Announcements

- Reading assignments
  - Today:
    - 7th Edition: 4.3 (the rest of the chapter is interesting!)
    - 6th Edition: 3.5, 3.6
    - 5th Edition: 2.5, 2.6 up to p. 191
  - Wednesday:
    - 7th Edition: 5.1, 5.2
    - 6th Edition: 4.1, 4.2
    - 5th Edition: 3.3, 3.4

Fast modular exponentiation

Fast exponentiation algorithm

- Compute \(78365^{65336} \mod 104729\)
- Compute \(78365^{81453} \mod 104729\)

Fast exponentiation algorithm

- What if the exponent is not a power of two?

\[81453 = 2^{16} + 2^{13} + 2^{12} + 2^{11} + 2^{10} + 2^9 + 2^8 + 2^7 + 2^6 + 2^0\]

The fast exponentiation algorithm computes \(a^n \mod m\) in time \(O(\log n)\)

Basic applications of mod

- Hashing
- Pseudo random number generation
- Simple cipher
Hashing
- Map values from a large domain, 0...M-1 in a
  much smaller domain, 0...N-1
- Index lookup
- Test for equality
- Hash(x) = x mod p
- Often want the hash function to depend on all
  of the bits of the data
  - Collision management

Simple cipher
- Caesar cipher, A = 1, B = 2, . . .
  - HELLO WORLD
- Shift cipher
  - f(p) = (p + k) mod 26
  - f⁻¹(p) = (p - k) mod 26
- f(p) = (ap + b) mod 26

Pseudo random number generation
- Linear Congruential method
  \[ x_{n+1} = (a \times x_n + c) \mod m \]

Primality
- An integer p greater than 1 is called prime if the
  only positive factors of p are 1 and p.
- A positive integer that is greater than 1 and is not
  prime is called composite.

Fundamental Theorem of Arithmetic
- Every positive integer greater than 1 has a
  unique prime factorization

Factorization
- If n is composite, it has a factor of size at most
  \( \sqrt{n} \)
Euclid’s theorem

There are an infinite number of primes.

Proof:
By contradiction
Suppose there are a finite number of primes: $p_1, p_2, \ldots, p_n$

Distribution of Primes

- If you pick a random number $n$ in the range $[x, 2x]$, what is the chance that $n$ is prime?

Famous Algorithmic Problems

- Primality Testing:
  - Given an integer $n$, determine if $n$ is prime
- Factoring
  - Given an integer $n$, determine the prime factorization of $n$

Factoring

- Factor the following 232 digit number [RSA768]:

Greatest Common Divisor

- GCD(a, b): Largest integer $d$ such that $d \mid a$ and $d \mid b$
  - GCD(100, 125) =
  - GCD(17, 49) =
  - GCD(11, 66) =
  - GCD(180, 252) =
GCD, LCM and Factoring

\[ a = 2^3 \cdot 3^1 \cdot 5^1 \cdot 7^1 = 46,200 \]

\[ b = 2^3 \cdot 3^2 \cdot 5^1 \cdot 7^1 = 204,750 \]

\[ \text{GCD}(a, b) = 2^{\min(3,1)} \cdot 3^{\min(1,2)} \cdot 5^{\min(1,1)} \cdot 7^{\min(1,1)} \]

\[ \text{LCM}(a, b) = 2^{\max(3,1)} \cdot 3^{\max(1,2)} \cdot 5^{\max(1,1)} \cdot 7^{\max(1,1)} \]

Theorem

Let \(a\) and \(b\) be positive integers. Then

\[ a \cdot b = \text{gcd}(a, b) \cdot \text{lcm}(a, b) \]

Euclid’s Algorithm

- \( \text{GCD}(x, y) = \text{GCD}(y, x \mod y) \)

Example: \( \text{GCD}(660, 126) \)

\[
\begin{align*}
\text{int } & \text{GCD}(\text{int } a, \text{int } b) \{ \\
& / \ast a >= b, \ b > 0 \ast / \\
& \text{int } \text{tmp}; \\
& \text{int } x = a; \\
& \text{int } y = b; \\
& \text{while } (y > 0) \{ \\
& \quad \text{tmp} = x \% y; \\
& \quad x = y; \\
& \quad y = \text{tmp}; \\
& \} \\
& \text{return } x; \\
\}
\end{align*}
\]

Extended Euclid’s Algorithm

- If \( \text{GCD}(x, y) = g \), there exist integers \( s, t \), such \( sx + ty = g \);

- The values \( x, y \) in Euclid’s algorithm are linear sums of \( a, b \).
  - A little book keeping can be used to keep track of the constants

Bézout’s Theorem

If \( a \) and \( b \) are positive integers, then there exist integers \( s \) and \( t \) such that

\[ \text{gcd}(a,b) = sa + tb. \]

Simple cipher

- Caesar cipher, \( a \to b, b \to c, \ldots \)
  - HELLOWORLD \( \to \) IFMMPXPSME

- Shift cipher
  - \( f(x) = (x + k) \mod 26 \)
  - \( f^{-1}(x) = (x - k) \mod 26 \)
  - \( f(x) = (ax + b) \mod 26 \)
  - How good is the cipher \( f(x) = (2x + 1) \mod 26 \)
Multiplicative Cipher: \( f(x) = ax \mod m \)

For a multiplicative cipher to be invertible:
\[
f(x) = ax \mod m : \{0, m-1\} \rightarrow \{0, m-1\}
\]
must be one to one and onto.

Lemma: If there is an integer \( b \) such that \( ab \mod m = 1 \), then the function \( f(x) = ax \mod m \) is one to one and onto.

Multiplicative Inverse mod \( m \)

Suppose \( \gcd(a, m) = 1 \)

By Bézout’s Theorem, there exist integers \( s \) and \( t \) such that \( sa + tm = 1 \).

\( s \) is the multiplicative inverse of \( a \):
\[
1 = (sa + tm) \mod m = sa \mod m
\]