Discrete Structures
Number Theory

Amotz Bar-Noy

Department of Computer and Information Science
Brooklyn College

Journey into cryptography: Ancient Cryptography

All videos

- https://www.khanacademy.org/computing/computer-science/cryptography

List of videos

- What is cryptography? https://youtu.be/Kf9KjCKmDcU
- The Caesar cipher: https://youtu.be/sMOZf4GN3oc
- Polyalphabetic cipher: https://youtu.be/BgFJD7oCmDE
- The one-time pad: https://youtu.be/FlIG3TvQCBQ
- Frequency stability property: https://youtu.be/vVXbgbMp0oY
- The Enigma encryption machine: https://youtu.be/-1ZFVwMXSXY
- Perfect secrecy: https://youtu.be/vKRMWewGE9A
- Pseudorandom number generators: https://youtu.be/GtOt7EBNEwQ

Prime Numbers

Prime and Composite Numbers

- A positive integer $p \geq 2$ is **prime** if its only divisors are 1 and itself.
- A positive integer $n \geq 2$ is **composite** if it has at least 3 divisors.
- **1** is either prime or not but it is not composite.

The Fundamental Theorem of Arithmetic

- Every integer greater than 1 is either prime itself or can be represented with a **unique** product of primes.
- **Corollary: 1** is not prime.
- **Story:** `https://youtu.be/8CluknrLeys`

Primality Test and Factoring

Tasks

- **Primality test:** determine whether an input integer is prime or composite.
- **Integer factorization:** decompose an input integer into its unique product of primes.

Hardness

- It is **relatively easy** to test if a very large integer is prime.
  - Can be done **almost surely** (with high probability).
- It is **extremely difficult** to factor a very large integer.
  - Especially if the integer is a product of two very large primes.

The Natural Primality Test

Algorithm

- Input: an integer $n \geq 2$
- Set $s = n - 1$
- For all $2 \leq d \leq s$ check if d is a divisor of n
  - If yes then **abort** because n is not prime
  - If no then **continue**
- If this step is reached then n is prime

Improvement

- Set $s = \lfloor \sqrt{n} \rfloor$
- **Proof:**
  - If $q > \lfloor \sqrt{n} \rfloor$ is a divisor of n then $n = d \cdot q$ for $d < \lfloor \sqrt{n} \rfloor$ and d is another divisor of n.
  - There is no need to check if q divides n because the algorithm will **abort** after checking if d is a divisor of n.

Example

Check if $n = 77$ is prime

- **Initially:** $s = 8$ and $d = 2$

$$\begin{array}{rcl} 2 \not| 77 & \Longrightarrow & d = 3 \\ 3 \not| 77 & \Longrightarrow & d = 4 \\ 4 \not| 77 & \Longrightarrow & d = 5 \\ 5 \not| 77 & \Longrightarrow & d = 6 \\ 6 \not| 77 & \Longrightarrow & d = 7 \\ 7 \mid 77 & \Longrightarrow & \textbf{ABORT} \end{array}$$

- **Return:** $77 = 7 \cdot 11$ is not prime

Example

Check if $n = 97$ is prime

- **Initially:** $s = 9$ and $d = 2$

$$\begin{aligned}
2 \not| \, 97 &\implies d = 3 \\
3 \not| \, 97 &\implies d = 4 \\
4 \not| \, 97 &\implies d = 5 \\
5 \not| \, 97 &\implies d = 6 \\
6 \not| \, 97 &\implies d = 7 \\
7 \not| \, 97 &\implies d = 8 \\
8 \not| \, 97 &\implies d = 9 \\
9 \not| \, 97 &
\end{aligned}$$

- **Return:** 97 is prime

The Natural Integer Factorization Algorithm

Algorithm

- **Input:** an integer $n \geq 2$
- Set $D = ()$ to be an empty list
- Set $d = 2$
- Set $m = n$
- **Repeat** the following procedure until $m = 1$
  - If d is a divisor of m then
    - Append d at the end of the list D
    - Set $m = m/d$
  - If d is not a divisor of m then increment d by one
- Assume: $D = (d_1 \leq d_2 \leq \cdots \leq d_j)$
- **Output:** $n = d_1 d_2 \cdots d_j = p_1^{k_1} p_2^{k_2} \cdots p_h^{k_h}$

Example

The Prime factors of 360

- **Initially:** $m = 360$, $d = 2$, and $D = ()$

$$\begin{array}{rcl} 2 \mid 360 & \Longrightarrow & m = 180 \quad d = 2 \quad D = (2) \\ 2 \mid 180 & \Longrightarrow & m = 90 \quad d = 2 \quad D = (2,2) \\ 2 \mid 90 & \Longrightarrow & m = 45 \quad d = 2 \quad D = (2,2,2) \\ 2 \nmid 45 & \Longrightarrow & m = 45 \quad d = 3 \quad D = (2,2,2) \\ 3 \mid 45 & \Longrightarrow & m = 15 \quad d = 3 \quad D = (2,2,2,3) \\ 3 \mid 15 & \Longrightarrow & m = 5 \quad d = 3 \quad D = (2,2,2,3,3) \\ 3 \nmid 5 & \Longrightarrow & m = 5 \quad d = 4 \quad D = (2,2,2,3,3) \\ 4 \nmid 5 & \Longrightarrow & m = 5 \quad d = 5 \quad D = (2,2,2,3,3) \\ 5 \mid 5 & \Longrightarrow & m = 1 \quad d = 5 \quad D = (2,2,2,3,3,5) \end{array}$$

- **Return:** $360 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 = 2^3 \cdot 3^2 \cdot 5$

Example

The Prime factors of 1001

- **Initially:** $m = 1001, d = 2, D = ()$

$$
\begin{array}{llcllll}
\{2,3,4,5,6\} & \not| & 1001 & \Longrightarrow & m = 1001 & d = 7 & D = () \\
7 & | & 1001 & \Longrightarrow & m = 143 & d = 7 & D = (7) \\
\{7,8,9,10\} & \not| & 143 & \Longrightarrow & m = 143 & d = 11 & D = (7) \\
11 & | & 143 & \Longrightarrow & m = 13 & d = 11 & D = (7,11) \\
\{11,12\} & \not| & 13 & \Longrightarrow & m = 13 & d = 13 & D = (7,11) \\
13 & | & 13 & \Longrightarrow & m = 1 & d = 13 & D = (7,11,13)
\end{array}
$$

- **Return:** $1001 = 7 \cdot 11 \cdot 13$

Sieve of Eratosthenes

Algorithm: Find all the primes that are smaller than $0 < N$

- **Set** all the numbers $2, 3, \ldots, N$ as prime **candidates**
- **Set** $p = 2$
- **Repeat** the following procedure until $p > \sqrt{N}$:
  - **Mark** p as prime
  - **Mark** the next $\lfloor N/p \rfloor - 1$ multiples of p as composite
  - **Set** p to be the smallest remaining **candidate**
- **Mark** all the remaining candidates as primes

Online resources

- `https://www.youtube.com/watch?v=dhfhu9Q5g8U`
- `https://youtu.be/klcIklsWzrY`

There are infinitely many prime numbers

Proof

- Let $p_1 < p_2 < \cdots < p_n$ be a set of n primes.
- Let $Q = p_1 p_2 \cdots p_n + 1$.
- If Q is prime, then a new prime is found.
- Otherwise, Q is a product of two or more primes due to **The Fundamental Theorem of Arithmetic**.
- **Observation:** None of these primes can be $p_1, \ldots, p_n$ because a number greater than 1 cannot be a divisor of both Q and $Q - 1$.
- Therefore, at least one of Q's factors must be a new prime.
- This process can continue to find infinitely many primes.

Online resources

- The original proof by Euclid: `https://youtu.be/dQmdHpvfyJs`
- $\approx \frac{n}{\log(n)}$ prime numbers are smaller than n: `https://youtu.be/EKfdRks8oMI`

Modular Arithmetic

Notations

$$\begin{aligned} n &= q \cdot d + r \quad (* \, 0 \le r < d \, *) \\ n \bmod d &= r \end{aligned}$$

- n: **dividend**; d: **divisor**; q: **quotient**; r: **remainder**

Examples

- $7 \bmod 3 = 1$ because $7 = 2 \cdot 3 + 1$
- $25 \bmod 5 = 0$ because $25 = 5 \cdot 5 + 0$
- $101 \bmod 7 = 3$ because $101 = 14 \cdot 7 + 3$
- $17 \bmod 12 = 5$ because $17 = 1 \cdot 12 + 5$

Definitions

- If $n \bmod d = 0$ then $d \mid n$
- d **divides** n and is a **divisor** of n while n is a **multiple** of d

Negative Numbers

Which parts can be negative?

- The **dividend** (n), **quotient** (q), and **remainder** (r) can be **negative**
- The **divisor** (d) is “always” **positive**

Negative n and q

- $-18 \bmod 7 = 3$ because $-18 = -3 \cdot 7 + 3$
- $-55 \bmod 5 = 0$ because $-55 = -11 \cdot 5 + 0$

Negative r

- If $n = q \cdot d + r$ for $0 \leq r < d$ then
  $n = (q + 1) \cdot d - (d - r)$ for $0 \leq d - r < d$
  - Useful for modular operations when $d - r < r$
- $103 \bmod 7 = 5 = -2$ since $103 = 14 \cdot 7 + 5 = 15 \cdot 7 - 2$

Congruence Modulo

Notation

- For integers $-\infty < n, m < \infty$ and positive integer $d > 1$:
  If $(n \bmod d) = (m \bmod d)$ **then** $n \equiv m \pmod{d}$

Congruence is an Equivalence Relation

- **Reflexive property**: $n \equiv n \pmod{d}$
  - $27 \equiv 27 \pmod{5}$
- **Symmetry property**: $n \equiv m \pmod{d} \iff m \equiv n \pmod{d}$
  - $27 \equiv 52 \pmod{5} \iff 52 \equiv 27 \pmod{5}$
- **Transitive property**:
  $(n \equiv m \pmod{d}) \wedge (m \equiv k \pmod{d}) \implies n \equiv k \pmod{d}$
  - $(52 \equiv 27 \pmod{5}) \wedge (27 \equiv 12 \pmod{5}) \implies 52 \equiv 12 \pmod{5}$

Proofs idea

- There exist q_n, q_m, q_k, and $0 \le r < d$ such that
  $n = q_n d + r$; $m = q_m d + r$; and $k = q_k d + r$

Basic Properties

Proposition

- For integers $-\infty < n, k < \infty$ and positive integer $d > 1$:

$$(n \bmod d) = ((n + kd) \bmod d) \implies n \equiv n + kd \pmod{d}$$

Examples

- $(7 \bmod 5) = (12 \bmod 5) = (112 \bmod 5) = 2$
  $\implies 7 \equiv 12 \equiv 112 \pmod{5}$
- $(-3 \bmod 7) = (4 \bmod 7) = (11 \bmod 7) = 4$
  $\implies -3 \equiv 4 \equiv 11 \pmod{7}$

Proof outline

- $n = qd + r$
- $n + kd = (q + k)d + r$

Basic Properties

Proposition

- For integers $-\infty < n, m < \infty$ and positive integer $d > 1$:
$$(n \bmod d) = (m \bmod d) \implies d \mid (n - m)$$

Examples

- $(100 \bmod 7) = (23 \bmod 7) = 2 \implies 7 \mid (100 - 23) = 77$
- $(10 \bmod 3) = (-8 \bmod 3) = 1 \implies 3 \mid (10 - (-8)) = 18$

Proof Outline

- $n = q_n d + r$
- $m = q_m d + r$
- $(n - m) = (q_n - q_m)d$

Modular Addition

Proposition

- For integers $-\infty < n, m < \infty$ and positive integer $d > 1$:

$$(n + m) \bmod d = ((n \bmod d) + (m \bmod d)) \bmod d$$

Example: compute $(34 + 21) \bmod 5$

- **Direct method:**

$$(34 + 21 = 55) \wedge (55 = 11 \cdot 5 + 0) \Rightarrow (34 + 21) \bmod 5 = 0$$

- **Modular addition method:**

$$\begin{aligned} (34 + 21) \bmod 5 &= ((34 \bmod 5) + (21 \bmod 5)) \bmod 5 \\ &= (4 + 1) \bmod 5 \\ &= 5 \bmod 5 \\ &= 0 \end{aligned}$$

A Modular Addition Table for $d = 5$

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

A Modular Addition Table for $d = 6$

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Modular Subtraction

Proposition

- For integers $-\infty < n, m < \infty$ and positive integer $d > 1$:

$$(n - m) \bmod d = ((n \bmod d) - (m \bmod d)) \bmod d$$

Example: compute $(21 - 13) \bmod 5$

- **Direct method:**

$$(21 - 13 = 8) \wedge (8 = 1 \cdot 5 + 3) \;\Rightarrow\; (21 - 13) \bmod 5 = 3$$

- **Modular subtraction method:**

$$\begin{aligned}(21 - 13) \bmod 5 &= ((21 \bmod 5) - (13 \bmod 5)) \bmod 5 \\ &= (1 - 3) \bmod 5 \\ &= -2 \bmod 5 \\ &= 3\end{aligned}$$

A Modular Subtraction Table for $d = 5$

$-$	0	1	2	3	4
0	0	4	3	2	1
1	1	0	4	3	2
2	2	1	0	4	3
3	3	2	1	0	4
4	4	3	2	1	0

A Modular Subtraction Table for $d = 6$

$-$	0	1	2	3	4	5
0	0	5	4	3	2	1
1	1	0	5	4	3	2
2	2	1	0	5	4	3
3	3	2	1	0	5	4
4	4	3	2	1	0	5
5	5	4	3	2	1	0

Modular Multiplication

Proposition

- For integers $-\infty < n, m < \infty$ and positive integer $d > 1$:

$$(n \cdot m) \bmod d = ((n \bmod d)(m \bmod d)) \bmod d$$

Example: compute $(12 \cdot 11) \bmod 7$

- **Direct method:**

$$(12 \cdot 11 = 132) \wedge (132 = 18 \cdot 7 + 6) \;\Rightarrow\; (12 \cdot 11) \bmod 7 = 6$$

- **Modular multiplication method:**

$$\begin{aligned} (12 \cdot 11) \bmod 7 &= ((12 \bmod 7)(11 \bmod 7)) \bmod 7 \\ &= (5 \cdot 4) \bmod 7 \\ &= 20 \bmod 7 \\ &= 6 \end{aligned}$$

A Modular Multiplication Table for $d = 5$

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

A Modular Multiplication Table for $d = 6$

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Modular Inverse

Definition

- Let $0 < n < d$ be two **relatively prime (coprime)** integers
  - There is no integer greater than 1 that is a divisor of both n and d
- The **inverse** of n modulo d is an integer $0 < m < d$ such that
  - $(mn \bmod d) = 1$

Symmetry

- If $(mn \bmod d) = 1$ then $(nm \bmod d) = 1$ and therefore n is the inverse of m modulo d **iff** m is the inverse of n modulo d

$$
\begin{array}{ccc}
(n^{-1} \bmod d) = m & \iff & (m^{-1} \bmod d) = n \\
m = n^{-1} & \iff & n = m^{-1}
\end{array}
$$

Modular Inverse

Examples

- 3 is the inverse of 5 modulo 7 because $((3 \cdot 5 = 15) \bmod 7) = 1$
- 5 is the inverse of itself modulo 6 because $((5 \cdot 5 = 25) \bmod 6) = 1$
- 3 has no inverse modulo 6 because $(3 \cdot x) \bmod 6$ is either 0 or 3

Propositions

- 1 is the inverse of itself modulo d

$$((1 \cdot 1) \bmod d) = (1 \bmod d) = 1$$

- $d - 1$ is the inverse of itself modulo d for any integer $d > 1$

$$\begin{aligned}
(d-1)^2 \bmod d &= (d^2 - 2d + 1) \bmod d \\
&= ((d-2)d + 1) \bmod d \\
&= ((((d-2)d) \bmod d) + (1 \bmod d)) \bmod d \\
&= (0 + 1) \bmod d \\
&= 1 \bmod d
\end{aligned}$$

Modular Division

Proposition

- For two integers $-\infty < n, m < \infty$ in which m is relatively prime to a positive integer $d > 1$

$$\begin{aligned}(n/m) \bmod d &= (n \cdot m^{-1}) \bmod d \\ &= ((n \bmod d)(m^{-1} \bmod d)) \bmod d\end{aligned}$$

Example: compute $(99/3) \bmod 7$

- **Direct method:**

$$(99/3 = 33) \wedge (33 = 4 \cdot 7 + 5) \Rightarrow (99/3) \bmod 7 = 5$$

- **Modular division method:**

$$\begin{aligned}(99/3) \bmod 7 &= ((99 \bmod 7)(3^{-1} \bmod 7)) \bmod 7 \\ &= (1 \cdot 5) \bmod 7 \\ &= 5 \bmod 7 \\ &= 5\end{aligned}$$

A Modular Division Table for $d = 5$

$\div$	0	1	2	3	4
0	$\perp$	0	0	0	0
1	$\perp$	1	3	2	4
2	$\perp$	2	1	4	3
3	$\perp$	3	4	1	2
4	$\perp$	4	2	3	1

A Modular Division Table for $d = 6$

$\div$	0	1	2	3	4	5
0	0	0	$\{0,3\}$	$\{0,2,4\}$	$\{0,3\}$	0
1	$\{\}$	1	$\{\}$	$\{\}$	$\{\}$	5
2	$\{\}$	2	$\{1,4\}$	$\{\}$	$\{2,5\}$	4
3	$\{\}$	3	$\{\}$	$\{1,3,5\}$	$\{\}$	3
4	$\{\}$	4	$\{2,5\}$	$\{\}$	$\{1,4\}$	2
5	$\{\}$	5	$\{\}$	$\{\}$	$\{0,3\}$	1

Modular Exponentiation

Proposition

- For integers $-\infty < n < \infty$, $k \geq 0$, and $d > 1$:

$$n^k \bmod d = ((n \bmod d)^k) \bmod d$$

Example: compute $9^3 \bmod 7$

- **Direct method:**

$$(9^3 = 729) \wedge (729 = 104 \cdot 7 + 1) \;\Rightarrow\; 9^3 \bmod 7 = 1$$

- **Modular exponentiation method:**

$$\begin{aligned}(9^3) \bmod 7 &= ((9 \bmod 7)^3) \bmod 7 \\ &= 2^3 \bmod 7 \\ &= 8 \bmod 7 \\ &= 1\end{aligned}$$

Modular Exponentiation

Example: compute $10^5 \bmod 7$

- **Direct method:**

$$(10^5 = 100000) \wedge (100000 = 14285 \cdot 7 + 5) \Rightarrow 10^5 \bmod 7 = 5$$

- **Modular exponentiation method:**

$$\begin{aligned} 10^5 \bmod 7 &= (10 \bmod 7)^5 \bmod 7 \\ &= 3^5 \bmod 7 \\ &= ((9 \bmod 7) \cdot (9 \bmod 7) \cdot (3 \bmod 7)) \bmod 7 \\ &= (2^2 \cdot 3) \bmod 7 \\ &= 12 \bmod 7 \\ &= 5 \end{aligned}$$

A Modular Exponentiation Table for $d = 5$

exp	0	1	2	3	4	5	6	7
0	1	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1
2	1	2	4	3	1	2	4	3
3	1	3	4	2	1	3	4	2
4	1	4	1	4	1	4	1	4

A Modular Exponentiation Table for $d = 6$

exp	0	1	2	3	4	5
0	1	0	0	0	0	0
1	1	1	1	1	1	1
2	1	2	4	2	4	2
3	1	3	3	3	3	3
4	1	4	4	4	4	4
5	1	5	1	5	1	5

Computing $n^k \bmod d$ for $n < d$ and large k

Method I: Outline

- Since $n < d$, it follows that $n \bmod d = n$; therefore, $n^{2^0} \bmod d = n$
- Observe that $n^{2^{i+1}} = n^{2^i \cdot 2} = \left(n^{2^i}\right)^2$
- Iteratively compute

$$
\begin{aligned}
n^2 &= n^{2^1} \mod d \\
n^4 &= n^{2^2} \mod d \\
n^8 &= n^{2^3} \mod d \\
n^{16} &= n^{2^4} \mod d
\end{aligned}
$$

- Stop the computation when $k < n^{2^{i+1}}$
- Using the binary representation of k set $k = 2^{i_1} + 2^{i_2} + \cdots + 2^{i_h}$
- It follows that $n^k = n^{2^{i_1} + 2^{i_2} + \cdots + 2^{i_h}} = n^{2^{i_1}} \cdot n^{2^{i_2}} \cdots n^{2^{i_h}}$
- $n^k \bmod d$ can be computed using modular multiplication among the already computed values of $n^{2^i} \bmod d$

Computing $2^{57} \bmod 7$ – Method I

Preprocessing

$$
\begin{aligned}
2^1 \bmod 7 &= & & & & & 2\\
2^2 \bmod 7 &= & (2^1)^2 \bmod 7 &= & 2^2 \bmod 7 &= & 4\\
2^4 \bmod 7 &= & (2^2)^2 \bmod 7 &= & 4^2 \bmod 7 &= & 2\\
2^8 \bmod 7 &= & (2^4)^2 \bmod 7 &= & 2^2 \bmod 7 &= & 4\\
2^{16} \bmod 7 &= & (2^8)^2 \bmod 7 &= & 4^2 \bmod 7 &= & 2\\
2^{32} \bmod 7 &= & (2^{16})^2 \bmod 7 &= & 2^2 \bmod 7 &= & 4
\end{aligned}
$$

Computation: $57 = 32 + 16 + 8 + 1$

$$
\begin{aligned}
2^{57} \bmod 7 &= (2^{32}2^{16}2^{8}2^{1}) \bmod 7\\
&= ((2^{32} \bmod 7)(2^{16} \bmod 7)(2^{8} \bmod 7)(2^{1} \bmod 7)) \bmod 7\\
&= (4 \cdot 2 \cdot 4 \cdot 2) \bmod 7\\
&= 64 \bmod 7\\
&= 1
\end{aligned}
$$

Computing $3^{101} \bmod 5$ – Method I

Preprocessing

$$\begin{array}{lclclcl}
3^1 \bmod 5 & = & & & & & 3 \\
3^2 \bmod 5 & = & (3^1)^2 \bmod 5 & = & 3^2 \bmod 5 & = & 4 \\
3^4 \bmod 5 & = & (3^2)^2 \bmod 5 & = & 4^2 \bmod 5 & = & 1 \\
3^8 \bmod 5 & = & (3^4)^2 \bmod 5 & = & 1^2 \bmod 5 & = & 1
\end{array}$$

$$3^{16} \bmod 5 = 3^{32} \bmod 5 = 3^{64} \bmod 5 = 1$$

Computation: $101 = 64 + 32 + 4 + 1$

$$\begin{aligned}
3^{101} \bmod 5 &= (3^{64}3^{32}3^{4}3^{1}) \bmod 5 \\
&= ((3^{64} \bmod 5)(3^{32} \bmod 5)(3^{4} \bmod 5)(3^{1} \bmod 5)) \bmod 5 \\
&= (1 \cdot 1 \cdot 1 \cdot 3) \bmod 5 \\
&= 3 \bmod 5 \\
&= 3
\end{aligned}$$

Computing $n^k \bmod d$ for $n < d$ and large k

Method II: Outline

- Express k as $k = a\ell + b$ such that $n^\ell \bmod d$ is 1 or -1 and $n^b \bmod d$ is relatively easy to compute
- It follows that $n^k = n^{a\ell+b} = (n^\ell)^a \cdot n^b$
- The modular exponentiation rule for d will replace n^ℓ and then $(n^\ell)^a$ with 1 and -1
- The final answer will be $(n^b \bmod d)$ or $-(n^b \bmod d)$

Computing $2^{57} \bmod 7$ – Method II

Preprocessing

$$(2^3 \bmod 7) \;=\; (8 \bmod 7) \;=\; 1$$

Computation: $57 = 3 \cdot 19$

$$\begin{aligned}
2^{57} \bmod 7 &= 2^{3\cdot 19} \bmod 7 \\
&= (2^3)^{19} \bmod 7 \\
&= (2^3 \bmod 7)^{19} \bmod 7 \\
&= (8 \bmod 7)^{19} \bmod 7 \\
&= 1^{19} \bmod 7 \\
&= 1 \bmod 7 \\
&= 1
\end{aligned}$$

Computing $3^{101} \bmod 5$ – Method II

Preprocessing

$$\begin{aligned}(3^2 \bmod 5) &= (9 \bmod 5) &= -1\\ (3^4 \bmod 5) &= (81 \bmod 5) &= 1\end{aligned}$$

First computation: $101 = 2 \cdot 50 + 1$

$$\begin{aligned}3^{101} \bmod 5 &= 3^{2\cdot 50+1} \bmod 5\\ &= ((3^2)^{50} \cdot 3) \bmod 5\\ &= ((-1)^{50} \cdot 3) \bmod 5\\ &= (1 \cdot 3) \bmod 5 = 3\end{aligned}$$

Second computation: $101 = 4 \cdot 25 + 1$

$$\begin{aligned}3^{101} \bmod 5 &= 3^{4\cdot 25+1} \bmod 5\\ &= ((3^4)^{25} \cdot 3) \bmod 5\\ &= ((1)^{25} \cdot 3) \bmod 5\\ &= (1 \cdot 3) \bmod 5 = 3\end{aligned}$$

Online Resources

Modular arithmetic

- Examples:
  https://youtu.be/2zEXtoQDpXY
- Modular exponentiation (first two examples):
  https://youtu.be/tTuWmcikE0Q

Application

- The Lazy Mathematician:
  https://youtu.be/FdmApk9V2-w

The Greatest Common Divisor (GCD)

Definition

- Let n and m be two positive integers and let g be the largest positive integer that is a divisor of both of them
- $g = \gcd(n, m)$ is the **Greatest Common Divisor** of n and m

Examples

- $5 = \gcd(5, 15)$
- $6 = \gcd(12, 18)$
- $1 = \gcd(13, 21)$

Bounds on $g = \gcd(n, m)$

- **Lower bound:** 1 is a divisor of all integers, therefore $g \geq 1$
- **Upper bound:** An integer cannot be a divisor of a smaller integer, therefore $g \leq \min\{n, m\}$

The Largest Divisor Algorithm

Algorithm

- Let $N = \{1 < n_1 < n_2 < \cdots < n_{r-2} < n\}$ be the set of all the r ($r \geq 2$) divisors of n including 1 and n
- Let $M = \{1 < m_1 < m_2 < \cdots < m_{s-2} < m\}$ be the set of all the S ($s \geq 2$) divisors of m including 1 and m
- Let $G = N \cap M$ be the intersection of N and M and let g be the largest number in G
- Then $g = \gcd(n, m)$

Proof

- All the positive integers (including 1) that are divisors of both n and m are in G
- Therefore, by definition, $g = \gcd(n, m)$

Examples

Example I

- **Input:** $n = 372$ and $m = 138$
- $N = \{1, 2, 3, 4, 6, 12, 31, 62, 93, 124, 186, 372\}$
- $M = \{1, 2, 3, 6, 23, 46, 69, 138\}$
- $G = \{1, 2, 3, 6\}$
- **Output:** $\gcd(372, 138) = 6$

Example II

- **Input:** $n = 480$ and $m = 360$
- $N = \{1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 20, 24, 30, 32, , 40, 48, 60, 80, 96, 120, 160, 240, 480\}$
- $M = \{1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 18, 20, 24, 30, 36, 40, 45, 60, 72, 90, 120, 180, 360\}$
- $G = \{1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60, 120\}$
- **Output:** $\gcd(480, 360) = 120$

The Common Prime Factors Algorithm

Algorithm

- Let $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ be the prime factorization of n
- Let $m = q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$ be the prime factorization of m
- Let $G = \{g_1, g_2, \ldots, g_t\} = \{p_1, p_2, \ldots, p_r\} \cap \{q_1, q_2, \ldots, q_s\}$
- If G is empty then $\gcd(n, m) = 1$
- Otherwise:
  - For all $1 \leq i \leq t$ such that $g_i = p_j = q_k$ set $h_i = \min\{a_j, b_k\}$
  - Then $\gcd(n, m) = g_1^{h_1} g_2^{h_2} \cdots g_t^{h_t}$

Proof outline

- Assume g^h is a divisor of $\gcd(n, m)$ for a prime integer g and $h \geq 1$
- Then $g = p_j$ and $g = q_k$ for some $1 \leq j \leq r$ and $1 \leq k \leq s$
- Also, $h \leq a_j$ and $h \leq b_k$
- Therefore, $g_1^{h_1} g_2^{h_2} \cdots g_t^{h_t}$ is the prime factorization of $\gcd(n, m)$

Examples

Example I

- **Input:** $n = 372$ and $m = 138$
- $372 = 2^2 \cdot 3^1 \cdot 31^1$
- $138 = 2^1 \cdot 3^1 \cdot 23^1$
- $G = \{2, 3\}$
- **Output:** $\text{gcd}(372, 138) = 2^1 \cdot 3^1 = 6$

Example II

- **Input:** $n = 480$ and $m = 360$
- $480 = 2^5 \cdot 3^1 \cdot 5^1$
- $360 = 2^3 \cdot 3^2 \cdot 5^1$
- $G = \{2, 3, 5\}$
- **Output:** $\text{gcd}(480, 360) = 2^3 \cdot 3^1 \cdot 5^1 = 120$

The Euclidean Algorithm

Idea and proof outline

- **Idea:** $\gcd(n, m) = \gcd(m, (n \bmod m))$ for $n > m$
- **Proof outline:** If d is a divisor of both n and m then it is a divisor of $(n \bmod m)$

Algorithm

- $gcd(n, m)$ (* $n \geq m$ *)
  `if` $(n \bmod m) = 0$
  `then return` m
  `else return` $gcd(m, (n \bmod m))$

Online examples

- https://youtu.be/klTIrnovoEE
- https://youtu.be/fwuj4yzoX1o

The Euclidean Algorithm

Example I

- **Input:** $n = 372$ and $m = 138$

n	m	$n = q \cdot m + r$
372	138	$372 = 2 \cdot 138 + 96$
138	96	$138 = 1 \cdot 96 + 42$
96	42	$96 = 2 \cdot 42 + 12$
42	12	$42 = 3 \cdot 12 + 6$
12	6	$12 = 2 \cdot 6 + 0$

- **Output:** $\gcd(372, 138) = 6$

The Euclidean Algorithm

Example II

- **Input:** $n = 480$ and $m = 360$

n	m	$n = q \cdot m + r$
480	360	$480 = 1 \cdot 360 + 120$
360	120	$360 = 3 \cdot 120 + 0$

- **Output:** $\gcd(480, 360) = 120$

The Euclidean Algorithm

Example III

- **Input:** $n = 21$ and $m = 13$

n	m	$n = q \cdot m + r$
21	13	$21 = 1 \cdot 13 + 8$
13	8	$13 = 1 \cdot 8 + 5$
8	5	$8 = 1 \cdot 5 + 3$
5	3	$5 = 1 \cdot 3 + 2$
3	2	$3 = 1 \cdot 2 + 1$
2	1	$2 = 2 \cdot 1 + 0$

- **Output:** $\gcd(21, 13) = 1$

The Extended Euclidean Algorithm

Bézout's identity

- Let $g = \gcd(n, m)$ for two positive integers n and m
- There exist integers (positive and/or negative) x and y such that
$$xn + ym = g$$
- All the integers that can be expressed as $zn + wm$ for two integers z and w are all the multiples of g

Algorithm's idea

- Run the Euclidean Algorithm to find $\gcd(n, m)$
- Find x and y by following the algorithm in a reverse order

Online example

- `https://youtu.be/FjliV5u2IVw`

Example

Compute $6 = \gcd(372, 138)$

$$\begin{aligned} 372 &= 2 \cdot 138 + 96 \\ 138 &= 1 \cdot 96 + 42 \\ 96 &= 2 \cdot 42 + 12 \\ 42 &= 3 \cdot 12 + 6 \\ 12 &= 2 \cdot 6 \end{aligned}$$

Compute $6 = (-10 \cdot 372) + (27 \cdot 138)$

$$\begin{aligned} 6 &= & &= (1 \cdot 42) - (3 \cdot 12) \\ &= (1 \cdot 42) - 3(96 - 2 \cdot 42) & &= (-3 \cdot 96) + (7 \cdot 42) \\ &= (-3 \cdot 96) + 7(138 - 96) & &= (7 \cdot 138) - (10 \cdot 96) \\ &= (7 \cdot 138) - 10(372 - 2 \cdot 138) & &= (-10 \cdot 372) + (27 \cdot 138) \end{aligned}$$

Computing the Modular Inverse

Bézout's identity for relatively prime integers

- Let $\gcd(n, d) = 1$ for two positive integers n and d
- There exist integers x and y such that $xn + yd = 1$

For relatively prime n and d, find the inverse of n modulo d

- Equivalently, find m such that $(mn \bmod d) = 1$
- Set $m = x$ in the above $xn + yd = 1$ Bézout's identity
- Therefore, $mn + yd = 1$

$$\begin{aligned} mn &= 1 - yd \\ (mn \bmod d) &= (1 \bmod d) - (yd \bmod d) = 1 \end{aligned}$$

- $m = n^{-1}$ is the inverse of n modulo d

Example

Find the inverse of 11 mudulo 17

- Using the extended Euclidean algorithm find

$$14 \cdot 11 - 9 \cdot 17 = 1$$

- Equivalently,

$$\begin{aligned} (14 \cdot 11) \bmod 17 &= 154 \bmod 17 \\ &= (9 \cdot 17 + 1) \bmod 17 \\ &= 1 \end{aligned}$$

- Therefore 14 is the inverse of 11 modulo 17

Online example

- `https://youtu.be/mgvA3z-vOzc`

The Least Common Multiple (LCM)

Definition

- Let n and m be two positive integers and let ℓ be the smallest positive integer that is a multiple of both of them
- $\ell = \mathrm{lcm}(n, m)$ is the **Least Common Multiple** of n and m

Examples

- $15 = \mathrm{lcm}(5, 15)$
- $36 = \mathrm{lcm}(12, 18)$
- $273 = \mathrm{lcm}(13, 21)$

Bounds on $\ell = \mathrm{lcm}(n, m)$

- **Upper bound:** nm is a multiple of both n and m, therefore $\ell \leq nm$
- **Lower bound:** An integer cannot be a multiple of a larger integer, therefore $\ell \geq \max\{n, m\}$

The Smallest Multiple Algorithm

Algorithm

- Initially $h = n$ and $k = m$
- While $h \neq k$
  - While $h < k$ set $h = h + n$
  - While $k < h$ set $k = k + m$
- Return $\mathrm{lcm}(n, m) = h = k$

Proof outline

- Let $\ell = \mathrm{lcm}(n, m)$
- By definition, any multiple $h < \ell$ of n is different than any multiple $k < \ell$ of m
- Eventually, $h = \ell$ and $k = \ell$ and the algorithm returns ℓ

Examples

Example I

- **Input:** $n = 48$ and $m = 36$
- $h = 48, 96, 144$
- $k = 36, 72, 108, 144$
- **Output:** $\mathrm{lcm}(48, 36) = 144$

Example II

- **Input:** $n = 126$ and $m = 60$
- $h = 126, 252, 378, 504, 630, 756, 882, 1008, 1134, 1260$
- $k = 60, 120, 180, \ldots, 600, 660, \ldots, 1140, 1200, 1260$
- **Output:** $\mathrm{lcm}(126, 60) = 1260$

The Factorization Algorithm

Algorithm

- Let $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ be the prime factorization of n
- Let $m = q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$ be the prime factorization of m
- Let $L = \{\ell_1, \ell_2, \ldots, \ell_w\} = \{p_1, p_2, \ldots, p_r\} \cup \{q_1, q_2, \ldots, q_s\}$
- For all $1 \leq i \leq w$:
  - If $\ell_i = p_j$ for some $1 \leq j \leq r$, set $f_i = a_j$
  - If $\ell_i = q_k$ for some $1 \leq k \leq s$, set $f_i = b_k$
  - If $\ell_i = p_j = q_k$ for some $1 \leq j \leq r$ and $1 \leq k \leq s$, set $f_i = \max\{a_j, b_k\}$
- Then $\mathrm{lcm}(n, m) = \ell_1^{f_1} \ell_2^{f_2} \cdots \ell_w^{f_w}$

Proof outline

- Assume ℓ^f is a divisor of $\mathrm{lcm}(n, m)$ for a prime integer ℓ and $f \geq 1$
- If $\ell = p_j$ for some $1 \leq j \leq r$ then $f \geq a_j$
- If $\ell = q_k$ for some $1 \leq k \leq s$ then $f \geq b_k$
- Therefore, $\ell_1^{f_1} \ell_2^{f_2} \cdots \ell_w^{f_w}$ is the prime factorization of $\mathrm{lcm}(n, m)$

Examples

Example I

- **Input:** $n = 48$ and $m = 36$
- $48 = 2^4 \cdot 3^1$
- $36 = 2^2 \cdot 3^2$
- $L = \{2, 3\}$
- **Output:** $\mathrm{lcm}(48, 36) = 2^4 \cdot 3^2 = 16 \cdot 9 = 144$

Example II

- **Input:** $n = 126$ and $m = 60$
- $126 = 2^1 \cdot 3^2 \cdot 7^1$
- $60 = 2^2 \cdot 3^1 \cdot 5^1$
- $L = \{2, 3, 5, 7\}$
- **Output:** $\mathrm{lcm}(126, 60) = 2^2 \cdot 3^2 \cdot 5^1 \cdot 7^1 = 4 \cdot 9 \cdot 5 \cdot 7 = 1260$

The GCD and the LCM

Theorem

- $n \cdot m = \mathrm{gcd}(n, m) \cdot \mathrm{lcm}(n, m)$ for any positive integers n and m

Examples

$$
\begin{array}{rcrcrcll}
75 & = & 5 \cdot 15 & = & 5 \cdot 15 & = & \mathrm{gcd}(5, 15) & \cdot \mathrm{lcm}(5, 15) \\
216 & = & 12 \cdot 18 & = & 6 \cdot 36 & = & \mathrm{gcd}(12, 18) & \cdot \mathrm{lcm}(12, 18) \\
273 & = & 13 \cdot 21 & = & 1 \cdot 273 & = & \mathrm{gcd}(13, 21) & \cdot \mathrm{lcm}(13, 21) \\
7560 & = & 126 \cdot 60 & = & 6 \cdot 1260 & = & \mathrm{gcd}(126, 60) & \cdot \mathrm{lcm}(126, 60)
\end{array}
$$

The GCD and the LCM

Theorem

- $n \cdot m = \gcd(n, m) \cdot \operatorname{lcm}(n, m)$ for any positive integers n and m

A special case

- $\operatorname{lcm}(n, m) = n \cdot m$ for any relatively prime positive integers n and m because $\gcd(n, m) = 1$

The Euclidean algorithm to compute $\operatorname{lcm}(n, m)$

- Run the Euclidean algorithm to compute $\gcd(n, m)$
- Return $\operatorname{lcm}(n, m) = (n \cdot m) / \gcd(n, m)$

The GCD and the LCM

Theorem

- $n \cdot m = \gcd(n, m) \cdot \mathrm{lcm}(n, m)$ for any positive integers n and m

Proof idea

- Let N be the multi-set of the prime factors of n
- Let M be the multi-set of the prime factors of m
- Then $N \cap M$ is the multi-set of the prime factors of $\gcd(n, m)$
- Then $N \cup M$ is the multi-set of the prime factors of $\mathrm{lcm}(n, m)$
- **Principle of Inclusion Exclusion:** for two multi-sets N and M

$$|N| + |M| = |N \cap M| + |N \cup M|$$

The GCD and the LCM

Theorem

- $n \cdot m = \mathrm{gcd}(n, m) \cdot \mathrm{lcm}(n, m)$ for any positive integers n and m

Proof outline

- Every prime factor of the product $n \cdot m$ that is a prime factor of both n and m appears twice in the product of n and m, once in $\mathrm{gcd}(n, m)$ and once in $\mathrm{lcm}(n, m)$ and therefore it also appears twice in the product of $\mathrm{gcd}(n, m)$ and $\mathrm{lcm}(n, m)$
- Every prime factor of the product $n \cdot m$ that is a prime factor of only n or only m appears only once in the product of n and m, and since it is a prime factor of $\mathrm{lcm}(n, m)$ but it is not a prime factor of $\mathrm{gcd}(n, m)$, it also appears only once in the product of $\mathrm{gcd}(n, m)$ and $\mathrm{lcm}(n, m)$

GCD and LCM For More Than Two Integers

Definition

- Let $n_1, n_2, \ldots, n_k$ be k positive integers
- $\gcd(n_1, n_2, \ldots, n_k)$ is the largest positive integer that is a divisor of these k integers
- $\mathrm{lcm}(n_1, n_2, \ldots, n_k)$ is the smallest positive integer that is a multiple of these k integers

Computation

- $\gcd(n_1, n_2, \ldots, n_k) = \gcd(\ldots(\gcd(\gcd(n_1, n_2), n_3), \ldots, n_k)$
- $\mathrm{lcm}(n_1, n_2, \ldots, n_k) = \mathrm{lcm}(\ldots(\mathrm{lcm}(\mathrm{lcm}(n_1, n_2), n_3), \ldots, n_k)$

Recursive Computation

- $\gcd(n_1, n_2, \ldots, n_k) = \gcd(n_1, \gcd(n_2, n_3, \ldots, n_k))$
- $\mathrm{lcm}(n_1, n_2, \ldots, n_k) = \mathrm{lcm}(n_1, \mathrm{lcm}(n_2, n_3, \ldots, n_k))$

GCD and LCM For More Than Two Integers

Example

$$\begin{aligned}\gcd(36,60,90) &= \gcd(\gcd(36,60),90) = \gcd(12,90) = 6\\ &= \gcd(36,\gcd(60,90)) = \gcd(36,30) = 6\end{aligned}$$

$$\begin{aligned}\operatorname{lcm}(36,60,90) &= \operatorname{lcm}(\operatorname{lcm}(36,60),90) = \operatorname{lcm}(180,90) = 180\\ &= \operatorname{lcm}(36,\operatorname{lcm}(60,90)) = \operatorname{lcm}(36,180) = 180\end{aligned}$$

Remark

- It is not always true that
$$\gcd(n_1,n_2,\ldots,n_k)\cdot\operatorname{lcm}(n_1,n_2,\ldots,n_k) = n_1 n_2 \cdots n_k$$
- Example: $\gcd(36,60,90)\cdot\operatorname{lcm}(36,60,90) = 6\cdot 180 = 1080$
but $36\cdot 60\cdot 90 = 194400$

The Efficiency of the gcd and lcm Algorithms

The gcd algorithms

- The largest divisor and the common factors algorithms are not efficient: their **running times** depend on the values of n and m
- The Euclidean algorithm is very efficient: its **running time** depends on the values of $\log(n)$ and $\log(m)$
- This is an **exponential** improvement!

The lcm algorithms

- The smallest multiple and the factorization algorithms are not efficient: their **running times** depend on the values of n and m
- The Euclidean algorithm is very efficient: its **running time** depends on the values of $\log(n)$ and $\log(m)$
- This is an **exponential** improvement!

Solving Modular Equations

Problem

- Let $0 < d_1 < d_2 < \cdots < d_k$ be k integers and let $0 \le r < d_1$
- Find the smallest $n > r$ such that $\mathbf{n} \bmod \mathbf{d_i} = \mathbf{r}$ for all $1 \le i \le k$

Solution

- $n = \operatorname{lcm}(d_1, d_2, \ldots, d_k) + r$
- Trivial solution: $n = r$ without the constraint $n > r$
- All solutions: $q \cdot \operatorname{lcm}(d_1, d_2, \ldots, d_k) + r$ for any integer $q \ge 0$

Proof outline

- Suppose $m \bmod d_i = r$ for all $1 \le i \le k$
- Then d_i is a divisor of $m - r$ for all $1 \le i \le k$
- Therefore, $\operatorname{lcm}(d_1, d_2, \ldots, d_k)$ is a divisor of $m - r$
- As a result, $m = q \cdot \operatorname{lcm}(d_1, d_2, \ldots, d_k) + r$

Example

Equations

$$\begin{aligned} n \bmod 4 &= 2 \\ n \bmod 6 &= 2 \\ n \bmod 9 &= 2 \end{aligned}$$

Solution

- $\mathrm{lcm}(4, 6, 9) = 36$
- $n = \mathrm{lcm}(4, 6, 9) + 2 = 38$

Verification

- $38 = 9 \cdot 4 + 2 \implies (38 \bmod 4) = 2$
- $38 = 6 \cdot 6 + 2 \implies (38 \bmod 6) = 2$
- $38 = 4 \cdot 9 + 2 \implies (38 \bmod 9) = 2$

The Chinese Remainder Theorem

Theorem

- Let $d_1, d_2, \ldots, d_k$ be k pairwise relatively prime positive integers
  - $\gcd(d_i, d_j) = 1$ for all $1 \leq i \neq j \leq k$
- Let $0 \leq r_i < d_i$ for all $1 \leq i \leq k$
- There exists a unique positive integer $n < d_1 d_2 \cdots d_k$ such that $\mathbf{n} \bmod \mathbf{d_i} = \mathbf{r_i}$ for all $1 \leq i \leq k$

Example

- $n = 53$ is the only positive integer less than $105 = 3 \cdot 5 \cdot 7$ such that

$$
\begin{aligned}
n \bmod 3 &= 2 && (* \; 53 = 17 \cdot 3 + 2 \; *) \\
n \bmod 5 &= 3 && (* \; 53 = 10 \cdot 5 + 3 \; *) \\
n \bmod 7 &= 4 && (* \; 53 = 7 \cdot 7 + 4 \; *)
\end{aligned}
$$

Online example

- `https://youtu.be/ru7mWZJlRQg`

Fermat's Little Theorem

Theorem

- For any prime p that is not a divisor of an integer $n > 0$:

$$p \mid (n^{p-1} - 1) \qquad n^{p-1} \equiv 1 \pmod{p}$$

- For any prime p and any integer $n > 0$:

$$p \mid (n^p - n) \qquad n^p \equiv n \pmod{p}$$

Online resources

- Story: https://youtu.be/OoQ16YCYksw
- Examples and proof: https://youtu.be/w0ZQvZLx2KA

Examples

$p = 3$

$$\begin{array}{rcrcrcrcr}
n=4 & \Longrightarrow & 4^2-1 & = & 16-1 & = & 15 & = & 5\cdot 3 \\
n=5 & \Longrightarrow & 5^2-1 & = & 25-1 & = & 24 & = & 8\cdot 3 \\
n=6 & \Longrightarrow & 6^2-1 & = & 36-1 & = & 35 & = & 11\cdot 3+2 \\
n=6 & \Longrightarrow & 6^3-6 & = & 216-6 & = & 210 & = & 70\cdot 3
\end{array}$$

$p = 5$

$$\begin{array}{rcrcrcr}
3^4 \bmod 5 & = & 81 \bmod 5 & = & & = & 1 \\
7^4 \bmod 5 & = & (7 \bmod 5)^4 \bmod 5 & = & 2^4 \bmod 5 & = & 16 \bmod 5 = 1 \\
9^4 \bmod 5 & = & (9 \bmod 5)^4 \bmod 5 & = & (-1)^4 \bmod 5 & = & 1 \bmod 5 = 1 \\
10^4 \bmod 5 & = & 10000 \bmod 5 & = & 0 & \neq & 1
\end{array}$$

$p = 6$

$$\begin{array}{rcrcrcrcr}
3^5 \bmod 6 & = & 243 \bmod 6 & = & 3 & = & 3 & \neq & 1 \\
7^5 \bmod 6 & = & (7 \bmod 6)^5 \bmod 6 & = & 1^5 \bmod 6 & = & 1 \bmod 6 & = & 1 \\
11^5 \bmod 6 & = & (11 \bmod 6)^5 \bmod 6 & = & (-1)^5 \bmod 6 & = & -1 \bmod 6 & \neq & 1
\end{array}$$

Exponentiation Modulo Primes

Example I

$$
\begin{aligned}
11^{48} \bmod 17 &= 11^{16\cdot 3} \bmod 17 \\
&= (11^{16})^3 \bmod 17 \\
&= (11^{16} \bmod 17)^3 \bmod 17 \\
&= 1^3 \bmod 17 \\
&= 1
\end{aligned}
$$

Example II

$$
\begin{aligned}
57^{38} \bmod 13 &= (57 \bmod 13)^{38} \bmod 13 \\
&= 5^{38} \bmod 13 \\
&= 5^{3\cdot 12+2} \bmod 13 \\
&= ((5^{12} \bmod 13)^3 \cdot (5^2 \bmod 13)) \bmod 13 \\
&= (1^3 \cdot 12) \bmod 13 \\
&= 12
\end{aligned}
$$

Online examples

- https://youtu.be/oT7kRlh1nVQ

Euler's Totient Function

Definition

- For a positive integer n, the **Euler's totient function** $\varphi(n)$ is the number of positive integers smaller than n that are relatively prime to n
- $\varphi(n)$ is the number of integers k ($1 \leq k \leq n$) for which $\gcd(n, k) = 1$

Examples

- $\varphi(4) = 2$ because only $\{1, 3\}$ are relatively prime to 4
- $\varphi(6) = 2$ because only $\{1, 5\}$ are relatively prime to 6
- $\varphi(7) = 6$ because $\{1, 2, 3, 4, 5, 6\}$ are all relatively prime to 7
- $\varphi(8) = 4$ because only $\{1, 3, 5, 7\}$ are relatively prime to 8
- $\varphi(9) = 6$ because only $\{1, 2, 4, 5, 7, 8\}$ are relatively prime to 9

Euler's Totient Function

Proposition

- For any prime p

$$\varphi(p) = p - 1$$

Proof

- By definition, for a prime integer p, all the numbers $1, 2, \ldots, p - 1$ are relatively prime to p

Examples

- The 4 integers in the set $\{1, 2, 3, 4\}$ are relatively prime to 5 and $\varphi(5) = 5 - 1 = 4$
- The 6 integers in the set $\{1, 2, 3, 4, 5, 6\}$ are relatively prime to 7 and $\varphi(7) = 7 - 1 = 6$

Euler's Totient Function

Proposition

- For any positive integer k and a prime integer p

$$\varphi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right)$$

Example I

- The 6 integers $\{1, 2, 4, 5, 7, 8\}$ are relatively prime to 9
- $\varphi(9) = \varphi(3^2) = 3^2 - 3^1 = 9 - 3 = 9\left(1 - \frac{1}{3}\right) = 6$

Example II

- The 8 integers $\{1, 3, 5, 7, 9, 11, 13, 15\}$ are relatively prime to 16
- $\varphi(16) = \varphi(2^4) = 2^4 - 2^3 = 16 - 8 = 16\left(1 - \frac{1}{2}\right) = 8$

Euler's Totient Function

Proposition

- For any positive integer k and a prime integer p

$$\varphi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right)$$

The $k = 1$ special case

$$\varphi(p^1) = p^1 - p^0 = p - 1 = p \left(1 - \frac{1}{p}\right)$$

Proof outline

- Only multiples of p (including p^k) are not relatively prime to p^k
- There are $p^{k-1} = p^k/p$ positive multiples of p: $p, 2p, \ldots, p^{k-1}p$
- Therefore, $\varphi(p^k) = p^k - p^{k-1}$

Euler's Totient Function

Proposition

- For any relatively prime positive integers n and m,

$$\varphi(nm) = \varphi(n)\varphi(m)$$

Proof

- Based on the Chinese Remainder Theorem

Example

- $\{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\}$ are relatively prime to 36
- $\varphi(36) = \varphi(4 \cdot 9) = \varphi(4)\varphi(9) = 2 \cdot 6 = 12$
- $\varphi(36) = \varphi(6 \cdot 6) \neq \varphi(6)\varphi(6) = 2 \cdot 2 = 4$
- $\varphi(36) = \varphi(6^2) \neq 6^2 - 6^1 = 30$

Euler's Totient Function

Corollary

- For any two different primes p and q,

$$\varphi(pq) = (p-1)(q-1)$$

Proof

- Implied by the two propositions for the φ value of a prime integer and the φ value of a product

$$\varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1)$$

Example

- $\{1, 2, 4, 7, 8, 11, 13, 14\}$ are relatively prime to 15
- $\varphi(15) = \varphi(3 \cdot 5) = \varphi(3)\varphi(5) = (3-1)(5-1) = 2 \cdot 4 = 8$

Euler's Totient Function

Theorem

- For a positive integer n
$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$
where the product is over the distinct prime factors of n

Example

- The distinct prime factors of 36 are 2 and 3. Therefore
$$\varphi(36) = 36\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 36 \cdot \frac{1}{2} \cdot \frac{2}{3} = 12$$

Online resources

- `https://youtu.be/qa_hksAzpSg`
- `https://youtu.be/EcAT1XmHouk`

Euler's Totient Function

Proof

- Let $n = p_1^{k_1} p_2^{k_2} \cdots p_h^{k_h}$ be the prime factorization of n

$$\begin{aligned}
\varphi(n) &= \varphi(p_1^{k_1})\varphi(p_2^{k_2})\cdots\varphi(p_h^{k_h}) \\
&= p_1^{k_1}\left(1-\frac{1}{p_1}\right)p_2^{k_2}\left(1-\frac{1}{p_2}\right)\cdots p_h^{k_h}\left(1-\frac{1}{p_h}\right) \\
&= \left(p_1^{k_1}p_2^{k_2}\cdots p_h^{k_h}\right)\left(\left(1-\frac{1}{p_2}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_h}\right)\right) \\
&= n\prod_{i=1}^{h}\left(1-\frac{1}{p_i}\right) \\
&= n\prod_{p|n}\left(1-\frac{1}{p}\right)
\end{aligned}$$

Euler's Theorem

Theorem

- For any relatively prime positive integers n and m

$$m^{\varphi(n)} \equiv 1 \pmod{n}$$

The Fermat's Little Theorem special case

- If n is prime then $\varphi(n) = n - 1$
- By the Euler's Theorem

$$m^{\varphi(n)} = m^{n-1} \equiv 1 \pmod{n}$$

Examples

- $\varphi(8) = 4$ because only $\{1, 3, 5, 7\}$ are relatively prime to 8

$$\begin{aligned} 1^4 = 1 &= 0 \cdot 8 + 1 \\ 3^4 = 81 &= 10 \cdot 8 + 1 \\ 5^4 = 625 &= 78 \cdot 8 + 1 \\ 7^4 = 2401 &= 300 \cdot 8 + 1 \end{aligned}$$

- $\varphi(12) = 4$ because only $\{1, 5, 7, 11\}$ are relatively prime to 12

$$\begin{aligned} 1^4 = 1 &= 0 \cdot 12 + 1 \\ 5^4 = 625 &= 52 \cdot 12 + 1 \\ 7^4 = 2401 &= 200 \cdot 12 + 1 \\ 11^4 = 14641 &= 1220 \cdot 12 + 1 \end{aligned}$$

Computing $17^{802} \bmod 24$

Preprocessing

- $\gcd(17, 24) = 1$
- $\varphi(24) = \varphi(3 \cdot 2^3) = \varphi(3)\varphi(2^3) = 2(2^3 - 2^2) = 2 \cdot 4 = 8$
- Therefore, Euler's Theorem implies that $17^8 \bmod 24 = 1$

Computation

$$\begin{aligned}
17^{802} \bmod 24 &= \left(17^2 \cdot 17^{800}\right) \bmod 24 \\
&= \left(\left(17^2 \bmod 24\right) \cdot \left(\left(17^8\right)^{100} \bmod 24\right)\right) \bmod 24 \\
&= \left(\left(289 \bmod 24\right) \cdot \left(\left(17^8\right) \bmod 24\right)^{100}\right) \bmod 24 \\
&= \left(1 \cdot 1^{100}\right) \bmod 24 \\
&= 1
\end{aligned}$$

Online example (first 4 minutes)

- `https://youtu.be/FHkS3ydTM3M`

Journey into cryptography: Modern Cryptography

All videos

- https://www.khanacademy.org/computing/computer-science/cryptography#modern-crypt

List of videos

- Public key cryptography: What is it? https://youtu.be/MsqqpO9R5Hc
- The discrete logarithm problem: https://youtu.be/SL7J8hPKEWY
- Diffie-hellman key exchange: https://youtu.be/M-0qt6tdHzk
- RSA encryption: Step 1: https://youtu.be/EPXilYOa71c
- RSA encryption: Step 2: https://youtu.be/IY8BXNFgnyI
- RSA encryption: Step 3: https://youtu.be/cJvoi0LuutQ
- RSA encryption: Step 4: https://youtu.be/UjIPMJd6Xks

Additional Online Resources

More about Public Key Systems and RSA

- How Encryption Works: https://youtu.be/IBocnou79yI
- RSA Code: https://youtu.be/t5lACDDoQTk

Relevant topics

- Perfect numbers: https://youtu.be/teBtVMSVRPc
- Wilson's Theorem: https://youtu.be/VLFjOP7iFI0

Magic with Modular Arithmetic

- The Chinese Remainder Theorem and Cards
  https://youtu.be/l9dXo5f3zDc