COMPUTATIONAL NUMBER THEORY

Notation

$\mathbf{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$

$\mathbf{N} = \{0, 1, 2, \ldots\}$

$\mathbf{Z}_+ = \{1, 2, 3, \ldots\}$

$d|a$ means d divides a

Example: $2|4$.

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

Example: $\gcd(30, 70) =$

Notation

$\mathbf{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$

$\mathbf{N} = \{0, 1, 2, \ldots\}$

$\mathbf{Z}_+ = \{1, 2, 3, \ldots\}$

$d|a$ means d divides a

Example: $2|4$.

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

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

Integers mod N

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

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

Example: $N = 12$

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

Integers mod N

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

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

Example: $N = 12$

- $\mathbf{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$
- $\mathbf{Z}_{12}^* = \{1, 5, 7, 11\}$
- $\varphi(12) =$

Integers mod N

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

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

Example: $N = 12$

- $\mathbf{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$
- $\mathbf{Z}_{12}^* = \{1, 5, 7, 11\}$
- $\varphi(12) = 4$

Division and mod

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

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

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

$$a \bmod N = r \in \mathbf{Z}_N$$

is the remainder when a is divided by N.

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

Examples:

- If $a = 17$ and $N = 3$ then the quotient and remainder are $q = ?$ and $r = ?$

Division and mod

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

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

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

$$a \bmod N = r \in \mathbf{Z}_N$$

is the remainder when a is divided by N.

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

Examples:

- If $a = 17$ and $N = 3$ then the quotient and remainder are $q = 5$ and $r = 2$

Division and mod

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

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

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

$$a \bmod N = r \in \mathbf{Z}_N$$

is the remainder when a is divided by N.

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

Examples:

- If $a = 17$ and $N = 3$ then the quotient and remainder are $q = 5$ and $r = 2$
- $17 \bmod 3 =$

Division and mod

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

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

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

$$a \bmod N = r \in \mathbf{Z}_N$$

is the remainder when a is divided by N.

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

Examples:

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

Division and mod

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

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

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

$$a \bmod N = r \in \mathbf{Z}_N$$

is the remainder when a is divided by N.

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

Examples:

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

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:

- $G = \mathbf{Z}_{12}$ and "$\cdot$" is addition modulo 12, meaning

$$a \cdot b = (a + b) \bmod 12$$

- $G = \mathbf{Z}_{12}^*$ and "$\cdot$" is multiplication modulo 12, meaning

$$a \cdot b = ab \bmod 12$$

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.

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 $\mathbf{1} \in G$ such that $a \cdot \mathbf{1} = \mathbf{1} \cdot a = a$ for all $a \in G$.
4. INVERTIBILITY: For every $a \in G$ there exists a unique $b \in G$ such that $a \cdot b = b \cdot a = \mathbf{1}$.

The element b in the invertibility condition is referred to as the inverse of the element a, and is denoted a^{-1}.

$\mathbf{Z}_N$ under MOD-ADD

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

Addition modulo N: $a, b \mapsto a + b \bmod N$

$\mathbf{Z}_N$ under MOD-ADD

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

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

$\mathbf{Z}_N$ under MOD-ADD

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

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

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

Check: $9 + 7 \bmod 12 = 16 \bmod 12 = 4 \in \mathbf{Z}_{12}$

$\mathbf{Z}_N$ under MOD-ADD

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

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

Associative:
$((a + b \bmod N) + c) \bmod N = (a + (b + c \bmod N)) \bmod N$

Check:

$$\begin{aligned}
(9 + 7 \bmod 12) + 10 \bmod 12 &= (16 \bmod 12) + 10 \bmod 12 \\
&= 4 + 10 \bmod 12 = 2 \\
9 + (7 + 10 \bmod 12) \bmod 12 &= 9 + (17 \bmod 12) \bmod 12 \\
&= 9 + 5 \bmod 12 = 2
\end{aligned}$$

$\mathbf{Z}_N$ under MOD-ADD

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

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

Identity: 0 is the identity element because $a + 0 \equiv 0 + a \equiv a \pmod{N}$ for every a.

$\mathbf{Z}_N$ under MOD-ADD

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

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

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

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

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

so $x =$

$\mathbf{Z}_N$ under MOD-ADD

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

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

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

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

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

so $x = 3$

$\mathbf{Z}_N^*$ under MOD-MULT

Fact: Let $N \in \mathbf{Z}_+$. Then $\mathbf{Z}_N^*$ is a group under multiplication modulo N.

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

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

$\mathbf{Z}_N^*$ under MOD-MULT

Fact: Let $N \in \mathbf{Z}_+$. Then $\mathbf{Z}_N^*$ is a group under multiplication modulo N.

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

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

$$\gcd(a, N) = \gcd(b, N) = 1 \Rightarrow \gcd(ab \bmod N, N) = 1$$

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

If $a, b \in \mathbf{Z}_{12}^*$, $ab \bmod 12$ can never be 3!

$\mathbf{Z}_N^*$ under MOD-MULT

Fact: Let $N \in \mathbf{Z}_+$. Then $\mathbf{Z}_N^*$ is a group under multiplication modulo N.

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

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

Check:

$$\begin{aligned}
(5 \cdot 7 \bmod 12) \cdot 11 \bmod 12 &= (35 \bmod 12) \cdot 11 \bmod 12 \\
&= 11 \cdot 11 \bmod 12 = 1 \\
5 \cdot (7 \cdot 11 \bmod 12) \bmod 12 &= 5 \cdot (77 \bmod 12) \bmod 12 \\
&= 5 \cdot 5 \bmod 12 = 1
\end{aligned}$$

$\mathbf{Z}_N^*$ under MOD-MULT

Fact: Let $N \in \mathbf{Z}_+$. Then $\mathbf{Z}_N^*$ is a group under multiplication modulo N.

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

Identity: 1 is the identity element because $a \cdot 1 \equiv 1 \cdot a \equiv a \pmod{N}$ for all a.

$\mathbf{Z}_N^*$ under MOD-MULT

Fact: Let $N \in \mathbf{Z}_+$. Then $\mathbf{Z}_N^*$ is a group under multiplication modulo N.

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

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

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

$$5x \equiv 1 \pmod{12}$$

so $x =$

$\mathbf{Z}_N^*$ under MOD-MULT

Fact: Let $N \in \mathbf{Z}_+$. Then $\mathbf{Z}_N^*$ is a group under multiplication modulo N.

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

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

Check: 5^{-1} is the x satisfying

$$5x \equiv 1 \pmod{12}$$

so $x = 5$

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

Computational Shortcuts

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

Slow way: First compute

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

and then compute $6400 \bmod 21 =$

Computational Shortcuts

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

Slow way: First compute

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

and then compute $6400 \bmod 21 = 16$

Fast way:

- $5 \cdot 8 \bmod 21 = 40 \bmod 21 = 19$
- $19 \cdot 10 \bmod 21 = 190 \bmod 21 = 1$
- $1 \cdot 16 \bmod 21 = 16$

Exponentiation

Let G be a group and $a \in G$. We let $a^0 = \mathbf{1}$ be the identity element and for $n \geq 1$, we let

$$a^n = \underbrace{a \cdot a \cdots a}_{n}.$$

Also we let

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

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

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

Meaning we can manipulate exponents "as usual".

Examples

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

$$5^3 =$$

Examples

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

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

Examples

Let $N = 14$ and $G = \mathbf{Z}_N^*$. 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

$$5^{-3} =$$

Let $N = 14$ and $G = \mathbf{Z}_N^*$. 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

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

Examples

Let $N = 14$ and $G = \mathbf{Z}_N^*$. 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 $G = \mathbf{Z}_N^*$. 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

$$5^{-3} = 5^{-1} \cdot 5^{-1} \cdot 5^{-1} \equiv 3 \cdot 3 \cdot 3 \equiv 27 \equiv 13$$

Group Orders

The order of a group G is its size $|G|$, meaning the number of elements in it.

Example: The order of $\mathbf{Z}_{21}^*$ is

Group Orders

The order of a group G is its size $|G|$, meaning the number of elements in it.

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

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

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

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 $i \in \mathbf{Z}$,

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

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

Group Orders

Corollary: Let G be a group of order m and $a \in G$. Then for any $i \in \mathbf{Z}$,

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

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

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

$$\begin{aligned} 5^{74} \bmod 21 &= 5^{74 \bmod 12} \bmod 21 \\ &= 5^2 \bmod 21 \\ &= 4. \end{aligned}$$

Measuring Running Time of Algorithms on Numbers

In an algorithms course, the cost of arithmetic is often assumed to be $\mathcal{O}(1)$, 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

$(a, b) \mapsto a + b$

$$\begin{array}{cccccccc} & & 1 & 0 & 1 & 1 & 0 & 1 \\ + & & & & 1 & 0 & 1 & 1 \\ \hline & & 1 & 1 & 1 & 0 & 0 & 0 \end{array}$$

By the usual "carry" algorithm, we can compute $a + b$ in time $\mathcal{O}(|a| + |b|)$.

Addition is linear time.

Multiplication

$(a, b) \mapsto ab$

$$
\begin{array}{cccccccccc}
 & & & & 1 & 0 & 1 & 1 & 1 & 0 \\
 & & & \times & & & & 1 & 0 & 1 \\
\hline
 & & & & 1 & 0 & 1 & 1 & 1 & 0 \\
 & & & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
+ & & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
\hline
 & & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0
\end{array}
$$

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

Multiplication is 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 $\mathcal{O}(|a| \cdot |N|)$.

Integer division is quadratic time.

MOD

$(a, N) \mapsto a \bmod N$

But

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

computes $a \bmod N$, so again the time needed is $\mathcal{O}(|a| \cdot |N|)$.

Mod is quadratic time.

About gcd

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

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

Corollary: If $d = \gcd(a, N)$ then there are "weights" $a', N' \in \mathbf{Z}$ 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 $a, N \in \mathbf{Z}$ and $(a, N) \neq (0, 0)$ then $\gcd(a, N)$ is the smallest positive integer in the set

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

Corollary: If $d = \gcd(a, N)$ then there are "weights" $a', N' \in \mathbf{Z}$ 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

$\text{EXT-GCD}(a, N) \mapsto (d, a', N')$ such that

$$d = \text{gcd}(a, N) = a \cdot a' + N \cdot N'.$$

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

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

Extended gcd

$\mathrm{EXT\text{-}GCD}(a, N) \mapsto (d, a', N')$ such that

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

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

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

Extended gcd

We know that $a = qN + r$ with $0 \le r < N$ and we have d, x, y satisfying
$$d = \gcd(N, r) = Nx + ry$$

Then

$$\begin{aligned} d &= Nx + ry \\ &= Nx + (a - qN)y \\ &= ay + N(x - qy) \end{aligned}$$

so $d = \gcd(a, N) = a \cdot a' + N \cdot N'$ with $a' = y$ and $N' = x - qy$.

Extended gcd

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

Modular Inverse

For a, N such that $\gcd(a, N) = 1$, we want to compute $a^{-1} \bmod N$, meaning the unique $a' \in \mathbf{Z}_N^*$ 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 $\mathrm{MOD\text{-}INV}(a, N)$
$(d, a', N') \leftarrow \mathrm{EXT\text{-}GCD}(a, N)$
return $a' \bmod N$

Modular inverse can be computed in quadratic time.

Modular Exponentiation

Let G be a group and $a \in G$. For $n \in \mathbf{N}$, 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?

Modular Exponentiation

Let G be a group and $a \in G$. For $n \in \mathbf{N}$, 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.

Fast exponentiation idea

We can compute

$$a \longrightarrow a^2 \longrightarrow a^4 \longrightarrow a^8 \longrightarrow a^{16} \longrightarrow a^{32}$$

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?

Fast Exponentiation Example

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

$$\begin{aligned} n &= 2^4 b_4 + 2^3 b_3 + 2^2 b_2 + 2^1 b_1 + 2^0 b_0 \\ &= 16 b_4 + 8 b_3 + 4 b_2 + 2 b_1 + b_0 \,. \end{aligned}$$

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:

$$\begin{array}{lllll} y_5 & = & \mathbf{1} & & \\ y_4 & = & y_5^2 \cdot a^{b_4} & = & a^{b_4} \\ y_3 & = & y_4^2 \cdot a^{b_3} & = & a^{2b_4 + b_3} \\ y_2 & = & y_3^2 \cdot a^{b_2} & = & a^{4b_4 + 2b_3 + b_2} \\ y_1 & = & y_2^2 \cdot a^{b_1} & = & a^{8b_4 + 4b_3 + 2b_2 + b_1} \\ y_0 & = & y_1^2 \cdot a^{b_0} & = & a^{16b_4 + 8b_3 + 4b_2 + 2b_1 + b_0} \,. \end{array}$$

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 $\mathrm{EXP}_G(a, n)$ $\quad$ // $a \in G$, $n \geq 1$
$b_{k-1} \ldots b_0 \leftarrow \text{bin}(n)$
$y \leftarrow 1$
for $i = k-1$ downto 0 do $y \leftarrow y^2 \cdot a^{b_i}$
return y

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

MOD-EXP(a, n, N) returns $a^n \bmod N$ in time $\mathcal{O}(|n| \cdot |N|^2)$, meaning is cubic time.

Algorithms Summary

Algorithm	Input	Output	Time
INT-DIV	$a,\ N$	q, r	quadratic
MOD	$a,\ N$	$a \bmod N$	quadratic
EXT-GCD	$a,\ N$	(d, a', N')	quadratic
MOD-ADD	$a,\ b,\ N$	$a + b \bmod N$	linear
MOD-MULT	$a,\ b,\ N$	$ab \bmod N$	quadratic
MOD-INV	$a,\ N$	$a^{-1} \bmod N$	quadratic
MOD-EXP	$a,\ n,\ N$	$a^n \bmod N$	cubic
EXP_G	$a,\ n$	$a^n \in G$	$\mathcal{O}(\lvert n \rvert)$ G-ops

Subgroups

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 $G = \mathbf{Z}_{11}^*$ 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.

Order of a group element

Let G be a (finite) group.

Definition: The order of $g \in G$, denoted $o(g)$, is the smallest integer $n \geq 1$ such than $g^n = \mathbf{1}$.

Order determinations

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

i	0	1	2	3	4	5	6	7	8	9	10
$2^i \mod 11$											

Order determinations

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

i	0	1	2	3	4	5	6	7	8	9	10
$2^i \mod 11$	1										

Order determinations

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

i	0	1	2	3	4	5	6	7	8	9	10
$2^i \mod 11$	1	2									

Order determinations

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

i	0	1	2	3	4	5	6	7	8	9	10
$2^i \mod 11$	1	2	4								

Order determinations

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

i	0	1	2	3	4	5	6	7	8	9	10
$2^i \mod 11$	1	2	4	8							

Order determinations

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

i	0	1	2	3	4	5	6	7	8	9	10
$2^i \mod 11$	1	2	4	8	5						

Order determinations

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

i	0	1	2	3	4	5	6	7	8	9	10
$2^i \mod 11$	1	2	4	8	5	10					

Order determinations

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

i	0	1	2	3	4	5	6	7	8	9	10
$2^i \mod 11$	1	2	4	8	5	10	9				

Order determinations

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

i	0	1	2	3	4	5	6	7	8	9	10
$2^i \mod 11$	1	2	4	8	5	10	9	7			

Order determinations

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

i	0	1	2	3	4	5	6	7	8	9	10
$2^i \mod 11$	1	2	4	8	5	10	9	7	3		

Order determinations

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

i	0	1	2	3	4	5	6	7	8	9	10
$2^i \mod 11$	1	2	4	8	5	10	9	7	3	6	

Order determinations

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

i	0	1	2	3	4	5	6	7	8	9	10
$2^i \mod 11$	1	2	4	8	5	10	9	7	3	6	1
$5^i \mod 11$											

Order determinations

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

i	0	1	2	3	4	5	6	7	8	9	10
$2^i \mod 11$	1	2	4	8	5	10	9	7	3	6	1
$5^i \mod 11$	1										

Order determinations

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

i	0	1	2	3	4	5	6	7	8	9	10
$2^i \mod 11$	1	2	4	8	5	10	9	7	3	6	1
$5^i \mod 11$	1	5									

Order determinations

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

i	0	1	2	3	4	5	6	7	8	9	10
$2^i \mod 11$	1	2	4	8	5	10	9	7	3	6	1
$5^i \mod 11$	1	5	3								

Order determinations

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

i	0	1	2	3	4	5	6	7	8	9	10
$2^i \mod 11$	1	2	4	8	5	10	9	7	3	6	1
$5^i \mod 11$	1	5	3	4							

Order determinations

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

i	0	1	2	3	4	5	6	7	8	9	10
$2^i \mod 11$	1	2	4	8	5	10	9	7	3	6	1
$5^i \mod 11$	1	5	3	4	9						

Order determinations

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

i	0	1	2	3	4	5	6	7	8	9	10
$2^i \mod 11$	1	2	4	8	5	10	9	7	3	6	1
$5^i \mod 11$	1	5	3	4	9	1					

Order determinations

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

i	0	1	2	3	4	5	6	7	8	9	10
$2^i \mod 11$	1	2	4	8	5	10	9	7	3	6	1
$5^i \mod 11$	1	5	3	4	9	1	5				

Order determinations

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

i	0	1	2	3	4	5	6	7	8	9	10
$2^i \mod 11$	1	2	4	8	5	10	9	7	3	6	1
$5^i \mod 11$	1	5	3	4	9	1	5	3			

Order determinations

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

i	0	1	2	3	4	5	6	7	8	9	10
$2^i \mod 11$	1	2	4	8	5	10	9	7	3	6	1
$5^i \mod 11$	1	5	3	4	9	1	5	3	4		

Order determinations

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

i	0	1	2	3	4	5	6	7	8	9	10
$2^i \mod 11$	1	2	4	8	5	10	9	7	3	6	1
$5^i \mod 11$	1	5	3	4	9	1	5	3	4	9	

Order determinations

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

i	0	1	2	3	4	5	6	7	8	9	10
$2^i \mod 11$	1	2	4	8	5	10	9	7	3	6	1
$5^i \mod 11$	1	5	3	4	9	1	5	3	4	9	1

Order determinations

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

i	0	1	2	3	4	5	6	7	8	9	10
$2^i \mod 11$	1	2	4	8	5	10	9	7	3	6	1
$5^i \mod 11$	1	5	3	4	9	1	5	3	4	9	1

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

- $o(2) =$

Order determinations

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

i	0	1	2	3	4	5	6	7	8	9	10
$2^i \mod 11$	1	2	4	8	5	10	9	7	3	6	1
$5^i \mod 11$	1	5	3	4	9	1	5	3	4	9	1

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

- $o(2) = 10$

Order determinations

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

i	0	1	2	3	4	5	6	7	8	9	10
$2^i \mod 11$	1	2	4	8	5	10	9	7	3	6	1
$5^i \mod 11$	1	5	3	4	9	1	5	3	4	9	1

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

- $o(2) = 10$
- $o(5) =$

Order determinations

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

i	0	1	2	3	4	5	6	7	8	9	10
$2^i \mod 11$	1	2	4	8	5	10	9	7	3	6	1
$5^i \mod 11$	1	5	3	4	9	1	5	3	4	9	1

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

- $o(2) = 10$
- $o(5) = 5$

Subgroup generated by $g \in G$

Definition: For $g \in G$ we let

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

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

Subgroup orders

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 $G = \mathbf{Z}_{11}^*$ then

- $|G| =$

Subgroup orders

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 $G = \mathbf{Z}_{11}^*$ then

- $|G| = 10$
- $o(2) = 10$ which divides 10
- $o(5) = 5$ which divides 10

Subgroups generated by a group element

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

i	0	1	2	3	4	5	6	7	8	9	10
$2^i \mod 11$	1	2	4	8	5	10	9	7	3	6	1
$5^i \mod 11$	1	5	3	4	9	1	5	3	4	9	1

so

$$\langle 2 \rangle =$$
$$\langle 5 \rangle =$$

Subgroups generated by a group element

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

i	0	1	2	3	4	5	6	7	8	9	10
$2^i \mod 11$	1	2	4	8	5	10	9	7	3	6	1
$5^i \mod 11$	1	5	3	4	9	1	5	3	4	9	1

so

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

Subgroups generated by a group element

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

i	0	1	2	3	4	5	6	7	8	9	10
$2^i \mod 11$	1	2	4	8	5	10	9	7	3	6	1
$5^i \mod 11$	1	5	3	4	9	1	5	3	4	9	1

so

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

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

i	0	1	2	3	4	5	6	7	8	9	10
$2^i \mod 11$	1	2	4	8	5	10	9	7	3	6	1
$5^i \mod 11$	1	5	3	4	9	1	5	3	4	9	1

so

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

Generators

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

i	0	1	2	3	4	5	6	7	8	9	10
$2^i \mod 11$	1	2	4	8	5	10	9	7	3	6	1
$5^i \mod 11$	1	5	3	4	9	1	5	3	4	9	1

so

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

- Is 2 a generator?

Generators

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

i	0	1	2	3	4	5	6	7	8	9	10
$2^i \mod 11$	1	2	4	8	5	10	9	7	3	6	1
$5^i \mod 11$	1	5	3	4	9	1	5	3	4	9	1

so

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

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

Generators

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

i	0	1	2	3	4	5	6	7	8	9	10
$2^i \mod 11$	1	2	4	8	5	10	9	7	3	6	1
$5^i \mod 11$	1	5	3	4	9	1	5	3	4	9	1

so

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

- Is 2 a generator?
  YES because $\langle 2 \rangle = \mathbf{Z}_{11}^*$.
- Is 5 a generator?

Generators

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

i	0	1	2	3	4	5	6	7	8	9	10
$2^i \mod 11$	1	2	4	8	5	10	9	7	3	6	1
$5^i \mod 11$	1	5	3	4	9	1	5	3	4	9	1

so

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

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

Generators

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

i	0	1	2	3	4	5	6	7	8	9	10
$2^i \mod 11$	1	2	4	8	5	10	9	7	3	6	1
$5^i \mod 11$	1	5	3	4	9	1	5	3	4	9	1

so

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

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

Generators

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

i	0	1	2	3	4	5	6	7	8	9	10
$2^i \mod 11$	1	2	4	8	5	10	9	7	3	6	1
$5^i \mod 11$	1	5	3	4	9	1	5	3	4	9	1

so

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

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

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

The discrete log function is the inverse of the exponentiation function

$$\begin{tikzcd}
i \arrow[rr, bend left, "\mathrm{Exp}_G"] & & g^i \arrow[ll, bend left, "\mathrm{DLog}_{G,g}"]
\end{tikzcd}$$

Discrete Log

Let $G = \mathbf{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. We know that 2 is a generator, so $\mathrm{DLog}_{G,2}(a)$ is the exponent $i \in \{0, \ldots, 9\}$ such that $2^i \equiv a \pmod{11}$.

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

a	1	2	3	4	5	6	7	8	9	10
$\mathrm{DLog}_{G,2}(a)$										

Discrete Log

Let $G = \mathbf{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. We know that 2 is a generator, so $\mathrm{DLog}_{G,2}(a)$ is the exponent $i \in \{0, \ldots, 9\}$ such that $2^i \equiv a \pmod{11}$.

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

a	1	2	3	4	5	6	7	8	9	10
$\mathrm{DLog}_{G,2}(a)$	0									

Discrete Log

Let $G = \mathbf{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. We know that 2 is a generator, so $\mathrm{DLog}_{G,2}(a)$ is the exponent $i \in \{0, \ldots, 9\}$ such that $2^i \equiv a \pmod{11}$.

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

a	1	2	3	4	5	6	7	8	9	10
$\mathrm{DLog}_{G,2}(a)$	0	1								

Discrete Log

Let $G = \mathbf{Z}_{11}^* = \{1,2,3,4,5,6,7,8,9,10\}$. We know that 2 is a generator, so $\mathrm{DLog}_{G,2}(a)$ is the exponent $i \in \{0,\ldots,9\}$ such that $2^i \equiv a \pmod{11}$.

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

a	1	2	3	4	5	6	7	8	9	10
$\mathrm{DLog}_{G,2}(a)$	0	1	8							

Discrete Log

Let $G = \mathbf{Z}_{11}^* = \{1,2,3,4,5,6,7,8,9,10\}$. We know that 2 is a generator, so $\mathrm{DLog}_{G,2}(a)$ is the exponent $i \in \{0,\ldots,9\}$ such that $2^i \equiv a \pmod{11}$.

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

a	1	2	3	4	5	6	7	8	9	10
$\mathrm{DLog}_{G,2}(a)$	0	1	8	2						

Discrete Log

Let $G = \mathbf{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. We know that 2 is a generator, so $\mathrm{DLog}_{G,2}(a)$ is the exponent $i \in \{0, \ldots, 9\}$ such that $2^i \equiv a \pmod{11}$.

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

a	1	2	3	4	5	6	7	8	9	10
$\mathrm{DLog}_{G,2}(a)$	0	1	8	2	4					

Discrete Log

Let $G = \mathbf{Z}_{11}^{*} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. We know that 2 is a generator, so $\mathrm{DLog}_{G,2}(a)$ is the exponent $i \in \{0, \ldots, 9\}$ such that $2^i \equiv a \pmod{11}$.

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

a	1	2	3	4	5	6	7	8	9	10
$\mathrm{DLog}_{G,2}(a)$	0	1	8	2	4	9				

Discrete Log

Let $G = \mathbf{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. We know that 2 is a generator, so $\mathrm{DLog}_{G,2}(a)$ is the exponent $i \in \{0, \ldots, 9\}$ such that $2^i \equiv a \pmod{11}$.

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

a	1	2	3	4	5	6	7	8	9	10
$\mathrm{DLog}_{G,2}(a)$	0	1	8	2	4	9	7			

Discrete Log

Let $G = \mathbf{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. We know that 2 is a generator, so $\mathrm{DLog}_{G,2}(a)$ is the exponent $i \in \{0, \ldots, 9\}$ such that $2^i \equiv a \pmod{11}$.

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

a	1	2	3	4	5	6	7	8	9	10
$\mathrm{DLog}_{G,2}(a)$	0	1	8	2	4	9	7	3		

Discrete Log

Let $G = \mathbf{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. We know that 2 is a generator, so $\mathrm{DLog}_{G,2}(a)$ is the exponent $i \in \{0, \ldots, 9\}$ such that $2^i \equiv a \pmod{11}$.

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

a	1	2	3	4	5	6	7	8	9	10
$\mathrm{DLog}_{G,2}(a)$	0	1	8	2	4	9	7	3	6	

Discrete Log

Let $G = \mathbf{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. We know that 2 is a generator, so $\mathrm{DLog}_{G,2}(a)$ is the exponent $i \in \{0, \ldots, 9\}$ such that $2^i \equiv a \pmod{11}$.

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

a	1	2	3	4	5	6	7	8	9	10
$\mathrm{DLog}_{G,2}(a)$	0	1	8	2	4	9	7	3	6	5

Finding Cyclic Groups

Fact 1: Let p be a prime. Then $\mathbf{Z}_p^*$ is cyclic.

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

Note: $|\mathbf{Z}_p^*| = p - 1$ is not prime, so Fact 2 doesn't imply Fact 1!

Computing Discrete Logs

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

Input: $X \in G$
Desired Output: $\mathrm{DLog}_{G,g}(X)$

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?

Computing Discrete Logs

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

Input: $X \in G$
Desired Output: $\mathrm{DLog}_{G,g}(X)$

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: $\mathrm{DLog}_{G,g}(X)$

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), but
- very, very SLOW!

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

Doing Better: Baby-step Giant-step

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.

Doing Better: Baby-step Giant-step

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

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

and we have $x = na + b$.

Question: Why do the lists have a common member?

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

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

and we have $x = na + b$.

Question: Why do the lists have a common member?

Answer: Let $(x_1, x_0) \leftarrow \mathrm{INT\text{-}DIV}(x, n)$. 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.

The Baby-step Giant-step Algorithm

Let $G = \langle g \rangle$ be a cyclic group. Given $X \in G$ the following algorithm finds $\mathrm{DLog}_{G,g}(X)$ in $O(\sqrt{|G|})$ exponentiations, where $m = |G|$:

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

$n \leftarrow \lceil \sqrt{m} \rceil N \leftarrow g^n$

For $b = 0, \ldots, n$ do $B[Xg^{-b}] \leftarrow b$

For $a = 0, \ldots, n$ do

$Y \leftarrow N^a$

If $B[Y] \neq \perp$ then $x_0 \leftarrow B[Y]; x_1 \leftarrow a$

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.

Index Calculus

Let p be a prime and $G = \mathbf{Z}_p^*$. 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.

Elliptic Curve Groups

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 $p = |G|$.

Comparison

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 $\mathbf{Z}_p^*$ (p a prime) we need to set $|\mathbf{Z}_p^*| = p - 1 \approx 2^{1024}$
- 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?

Group Size	Cost of Exponentiation
2^{160}	1
2^{1024}	260

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

Encryption and decryption will be 260 times faster in the smaller group!

DL and Friends

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

Problem	**Given**	**Figure out**
Discrete logarithm (DL)	g^x	x
Computational Diffie-Hellman (CDH)	g^x, g^y	g^{xy}
Decisional Diffie-Hellman (DDH)	g^x, g^y, g^z	is $z \equiv xy \pmod{\lvert G \rvert}$?

DL and Friends

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

Problem	**Given**	**Figure out**
Discrete logarithm (DL)	g^x	x
Computational Diffie-Hellman (CDH)	g^x, g^y	g^{xy}
Decisional Diffie-Hellman (DDH)	g^x, g^y, g^z	is $z \equiv xy \pmod{\|G\|}$?

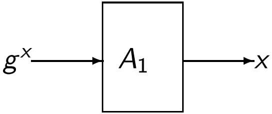
$$\mathrm{DL} \longrightarrow \mathrm{CDH} \longrightarrow \mathrm{DDH}$$

$\mathrm{A} \longrightarrow \mathrm{B}$ means

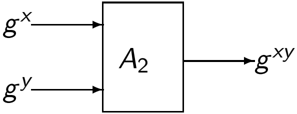
- If you can solve A then you can solve B; equivalently
- If A is easy then B is easy; equivalently
- If B is hard then A is hard.

DL $\longrightarrow$ CDH

Given: DL solver A_1

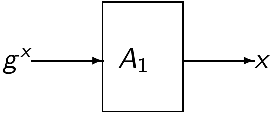


Want: CDH solver A_2

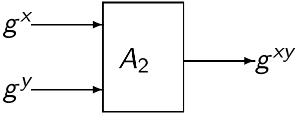


Construction:

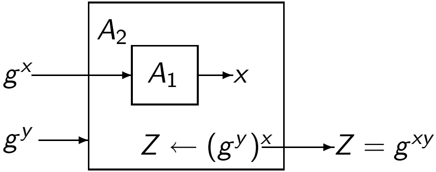
Given: DL solver A_1



Want: CDH solver A_2



Construction:



Formal Definitions

Problem	**Given**	**Figure out**
Discrete logarithm (DL)	g^x	x
Computational Diffie-Hellman (CDH)	g^x, g^y	g^{xy}
Decisional Diffie-Hellman (DDH)	g^x, g^y, g^z	is $z \equiv xy (\text{mod } \lvert G \rvert)$?

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

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

for an adversary A that equal their success probability.

DL Formally

Let $G = \langle g \rangle$ be a cyclic group of order m, and A an adversary.

Game $\mathrm{DL}_{G,g}$	
procedure Initialize $x \xleftarrow{\$} \mathbf{Z}_m; X \leftarrow g^x$ return X	**procedure Finalize**(x') return $(x = x')$

The dl-advantage of A is

$$\mathbf{Adv}^{\mathrm{dl}}_{G,g}(A) = \Pr\left[\mathrm{DL}^{A}_{G,g} \Rightarrow \mathsf{true}\right]$$

Status

Problem	Group	
	$\mathbf{Z}_p^*$	EC
DL	hard	harder
CDH	hard	harder
DDH	easy	harder

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.

Finding cyclic groups

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 $g \in G - \{\mathbf{1}\}$ is a generator.

If $G = Z_p^*$ 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
  $g \xleftarrow{\$} G - \{1\}$
until $(\text{TEST-GEN}_G(g) = \mathsf{true})$

- How do we design TEST-GEN_G?
- How many iterations does the algorithm take?

Finding generators: Randomly pick and check

repeat
  $g \xleftarrow{\$} G - \{1\}$
until $(\text{TEST-GEN}_G(g) = \mathsf{true})$

- How do we design 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.

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

i	1	2	3	4	5	6
1^i						

Generators mod 7

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

i	1	2	3	4	5	6
1^i	1					

Generators mod 7

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

i	1	2	3	4	5	6
1^i	1	1	1	1	1	1
2^i						

Generators mod 7

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

i	1	2	3	4	5	6
1^i	1	1	1	1	1	1
2^i	2					

Generators mod 7

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

i	1	2	3	4	5	6
1^i	1	1	1	1	1	1
2^i	2	4	1	2	4	1
3^i						

Generators mod 7

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

i	1	2	3	4	5	6
1^i	1	1	1	1	1	1
2^i	2	4	1	2	4	1
3^i	3					

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

i	1	2	3	4	5	6
1^i	1	1	1	1	1	1
2^i	2	4	1	2	4	1
3^i	3	2				

Generators mod 7

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

i	1	2	3	4	5	6
1^i	1	1	1	1	1	1
2^i	2	4	1	2	4	1
3^i	3	2	6			

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

i	1	2	3	4	5	6
1^i	1	1	1	1	1	1
2^i	2	4	1	2	4	1
3^i	3	2	6	4		

Generators mod 7

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

i	1	2	3	4	5	6
1^i	1	1	1	1	1	1
2^i	2	4	1	2	4	1
3^i	3	2	6	4	5	

Generators mod 7

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

i	1	2	3	4	5	6
1^i	1	1	1	1	1	1
2^i	2	4	1	2	4	1
3^i	3	2	6	4	5	1

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

i	1	2	3	4	5	6
1^i	1	1	1	1	1	1
2^i	2	4	1	2	4	1
3^i	3	2	6	4	5	1
4^i	4	2	1	4	2	1
5^i	5	4	6	2	3	1
6^i	6	1	6	1	6	1

Generators mod 7

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

i	1	2	3	4	5	6
1^i	1	1	1	1	1	1
2^i	2	4	1	2	4	1
3^i	3	2	6	4	5	1
4^i	4	2	1	4	2	1
5^i	5	4	6	2	3	1
6^i	6	1	6	1	6	1

The generators are

Generators mod 7

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

i	1	2	3	4	5	6
1^i	1	1	1	1	1	1
2^i	2	4	1	2	4	1
3^i	3	2	6	4	5	1
4^i	4	2	1	4	2	1
5^i	5	4	6	2	3	1
6^i	6	1	6	1	6	1

The generators are 3 and 5

Generators mod 7

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

i	2	3
1^i	1	1
2^i	4	1
3^i	2	6
4^i	2	1
5^i	4	6
6^i	1	6

We observe that g is a generator if and only if $g^2 \neq 1$ and $g^3 \neq 1$.

Testing whether a group element is a generator

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

Fact: $g \in \mathbf{Z}_p^*$ 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 $g \in \mathbf{Z}_7^*$ 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: $\mathbf{Z}_p^*$ has $q-1$ generators

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

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

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

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

$$\Pr\left[\langle g\rangle = \mathbf{Z}_7^*\right] = \frac{3-1}{7-2} = \frac{2}{5}$$

Finding generators: Randomly pick and check

repeat
$\quad g \xleftarrow{\$} G - \{1\}$
until $(\mathrm{TEST\text{-}GEN}_G(g) = \mathsf{true})$

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

We are addressing the two questions for the case that p is a SG prime.

Finding generators modulo SG primes

Suppose p is a SG prime with $p - 1 = 2q$.

repeat
  $g \xleftarrow{\$} G - \{1\}$
until $(g^2 \not\equiv 1 \pmod{p}$ and $g^q \not\equiv 1 \pmod{p})$

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 $\mathbf{Z}_p^*$

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

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
  $p \xleftarrow{\$} \{2^{k-1}, \ldots, 2^k - 1\}$
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?

Primality Testing

Given: integer N
Output: TRUE if N is prime, FALSE otherwise.

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

Primality Testing

Given: integer N
Output: TRUE if N is prime, FALSE otherwise.

for $i = 2, \ldots, \lceil \sqrt{N} \rceil$ do
  if $N \bmod i = 0$ 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 $p \xleftarrow{\$} \{1, \ldots, N\}$ then

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

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

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.