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/F1IG3TvQCBQ
- 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 a prime or not but it is not a composite number.

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](https://youtu.be/8CluknrLeys)
Primality Test and Factoring

**Tasks**

- **Primality test:** determine whether an input integer is a prime number or a composite number
- **Integer factorization:** decompose an input 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** because $n$ is not a prime number
  - 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 will **abort** after checking if $d$ is a divisor of $n$
Example

Check if $n = 77$ is prime

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

  \[ 2 \nmid 77 \implies d = 3 \]
  \[ 3 \nmid 77 \implies d = 4 \]
  \[ 4 \nmid 77 \implies d = 5 \]
  \[ 5 \nmid 77 \implies d = 6 \]
  \[ 6 \nmid 77 \implies d = 7 \]
  \[ 7 \mid 77 \implies \text{ABORT} \]

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

Check if $n = 97$ is prime

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

  - $2 \not| 97 \implies d = 3$
  - $3 \not| 97 \implies d = 4$
  - $4 \not| 97 \implies d = 5$
  - $5 \not| 97 \implies d = 6$
  - $6 \not| 97 \implies d = 7$
  - $7 \not| 97 \implies d = 8$
  - $8 \not| 97 \implies d = 9$
  - $9 \not| 97 \implies d = 10$

- **Return**: 93 is a prime number
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:** \( n = d_1 d_2 \cdots d_j = p_1^{k_1} p_2^{k_2} \cdots p_h^{k_h} \)
The Prime factors of 360

Initially: \( m = 360, \ d = 2, \) and \( D = () \)

\[
\begin{align*}
2 & \mid 360 \implies m = 180 \quad d = 2 \quad D = (2) \\
2 & \mid 180 \implies m = 90 \quad d = 2 \quad D = (2, 2) \\
2 & \mid 90 \implies m = 45 \quad d = 2 \quad D = (2, 2, 2) \\
2 & \nmid 45 \implies m = 45 \quad d = 3 \quad D = (2, 2, 2) \\
3 & \mid 45 \implies m = 15 \quad d = 3 \quad D = (2, 2, 2, 3) \\
3 & \nmid 15 \implies m = 5 \quad d = 3 \quad D = (2, 2, 2, 3, 3) \\
3 & \nmid 5 \implies m = 5 \quad d = 4 \quad D = (2, 2, 2, 3, 3) \\
4 & \nmid 5 \implies m = 5 \quad d = 5 \quad D = (2, 2, 2, 3, 3) \\
5 & \mid 5 \implies m = 1 \quad d = 5 \quad D = (2, 2, 2, 3, 3, 5)
\end{align*}
\]

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:** \( m = 1001, \ d = 2, \ D = () \)
  - \( \{2, 3, 4, 5, 6\} \not|\ 1001 \implies m = 1001 \quad d = 7 \quad D = () \)
  - 7 \mid 1001 \implies m = 143 \quad d = 7 \quad D = (7) \)
  - \( \{7, 8, 9, 10\} \not|\ 143 \implies m = 143 \quad d = 11 \quad D = (7) \)
  - 11 \mid 143 \implies m = 13 \quad d = 11 \quad D = (7, 11) \)
  - \( \{11, 12\} \not|\ 13 \implies m = 13 \quad d = 13 \quad D = (7, 11) \)
  - 13 \mid 13 \implies m = 1 \quad d = 13 \quad D = (7, 11, 13) \)

- **Return:** \( 1001 = 7 \cdot 11 \cdot 13 \)
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://www.youtube.com/watch?v=dhfhu9Q5g8U](https://www.youtube.com/watch?v=dhfhu9Q5g8U)
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 due to The Fundamental Theorem of Arithmetic
- 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, 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
- \( \approx \frac{n}{\log(n)} \) prime numbers are smaller than \( n \): https://youtu.be/EKfdRks8oMI
Modular Arithmetic

Notations

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

\[ n \mod d = r \]

- \( n \): \textit{dividend}; \( d \): \textit{divisor}; \( q \): \textit{quotient}; \( r \): \textit{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 \( 101 = 14 \cdot 7 + 3 \)
- \( 17 \mod 12 = 5 \) because \( 17 = 1 \cdot 12 + 5 \)

Definitions

- If \( n \mod d = 0 \) then \( d \mid n \)
- \( d \) \textit{divides} \( n \) and is a \textit{divisor} of \( n \) while \( n \) is a \textit{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 \(q\)

- \(-18 \mod 7 = 3\) 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
  \[ n = (q + 1) \cdot d - (d - r) \text{ for } 0 \leq d - r < d \]
  - 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 $d > 1$:

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

Proofs idea

There exist $q_n, q_m, q_k$, and $0 \leq r < d$ such that

$n = q_n d + r; m = q_m d + r; \text{and } k = q_k d + r$
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 $d > 1$:

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

**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**

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

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: compute $(34 + 21) \mod 5$

- **Direct method:**
  
  $$(34 + 21 = 55) \land (55 = 11 \cdot 5 + 0) \Rightarrow (34 + 21) \mod 5 = 0$$

- **Modular addition method:**

  $$(34 + 21) \mod 5 = ((34 \mod 5) + (21 \mod 5)) \mod 5$$
  
  $$= (4 + 1) \mod 5$$
  
  $$= 5 \mod 5$$
  
  $$= 0$$
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: compute $(21 - 13) \mod 5$

- **Direct method:**
  $$(21 - 13 = 8) \land (8 = 1 \cdot 5 + 3) \Rightarrow (21 - 13) \mod 5 = 3$$

- **Modular subtraction method:**
  $$(21 - 13) \mod 5 = ((21 \mod 5) - (13 \mod 5)) \mod 5$$
  $$= (1 - 3) \mod 5$$
  $$= -2 \mod 5$$
  $$= 3$$
## 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: compute $(12 \cdot 11) \mod 7$

- Direct method:

  $$(12 \cdot 11 = 132) \land (132 = 18 \cdot 7 + 6) \Rightarrow (12 \cdot 11) \mod 7 = 6$$

- Modular multiplication method:

  $$(12 \cdot 11) \mod 7 = ((12 \mod 7)(11 \mod 7)) \mod 7$$
  $$= (5 \cdot 4) \mod 7$$
  $$= 20 \mod 7$$
  $$= 6$$
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>$\times$</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
  - There is no integer greater than 2 that is a divisor of both $n$ and $d$
- The inverse of $n$ modulo $d$ is an integer $0 < m < d$ such that
  - $(mn \mod d) = 1$

**Symmetry**
- If $(mn \mod d) = 1$ then $(nm \mod d) = 1$ and therefore $n$ is the inverse of $m$ modulo $d$ iff $m$ is the inverse of $n$ modulo $d$
  - $(n^{-1} \mod d) = m \iff (m^{-1} \mod d) = n$
  - $m = n^{-1} \iff n = m^{-1}$
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 two integers \(-\infty < n, m < \infty\) in which \(m\) is 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: compute\((99/3) \mod 7\)**

- **Direct method:**
  
  \[
  (99/3 = 33) \land (33 = 4 \cdot 7 + 5) \Rightarrow (99/3) \mod 7 = 5
  \]

- **Modular division method:**

  \[
  (99/3) \mod 7 = ((99 \mod 7)(3^{-1} \mod 7)) \mod 7 \\
  = (1 \cdot 5) \mod 7 \\
  = 5 \mod 7 \\
  = 5
  \]
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>⊥</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>⊥</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>⊥</td>
<td>2</td>
<td>1</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>⊥</td>
<td>3</td>
<td>4</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>⊥</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>
Proposition

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

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

Example: compute $9^3 \mod 7$

- **Direct method:**

  $$(9^3 = 729) \land (729 = 104 \cdot 7 + 1) \Rightarrow 9^3 \mod 7 = 1$$

- **Modular exponentiation method:**

  $$(9^3) \mod 7 = ((9 \mod 7)^3) \mod 7$$

  $= 2^3 \mod 7$

  $= 8 \mod 7$

  $= 1$$
Modular Exponentiation

Example: compute $10^5 \mod 7$

- **Direct method:**
  \[
  (10^5 = 100000) \land (100000 = 14285 \cdot 7 + 5) \implies 10^5 \mod 7 = 5
  \]

- **Modular exponentiation method:**
  
  
  \[
  10^5 \mod 7 = (10 \mod 7)^5 \mod 7
  \]
  
  \[
  = 3^5 \mod 7
  \]
  
  \[
  = ((9 \mod 7) \cdot (9 \mod 7) \cdot (3 \mod 7)) \mod 7
  \]
  
  \[
  = (2^2 \cdot 3) \mod 7
  \]
  
  \[
  = 12 \mod 7
  \]
  
  \[
  = 5
  \]
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 \( n^k \mod d \) for \( n < d \) and large \( k \)

Method I: Outline

- Since \( n < d \), it follows that \( n \mod d = n \); therefore, \( n^{2^0} \mod d = n \)
- Observe that \( n^{2^{i+1}} = n^{2^i \cdot 2} = (n^{2^i})^2 \)
- Iteratively compute
  \[
  \begin{align*}
  n^2 &= n^{2^1} \mod d \\
  n^4 &= n^{2^2} \mod d \\
  n^8 &= n^{2^3} \mod d \\
  n^{16} &= n^{2^4} \mod d
  \end{align*}
  \]
- 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 \( n^k = n^{2^{i_1}} + n^{2^{i_2}} + \cdots + n^{2^{i_h}} = n^{2^{i_1}} \cdot n^{2^{i_2}} \cdot \cdots \cdot n^{2^{i_h}} \)
- \( n^k \mod d \) can be computed using modular multiplication among the already computed values of \( n^{2^i} \mod d \)
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: $57 = 32 + 16 + 8 + 1$

\[
\begin{align*}
2^{57} \mod 7 & = (2^{32}2^{16}2^82^1) \mod 7 \\
& = (((2^{32} \mod 7)(2^{16} \mod 7)(2^8 \mod 7)(2^1 \mod 7)) \mod 7 \\
& = (4 \cdot 2 \cdot 4 \cdot 2) \mod 7 \\
& = 64 \mod 7 \\
& = 1
\end{align*}
\]
Computing $3^{101} \mod 5$ – Method I

**Preprocessing**

$$
egin{align*}
3^1 \mod 5 &= 3 \\
3^2 \mod 5 &= (3^1)^2 \mod 5 = 3^2 \mod 5 = 4 \\
3^4 \mod 5 &= (3^2)^2 \mod 5 = 4^2 \mod 5 = 1 \\
3^8 \mod 5 &= (3^4)^2 \mod 5 = 1^2 \mod 5 = 1 \\
3^{16} \mod 5 &= 3^{32} \mod 5 = 3^{64} \mod 5 = 1
\end{align*}
$$

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

$$
egin{align*}
3^{101} \mod 5 &= (3^{64}3^{32}3^43^1) \mod 5 \\
&= ((3^{64} \mod 5)(3^{32} \mod 5)(3^4 \mod 5)(3^1 \mod 5)) \mod 5 \\
&= (1 \cdot 1 \cdot 1 \cdot 3) \mod 5 \\
&= 3 \mod 5 \\
&= 3
\end{align*}
$$
Computing $n^k \mod d$ for $n < d$ and large $k$

**Method II: Outline**

- Express $k$ as $k = a\ell + b$ such that $n^\ell \mod d$ is 1 or −1 and $n^b \mod d$ 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 $n^\ell$ and then $(n^\ell)^a$ with 1 and −1.
- The final answer will be $(n^b \mod d)$ or $-(n^b \mod d)$. 
Computing $2^{57} \mod 7$ – Method II

Preprocessing

$(2^3 \mod 7) = (8 \mod 7) = 1$

Computation: $57 = 3 \cdot 19$

$2^{57} \mod 7 = 2^{3 \cdot 19} \mod 7$

$= (2^3)^{19} \mod 7$

$= (2^3 \mod 7)^{19} \mod 7$

$= (8 \mod 7)^{19} \mod 7$

$= 1^{19} \mod 7$

$= 1 \mod 7$

$= 1$
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:**

$101 = 2 \cdot 50 + 1$

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

$$= ((3^2)^{50} \cdot 3) \mod 5$$

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

$$= (1 \cdot 3) \mod 5 = 3$$

**Second computation:**

$101 = 4 \cdot 25 + 1$

$$3^{101} \mod 5 = 3^{4 \cdot 25 + 1} \mod 5$$

$$= ((3^4)^{25} \cdot 3) \mod 5$$

$$= ((1)^{25} \cdot 3) \mod 5$$

$$= (1 \cdot 3) \mod 5 = 3$$
Online Resources

Modular arithmetic

- 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 $r \geq 2$ 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

- \( \gcd(n, m) \quad (* n \geq m *) \)
  
  \[
  \begin{align*}
  \text{if } (n \mod m) &= 0 \\
  \text{then return } m \\
  \text{else return } \gcd(m, (n \mod m))
  \end{align*}
  \]

Online examples

- [https://youtu.be/klTIrnoVOEE](https://youtu.be/klTIrnoVOEE)
- [https://youtu.be/fwuj4yzoXlo](https://youtu.be/fwuj4yzoXlo)
The Euclidean Algorithm

Example I

- **Input:** \( n = 372 \) and \( m = 138 \)

\[
\begin{array}{|c|c|c|}
\hline
n & m & n = q \cdot m + r \\
\hline
372 & 138 & 372 = 2 \cdot 138 + 96 \\
138 & 96 & 138 = 1 \cdot 96 + 42 \\
96 & 42 & 96 = 2 \cdot 42 + 12 \\
42 & 12 & 42 = 3 \cdot 12 + 6 \\
12 & 6 & 12 = 2 \cdot 6 + 0 \\
\hline
\end{array}
\]

- **Output:** \( \gcd(372, 138) = 6 \)
The Euclidean Algorithm

Example III

**Input:** \( n = 480 \) and \( m = 360 \)

<table>
<thead>
<tr>
<th>( n )</th>
<th>( m )</th>
<th>( n = q \cdot m + r )</th>
</tr>
</thead>
<tbody>
<tr>
<td>480</td>
<td>360</td>
<td>( 480 = 1 \cdot 360 + 120 )</td>
</tr>
<tr>
<td>360</td>
<td>120</td>
<td>( 360 = 3 \cdot 120 + 0 )</td>
</tr>
</tbody>
</table>

**Output:** \( \gcd(480, 360) = 120 \)
The Euclidean Algorithm

Example III

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

<table>
<thead>
<tr>
<th>( n )</th>
<th>( m )</th>
<th>( n = q \cdot m + r )</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>13</td>
<td>( 21 = 1 \cdot 13 + 8 )</td>
</tr>
<tr>
<td>13</td>
<td>8</td>
<td>( 13 = 1 \cdot 8 + 5 )</td>
</tr>
<tr>
<td>8</td>
<td>5</td>
<td>( 8 = 1 \cdot 5 + 3 )</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
<td>( 5 = 1 \cdot 3 + 2 )</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>( 3 = 1 \cdot 2 + 1 )</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>( 2 = 2 \cdot 1 + 0 )</td>
</tr>
</tbody>
</table>

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

$$
372 = 2 \cdot 138 + 96 \\
138 = 1 \cdot 96 + 42 \\
96 = 2 \cdot 42 + 12 \\
42 = 3 \cdot 12 + 6 \\
12 = 2 \cdot 6
$$

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

$$
6 = (1 \cdot 42) - (3 \cdot 96) \\
= (1 \cdot 42) - 3(96 - 2 \cdot 42) \\
= (1 \cdot 42) - 3(96 - 2 \cdot 42) \\
= (-3 \cdot 96) + (7 \cdot 138) \\
= (7 \cdot 138) - 10(372 - 2 \cdot 138) \\
= (-10 \cdot 372) + (27 \cdot 138)
$$
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 smallest 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 on $\ell = \text{lcm}(n, m)$
- **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 $\text{lcm}(n, m) = h = k$

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 $\lcm(n, m) = \ell_1^{f_1} \ell_2^{f_2} \cdots \ell_w^{f_w}$

Proof outline

- Assume that $\ell^f$ is a divisor of $\lcm(n, m)$ 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 $\lcm(n, m)$
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

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

Examples

\[
\begin{align*}
75 & = 5 \cdot 15 = 5 \cdot 15 = \gcd(5, 15) \cdot \text{lcm}(5, 15) \\
216 & = 12 \cdot 18 = 6 \cdot 36 = \gcd(12, 18) \cdot \text{lcm}(12, 18) \\
273 & = 13 \cdot 21 = 1 \cdot 273 = \gcd(13, 21) \cdot \text{lcm}(13, 21) \\
7560 & = 126 \cdot 60 = 6 \cdot 1260 = \gcd(126, 60) \cdot \text{lcm}(126, 60)
\end{align*}
\]
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 \( m \) because \( \gcd(n, m) = 1 \)

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

- Run the Euclidean algorithm to compute \( \gcd(n, m) \)
- Return \( \lcm(n, m) = (n \cdot m) / \gcd(n, m) \)
The GCD and the LCM

Theorem

\[ n \cdot m = \gcd(n, m) \cdot \lcm(n, m) \] 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 \( \lcm(n, m) \)
- **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**

\[ n \cdot m = \gcd(n, m) \cdot \lcm(n, m) \] 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 \( \gcd(n, m) \) and once in \( \lcm(n, m) \) and therefore it also appears twice in the product of \( \gcd(n, m) \) and \( \lcm(n, m) \).

- 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 \( \lcm(n, m) \) but it is not a prime factor of \( \gcd(n, m) \), it also appears only once in the product of \( \gcd(n, m) \) and \( \lcm(n, m) \).
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
- $\text{lcm}(n_1, n_2, \ldots, n_k)$ is the smallest positive integer that is a multiple of these $k$ integers

**Computation**

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

**Recursive Computation**

- $\gcd(n_1, n_2, \ldots, n_k) = \gcd(\gcd(n_1, n_2, \ldots, n_{k-1}), n_k)$
- $\text{lcm}(n_1, n_2, \ldots, n_k) = \text{lcm}(\text{lcm}(n_1, n_2, \ldots, n_{k-1}), n_k)$
GCD and LCM For More Than Two Integers

Example

\[
gcd(36, 60, 90) = gcd(gcd(36, 60), 90) = gcd(12, 90) = 6 \\
= gcd(36, gcd(60, 90)) = gcd(36, 30) = 6 \\
lcm(36, 60, 90) = lcm(lcm(36, 60), 90) = lcm(180, 180) = 180 \\
= lcm(36, lcm(60, 90)) = lcm(36, 180) = 180
\]

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 $\text{lcm}$ 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 $\text{lcm}$ 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 $0 \leq r < d_1$
- 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

\[
\begin{align*}
n \mod 4 &= 2 \\
n \mod 6 &= 2 \\
n \mod 9 &= 2 
\end{align*}
\]

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
  - \( n \mod 3 = 2 \)
  - \( n \mod 5 = 3 \)
  - \( n \mod 7 = 4 \)

**Online example**
- [https://youtu.be/ru7mWZJlRQg](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 $n > 0$:
  \[
  p \mid (n^p - n) \quad n^p \equiv n \pmod{p}
  \]

**Online resources**

- **Story**: [https://youtu.be/OoQ16YCYksw](https://youtu.be/OoQ16YCYksw)
- **Examples and proof**: [https://youtu.be/w0ZQvZLx2KA](https://youtu.be/w0ZQvZLx2KA)
### Examples

#### $p = 3$

- $n = 4 \implies 4^2 - 1 = 16 - 1 = 15 = 5 \cdot 3$
- $n = 5 \implies 5^2 - 1 = 25 - 1 = 24 = 8 \cdot 3$
- $n = 6 \implies 6^2 - 1 = 36 - 1 = 35 = 11 \cdot 3 + 2$
- $n = 6 \implies 6^3 - 6 = 216 - 6 = 210 = 70 \cdot 3$

#### $p = 5$

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

#### $p = 6$

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

Example I

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

Example II

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

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 $p$, 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 \( m \),

\[
\phi(nm) = \phi(n) \phi(m)
\]

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

\[
\phi(36) = \phi(4 \cdot 9) = \phi(4) \phi(9) = 2 \cdot 6 = 12
\]

\[
\phi(36) = \phi(6 \cdot 6) \neq \phi(6) \phi(6) = 2 \cdot 2 = 4
\]
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**
- [video](https://youtu.be/qa_hksAzpSg)
- [video](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 \( n \)

\[
\varphi(n) = \varphi(p_1^{k_1}) \varphi(p_2^{k_2}) \cdots \varphi(p_h^{k_h})
\]

\[
= p_1^{k_1} \left( 1 - \frac{1}{p_1} \right) p_2^{k_2} \left( 1 - \frac{1}{p_2} \right) \cdots p_h^{k_h} \left( 1 - \frac{1}{p_h} \right)
\]

\[
= \left( p_1^{k_1} p_2^{k_2} \cdots p_h^{k_h} \right) \left( \left( 1 - \frac{1}{p_2} \right) \left( 1 - \frac{1}{p_2} \right) \cdots \left( 1 - \frac{1}{p_h} \right) \right)
\]

\[
= n \prod_{i=1}^{h} \left( 1 - \frac{1}{p_i} \right)
\]

\[
= n \prod_{p|n} \left( 1 - \frac{1}{p} \right)
\]
Euler’s Theorem

Theorem
For any relatively prime positive integers $n$ and $m$

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

The Fermat’s Little Theorem special case
- Let $n$ be a prime number and therefore $\phi(n) = n - 1$
- By the Euler’s Theorem

$$m^{\phi(n)} = m^{n-1} \equiv 1 \pmod{n}$$
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
$$17^{802} \mod 24 = (17^2 \cdot 17^{800}) \mod 24$$
$$= ((17^2 \mod 24) \cdot ((17^8)^{100} \mod 24)) \mod 24$$
$$= ((289 \mod 24) \cdot ((17^8) \mod 24)^{100}) \mod 24$$
$$= (1 \cdot 1^{100}) \mod 24$$
$$= 1$$

Online example (first 4 minutes)
- [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
Additional Online Resources

More about Public Key Systems and RSA
- RSA Code: https://youtu.be/t5lACDDoQTk

Relevant topics
- Perfect numbers: https://youtu.be/teBtVMSVRPc
- Wilson’s Theorem: https://youtu.be/VLFjOP7iFIO

Magic with Modular Arithmetic
- The Chinese Remainder Theorem and Cards
  https://youtu.be/19dXo5f3zDc