Discrete Mathematics: Lecture 13

- Last time:
  - Chap 4.2: Integer representations and algorithms
  - Chap 4.3: Primes and greatest common divisors
- Today:
  - Chap 4.4: Solving congruences
  - Chap 4.6: Cryptography (a simple introduction)
- Next time:
  - Chap 5.1: Mathematical induction
  - Chap 5.2: Strong induction and well-ordering

Review of last time

- The fundamental theorem of arithmetic
- There are infinitely many primes
- Greatest common divisors, least common multiples
- Euclidean algorithm
- Base b representation of integers
- Algorithms for addition and multiplication of integers
- Modular exponentiation algorithm

Some useful results

- Theorem: If a and b are positive integers, then there exist integers s and t such that $gcd(a, b) = sa + tb$.
- Example: $gcd(252, 198) = 18$
- Lemma 1: If a, b, and c are positive integers such that $gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.
- Lemma 2: If p is a prime and $p \mid a_1 a_2 \ldots a_n$, where each a_i is an integer, then $p \mid a_i$ for some i.
- The uniqueness of prime factorization of integers
- Theorem: Let m be a positive integer and let a, b, and c be integers. If $ac \equiv bc \pmod{m}$ and $gcd(c, m) = 1$, then $a \equiv b \pmod{m}$.

Linear congruences

- A congruence of the form $ax \equiv b(\text{ mod } m)$ is called a linear congruence. How to solve linear congruences?
- An integer $\bar{a}$ such that $\bar{a}a \equiv 1(\text{ mod } m)$ is called an inverse of a modulo m.
- Theorem: If $m > 1$ and $gcd(a, m) = 1$, then an inverse of a modulo m exists. Moreover, this inverse is unique modulo m.
- Example: Find an inverse of 3 modulo 7
- Example: Solve $3x = 4(\text{ mod } 7)$

Sun-Tsu's puzzle

There are certain things whose number is unknown. When divided by 3, the remainder is 2; when divided by 5, the remainder is 3; and when divided by 7, the remainder is 2. What will be the number of things?

What are the solutions of the system of congruences:

$x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 2 \pmod 7$

The Chinese remainder theorem

- Theorem: Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers and $a_1, a_2, \ldots, a_n$ arbitrary integers. Then the system $x \equiv a_i \pmod{m_i}$, $i = 1, 2, \ldots, n$ has a unique solution modulo $m = m_1 m_2 \ldots m_n$.
- Example: solve the system
  $x \equiv 2 \pmod{3}$
  $x \equiv 3 \pmod{5}$
  $x \equiv 2 \pmod{7}$

Format's little theorem

- An integer n is prime when it is not divisible by any prime $p \leq \sqrt{n}$.
- Are there more efficient ways for primality testing?
- Ancient Chinese mathematicians believed: n is prime iff $2^{n-1} \equiv 1 \pmod{n}$
- Counterexample: $2^{340} \equiv 1 \pmod{341}$, but 341=11·31 (Ex 27)
- Format's little theorem: If p is prime and $gcd(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$. Furthermore, for every integer a we have: $a^p \equiv a \pmod{p}$. (Ex 19)

Applications of number theory: Cryptology (optional)

- Cryptology is the study of secret messages.
- Encryption is the process of making a secret message.
- Decryption is the process of recovering the original message from the secret message.

Caesar's encryption method

- One of the earliest known uses of cryptology is by Caesar.
- He made messages secret by shifting each letter 3 letters forward in the alphabet.
- $f : \{0, 1, \ldots, 25\} \to \{0, 1, \ldots, 25\}$
  $f(p) = (p + 3) \bmod 26$, called a shift cipher
- $f^{-1}(p) = (p - 3) \bmod 26$
- Generalization of Caesar's method: $f(p) = (ap + b) \bmod 26$ such that f is a bijection, called an affine transformation
- Example: what letter replace the letter K (10) when $f(p) = (7p + 3) \bmod 26$

Public key cryptography

- Caesar's encryption method is an example of private key cryptosystems
- Knowing the encryption key lets one quickly find the decryption key
- People wanting to communicate must have a separate key
- Public key cryptosystem: everybody can have a publicly known encryption key, and the encryption key does not let one find the decryption key without an extraordinary amount of time