University of Hawaii

ICS141: Discrete Mathematics for Computer Science I

Dept. Information & Computer Sci., University of Hawaii

Jan Stelovsky

based on slides by Dr. Baek and Dr. Still

Originals by Dr. M. P. Frank and Dr. J.L. Gross

Provided by McGraw-Hill

Lecture 18a

Chapter 3. The Fundamentals

3.6 Applications of Integers Algorithms

Quiz

1. What is the decimal expansion $(1AF)_{16}$?
2. What is the hexadecimal expansion of $(287)_{10}$?
3. What is the two's complement of -7?
4. Multiply $(100)_2$ and $(101)_2$ in binary system.

- Hints
  - $16^2 = 256$

Applications

University of Hawaii

- Miscelaneous useful results
- Linear congruences
- Chinese Remainder Theorem
- Pseudoprimes
  - Fermat's Little Theorem
- Public Key Cryptography
  - The Rivest-Shamir-Adleman (RSA) cryptosystem

Miscelaneous Results

University of Hawaii

- **Theorem 1:**
  - $\forall a,b \in \mathbf{Z}^+$: $\exists s,t \in \mathbf{Z}$: $\gcd(a,b) = sa + tb$
- **Lemma 1:**
  - $\forall a,b,c \in \mathbf{Z}^+$: $\gcd(a,b)=1 \wedge a \mid bc \rightarrow a|c$
- **Lemma 2:**
  - If p is prime and $p|a_1a_2\ldots a_n$ (integers a_i) then $\exists i$: $p|a_i$.
- **Theorem 2:**
  - If $ac \equiv bc \pmod{m}$ and $\gcd(c,m)=1$, then $a \equiv b \pmod{m}$. ($m\in\mathbf{Z}^+$, $a,b,c\in\mathbf{Z}$)

Theorem 1

- **Theorem 1:**
  $\forall a,b \in \mathbf{Z}^+: \exists s,t \in \mathbf{Z}$ such that $\gcd(a,b) = sa + tb$
  - Proof: By induction over the value of the larger argument *a*.
- Example:
  - Express gcd(252, 198) = 18 as a linear combination of 252 and 198.

Proof of Theorem 1

University of Hawaii

Theorem 1: $\forall b,a \in \mathbf{Z}^+: \exists s,t \in \mathbf{Z}: \gcd(a,b) = sa + tb$

Proof: (By induction over the value of the larger argument *a*.)

- ByTheorem 0 $\gcd(a,b) = \gcd(b,c)$ if $c = a \bmod b$, i.e., $a = kb + c$ for some integer k, and thus $c = a - kb$.
- Now, since $b<a$ and $c<b$, by inductive hypothesis, we can assume that $\exists u,v: \gcd(b,c) = ub + vc$.
- Substituting for c, this is $ub+v(a-kb)$, which we can regroup to get $va + (u-vk)b$.
- So now let $s = v$, and let $t = u-vk$, and we're finished.
- The base case: $s = 1$ and $t = 0$.
  This works for $\gcd(a,0)$, or if $a=b$ originally. ■

Theorem 1: Example

- Express gcd(252, 198) = 18 as a linear combination of 252 and 198.
  - $$\left.\begin{aligned} 252 &= 1 \cdot 198 + 54 \\ 198 &= 3 \cdot 54 + 36 \\ 54 &= 1 \cdot 36 + 18 \\ 36 &= 2 \cdot 18 \end{aligned}\right\} \text{Euclidean algorithm}$$
  - $$\begin{aligned} 18 &= 54 - 1 \cdot 36 = 54 - 1 \cdot (198 - 3 \cdot 54) \\ &= 4 \cdot 54 - 1 \cdot 198 \\ &= 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 \\ &= 4 \cdot 252 - 5 \cdot 198 \end{aligned}$$
  - Therefore, gcd(252, 198) = $18 = 4 \cdot 252 - 5 \cdot 198$

Proof of Lemma 1

University of Hawaii

- **Lemma 1:**

  $\forall a,b,c \in \mathbf{Z}^+\colon \gcd(a,b)=1 \wedge a|bc \rightarrow a|c$

  Proof:

  - Applying theorem 1, $\exists s, t\colon sa + tb = 1$.
  - Multiplying through by c, we have that $sac + tbc = c$.
  - Since $a|bc$ is given, we know that $a|tbc$, and obviously $a|sac$.
  - Thus (using the theorem on pp.202), it follows that $a|(sac+tbc)$; in other words, that $a|c$. ■

Proof of Lemma 2

University of Hawaii

- **Lemma 2:** If p is prime and $p|a_1a_2\ldots a_n$ (integers a_i) then $p|a_i$ for some i.

  Proof (by induction):

  - If $n=1$, this is immediate since $p|a_0 \rightarrow p|a_0$.
    Suppose the lemma is true for all $n<k$ and $p|a_1\ldots a_k$.
  - If $p|m$ where $m=a_1\ldots a_{k-1}$ then we have it inductively.
  - Otherwise, we have $p|ma_k$ but $\neg(p|m)$.
    Since m is not a multiple of p, and p has no factors, m has no common factors with p, thus $\gcd(m,p)=1$.
    So by applying Lemma 1, $p|a_k$. ■

Theorem 2

- **Theorem 2:** Let $m \in \mathbf{Z}^+$ and $a,b,c \in \mathbf{Z}$.
  If $ac \equiv bc \pmod{m}$ and $\gcd(c,m)=1$, then $a \equiv b \pmod{m}$.

  Proof:
  - Since $ac \equiv bc \pmod{m}$, this means $m \mid ac-bc$.
  - Factoring the right side, we get $m \mid c(a-b)$.
    Since $\gcd(c,m)=1$, lemma 1 implies that $m \mid a-b$,
    in other words, that $a \equiv b \pmod{m}$. ∎
- Examples
  - $20 \equiv 8 \pmod{3}$ i.e. $5 \cdot 4 \equiv 2 \cdot 4 \pmod{3}$
    Since $\gcd(4, 3) = 1$, $5 \equiv 2 \pmod{3}$
  - $14 \equiv 8 \pmod{6}$ but $7 \not\equiv 4 \pmod{6}$ (as $\gcd(2,6) \neq 1$)

Linear Congruences, Inverses

- A congruence of the form $ax \equiv b \pmod{m}$ is called a ***linear congruence***. ($m \in \mathbf{Z}^+$, $a, b \in \mathbf{Z}$, and x: variable)
  - To *solve* the congruence is to find the x's that satisfy it.
- An ***inverse of a, modulo m*** is any integer a^{-1} such that $a^{-1}a \equiv 1 \pmod{m}$.
  - If we can find such an a^{-1}, notice that we can then solve $ax \equiv b \pmod{m}$ by multiplying through by it, giving $a^{-1}ax \equiv a^{-1}b \pmod{m}$, thus $1 \cdot x \equiv a^{-1}b \pmod{m}$, thus $x \equiv a^{-1}b \pmod{m}$.

Theorem 3

University of Hawaii

- **Theorem 3:** If $\gcd(a,m)=1$ (i.e. a and m are relatively prime) and $m > 1$,
  then a has a inverse a^{-1} unique modulo m.

  Proof:
  - By theorem 1, $\exists s,t$: $sa + tm = 1$, so $sa + tm \equiv 1 \pmod{m}$.
  - Since $tm \equiv 0 \pmod{m}$, $sa \equiv 1 \pmod{m}$.
    Thus s is an inverse of a (mod m).
  - Theorem 2 guarantees that if $ra \equiv sa \equiv 1$ then $r \equiv s$,
    thus this inverse is unique modulo m.
    (All inverses of a are in the same congruence class as s.)
    ■

Example

- Find an inverse of 3 modulo 7
  - Since gcd(3, 7) = 1, by Theorem 3 there exists an inverse of 3 modulo 7.
  - $7 = 2 \cdot 3 + 1$
  - From the above equation, $-2 \cdot 3 + 1 \cdot 7 = 1$
  - Therefore, –2 is an inverse of 3 modulo 7
  - Note that every integer congruent to –2 modulo 7 is also an inverse of 3, such as 5, –9, 12, and so on.)

Example

- What are the solutions of the linear congruence $3x \equiv 4 \pmod 7$?
  - -2 is an inverse of 3 modulo 7 (previous slide)
  - Multiply both side by -2: $-2 \cdot 3x \equiv -2 \cdot 4 \pmod 7$
  - $-6 \cdot x \equiv x \equiv -8 \equiv 6 \pmod 7$
  - Therefore, the solutions to the congruence are the integers x such that $x \equiv 6 \pmod 7$, i.e. 6, 13, 20, 27,… and –1, –8, –15,…
  - e.g. $3 \cdot 13 = 39 \equiv 4 \pmod 7$

An Application of Primes!

- When you visit a secure web site (https:… address, indicated by padlock icon in IE, key icon in Netscape), the browser and web site may be using a technology called *RSA encryption*.
- This *public-key cryptography* scheme involves exchanging *public keys* containing the product *pq* of two random large primes *p* and *q* (a *private key*) which must be kept secret by a given party.
- So, the security of your day-to-day web transactions depends critically on the fact that all known factoring algorithms are intractable!

Public Key Cryptography

- In ***private key cryptosystems***, the same secret "key" string is used to both encode and decode messages.
  - This raises the problem of how to securely communicate the key strings.
- In ***public key cryptosystems***, there are two *complementary* keys instead.
  - One key decrypts the messages that the other one encrypts.
- This means that one key (the *public key*) can be made public, while the other (the *private key*) can be kept secret from everyone.
  - Messages to the owner can be encrypted by anyone using the public key, but can *only* be decrypted by the owner using the private key.
    - Like having a private lock-box with a slot for messages.
  - Or, the owner can encrypt a message with their private key, and then anyone can decrypt it, and know that *only* the owner could have encrypted it.
    - This is the basis of digital signature systems.
- The most famous public-key cryptosystem is RSA.
  - It is based entirely on number theory!

Rivest-Shamir-Adleman (RSA)

- Choose a pair p, q of large random prime numbers with about the same number of bits
  - Let $n = pq$
- Choose exponent e that is relatively prime to $(p-1)(q-1)$ and $1 < e < (p-1)(q-1)$
- Compute d, the inverse of e modulo $(p-1)(q-1)$.

- The **public key** consists of: n, and e.
- The **private key** consists of: n, and d.

RSA Encryption

University of Hawaii

- To encrypt a message encoded as an integer:
  - Translate each letter into an integer and group them to form larger integers, each representing a block of letters. Each block is encrypted using the mapping

$$C = M^e \bmod n.$$

- Example: RSA encryption of the message **STOP** with $p = 43$, $q = 59$, and $e = 13$
  - $n = 43 \times 59 = 2537$
  - $\gcd(e, (p-1)(q-1)) = \gcd(13, 42 \cdot 58) = 1$
  - **STOP** -> 1819 1415
  - 1819^{13} **mod** $2537 = 2081$; 1415^{13} **mod** $2537 = 2182$
  - Encrypted message: **2081 2182**

RSA Decryption

- To decrypt the encoded message C,
  - Compute $M = C^d \bmod n$
  - Recall that d is an inverse of e modulo $(p-1)(q-1)$.

- Example: RSA decryption of the message **0981 0461** encrypted with $p = 43$, $q = 59$, and $e = 13$
  - $n = 43 \times 59 = 2537$; $d = 937$
  - 0981^{937} **mod** $2537 = 0704$
  - 0461^{937} **mod** $2537 = 1115$
  - Decrypted message: **0704 1115**
  - Translation back to English letters: **HELP**

Why RSA Works

Theorem (Correctness of RSA): $(M^e)^d \equiv M \pmod{n}$. **Proof:**

- By the definition of d, we know that $de \equiv 1 \ [\bmod\ (p-1)(q-1)]$.
  - Thus by the definition of modular congruence, $\exists k$: $de = 1 + k(p-1)(q-1)$.
  - So, the result of decryption is $C^d \equiv (M^e)^d = M^{de} = M^{1+k(p-1)(q-1)} \pmod{n}$
- Assuming that M is not divisible by either p or q,
  - Which is nearly always the case when p and q are very large,
  - Fermat's Little Theorem tells us that $M^{p-1} \equiv 1 \pmod{p}$ and $M^{q-1} \equiv 1 \pmod{q}$
- Thus, we have that the following two congruences hold:
  - First: $C^d \equiv M \cdot (M^{p-1})^{k(q-1)} \equiv M \cdot 1^{k(q-1)} \equiv M \pmod{p}$
  - Second: $C^d \equiv M \cdot (M^{q-1})^{k(p-1)} \equiv M \cdot 1^{k(p-1)} \equiv M \pmod{q}$
- And since $\gcd(p,q)=1$, we can use the Chinese Remainder Theorem to show that therefore $C^d \equiv M \pmod{pq}$:
  - If $C^d \equiv M \pmod{pq}$ then $\exists s$: $C^d = spq + M$, so $C^d \equiv M \pmod{p}$ and $\pmod{q}$. Thus M is a solution to these two congruences, so (by CRT) it's the only solution.■

Uniqueness of Prime Factorizations

The "hard" part of proving the Fundamental Theorem of Arithmetic.

"The prime factorization of any positive integer *n* is unique."

Proof: Suppose that the positive integer *n* can be written as the product of two different ways, i.e. $n = p_1 \ldots p_s = q_1 \ldots q_t$ are equal products of two nondecreasing sequences of primes.

Assume (without loss of generality) that all primes in common have already been divided out, so that $\forall ij$: $p_i \neq q_j$. But since $p_1 \ldots p_s = q_1 \ldots q_t$, we have that $p_1 | q_1 \ldots q_t$, since $p_1 \cdot (p_2 \ldots p_s) = q_1 \ldots q_t$. Then applying lemma 2, $\exists j$: $p_1 | q_j$. Since q_j is prime, it has no divisors other than itself and 1, so it must be that $p_i = q_j$. This contradicts the assumption $\forall ij$: $p_i \neq q_j$.

Consequently, the two lists must have been identical to begin with! ■

Chinese Remainder Theorem

University of Hawaii

- **Theorem:** (Chinese remainder theorem.)
  Let $m_1,\ldots,m_n > 0$ be pairwise relatively prime and $a_i,\ldots,a_n$ arbitrary integers.
  Then the equations system $x \equiv a_i \pmod{m_i}$ (for i=1,..,n) has a unique solution modulo $m = m_1 m_2 \cdots m_n$.

  Proof:
  - Let $M_i = m/m_i$. (Thus $\gcd(m_i, M_i)=1$.)
  - So by Theorem 3, $\exists y_i = M_i$ such that $y_i M_i \equiv 1 \pmod{m_i}$.
  - Now let $x = \sum_i a_i y_i M_i = a_1 y_1 M_1 + a_2 y_2 M_2 + \cdots + a_n y_n M_n$.
  - Since $m_i | M_k$ for $k \neq i$, $M_k \equiv 0 \pmod{m_i}$, so $x \equiv a_i y_i M_i \equiv a_i \pmod{m_i}$. Thus, the congruences hold. (Uniqueness is an exercise.) □

Computer Arithmetic with Large Integers

- By Chinese Remainder Theorem, an integer a where $0 \leq a < m = \prod m_i$, $\gcd(m_i, m_{j \neq i}) = 1$, can be represented by a's residues mod m_i:

  $(a \bmod m_1, a \bmod m_2, \ldots, a \bmod m_n)$
- To perform arithmetic with large integers represented in this way,
  - Simply perform operations on the separate residues!
    - Each of these might be done in a single machine operation.
    - The operations may be easily parallelized on a vector machine.
  - Works so long as $m >$ the desired result.

Computer Arithmetic Example

University of Hawaii

- For example, the following numbers are relatively prime:

  $m_1 = 2^{25}-1 = 33{,}554{,}431 = 31 \cdot 601 \cdot 1{,}801$
  $m_2 = 2^{27}-1 = 134{,}217{,}727 = 7 \cdot 73 \cdot 262{,}657$
  $m_3 = 2^{28}-1 = 268{,}435{,}455 = 3 \cdot 5 \cdot 29 \cdot 43 \cdot 113 \cdot 127$
  $m_4 = 2^{29}-1 = 536{,}870{,}911 = 233 \cdot 1{,}103 \cdot 2{,}089$
  $m_5 = 2^{31}-1 = 2{,}147{,}483{,}647$ (prime)
- Thus, we can uniquely represent all numbers up to $m = \prod m_i \approx 1.4\times10^{42} \approx 2^{139.5}$ by their residues r_i modulo these five m_i.
  - *E.g.*, $10^{30} = (r_1 = 20{,}900{,}945;\ r_2 = 18{,}304{,}504;\ r_3 = 65{,}829{,}085;\ r_4 = 516{,}865{,}185;\ r_5 = 1{,}234{,}980{,}730)$
- To add two such numbers in this representation,
  - Just add the residues using machine-native 32-bit integers.
  - Take the result mod 2^k-1:
    - If result is ≥ the appropriate 2^k-1 value, subtract out 2^k-1
      - or just take the low k bits and add 1.
  - Note: No carries are needed between the different pieces!

Pseudoprimes

University of Hawaii

- Ancient Chinese mathematicians noticed that whenever n is prime, $2^{n-1} \equiv 1 \pmod{n}$.
  - Some also claimed that the converse was true.
- However, it turns out that the converse is not true!
  - If $2^{n-1} \equiv 1 \pmod{n}$, it doesn't follow that n is prime.
    - For example, $341 = 11 \cdot 31$, but $2^{340} \equiv 1 \pmod{341}$.
- Composites n with this property are called ***pseudoprimes***.
  - More generally, if $b^{n-1} \equiv 1 \pmod{n}$ and n is composite, then n is called a *pseudoprime to the base b*.

Carmichael Numbers

University of Hawaii

- These are sort of the "ultimate pseudoprimes."
- A *Carmichael number* is a composite n such that $b^{n-1} \equiv 1 \pmod{n}$ for all b relatively prime to n.
- The smallest few are 561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341.
- Well, so what? Who cares?
  - **Exercise for the student:** Do some research and find me a useful & interesting application of Carmichael numbers.

Fermat's Little Theorem

University of Hawaii

- Fermat generalized the ancient observation that $2^{p-1} \equiv 1 \pmod{p}$ for primes p to the following more general theorem:
- **Theorem:** (Fermat's Little Theorem.)
  - If p is prime and a is an integer not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$.
  - Furthermore, for every integer a we have $a^p \equiv a \pmod{p}$.
- Example (Exponentiation MOD a Prime)
  - Find 2^{301} mod 5: By FLT, $2^4 \equiv 1 \pmod{5}$. Hence, $2^{300} = (2^4)^{75} \equiv 1 \pmod{5}$.

    Therefore, $2^{301} = (2^{300}) \cdot 2 \equiv 1 \cdot 2 \pmod{5} \equiv 2 \pmod{5}$