Discrete Structures: Cryptography and Number Theory

Amotz Bar-Noy

Department of Computer and Information Science
Brooklyn College
Journey into cryptography: Ancient Cryptography

What is cryptography? https://www.khanacademy.org/computing/computer-science/cryptography/crypt/v/intro-to-cryptography

The Caesar cipher https://www.khanacademy.org/computing/computer-science/cryptography/crypt/v/caesar-cipher

Polyalphabetic cipher https://www.khanacademy.org/computing/computer-science/cryptography/crypt/v/polyalphabetic-cipher

The one-time pad https://www.khanacademy.org/computing/computer-science/cryptography/crypt/v/polyalphabetic-cipher

Frequency stability property https://www.khanacademy.org/computing/computer-science/cryptography/crypt/v/frequency-stability

The Enigma encryption machine https://www.khanacademy.org/computing/computer-science/cryptography/crypt/v/frequency-stability

Perfect secrecy https://www.khanacademy.org/computing/computer-science/cryptography/crypt/v/perfect-secrecy

Pseudorandom number generators https://www.khanacademy.org/computing/computer-science/cryptography/crypt/v/random-vs-pseudorandom-number-generators
Prime Numbers

Prime and Composite Numbers

- A definition via a song: https://www.youtube.com/watch?v=1qAc22WxsWA
- 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.
- Video: https://www.youtube.com/watch?v=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.

Is 1 a prime number?

- Option I: 1 is a prime number.
- Option II: 1 is neither a prime number nor a composite number.
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.

Journey into cryptography: Primality Test

- [https://www.khanacademy.org/computing/computer-science/cryptography#comp-number-theory](https://www.khanacademy.org/computing/computer-science/cryptography#comp-number-theory)

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.
Let $n \geq 2$ be an integer.

Let $s = \lceil \sqrt{n} \rceil$.

For all $2 \leq d \leq s$ check if $d$ divides $n$.

* If yes then abort
* If no then continue.

if $d > s$ then $n$ is a prime number.
The Natural Primality Test

Data: An integer \( n \geq 2 \)
Result: \( n \) is a prime or a composite number

\[
s := \lceil \sqrt{n} \rceil; \quad d := 2;
\]

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;
else
  \( n \) is composite;
end
The Natural Integer Factorization Algorithm

- Let $n \geq 2$ be an integer.
- Let $D := ()$ be an empty list.
- Let $d = 2$.
- Let $m = n$.
- Repeat the following procedure until $m = 1$.
  - If $d$ divides $m$ then
    - Append $d$ at the end of the list $S$.
    - Set $m = m/d$.
  - If $d$ does not divide $m$ then increment $d$ by one.
- Let $S = (d_1 \leq d_2 \leq \cdots \leq d_k)$.
- Output: $n = d_1 d_2 \cdots d_k$
The Natural Integer Factorization Algorithm

**Data:** An integer \( n \geq 2 \)

**Result:** The unique prime factorization of \( n \)

\[
D = () \quad (* \text{an empty list} *) ;
\]

\( d := 2; \)

\( m := n; \)

**while** \( m > 1 \) **do**

**if** \( d \) divides \( m \) **then**

\( m := m / d ; \)

Append \( d \) 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

Goal

- Find all the prime numbers that are smaller than \( N \).

Algorithm

- Initially all the numbers 2, 3, \ldots, \( N \) are candidates to be primes.
- Let \( p = 2 \).
- Repeat the following procedure until \( p > \sqrt{N} \)
  - Mark \( p \) as a prime number.
  - Mark all the \( \lfloor N/p - 1 \rfloor \) multiples of \( p \) as non-prime numbers.
  - Let \( p \) be the smallest candidate left.
- Mark all the remaining candidates as prime numbers.
Resources

- https://www.youtube.com/watch?v=V08g_1kKj6Q
- https://www.youtube.com/watch?v=FBbHzy7v2Kg
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 $p_1, \ldots, p_n$.
- Therefore, a new prime is found.
- This process can continue to find infinitely many primes.
Resources

The original proof by Euclid:

- https://www.youtube.com/watch?v=dQmdHpvyfJs

Another proof:

- https://www.youtube.com/watch?v=fOXZgcAsrP8
What is Modular Arithmetic?

Notations

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

\[ n \mod d = r \]

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

Examples

- \( 7 \mod 3 = 1 \) because \( 7 = 2 \cdot 3 + 1 \).
- \( 25 \mod 5 = 0 \) because \( 25 = 5 \cdot 5 \).
- \( 17 \mod 9 = -1 = 8 \) because \( 17 = 2 \cdot 9 - 1 = 9 + 8 \).
- \( -18 \mod 7 = 3 \) because \( -18 = -3 \cdot 7 + 3 \).

Definition

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

The Lazy Mathematician

- https://www.youtube.com/watch?v=FdmApk9V2-w
Notation

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

**Proposition**

- \( n \mod d = (n + kd) \mod d \)

**Examples**

- \( 7 \mod 5 = 12 \mod 5 = 107 \mod 5 = 2 \)
- \( -3 \mod 7 = 4 \mod 7 = 11 \mod 7 = 4 \)

**Proof**

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

Proposition

- If $n \mod d = m \mod d$ then $d \mid (n - m)$

Example

- $100 \mod 7 = 23 \mod 7 = 2 \implies 7 \mid (100 - 23) = 77$

Proof

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

Proposition

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

Example

- 31 \mod 5 = 1 because 31 = 6 \cdot 5 + 1

\[
\begin{align*}
31 \mod 5 &= (14 + 17) \mod 5 \\
&= ((14 \mod 5) + (17 \mod 5)) \mod 5 \\
&= (4 + 2) \mod 5 \\
&= 6 \mod 5 \\
&= 1
\end{align*}
\]
Modular Subtraction

Proposition

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

Example

- \(8 \mod 5 = 3\) because \(8 = 1 \cdot 5 + 3\)

\[
\begin{align*}
8 \mod 5 & = (21 - 13) \mod 5 \\
& = ((21 \mod 5) - (13 \mod 5)) \mod 5 \\
& = (1 - 3) \mod 5 \\
& = -2 \mod 5 \\
& = 3
\end{align*}
\]
Modular Multiplication

Proposition

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

Example

132 \mod 7 = 6 because 132 = 18 \cdot 7 + 6

\[
132 \mod 7 = (12 \cdot 11) \mod 7 \\
= ((12 \mod 7)(11 \mod 7)) \mod 7 \\
= (5 \cdot 4) \mod 7 \\
= 20 \mod 7 \\
= 6
\]
Modular Inverse

**Definition**

For relatively prime (coprime) positive integers $n < d$ ($\gcd(n, m) = 1$), the inverse of $n$ modulo $d$, is an integer $m < d$ such that $(mn \mod d) = 1$.

If $(mn \mod d) = 1$ then $(n^{-1} \mod d) = m$ and $(m^{-1} \mod d) = n$

**Examples**

- 3 is the inverse of 5 modulo 7.
  - $3 \cdot 5 = 15$ and $(15 \mod 7) = 1$.

- 5 is the inverse of itself modulo 6.
  - $5 \cdot 5 = 25$ and $(25 \mod 6) = 1$. 
Modular Division

Proposition

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

Example

- 33 mod 7 = 5 because 33 = 4 \cdot 7 + 5

\[
33 \mod 7 = (99/3) \mod 7 \\
= ((99 \mod 7)(3^{-1} \mod 7)) \mod 7 \\
= (1 \cdot 5) \mod 7 \\
= 5 \mod 7 \\
= 5
\]
Modular Exponentiation

**Proposition**

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

**Example**

- \( 729 \mod 7 = 1 \) because \( 729 = 104 \cdot 7 + 1 \)
  
  \[
  729 \mod 7 = (9^3) \mod 7 \\
  = ((9 \mod 7)^3) \mod 7 \\
  = 2^3 \mod 7 \\
  = 8 \mod 7 \\
  = 1
  \]
Example

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

$$100000 \mod 7 = (10 \cdot 10 \cdot 10 \cdot 10 \cdot 10) \mod 7$$
$$= ((10 \mod 7)^5) \mod 7$$
$$= 3^5 \mod 7$$
$$= ((9 \mod 7) \cdot (9 \mod 7) \cdot 3) \mod 7$$
$$= (2^2 \cdot 3) \mod 7$$
$$= 12 \mod 7$$
$$= 5$$
Example: Compute $2^{58} \mod 7$

\[
\begin{align*}
2^1 \mod 7 &= 2 \\
2^2 \mod 7 &= (2^1)^2 \mod 7 = 2^2 \mod 7 = 4 \\
2^4 \mod 7 &= (2^2)^2 \mod 7 = 4^2 \mod 7 = 2 \\
2^8 \mod 7 &= (2^4)^2 \mod 7 = 2^2 \mod 7 = 4 \\
2^{16} \mod 7 &= (2^8)^2 \mod 7 = 4^2 \mod 7 = 2 \\
2^{32} \mod 7 &= (2^{16})^2 \mod 7 = 2^2 \mod 7 = 4 \\
2^{59} \mod 7 &= (2^{32}2^{16}2^82^1) \mod 7 \\
&= (4 \cdot 2 \cdot 4 \cdot 2) \mod 7 \\
&= 64 \mod 7 \\
&= 1
\end{align*}
\]
Modular Arithmetic: Resources

- Modular arithmetic: https://www.youtube.com/watch?v=2zEXtoQDpXY
- Modular exponentiation: https://www.youtube.com/watch?v=tTuWmcikE0Q
- Modular inverse: https://www.youtube.com/watch?v=mgvA3z-vOzc
Computing the Greatest Common Divisor

**Input:** Two integers $x > 0$ and $y > 0$.

**Output:** The maximum integer $z \geq 1$ such that $z$ divides both $x$ and $y$.

**Notation:** $z = \gcd(x, y)$.

**Examples:**
- $5 = \gcd(5, 15)$
- $6 = \gcd(12, 18)$
- $1 = \gcd(13, 21)$
Euclid Algorithm

- **Idea and proof of correctness:**
  \[ \text{gcd}(x, y) = \text{gcd}(y, (x \mod y)) \text{ for } x > y. \]

- **Proof:** If \( w \) divides \( x \) and \( y \) it divides \( (x \mod y) \).

- \( \text{gcd}(x, y) \)
  
  \[
  \text{if } (x \mod y) = 0 \text{ then return } y \\
  \text{return } \text{gcd}(y, (x \mod y))
  \]
Example I

**Input:** $x = 372$ and $y = 138$.

<table>
<thead>
<tr>
<th>$x$</th>
<th>$y$</th>
</tr>
</thead>
<tbody>
<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 II

**Input:** \( x = 21 \) and \( y = 13 \).

\[
\begin{array}{c|c}
 x & y \\
 21 & 13 \\
 13 & 8 \\
 8 & 5 \\
 5 & 3 \\
 3 & 2 \\
 2 & 1 \\
\end{array}
\]

**Output:** \( \gcd(21, 13) = 1 \).
The GCD and Beyond

- **The Greatest Common Divisor**: [https://www.youtube.com/watch?v=klTIrnovoEE](https://www.youtube.com/watch?v=klTIrnovoEE)

- **The Chinese Remainder Theorem**: [https://www.youtube.com/watch?v=ru7mWZJlRQg](https://www.youtube.com/watch?v=ru7mWZJlRQg)
Important Concepts and Theorems

- Fermat’s little theorem
- Euler’s totient function
- Euler’s theorem
Fermat’s Little Theorem

**Theorem**
- $n^p - n$ is a multiple of $p$ for any prime $p$ and an integer $n$:
  \[ n^p \equiv n \pmod{p} \]
- Example: $p = 7$ and $n = 2 \implies 2^7 - 2 = 126 = 7 \cdot 18$.

**A Special case**
- If $n$ is not divisible by $p$, Fermat’s little theorem is equivalent to the statement that $n^{p-1} - 1$ is a multiple of $p$: $n^{p-1} \equiv 1 \pmod{p}$
- Example: $p = 7$ and $n = 2 \implies 2^6 - 1 = 63 = 7 \cdot 9$.

**Resources**
- [https://www.youtube.com/watch?v=oT7kRlh1nVQ](https://www.youtube.com/watch?v=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 only $\{1, 2, 3, 4, 5, 6\}$ are 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 numbers in the set \{1, 2, 3, 4\} are relatively prime to 5 and \[ \varphi(5) = 5 - 1 = 4. \]
- The 6 numbers 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**

- Only multiples of \( p \) 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.
- \( \varphi(16) = \varphi(2^4) = 16 \left(1 - \frac{1}{2}\right) = 8 \).
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 Reminder Theorem.

Example

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

Example

$\{1, 2, 4, 7, 8, 11, 13, 14\}$ are relatively prime to 15.

$$\varphi(15) = \varphi(3 \cdot 5) = \varphi(3)\varphi(5) = (3 - 1)(5 - 1) = 8$$
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 numbers that divide $n$.

Proof

- Implied by the two propositions for the $\varphi$ value of a power of a prime and the $\varphi$ value of a product.

Example

- The distinct prime factors of 36 are 2 and 3. Therefore,

$$\varphi(36) = 36 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) = 36 \cdot \frac{1}{2} \cdot \frac{2}{3} = 12$$
Resources

https://www.youtube.com/watch?v=EcAT1XmHouk

https://www.khanacademy.org/computing/computer-science/cryptography/modern-crypt/v/euler-s-totient-function-phi-function
Euler’s Theorem

Theorem

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

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

Example

$\varphi(10) = 4$ because only $\{1, 3, 7, 9\}$ are relatively prime to 10.

$$3^4 = 81 = 8 \cdot 10 + 1$$
$$7^4 = 2401 = 240 \cdot 10 + 1$$
$$9^4 = 6561 = 656 \cdot 10 + 1$$

Resource

https://www.youtube.com/watch?v=FHkS3ydTM3M
Journey into cryptography: Modern Cryptography

https://www.khanacademy.org/computing/computer-science/cryptography#comp-number-theory

- Public key cryptography: What is it?  
  https://www.khanacademy.org/computing/computer-science/cryptography/modern-crypt/v/diffie-hellman-key-exchange-part-1

- The discrete logarithm problem  

- Diffie-hellman key exchange  
  https://www.khanacademy.org/computing/computer-science/cryptography/modern-crypt/v/diffie-hellman-key-exchange-part-2

- RSA encryption: Step 1  
  https://www.khanacademy.org/computing/computer-science/cryptography/modern-crypt/v/intro-to-rsa-encryption

- RSA encryption: Step 2  

- RSA encryption: Step 3  

- RSA encryption: Step 4  
  https://www.khanacademy.org/computing/computer-science/cryptography/modern-crypt/v/rsa-encryption-part-4
More about Public Key Systems and RSA

How Encryption Works
https://www.youtube.com/watch?v=IBocnou79yI&t=12s

RSA Code
https://www.youtube.com/watch?v=t5lACDDoQTk