Discrete Structures
Number Theory and Cryptography

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

List of videos

- What is cryptography? [https://youtu.be/Kf9KjCKmDcU](https://youtu.be/Kf9KjCKmDcU)
- The Caesar cipher: [https://youtu.be/sMOZf4GN3oc](https://youtu.be/sMOZf4GN3oc)
- Polyalphabetic cipher: [https://youtu.be/BgFJD7oCmDE](https://youtu.be/BgFJD7oCmDE)
- The one-time pad: [https://youtu.be/F1IG3TvQCBQ](https://youtu.be/F1IG3TvQCBQ)
- Frequency stability property: [https://youtu.be/vVXbgbMp0oY](https://youtu.be/vVXbgbMp0oY)
- The Enigma encryption machine: [https://youtu.be/-1ZFVwMXSXY](https://youtu.be/-1ZFVwMXSXY)
- Perfect secrecy: [https://youtu.be/vKRMWewGE9A](https://youtu.be/vKRMWewGE9A)
- Pseudorandom number generators: [https://youtu.be/GtOt7EBNEwQ](https://youtu.be/GtOt7EBNEwQ)
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 a prime or not but it is not a composite number.
- **Video:** https://youtu.be/9pgA-H77BLc

The Fundamental Theorem of Arithmetic

- Every integer greater than 1 is either a prime number itself or can be represented with a unique product of prime numbers.
- **Story:** https://youtu.be/8CluknrLeys
Primality Test and Factoring

Definitions

- A **primality test** is an algorithm for determining whether an input integer is prime
- **Integer factorization** is the decomposition of a composite integer into its unique product of primes

Hardness

- It is **relatively easy** to test if a very large number is prime
  - Almost surely with high probability
- It is **extremely difficult** to factor a very large number
  - Especially if the number is a product of 2 very large prime numbers
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
  - If no then continue
- If this step is reached then $n$ is a prime number

Improvement

- Set $s = \lfloor \sqrt{n} \rfloor$
- 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 would abort after checking if $d$ is a divisor of $n$
The Natural Primality Test

**Pseudocode**

Data: An integer $n \geq 2$

Result: $n$ is a prime or a composite number

$s := \lfloor \sqrt{n} \rfloor$; $d := 2$;

while $d \leq s$ do
  if $d$ is not a divisor of $n$ then
    $d := d + 1$;
  else
    abort;
  end
end

if $d > s$ then
  $n$ is a prime number;
else
  $n$ is a composite number;
end
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: $D = (d_1 \leq d_2 \leq \cdots \leq d_k)$
- **Output:** $n = d_1 d_2 \cdots d_k = p_1^{k_1} p_2^{k_2} \cdots p_h^{k_h}$
The Prime factors of 360

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

  - $2 \mid 360 \implies m = 180, d = 2, D = (2)$
  - $2 \mid 180 \implies m = 90, d = 2, D = (2, 2)$
  - $2 \mid 90 \implies m = 45, d = 2, D = (2, 2, 2)$
  - $2 \not\mid 45 \implies m = 45, d = 3, D = (2, 2, 2)$
  - $3 \mid 45 \implies m = 15, d = 3, D = (2, 2, 2, 3)$
  - $3 \mid 15 \implies m = 5, d = 3, D = (2, 2, 2, 3, 3)$
  - $3 \not\mid 5 \implies m = 5, d = 4, D = (2, 2, 2, 3, 3)$
  - $4 \not\mid 5 \implies m = 5, d = 5, D = (2, 2, 2, 3, 3)$
  - $5 \mid 5 \implies m = 1, d = 5, D = (2, 2, 2, 3, 3, 5)$

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

\[
\begin{align*}
\{2, 3, 4, 5, 6\} \not| 1001 & \implies m = 1001, d = 7, D = () \\
7 \mid 1001 & \implies m = 143, d = 7, D = (7) \\
\{7, 8, 9, 10\} \not| 143 & \implies m = 143, d = 11, D = (7) \\
11 \mid 143 & \implies m = 13, d = 11, D = (7, 11) \\
\{11, 12\} \not| 13 & \implies m = 13, d = 13, D = (7, 11) \\
13 \mid 13 & \implies m = 1, d = 13, D = (7, 11, 13)
\end{align*}
\]

- **Return:** \( 1001 = 7 \cdot 11 \cdot 13 \)
The Natural Integer Factorization Algorithm

Pseudocode

Data: An integer \( n \geq 2 \)
Result: The unique prime factorization of \( n \)

\[
d := 2; \quad m := n; \quad D := () \quad (* \text{an empty list} *)\;
\]

while \( m > 1 \) do
    if \( d \) is a divisor of \( m \) then
        \[
m := m/d; \\
        \text{Append } d \text{ to the end of the list } D;
        \]
    else
        \[
d := d + 1
        \]
    end
end

\[ D = (d_1, d_2, \ldots, d_k); \]

Return: \( n = d_1 d_1 \cdots d_k \)
Sieve of Eratosthenes

Algorithm: Find all the prime numbers that are smaller than $N$

- Initially: 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 a prime number
  - Mark all the $\left\lfloor \frac{N}{p} \right\rfloor - 1$ multiples of $p$ (except $p$) as non-prime numbers
  - Set $p$ to be the smallest remaining candidate
- Mark all the remaining candidates as prime numbers

Online resources

- [https://youtu.be/FBbHzy7v2Kg](https://youtu.be/FBbHzy7v2Kg)
- [https://youtu.be/V08g_lkJ6Q](https://youtu.be/V08g_lkJ6Q)
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 a prime, then a new prime is found
- Otherwise, $Q$ is a product of two or more primes.
  - The Fundamental Theorem of Arithmetic
- None of these primes can be $p_1, \ldots, p_n$
  - Because a number greater than 1 cannot divide both $Q$ and $Q - 1$
- Therefore, a new prime is found
- This process can continue to find infinitely many primes

Online resources
- The original proof by Euclid: https://youtu.be/dQmdHpvfyJs
- Another proof: https://youtu.be/fOXZgcAsrP8
Modular Arithmetic

Notations

\[ n = q \cdot d + r \quad (* 0 \leq r < d *) \]

\[ n \mod d = r \]

- \( n \): dividend; \( d \): divisor; \( q \): quotient; \( r \): remainder

Examples

- \( 7 \mod 3 = 1 \) because \( 7 = 2 \cdot 3 + 1 \)
- \( 25 \mod 5 = 0 \) because \( 25 = 5 \cdot 5 + 0 \)
- \( 101 \mod 7 = 3 \) because \( 101 = 14 \cdot 7 + 3 \)

Definitions

- If \( n \mod d = 0 \) then \( d \mid n \)
- \( d \) is a divisor of \( n \) and \( n \) is a multiple of \( d \)

The Lazy Mathematician

https://youtu.be/FdmApk9V2-w
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 \(q\)

- \(-18 \mod 7 = 3\) because \(-18 = -3 \cdot 7 + 3\)
- \(-55 \mod 5 = 0\) 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 \(d - r < r\)
- \(103 \mod 7 = 5 = -2\) since \(103 = 14 \cdot 7 + 5 = 15 \cdot 7 - 2\)
Congruence Modulo

Notation

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

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**:
  
  \[
  (n \equiv m \pmod{d}) \land (m \equiv k \pmod{d}) \implies n \equiv k \pmod{d}
  \]
  
  - $(52 \equiv 27 \pmod{5}) \land (27 \equiv 12 \pmod{5}) \implies 52 \equiv 12 \pmod{5}$

Proofs idea

- There exist $q_n, q_m, q_k$, and $0 \leq r < d$ such that
  
  \[
  n = q_n d + r; \quad m = q_m d + r; \quad \text{and } k = q_k d + r
  \]
**Basic Properties**

**Proposition**
- For integers $-\infty < n, k < \infty$ and positive integer $d > 1$:
  \[(n \mod d) = ((n + kd) \mod d) \implies n \equiv n + kd \pmod{d}\]

**Examples**
- \((7 \mod 5) = (12 \mod 5) = (112 \mod 5) = 2\)
  \[\implies 7 \equiv 12 \equiv 112 \pmod{5}\]
- \((-3 \mod 7) = (4 \mod 7) = (11 \mod 7) = 4\)
  \[\implies -3 \equiv 4 \equiv 11 \pmod{7}\]

**Proof outline**
- \(n = qd + r\)
- \(n + kd = (q + k)d + r\)
Basic Properties

Proposition

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

Examples

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

Proof Outline

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

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

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

Example

55 mod 5 = 0 because 55 = 11 \cdot 5 + 0

\[
\begin{align*}
55 \mod 5 & = (34 + 21) \mod 5 \\
& = ((34 \mod 5) + (21 \mod 5)) \mod 5 \\
& = (4 + 1) \mod 5 \\
& = 5 \mod 5 \\
& = 0
\end{align*}
\]
A Modular Addition Table for $d = 5$

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>
A Modular Addition Table for $d = 6$

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>
Modular Subtraction

Proposition

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

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

Example

$8 \mod 5 = 3$ because $8 = 1 \cdot 5 + 3$

$8 \mod 5 = (21 - 13) \mod 5$

$= ((21 \mod 5) - (13 \mod 5)) \mod 5$

$= (1 - 3) \mod 5$

$= -2 \mod 5$

$= 3$
A Modular Subtraction Table for $d = 5$

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>4</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
A Modular Subtraction Table for $d = 6$

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>5</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
Modular Multiplication

**Proposition**

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

\[
(n \cdot m) \mod d = ((n \mod d)(m \mod d)) \mod d
\]

**Example**

- \(132 \mod 7 = 6\) because \(132 = 18 \cdot 7 + 6\)

\[
132 \mod 7 = (12 \cdot 11) \mod 7 = ((12 \mod 7)(11 \mod 7)) \mod 7 = (5 \cdot 4) \mod 7 = 20 \mod 7 = 6
\]
A Modular Multiplication Table for $d = 5$

<table>
<thead>
<tr>
<th>×</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>1</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>
## A Modular Multiplication Table for $d = 6$

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>
Modular Inverse

**Definition**
- Let $0 < n < d$ be two relatively prime (coprime) integers
  - $\gcd(n, d) = 1$
- The **inverse** of $n$ modulo $d$ is an integer $0 < m < d$ such that
  - $(mn \mod d) = 1$
- If $(mn \mod d) = 1$ then
  - $(n^{-1} \mod d) = m$ and $(m^{-1} \mod d) = n$

**Symmetry**
- $n$ is the inverse of $m$ modulo $d$ iff $m$ is the inverse of $n$ modulo $d$
  - $m = n^{-1} \iff n = m^{-1}$
Modular Inverse

Examples

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

Propositions

- 1 is the inverse of itself modulo \(d\)
  \[
  (1 \cdot 1) \mod d = 1 \mod d = 1
  \]

- \(d - 1\) is the inverse of itself modulo \(d\) for any integer \(d > 1\)
  \[
  (d - 1)^2 \mod d = (d^2 - 2d + 1) \mod d = ((d - 2)d + 1) \mod d = (((((d - 2)d) \mod d) + (1 \mod d)) \mod d = (0 + 1) \mod d = 1 \mod d
  \]
Modular Division

**Proposition**
- For integers $-\infty < n, m < \infty$ relatively prime to a positive integer $d > 1$

\[
\frac{n}{m} \mod d = (n \cdot m^{-1}) \mod d = ((n \mod d)(m^{-1} \mod d)) \mod d
\]

**Example**
- $33 \mod 7 = 5$ because $33 = 4 \cdot 7 + 5$

\[
33 \mod 7 = (99/3) \mod 7 = ((99 \mod 7)(3^{-1} \mod 7)) \mod 7 = (1 \cdot 5) \mod 7 = 5 \mod 7 = 5
\]
### A Modular Division Table for $d = 5$

<table>
<thead>
<tr>
<th>$\div$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$\perp$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>$\perp$</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>$\perp$</td>
<td>2</td>
<td>1</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>$\perp$</td>
<td>3</td>
<td>4</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>$\perp$</td>
<td>4</td>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
</tbody>
</table>
A Modular Division Table for $d = 6$

<table>
<thead>
<tr>
<th>$\div$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>${0, 3}$</td>
<td>${0, 2, 4}$</td>
<td>${0, 3}$</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>${}$</td>
<td>1</td>
<td>${}$</td>
<td>${}$</td>
<td>${}$</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>${}$</td>
<td>2</td>
<td>${1, 4}$</td>
<td>${}$</td>
<td>${2, 5}$</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>${}$</td>
<td>3</td>
<td>${}$</td>
<td>${1, 3, 5}$</td>
<td>${}$</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>${}$</td>
<td>4</td>
<td>${2, 5}$</td>
<td>${}$</td>
<td>${1, 4}$</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>${}$</td>
<td>5</td>
<td>${}$</td>
<td>${}$</td>
<td>${0, 3}$</td>
<td>1</td>
</tr>
</tbody>
</table>
Modular Exponentiation

Proposition

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

\[ n^k \mod d = ((n \mod d)^k) \mod d \]

Example

729 mod 7 = 1 because 729 = 104 \cdot 7 + 1

\[
729 \mod 7 = (9^3) \mod 7 \\
= ((9 \mod 7)^3) \mod 7 \\
= 2^3 \mod 7 \\
= 8 \mod 7 \\
= 1
\]
Another Example

100000 mod 7 = 5 because 100000 = 14285 \cdot 7 + 5

100000 mod 7

= 10^5 mod 7

= (10 mod 7)^5 mod 7

= 3^5 mod 7

= ((9 mod 7) \cdot (9 mod 7) \cdot (3 mod 7)) mod 7

= (2^2 \cdot 3) mod 7

= 12 mod 7

= 5
A Modular Exponentiation Table for $d = 5$

<table>
<thead>
<tr>
<th>exp</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>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<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>2</td>
<td>4</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>3</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>4</td>
</tr>
</tbody>
</table>
A Modular Exponentiation Table for $d = 6$

<table>
<thead>
<tr>
<th>exp</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<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>2</td>
<td>4</td>
<td>2</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>5</td>
<td>1</td>
<td>5</td>
<td>1</td>
<td>5</td>
</tr>
</tbody>
</table>
Computing $2^{57} \mod 7$ – Method I

**Preprocessing**

\[
\begin{align*}
2^1 \mod 7 & = 2 \\
2^2 \mod 7 & = (2^1)^2 \mod 7 = 2^2 \mod 7 = 4 \\
2^4 \mod 7 & = (2^2)^2 \mod 7 = 4^2 \mod 7 = 2 \\
2^8 \mod 7 & = (2^4)^2 \mod 7 = 2^2 \mod 7 = 4 \\
2^{16} \mod 7 & = (2^8)^2 \mod 7 = 4^2 \mod 7 = 2 \\
2^{32} \mod 7 & = (2^{16})^2 \mod 7 = 2^2 \mod 7 = 4
\end{align*}
\]

**Computation**

\[
\begin{align*}
2^{57} \mod 7 & = (2^{32}2^{16}2^82^1) \mod 7 \\
& = (4 \cdot 2 \cdot 4 \cdot 2) \mod 7 \\
& = 64 \mod 7 \\
& = 1
\end{align*}
\]
Computing $2^{57} \mod 7$ – Method II

**Preprocessing**

\[
(2^3 \mod 7) = (8 \mod 7) = 1
\]
\[
(2^6 \mod 7) = (64 \mod 7) = 1
\]

**Computation**

\[
2^{57} \mod 7 = 2^{6 \cdot 9 + 3} \mod 7
\]
\[
= \left( \left( 2^6 \right)^9 \cdot 2^3 \right) \mod 7
\]
\[
= \left( \left( \left( 64 \mod 7 \right)^9 \mod 7 \right) \cdot 8 \mod 7 \right) \mod 7
\]
\[
= \left( \left( 1^9 \mod 7 \right) \cdot 1 \right) \mod 7
\]
\[
= 1 \mod 7
\]
\[
= 1
\]
Computing $3^{101} \mod 5$ – Method II

Preprocessing

$$(3^2 \mod 5) = (9 \mod 5) = -1$$
$$(3^4 \mod 5) = (81 \mod 5) = 1$$

First computation

$$3^{101} \mod 5 = 3^{2 \cdot 50 + 1} \mod 5$$
$$= ((3^2)^{50} \cdot 3) \mod 5$$
$$= ((-1)^{50} \cdot 3) \mod 5$$
$$= (1 \cdot 3) \mod 5 = 3$$

Second computation

$$3^{101} \mod 5 = 3^{4 \cdot 25 + 1} \mod 5$$
$$= ((3^4)^{25} \cdot 3) \mod 5$$
$$= ((1)^{25} \cdot 3) \mod 5$$
$$= (1 \cdot 3) \mod 5 = 3$$
Online Resources

- Modular arithmetic:
  https://youtu.be/2zEXtoQDpXY

- Modular exponentiation: first two examples
  https://youtu.be/tTuWmcikE0Q
The Greatest Common Divisor (GCD)

Definition
- Let \( n \) and \( m \) be two positive integers and let \( g \) be the greatest 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
- **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 \( r \geq 2 \) 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 \( s \geq 2 \) 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 that \( g^h \) is a divisor of \( \gcd(n, m) \) for a prime \( g \) 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:** \( \gcd(372, 138) = 2^1 \cdot 3^1 = 6 \)

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:** \( \gcd(480, 360) = 2^3 \cdot 3^1 \cdot 5^1 = 120 \)
The Euclidean Algorithm

Idea and proof outline

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

Algorithm

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

An online example

- [https://youtu.be/klTlrnovoEE](https://youtu.be/klTlrnovoEE)
Example

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

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$n$</td>
<td>$m$</td>
</tr>
<tr>
<td>372</td>
<td>138</td>
</tr>
<tr>
<td>138</td>
<td>96</td>
</tr>
<tr>
<td>96</td>
<td>42</td>
</tr>
<tr>
<td>42</td>
<td>12</td>
</tr>
<tr>
<td>12</td>
<td>6</td>
</tr>
</tbody>
</table>

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

- **Input:** \( n = 21 \) and \( m = 13 \)

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>( n )</td>
<td>( m )</td>
</tr>
<tr>
<td>21</td>
<td>13</td>
</tr>
<tr>
<td>13</td>
<td>8</td>
</tr>
<tr>
<td>8</td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

- **Output:** \( \text{gcd}(21, 13) = 1 \)
The Extended Euclidean Algorithm

Bézout’s identity
- Let \( g = \gcd(n, m) \) for two positive integers \( n \) and \( m \)
- There exist integers \( x \) 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
Example

\textbf{Compute} \ 6 = \gcd(372, \ 138)

\begin{align*}
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{align*}

\textbf{Compute} \ 6 = -10 \cdot 372 + 27 \cdot 138

\begin{align*}
6 &= 42 - 3(96 - 2 \cdot 42) \\
&= -3 \cdot 96 + 7(138 - 96) \\
&= 7 \cdot 138 - 10(372 - 2 \cdot 138)
\end{align*}

\begin{align*}
&= 1 \cdot 42 - 3 \cdot 12 \\
&= -3 \cdot 96 + 7 \cdot 42 \\
&= 7 \cdot 138 - 10 \cdot 96 \\
&= -10 \cdot 372 + 27 \cdot 138
\end{align*}
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 \( (mn \mod d) = 1 \)
- Set \( m = x \) in the above \( xn + yd = 1 \) Bézout’s identity
- Therefore, \( mn + yd = 1 \)

\[
mn = 1 - yd
\]

\[
(mn \mod d) = (1 \mod d) - (yd \mod d) = 1
\]

\( m = n^{-1} \) is the inverse of \( n \) modulo \( d \)
Example

Find the inverse of 11 modulo 17

- Using the extended Euclidean algorithm find

  \[ 14 \cdot 11 - 9 \cdot 17 = 1 \]

- Equivalently,

  \[ (14 \cdot 11) \mod 17 = 154 \mod 17 = (9 \cdot 17 + 1) \mod 17 = 1 \]

Therefore 14 is the inverse of 11 modulo 17

Online example

- [https://youtu.be/mgvA3z-vOzc](https://youtu.be/mgvA3z-vOzc)
The Least Common Multiple (LCM)

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

**Examples**
- \( 15 = \text{lcm}(5, 15) \)
- \( 36 = \text{lcm}(12, 18) \)
- \( 273 = \text{lcm}(13, 21) \)

**Bounds**
- **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 $\text{lcm}(n, m) = h = k$

**Proof outline**
- Let $\ell = \text{lcm}(n, m)$
- 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 $\ell$
Examples

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

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:** $\text{lcm}(126, 60) = 1260$
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 \( \text{lcm}(n, m) = \ell_1^{f_1} \ell_2^{f_2} \cdots \ell_w^{f_w} \)

Proof outline

Assume that \( \ell^f \) is a divisor of \( \text{lcm}(n, m) \) for a prime \( \ell \) 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 \( \text{lcm}(n, m) \)
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:** $\text{lcm}(48, 36) = 2^4 \cdot 3^2 = 16 \cdot 9 = 144$

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:** $\text{lcm}(126, 60) = 2^2 \cdot 3^2 \cdot 5^1 \cdot 7^1 = 4 \cdot 9 \cdot 5 \cdot 7 = 1260$
The GCD and the LCM

Theorem

\[ n \cdot m = \gcd(n, m) \cdot \lcm(n, m) \] for any positive integers \( n \) and \( m \)

A special case

\[ \lcm(n, m) = n \cdot m \] for any relatively prime positive integers \( n \) and \( m \)

Examples

\[ 75 = 5 \cdot 15 = \gcd(5, 15) \cdot \lcm(5, 15) \]
\[ 216 = 12 \cdot 18 = 6 \cdot 36 = \gcd(12, 18) \cdot \lcm(12, 18) \]
\[ 273 = 13 \cdot 21 = 1 \cdot 273 = \gcd(13, 21) \cdot \lcm(13, 21) \]

The Euclidean algorithm to compute \( \lcm(n, m) \)

- Run the Euclidean algorithm to compute \( \gcd(n, m) \)
- Return \( \lcm(n, m) = (n \cdot m) / \gcd(n, m) \)
Proof Idea and Outline

Proof idea

- \(|N| + |M| = |N \cap M| + |N \cup M|\) for two sets \(N\) and \(M\):
  - \(N\) is the multi-set of the prime factors of \(n\)
  - \(M\) is the multi-set of the prime factors of \(m\)
  - \(N \cap M\) is the multi-set of the prime factors of \(\gcd(n, m)\)
  - \(N \cup M\) is the multi-set of the prime factors of \(\text{lcm}(n, m)\)

Proof outline

- Every prime factor of the product \(n \cdot m\) that is a prime factor of both \(n\) and \(m\) is a prime factor of both \(\gcd(n, m)\) and \(\text{lcm}(n, m)\)
- Every prime factor of the product that is a prime factor of only \(n\) or only \(m\) is a prime factor of \(\text{lcm}(n, m)\) but is not a prime factor of \(\gcd(n, m)\)
GCD and LCM For More Than Two Integers

Recursive Computation

Let $n_1, n_2, \ldots, n_k$ be $k$ positive integers

\[
\gcd(n_1, n_2, \ldots, n_k) = \gcd(n_1, \gcd(n_2, n_3, \ldots, n_k))
\]

\[
\lcm(n_1, n_2, \ldots, n_k) = \lcm(n_1, \lcm(n_2, n_3, \ldots, n_k))
\]

Example

\[
\gcd(36, 60, 90) = \gcd(36, \gcd(60, 90)) = \gcd(36, 30) = 6
\]

\[
\lcm(36, 60, 90) = \lcm(36, \lcm(60, 90)) = \lcm(36, 180) = 180
\]

Remark

It is not always true that

\[
\gcd(n_1, n_2, \ldots, n_k) \cdot \lcm(n_1, n_2, \ldots, n_k) = n_1 n_2 \cdots n_k
\]

Example: $\gcd(36, 60, 90) \cdot \lcm(36, 60, 90) = 6 \cdot 180 = 1080$

but $36 \cdot 60 \cdot 90 = 194400$
The Efficiency of the gcd and lcm Algorithms

The gcd algorithm
- 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 algorithm
- 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 $0 \leq r < d_1$
- Find the smallest $n > r$ such that $n \mod d_i = r$ for all $1 \leq i \leq k$

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

**Proof outline**
- Suppose $m \mod d_i = r$ for all $1 \leq i \leq k$
- Then $d_i$ is a divisor of $m - r$ for all $1 \leq i \leq k$
- Therefore, $\text{lcm}(d_1, d_2, \ldots, d_k)$ is a divisor of $m - r$
- As a result, $m = q \cdot \text{lcm}(d_1, d_2, \ldots, d_k) + r$
Example

Equations

\[ n \mod 4 = 2 \]
\[ n \mod 6 = 2 \]
\[ n \mod 9 = 2 \]

Solution

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

Verification

- \( 38 = 9 \cdot 4 + 2 \implies (38 \mod 4) = 2 \)
- \( 38 = 6 \cdot 6 + 2 \implies (38 \mod 6) = 2 \)
- \( 38 = 4 \cdot 9 + 2 \implies (38 \mod 9) = 2 \)
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 $n \mod d_i = r_i$ 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
  
  $n \mod 3 = 2$
  
  $n \mod 5 = 3$
  
  $n \mod 7 = 4$

**An online example**

https://youtu.be/ru7mWZJlRQg
Fermat’s Little Theorem

**Theorem**

- For any prime \( p \) that is not a divisor of an integer \( n > 0 \):
  \[
  p \mid (n^{p-1} - 1) \quad n^{p-1} \equiv 1 \pmod{p}
  \]
- For any prime \( p \) and any integer \( n > 0 \):
  \[
  p \mid (n^p - n) \quad n^p \equiv n \pmod{p}
  \]

**Examples**

- \( p = 5 \) and \( n = 3 \) \( \implies \) \( 3^4 - 1 = 81 - 1 = 80 = 16 \cdot 5 \)
- \( p = 3 \) and \( n = 5 \) \( \implies \) \( 5^2 - 1 = 25 - 1 = 24 = 8 \cdot 3 \)
- \( p = 3 \) and \( n = 6 \) \( \implies \) \( 6^2 - 1 = 36 - 1 = 35 = 11 \cdot 3 + 2 \)
- \( p = 3 \) and \( n = 6 \) \( \implies \) \( 6^3 - 6 = 216 - 6 = 210 = 70 \cdot 3 \)

**Story**

- [https://youtu.be/OoQ16YCYksw](https://youtu.be/OoQ16YCYksw)
More Examples

$p = 5$

- $3^4 \mod 5 = 81 \mod 5 = 1$
- $7^4 \mod 5 = (7 \mod 5)^4 \mod 5 = 2^4 \mod 5 = 16 \mod 5 = 1$
- $9^4 \mod 5 = (9 \mod 5)^4 \mod 5 = (-1)^4 \mod 5 = 1 \mod 5 = 1$
- $10^4 \mod 5 = 10000 \mod 5 = 0 \neq 1$

$p = 6$

- $3^5 \mod 6 = 243 \mod 6 = 3 \neq 1$
- $7^5 \mod 6 = (7 \mod 6)^5 \mod 6 = 1^5 \mod 6 = 1 \mod 6 = 1$
- $11^5 \mod 6 = (11 \mod 6)^5 \mod 6 = (-1)^5 \mod 6 = -1 \mod 6 \neq 1$

$p = 9$

- $11^8 \mod 9 = (11 \mod 9)^8 \mod 9 = 2^8 \mod 9 = 256 \mod 9 = 4 \neq 1$
Exponentiation Modulo Primes

**Example I**

\[ 11^{48} \mod 17 = (11^{16})^3 \mod 17 = (11^{16} \mod 17)^3 \mod 17 = 1^3 \mod 17 = 1 \]

**Example II**

\[ 57^{38} \mod 13 = (57 \mod 13)^{38} \mod 13 = 5^{3\cdot 12+2} \mod 13 = ((5^{12} \mod 13)^3 \cdot (5^2 \mod 13)) \mod 13 = (1^3 \cdot 12) \mod 13 = 12 \]

An online resource

[https://youtu.be/oT7kRlh1nVQ](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 $p$, 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 $p$

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

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, $\varphi(p^k) = p^k - p^{k-1}$

Example
- $\{1, 3, 5, 7, 9, 11, 13, 15\}$ are relatively prime to 16
- $\varphi(16) = \varphi(2^4) = 2^4 - 2^3 = 16 - 8 = 8$
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
- \( \varphi(36) = \varphi(4 \cdot 9) = \varphi(4)\varphi(9) = 2 \cdot 6 = 12 \)
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 $\varphi$ value of a prime and the $\varphi$ 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/qa_hksAzpSg)
- [https://youtu.be/EcAT1XmHouk](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 \( n \)

\[
\varphi(n) = \varphi(p_1^{k_1}) \varphi(p_2^{k_2}) \cdots \varphi(p_h^{k_h}) \\
= p_1^{k_1} \left( 1 - \frac{1}{p_1} \right) p_2^{k_2} \left( 1 - \frac{1}{p_2} \right) \cdots p_h^{k_h} \left( 1 - \frac{1}{p_h} \right) \\
= (p_1^{k_1} p_2^{k_2} \cdots p_h^{k_h}) \left( \left( 1 - \frac{1}{p_2} \right) \left( 1 - \frac{1}{p_2} \right) \cdots \left( 1 - \frac{1}{p_h} \right) \right) \\
= n \prod_{i=1}^{h} \left( 1 - \frac{1}{p_i} \right) \\
= n \prod_{p | n} \left( 1 - \frac{1}{p} \right)
\]
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

- Let \( n \) be a prime number and therefore \( \varphi(n) = n - 1 \)
- 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

\[
\begin{align*}
1^4 &= 1 &= 0 \cdot 8 + 1 \\
3^4 &= 81 &= 10 \cdot 8 + 1 \\
5^4 &= 625 &= 78 \cdot 8 + 1 \\
7^4 &= 2401 &= 300 \cdot 8 + 1
\end{align*}
\]

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

\[
\begin{align*}
1^4 &= 1 &= 0 \cdot 12 + 1 \\
5^4 &= 625 &= 52 \cdot 12 + 1 \\
7^4 &= 2401 &= 200 \cdot 12 + 1 \\
11^4 &= 14641 &= 1220 \cdot 12 + 1
\end{align*}
\]
Computing $17^{802} \mod 24$

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 $17^8 \mod 24 = 1$

Computation

\[
17^{802} \mod 24 = (17^2 \cdot 17^{800}) \mod 24 \\
= ((17^2 \mod 24) \cdot ((17^8)^{100} \mod 24)) \mod 24 \\
= ((289 \mod 24) \cdot ((17^8) \mod 24)^{100}) \mod 24 \\
= (1 \cdot 1^{100}) \mod 24 \\
= 1
\]

An online resource
- [https://youtu.be/FHkS3ydTM3M](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/Msqqp09R5Hc
- 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
More about Public Key Systems and RSA

How Encryption Works

https://youtu.be/IBocnou79yI

RSA Code

https://youtu.be/t5lACDDoQTk
Magic with Modular Arithmetic

Chinese Remainder Theorem and Cards

https://www.youtube.com/watch?v=l9dXo5f3zDc