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>6</td>
<td>5</td>
</tr>
</tbody>
</table>
Fact 1: Let $p$ be a prime. Then $\mathbb{Z}_p^*$ is cyclic.

Fact 2: Let $G$ be any group whose order $m = |G|$ is a prime number. Then $G$ is cyclic.

Note: $|\mathbb{Z}_p^*| = p - 1$ is not prime, so Fact 2 doesn’t imply Fact 1!
Let $G = \langle g \rangle$ be a cyclic group with generator $g \in G$.

**Input:** $X \in G$

**Desired Output:** $\text{DLog}_{G,g}(X)$

That is, we want $x$ such that $g^x = X$.

for $x = 0, \ldots, |G| - 1$ do
  $X' \leftarrow g^x$
  if $X' = X$ then return $x$

Is this a good algorithm?
Let $G = \langle g \rangle$ be a cyclic group with generator $g \in G$.

**Input:** $X \in G$

**Desired Output:** $\text{DLog}_{G,g}(X)$

That is, we want $x$ such that $g^x = X$.

for $x = 0, \ldots, |G| - 1$ do

$X' \leftarrow g^x$

if $X' = X$ then return $x$

Is this a good algorithm? It is

- Correct (always returns the right answer)
Computing Discrete Logs

Let $G = \langle g \rangle$ be a cyclic group with generator $g \in G$.

**Input:** $X \in G$

**Desired Output:** $\text{DLog}_{G,g}(X)$

That is, we want $x$ such that $g^x = X$.

```plaintext
for $x = 0, \ldots, |G| - 1$ do
  $X' \leftarrow g^x$
  if $X' = X$ then return $x$
```

Is this a good algorithm? It is

- Correct (always returns the right answer), but
- very, very SLOW!

Run time is $O(|G|)$ exponentiations, which for $G = \mathbb{Z}^*_N$ is $O(N)$, which is exponential time and prohibitive for large $N$. 

Let $G = \langle g \rangle$ be a cyclic group. Let $m = |G|$ and $n = \lceil \sqrt{m} \rceil$. Given $X \in G$ we seek $x$ such that $g^x = G$.

Will get an algorithm that uses $O(n) = O(\sqrt{m})$ exponentiations.
Let $G = \langle g \rangle$ be a cyclic group. Let $m = |G|$ and $n = \lceil \sqrt{m} \rceil$. Given $X \in G$ we seek $x$ such that $g^x = G$.

Will get an algorithm that uses $O(n) = O(\sqrt{m})$ exponentiations.

**Idea of algorithm:** Compute two lists

- $Xg^{-b}$ for $b = 0, 1, \ldots, n$
- $(g^n)^a$ for $a = 0, 1, \ldots, n$

And find a value $Y$ that is in both lists. This means there are $a, b$ such that

$$Y = Xg^{-b} = (g^n)^a$$

and hence

$$X = (g^n)^a g^b = g^{an+b}$$

and we have $x = na + b$. 
Doing Better: Baby-step Giant-step

Let $G = \langle g \rangle$ be a cyclic group. Let $m = |G|$ and $n = \lceil \sqrt{m} \rceil$.

**Idea of algorithm:** Compute two lists

- $Xg^{-b}$ for $b = 0, 1, \ldots, n$
- $(g^n)^a$ for $a = 0, 1, \ldots, n$

And find a value $Y$ that is in both lists. This means there are $a, b$ such that

$$Y = Xg^{-b} = (g^n)^a$$

and hence

$$X = (g^n)^ag^b = g^{an+b}$$

and we have $x = na + b$.

**Question:** Why do the lists have a common member?
Let $G = \langle g \rangle$ be a cyclic group. Let $m = |G|$ and $n = \lceil \sqrt{m} \rceil$.

**Idea of algorithm:** Compute two lists

- $Xg^{-b}$ for $b = 0, 1, \ldots, n$
- $(g^n)^a$ for $a = 0, 1, \ldots, n$

And find a value $Y$ that is in both lists. This means there are $a, b$ such that

$$Y = Xg^{-b} = (g^n)^a$$

and hence

$$X = (g^n)^a g^b = g^{an+b}$$

and we have $x = na + b$.

**Question:** Why do the lists have a common member?

**Answer:** Let $(x_1, x_0) \leftarrow \text{INT-DIV}(x, n)$. Then $x = nx_1 + x_0$ and $0 \leq x_0, x_1 \leq n$ so $Xg^{-x_0}$ is on first list and $(g^n)^{x_1}$ is on the second list.
Let $G = \langle g \rangle$ be a cyclic group. Given $X \in G$ the following algorithm finds $\text{DLog}_{G,g}(X)$ in $O(\sqrt{|G|})$ exponentiations, where $m = |G|$:

Algorithm $A_{\text{bsgs}}(X)$

1. $n \leftarrow \lceil \sqrt{m} \rceil$
2. $N \leftarrow g^n$
3. For $b = 0, \ldots, n$ do $B[Xg^{-b}] \leftarrow b$
4. For $a = 0, \ldots, n$ do
   - $Y \leftarrow N^a$
   - If $B[Y] \neq \perp$ then $x_0 \leftarrow B[Y]; x_1 \leftarrow a$
5. Return $ax_1 + x_0$
So Far

There is a better-than-exhaustive-search method to compute discrete logarithms, but its $O(\sqrt{|G|})$ running time is still exponential and prohibitive.

- Is there a faster algorithm?
- Is there a polynomial time algorithm, meaning one with running time $O(n^c)$ for some constant $c$ where $n = \log |G|$?

State of the art: There are faster algorithms in some groups, but no polynomial time algorithm is known.

This (apparent, conjectured) computational intractability of the discrete log problem makes it the basis for cryptographic schemes in which breaking the scheme requires discrete log computation.
Let $p$ be a prime and $G = \mathbb{Z}_p^*$. Then there is an algorithm that finds discrete logs in $G$ in time

$$e^{1.92(\ln p)^{1/3}(\ln \ln p)^{2/3}}$$

This is sub-exponential, and quite a bit less than

$$\sqrt{p} = e^{(\ln p)/2}$$

**Note:** The actual running time is $e^{1.92(\ln q)^{1/3}(\ln \ln q)^{2/3}}$ where $q$ is the largest prime factor of $p - 1$, but we chose $p$ so that $q \approx p$, for example $p - 1 = 2q$ for $q$ a prime.
Let $G$ be a prime-order group of points over an elliptic curve. Then the best known algorithm to compute discrete logs takes time

$$O(\sqrt{p})$$

where $p = |G|$. 
Say we want 80-bits of security, meaning discrete log computation by the best known algorithm should take time $2^{80}$. Then

- If we work in $\mathbb{Z}_p^*$ ($p$ a prime) we need to set $|\mathbb{Z}_p^*| = p - 1 \approx 2^{1024}$
- But if we work on an elliptic curve group of prime order $p$ then it suffices to set $p \approx 2^{160}$.

Why?

$$e^{1.92(\ln 2^{1024})^{1/3}(\ln \ln 2^{1024})^{2/3}} \approx \sqrt{2^{160}} = 2^{80}$$
Why are Smaller Groups Preferable?

<table>
<thead>
<tr>
<th>Group Size</th>
<th>Cost of Exponentiation</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^{160}$</td>
<td>1</td>
</tr>
<tr>
<td>$2^{1024}$</td>
<td>260</td>
</tr>
</tbody>
</table>

Exponentiation takes time cubic in $\log |G|$ where $G$ is the group.

Encryption and decryption will be 260 times faster in the smaller group!
Let $G = \langle g \rangle$ be a cyclic group.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Given</th>
<th>Figure out</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discrete logarithm (DL)</td>
<td>$g^x$</td>
<td>$x$</td>
</tr>
<tr>
<td>Computational Diffie-Hellman (CDH)</td>
<td>$g^x, g^y$</td>
<td>$g^{xy}$</td>
</tr>
<tr>
<td>Decisional Diffie-Hellman (DDH)</td>
<td>$g^x, g^y, g^z$</td>
<td>$z \equiv xy \pmod{</td>
</tr>
</tbody>
</table>
Let $G = \langle g \rangle$ be a cyclic group.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Given</th>
<th>Figure out</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discrete logarithm (DL)</td>
<td>$g^x$</td>
<td>$x$</td>
</tr>
<tr>
<td>Computational Diffie-Hellman (CDH)</td>
<td>$g^x, g^y$</td>
<td>$g^{xy}$</td>
</tr>
<tr>
<td>Decisional Diffie-Hellman (DDH)</td>
<td>$g^x, g^y, g^z$</td>
<td>$z \equiv xy \pmod{</td>
</tr>
</tbody>
</table>

$$DL \longrightarrow CDH \longrightarrow DDH$$

A $\longrightarrow$ B means

- If you can solve A then you can solve B; equivalently
- If A is easy then B is easy; equivalently
- If B is hard then A is hard.
Given: DL solver $A_1$

Want: CDH solver $A_2$

Construction:
DL $\rightarrow$ CDH

**Given:** DL solver $A_1$

$$g^x \rightarrow A_1 \rightarrow x$$

**Want:** CDH solver $A_2$

$$g^x \rightarrow A_2 \rightarrow g^{xy}$$

$$g^y \rightarrow g^{xy}$$

**Construction:**

$$g^x \rightarrow A_1 \rightarrow x$$

$$g^y \rightarrow (g^y)^x \rightarrow Z = g^{xy}$$

$$Z \leftarrow (g^y)^x$$
Formal Definitions

<table>
<thead>
<tr>
<th>Problem</th>
<th>Given</th>
<th>Figure out</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discrete logarithm (DL)</td>
<td>$g^x$</td>
<td>$x$</td>
</tr>
<tr>
<td>Computational Diffie-Hellman (CDH)</td>
<td>$g^x, g^y$</td>
<td>$g^{xy}$</td>
</tr>
<tr>
<td>Decisional Diffie-Hellman (DDH)</td>
<td>$g^x, g^y, g^z$</td>
<td>$z \equiv xy \pmod{</td>
</tr>
</tbody>
</table>

In the formalizations:

- $x, y$ will be chosen at random.
- In DDH the problem will be to figure out whether $z = xy$ or was chosen at random.

We will get advantage measures

$$\text{Adv}_{G,g}^{\text{dl}}(A), \quad \text{Adv}_{G,g}^{\text{cdh}}(A), \quad \text{Adv}_{G,g}^{\text{ddh}}(A)$$

for an adversary $A$ that equal their success probability.
Let $G = \langle g \rangle$ be a cyclic group of order $m$, and $A$ an adversary.

**Game $DL_{G,g}$**

**procedure Initialize**

$x \leftarrow Z_m; X \leftarrow g^x$

return $X$

**procedure Finalize($x'$)**

return $(x = x')$

The **dl-advantage** of $A$ is

$$Adv_{G,g}^{dl}(A) = \Pr[DL_{G,g}^A \Rightarrow true]$$
### Status

<table>
<thead>
<tr>
<th>Problem</th>
<th>Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>DL</td>
<td>hard</td>
</tr>
<tr>
<td>CDH</td>
<td>hard</td>
</tr>
<tr>
<td>DDH</td>
<td>easy</td>
</tr>
<tr>
<td>$\mathbb{Z}_p^*$</td>
<td>EC</td>
</tr>
</tbody>
</table>

- **hard**: best known algorithm takes time $e^{1.92(\ln p)^{1/3}(\ln \ln p)^{2/3}}$
- **harder**: best known algorithm takes time $\sqrt{p}$, where $p$ is the prime order of the group.
- **easy**: There is a polynomial time algorithm.
We will need to build (large) groups over which our cryptographic schemes can work, and find generators in these groups.

How do we do this efficiently?
Finding generators

If $|G|$ is prime then every $g \in G - \{1\}$ is a generator.

If $G = \mathbb{Z}_p^*$ where $p$ is a prime

- It may be hard in general to find a generator
- But easy if the prime factorization of $p - 1$ is known
Finding generators: Randomly pick and check

repeat
    \[ g \leftarrow G \setminus \{1\} \]
until \( (\text{TEST-GEN}_G(g) = \text{true}) \)

- How do we design \( \text{TEST-GEN}_G \)?
- How many iterations does the algorithm take?
Finding generators: Randomly pick and check

repeat
\[ g \leftarrow G - \{1\} \]
until \((\text{TEST-GEN}_G(g) = \text{true})\)

- How do we design \(\text{TEST-GEN}_G\)?
- How many iterations does the algorithm take?

We say that \(p\) is a SG prime if \(p - 1 = 2q\) for some prime \(q\).

**Example:** 7 is a SG prime because 7-1 = 2(3) and 3 is a prime.

We will address the above question for SG primes.
Generators mod 7

Let $G = \mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>$i$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$1'$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Generators mod 7

Let $G = \mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

<table>
<thead>
<tr>
<th>$i$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>1'</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$i$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>1'</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>
Generators mod 7

Let $G = \mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

<table>
<thead>
<tr>
<th>$i$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1'$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$2'$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
Generators mod 7

Let $G = \mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

\[
\begin{array}{c|ccccccc}
  i & 1 & 2 & 3 & 4 & 5 & 6 \\
\hline
 1' & 1 & 1 & 1 & 1 & 1 & 1 \\
 2' & 2 & & & & & \\
\end{array}
\]
Let $G = \mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

<table>
<thead>
<tr>
<th>$i$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1'$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$2'$</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>$3'$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Let \( G = \mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\} \)

<table>
<thead>
<tr>
<th>( i )</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>1'</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2'</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>3'</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Generators mod 7

Let $G = \mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

<table>
<thead>
<tr>
<th>$i$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1^i$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$2^i$</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>$3^i$</td>
<td>3</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Generators mod 7

Let \( G = \mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\} \)

<table>
<thead>
<tr>
<th>( i )</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>1'</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2'</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>3'</td>
<td>3</td>
<td>2</td>
<td>6</td>
<td>3</td>
<td>2</td>
<td>6</td>
</tr>
</tbody>
</table>
Generators mod 7

Let $G = \mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

\[
\begin{array}{c|ccccccc}
  i & 1 & 2 & 3 & 4 & 5 & 6 \\
\hline
  1' & 1 & 1 & 1 & 1 & 1 & 1 \\
  2' & 2 & 4 & 1 & 2 & 4 & 1 \\
  3' & 3 & 2 & 6 & 4 &   &   \\
\end{array}
\]
Generators mod 7

Let $G = \mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

<table>
<thead>
<tr>
<th>$i$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1'$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$2'$</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>$3'$</td>
<td>3</td>
<td>2</td>
<td>6</td>
<td>4</td>
<td>5</td>
<td></td>
</tr>
</tbody>
</table>
Generators mod 7

Let $G = \mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

<table>
<thead>
<tr>
<th>$i$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1^i$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$2^i$</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>$3^i$</td>
<td>3</td>
<td>2</td>
<td>6</td>
<td>4</td>
<td>5</td>
<td>1</td>
</tr>
</tbody>
</table>
Generators mod 7

Let $G = \mathbb{Z}^*_7 = \{1, 2, 3, 4, 5, 6\}$

<table>
<thead>
<tr>
<th>$i$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1'$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$2'$</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>$3'$</td>
<td>3</td>
<td>2</td>
<td>6</td>
<td>4</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>$4'$</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>$5'$</td>
<td>5</td>
<td>4</td>
<td>6</td>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>$6'$</td>
<td>6</td>
<td>1</td>
<td>6</td>
<td>1</td>
<td>6</td>
<td>1</td>
</tr>
</tbody>
</table>
Generators mod 7

Let \( G = \mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\} \)

<table>
<thead>
<tr>
<th>( i )</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>1'</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2'</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>3'</td>
<td>3</td>
<td>2</td>
<td>6</td>
<td>4</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>4'</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>5'</td>
<td>5</td>
<td>4</td>
<td>6</td>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>6'</td>
<td>6</td>
<td>1</td>
<td>6</td>
<td>1</td>
<td>6</td>
<td>1</td>
</tr>
</tbody>
</table>

The generators are
Generators mod 7

Let $G = \mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

<table>
<thead>
<tr>
<th>$i$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>1'</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2'</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>3'</td>
<td>3</td>
<td>2</td>
<td>6</td>
<td>4</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>4'</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>5'</td>
<td>5</td>
<td>4</td>
<td>6</td>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>6'</td>
<td>6</td>
<td>1</td>
<td>6</td>
<td>1</td>
<td>6</td>
<td>1</td>
</tr>
</tbody>
</table>

The generators are 3 and 5
Generators mod 7

Let $G = \mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

<table>
<thead>
<tr>
<th>$i$</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>1'</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2'</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>3'</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>4'</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>5'</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>6'</td>
<td>1</td>
<td>6</td>
</tr>
</tbody>
</table>

We observe that $g$ is a generator if and only if $g^2 \neq 1$ and $g^3 \neq 1$. 
Suppose $p$ is a SG prime, meaning $p - 1 = 2q$ for a prime $q$.

**Fact:** $g \in \mathbb{Z}_p^*$ is a generator if and only if $g^2 \not\equiv 1$ and $g^q \not\equiv 1$ modulo $p$.

**Example:** Let $p = 7$ so that $q = 3$. Then $g \in \mathbb{Z}_7^*$ is a generator if and only if $g^2 \not\equiv 1$ and $g^3 \not\equiv 1$ modulo 7.
How many generators are there?

Suppose $p$ is a SG prime, meaning $p - 1 = 2q$ for a prime $q$.

Fact: $\mathbb{Z}_p^*$ has $q - 1$ generators

Example: Suppose $p = 7$ so that $q = 3$. Then $\mathbb{Z}_7^*$ has $q - 1 = 2$ generators.

So if $g \leftarrow G - \{1\}$ then

$$\Pr \left[ \langle g \rangle = \mathbb{Z}_p^* \right] = \frac{q - 1}{p - 2} = \frac{q - 1}{2q - 1} \approx \frac{1}{2}$$

Example: If $p = 7$ and $g \leftarrow \mathbb{Z}_7^* - \{1\}$ then

$$\Pr \left[ \langle g \rangle = \mathbb{Z}_7^* \right] = \frac{3 - 1}{7 - 2} = \frac{2}{5}$$
Finding generators: Randomly pick and check

repeat
   \[ g \leftarrow G - \{1\} \]
until \((\text{TEST-GEN}_G(g) = \text{true})\)

- How do we design \(\text{TEST-GEN}_G\)?
- How many iterations does the algorithm take?

We are addressing the two questions for the case that \(p\) is a SG prime.
Suppose $p$ is a SG prime with $p - 1 = 2q$.

repeat

$g \leftarrow G - \{1\}$

until $(g^2 \not\equiv 1 \pmod{p} \land g^q \not\equiv 1 \pmod{p})$

The probability that a generator is found in a given step is

\[
\frac{q - 1}{2q - 1} \approx \frac{1}{2}
\]

so the expected number of iterations of the algorithm is about 2.
Recall ...

We want to figure out how to find

- A large SG prime $p$
- A generator $g$ of $\mathbb{Z}_p^*$

so that we can work over $\mathbb{Z}_p^* = \langle g \rangle$.

So far we solved the second problem. What about the first?
**Finding primes**

**Desired:** An efficient algorithm that given an integer $k$ returns a prime $p \in \{2^{k-1}, \ldots, 2^k - 1\}$ such that $q = (p - 1)/2$ is also prime.

**Alg** `Findprime(k)`

do
  $p \leftarrow \{2^{k-1}, \ldots, 2^k - 1\}$
until $(p$ is prime and $(p - 1)/2$ is prime$)$
return $p$

- How do we test primality?
- How many iterations do we need to succeed?
Given: integer $N$
Output: TRUE if $N$ is prime, FALSE otherwise.

for $i = 2, \ldots, \lceil \sqrt{N} \rceil$ do
    if $N \mod i = 0$ then return false
return true
Primality Testing

**Given:** integer \( N \)

**Output:** TRUE if \( N \) is prime, FALSE otherwise.

\[
\text{for } i = 2, \ldots, \lceil \sqrt{N} \rceil \text{ do}
\]
\[
\text{if } N \mod i = 0 \text{ then return false}
\]

return true

Correct but SLOW! \( O(N) \) running time, exponential. However, we have:

- \( O(|N|^3) \) time randomized algorithms
- Even a \( O(|N|^8) \) time deterministic algorithm
Density of primes

Let $\pi(N)$ be the number of primes in the range $1, \ldots, N$. So if $p \leftarrow \{1, \ldots, N\}$ then

$$\Pr [p \text{ is a prime}] = \frac{\pi(N)}{N}$$

Fact: $\pi(N) \sim \frac{N}{\ln(N)}$

so

$$\Pr [p \text{ is a prime}] \sim \frac{1}{\ln(N)}$$

If $N = 2^{1024}$ this is about $0.001488 \approx 1/1000$.

So the number of iterations taken by our algorithm to find a prime is not too big.