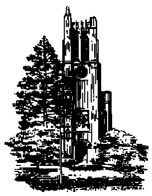
Tuesday June 14, 2016
Lecture 17

Number Theory



Notables

Homework 10; Due Thursday June 16

1. Using the method discussed in class, convert (long hand)
   a. Decimal (that is, base 10) 8888 to binary
   b. Decimal 2555 to base 6
   c. Decimal 8990 to base 19; use symbols 0-9 and A-Z
   You must show ALL your steps to receive full credit.
2. Convert $(260.260)_9$ to base 10.
3. Carry out the following additions in the given base:
   a. $(5665)_7 + (4664)_7 = (\quad)_7$
   b. $(AB56)_{16} + (9868)_{16} = (\quad)_{16}$
4. Page 255, Problem 26
5. Page 256, Problem 30(d), and Problem 48(d)
6. Page 272, Problem 4(f), 21(c), 24(b), and 40(e)

Base Conversion, Recap

- From decimal to any base:
  - For the whole (integer) part
    - Repeated divisions, collecting the remainder
  - For the fraction part
    - Repeated multiplications, collecting the whole part
- From another base to decimal
  - Expand according to positional system
- A good site for binary conversion is:
  - http://en.wikipedia.org/wiki/Binary_numeral_system

Base Conversion

Number in Base 10 xxxxxxxxxxxxxxx.yyyyyyyyyyyyyyy

/, % expand *b

Number in Base b qqqqqqqqqqqqqq.wwwwwwwwwww

Answer to the pop quiz

- Represent $(5.875)_{10}$ in binary
- Answer:
  - First the whole part
    - 5 = 2 * 2 + 1
    - 2 = 1 * 2 + 0
    - 1 = 0 * 2 + 1
  - Now, the fraction part
    - 0.875 * 2 = 1.75
    - 0.75 * 2 = 1.5
    - 0.5 * 2 = 1.0
  - Number 5.875 in decimal has 101.111 representation in base 2

Exercise

- Represent $(123.213)_4$ in base 10
  - $(123)_4 = 3 \times 4^0 + 2 \times 4^1 + 1 \times 4^2 = 3 + 8 + 16 = 27$
  - $(0.213)_4 = 2 \times 4^{-1} + 1 \times 4^{-2} + 3 \times 4^{-3} = 0.609375$
  - Thus $(123.213)_4$ is (27.609375) in base 10

Bases used in Computer Science

- The base b expansion of integer n is written as $n = (a_k \dots a_1 \, a_0)_b$
- We omit b and () for base 10
- Base 2 (Binary),
  - bits in computer, has two symbols {0,1}
  - The Presence/Absence (PandA) representation
- Base 8 (Octal),
  - has eight symbols {0,1,2,3,4,5,6,7}
- Base 16 (Hexadecimal)
  - has sixteen symbols {0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F}
  - Note that A=10, B=11, C=12, D=13, E=14, F=15.

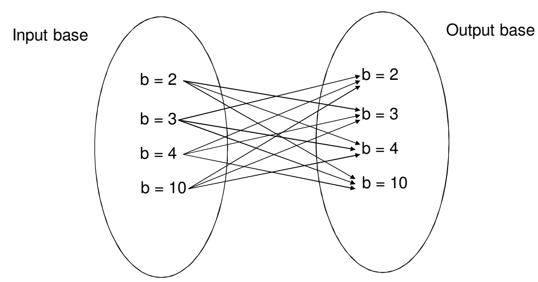
Bases used in Computer Science

- Base 2 (Binary),
  - bits in computer, has two symbols {0,1}
- Base 8 (Octal),
  - has eight symbols {0,1,2,3,4,5,6,7}
- Base 16 (Hexadecimal)
  - has sixteen symbols {0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F}.
  - Note that A=10, B=11, C=12, D=13, E=14, F=15.

Exercise

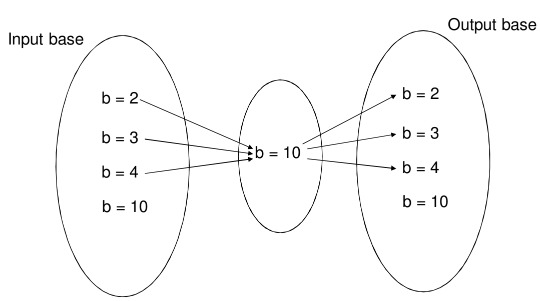
- Covert binary 110000111010
  - To octal (base 8)
    - 6072
  - To hex
    - C3A
- Convert Hex (base 16) ABC
  - To binary
    - 101010111100
  - To octal
    - 5274
- 4 bits in binary is equal to one digit in Hex. One binary byte can be represented by a two-digit Hex

Conversion between Bases



A total of 12 converters

Conversion between Bases…



A total of 6 converters

Other number representations

- Theorem: Every integer can be *uniquely* represented in the form:

$$n = a_k 3^k + a_{k-1} 3^{k-1} + \cdots + a_1 3^1 + a_0$$

$$\text{where} \quad a_i \in \{-1, 0, 1\}$$

- This is known as the Balanced Ternary Expansion
- Example,
  - Find BTE of 79.
  - $79 = 3^4 - 3 + 1$

Example

- Give the BTE representation of decimal number 223.
  - $223 = 2*3^4 + 2*3^3 + 2*3 + 1$
  - $223 = 2*3^4 + 2*3^3 + (3-1)*3 + 1$
  - $223= 2*3^4 + 2*3^3 + 3^2 - 3 + 1$
  - $223= 2*3^4 + (3-1)*3^3 + 3^2 - 3 + 1$
  - $223= 2*3^4 + 3^4 - 3^3 + 3^2 - 3 + 1$
  - $223= 3^5 - 3^3 + 3^2 - 3 + 1 = (1,0,-1,1,-1,1)_{BTE}$

495

In-Class Exercise

- Covert decimal 238 to BTE
  - $238 = 2\times3^4 + 2\times3^3 + 2\times3^2 + 3 + 1 = (22211)_3$
  - $238 = (3-1)\times3^4 + (3-1)\times3^3 + (3-1)\times3^2 + 3 + 1$
  - $238 = 3^5 - 3^4 + 3^4 - 3^3 + 3^3 - 3^2 + 3 + 1$
  - $238 = 3^5 - 3^2 + 3 + 1 = (1,0,0,-1,1,1)_{BTE}$

496

Other number representations…

- Theorem: Every integer x can be *uniquely* represented in the form:

$$x = a_n n! + a_{n-1}(n-1)! + \cdots + a_2 2! + a_1 1!$$
$$\text{where } a_i \text{ is an integer with}$$
$$0 \le a_i \le i \quad \text{for } i = 1, 2, \ldots, n.$$

- This is known as the Cantor Expansion
- Example,
  - Find Cantor expansion of 87.
  - $87 = 3*4! + 2*3! + 2! + 1!$

497

In-Class Exercise

- Convert decimal 319 to Cantor Expansion
  - $319 = 159\times2 + 1$
  - $159 = 53\times3 + 0$
  - $53 = 13\times4 + 1$
  - $13 = 2\times5 + 3$
  - $2 = 0\times6 + 2$
  - $319 = 2\times5! + 3\times4! + 1\times3! + 0\times2! + 1\times1! = (23101)_{CE}$

498

Algorithms for Integer Operation

- Computers use binary numbers to perform operations in integers.
- In order to handle integer operations in binary system first we should convert the decimal numbers into integers and then do the operations using binary numbers.

499

Addition of Integers in Base 2

- A procedure to perform addition is based on the usual method for adding numbers with pencil and paper.
- Example:

1 1	← carry bits	
1 1 1 0	→	$(14)_{10}$
+ 1 0 1 1	→	$(11)_{10}$
= 1 1 0 0 1	→	$(25)_{10}$

- An overflow may happen when adding two numbers.

500

Multiplying Integers in Base 2

- Example

$$
\begin{array}{rrcl}
 & 110 & \rightarrow & (6)_{10} \\
\times & \underline{101} & \rightarrow & (5)_{10} \\
 & 110 & & \\
+ & 000 & & \\
 & \underline{110} & & \\
= & 11110 & \rightarrow & (30)_{10}
\end{array}
$$

- Up to $2n$ bits may be needed to represent the product of two n-bit numbers.

501

More Examples on Base Arithmetic

- Compute $222 + 222$ in base 3.
  - Answer:
    - $(1221)_3$
- Compute $222 + 222$ in base 4.
  - Answer:
    - $(1110)_4$
- Compute $222 + 222$ in base 5.
  - Answer:
    - $(444)_5$

502

Modular Exponentiation

- In cryptography it is often required to compute
  $b^n \bmod m$
  efficiently.
- Direct computation, that is, computing b^n first and then dividing it by m to find the remainder is impractical (when dealing with very large numbers).
- Example: Compute $3^{644} \bmod 645$.
  - Answer is 36

503

Modular Exponentiation…

Suppose b, n and m are positive integers, and

and that we have computed $b^n \equiv r \pmod{m}$.

That is, $b^n = md + r$. How can we compute $(b^n)^2 \bmod m$?

Observe that $(b^n)^2 = (md + r)^2 = (md)^2 + 2mdr + r^2$.

Thus, the remainder of $(b^n)^2$ divided by m comes from

the remainder of r^2 divided by m. That is,

$(b^n)^2 \bmod m = (b^n \bmod m)^2 \bmod m$.

504

Modular Exponentiation…

- To compute $b^n \bmod m$, first represent n in powers of 2.
  - Example: Compute $3^{644} \bmod 645$,

$$n = 644 = (1010000100)_2 = 2^9 + 2^7 + 2^2$$

$$3^{644} = 3^{(2^9+2^7+2^2)} = 3^{2^9} \times 3^{2^7} \times 3^{2^2}$$

$$3^{644} \bmod 645$$

$$= (3^{2^9} \bmod 645) \times (3^{2^7} \bmod 645) \times (3^{2^2} \bmod 645)$$

$$= 111 \times 396 \times 81 \bmod 645 = 36$$

505

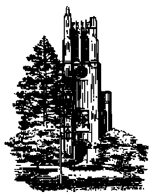
Example

- Computer
  $23^{450} \bmod 987$
  using the fact that:
  - $23^{200} \equiv 739 \bmod 987$
  - $23^{150} \equiv 967 \bmod 987$
  - $23^{100} \equiv 667 \bmod 987$
    - Answer: $23^{450} \bmod 987 \equiv 739*967*667 \bmod 987$
    - $739*967*667 \equiv 883 \bmod 987$
    - $23^{450} \equiv 883 \bmod 987$

506

Primes

Section 4.3



Primes

- Definition: A positive integer $p > 1$ 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*.
  - Note that number 1 is neither prime nor composite.
  - Some primes: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47…
  - How many digits in the largest prime found to-date (2016)?
    - 22,338,618 digits
    - A Mersenne prime = $2^{74,207,281} - 1$

Prime Theorems

- Theorem 1: Every positive integer $n > 1$ has a prime factor $\leq n$. Why?
- Theorem 2: Every positive integer $n > 1$ can be written *uniquely* as a prime or as the product of primes, in non-decreasing order. (proof later)
- Theorem 3: If n is a composite integer, then n has a prime factor $\leq \sqrt{n}$. Why?
- Corollary: If n does not have a prime factor $\leq \sqrt{n}$ then it is prime. Why?
- Conjecture: Every even integer > 2 can be written as the sum of two primes.

Prime Factorization Algorithm

1. Try to find a prime factor of n beginning with 2, 3, 5, … up to $\sqrt{n}$
2. If no prime factor is found, n is prime.
3. If a prime factor p is found, continue by factoring n/p in the same way. Note that n/p doesn't have any prime factor less than p so start with p again.

- Question: For this method, don't we need to know the list of primes?

Example

- Find Prime factors of 3960
  - Dividing by 2: 3960 = 2 x 1960
  - Dividing by 2: 1960 = 2 x 990
  - Dividing by 2: 990 = 2 x 495
  - Dividing by 2: not possible
  - Dividing by 3: 495 = 3 x 165
  - Dividing by 3: 165 = 3 x 55
  - Dividing by 3: not possible
  - Dividing by 5: 55 = 5 x 11
  - So, the answer is : 2x2x2x3x3x5x11= 2^3x3^2x5x11

Example

- Find prime factors of 143
  - Dividing by 2: not possible
  - Dividing by 3: not possible
  - Dividing by 5: not possible
  - Dividing by 7: not possible
  - Dividing by 11: 143 = 11x13

How to find all primes ≤ 100?

- First note that if a number ≤ 100 is composite it has a factor ≤ 10.
- Find all the primes ≤ 10; these are 2, 3, 5, and 7.
- Then eliminate all multiples (other than itself) of 2, all multiples of 3, all multiples of 5, and finally, all multiples of 7.
- All the remaining numbers are primes ≤ 100.
- These are: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, and 97.
- We can now use this list and find all the primes ≤ 10000

513

Question

- Let p be a prime number. Further, let p_1, p_2, …, p_k be all the primes < p. Moreover, let $N = p_1 \times p_2 \times \ldots \times p_k \times p + 1$
  - For example, when $p = 5$, then $N = 2 \times 3 \times 5 + 1 = 31$
- Prove or disprove that N as defined above is always a prime number.
- Disprove: p = 13, N = 2*3*5*7*11*13+1 = 30031= 59*509

514

Infinitude of Primes

- Theorem 4: There are infinitely many primes.
- Proof:
  - What method of proof should we use?
  - We'll do a proof by contradiction as follows:
    - Assume there is a finite number of primes, and let p be the largest (last) prime.
    - Consider the number $N = p! + 1$, that is $N = 1\times2\times3\times4\times \ldots \times(p\text{-}2)\times(p\text{-}1)\times p + 1$
    - Based on Theorem 1, N must have a prime factor (could be itself!)
    - N does not have any non-unity factor ≤ p. WHY?
    - N has a prime factor which is > p.
    - There is a prime > p.
    - A contradiction. Therefore, there infinitely many primes.

515

Prime numbers distribution

- Let $\pi(x)$ be the number of primes ≤ x
- It is known that asymptotically
  $\pi(x) \approx x / \ln x$
- Asymptotically, the x^{th} prime is about $x \ln x$

x	$\pi(x)$	$x / \ln x$
1000	168	145
10000	1229	1086
100000	9592	8686
1000000	78498	72382
10000000	664579	620420
100000000	5761455	5428681

516

Prime theorems…

- Theorem: If n is not prime, then $2^n - 1$ is not prime. In other words, if $2^n - 1$ is prime, so is n. (Note that n being prime does not imply $2^n - 1$ is prime. Try $n = 11$)
- Proof: Let $r > 1$ and $s > 1$ be positive integers. It is known that
  $$x^{r\cdot s} - 1 = (x^s - 1)(x^{s(r-1)} + x^{s(r-2)} + \cdots + x^s + 1)$$
- For example: $x^{3\cdot 2} - 1 = (x^2 - 1)\big(x^{2(3-1)} + x^{2(3-2)} + x^{2(3-3)}\big) = (x^2 - 1)(x^4 + x^2 + 1) = x^6 - 1$
- Therefore, using the above fact, and setting $x = 2$, when $n = r \cdot s$, that is, not prime, then $2^n - 1$ is not prime.

517

More on Primes (Fermat's Little Theorem)

- Consider the following function:
  $f(n) = 2^{n-1}\ mod\ n$
  for prime integers $n > 2$
  - $f(3) = 2^{3\text{-}1}$ mod 3 = 4 mod 3 = 1
  - $f(5) = 2^{5\text{-}1}$ mod 5 = 16 mod 5 = 1
  - $f(7) = 2^{7\text{-}1}$ mod 7 = 64 mod 7 = 1
  - ….
  - $f(89) = 2^{89\text{-}1}$ mod 89 = 618970019642690137449562112 mod 89 = 1
  - …
- Any observation?
  - Holds for every prime, but the converse is not true.
  - $f(341) = 2^{341\text{-}1}$ mod 341 = 1 but 341 = 11x31 is obviously not prime.

518

Greatest Common Divisors

- Definition: Let a and b be integers, not both zero. The largest integer d such that $d \mid a$ and $d \mid b$, is called the *greatest common divisor* of a and b, and is denoted by $d = \gcd(a, b)$.
- How to find gcd?
  - Euclid's Algorithm
  - Using prime factorization

519

Euclid's Algorithm for GCD

1. Input: Positive integers m and n
2. Divide m by n and let r be the remainder
3. If $r = 0$, the algorithm terminates with n as the answer.
4. Set $m \leftarrow n$, followed by set $n \leftarrow r$, and then go to step 2.

520

Example of Euler's GCD algorithm

- Find gcd(252,198)
  - $252 = 1 \times 198 + 54$
  - $198 = 3 \times 54 + 36$
  - $54 = 1 \times 36 + 18$
  - $36 = 2 \times 18$
  - Thus gcd(252, 198) = 18

521

Fact on GCD

- Theorem: Let n and m be positive integers. Then there are integers s and t such that $\gcd(n, m) = sn + tm$
- Proof: Using the next-to-last division in GCD algorithm, and we working our way up we can obtain the desired relation. In the previous example, we would find the following :

522

Example

- Find gcd(252, 198)
  - $252 = 1 \times 198 + 54$
  - $198 = 3 \times 54 + 36$
  - $54 = 1 \times 36 + 18$
  - $36 = 2 \times 18$
- $\gcd(n, m) = sn + tm$
  - $18 = 54 - 1 \times 36 = 54 - 1 \times (198 - 3 \times 54)$
    $= (252 - 1 \times 198) - 1 \times (198 - 3 \times (252 - 1 \times 198))$
    $= 4 \times 252 - 5 \times 198$

523

GCD

- Find the prime factorization of a and b.
  - If $a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$,
    $b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$,
  then
  $\gcd(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \dots p_n^{\min(a_n,b_n)}$
- Example:
  - Find gcd(1000, 625)
    - $1000 = 2 \times 2 \times 2 \times 5 \times 5 \times 5 = 2^3 \times 5^3$
    - $625 = 5 \times 5 \times 5 \times 5 = 5^4 = 2^0 \times 5^4$
    - $\gcd(1000,625) = 2^{\min(0,3)} \times 5^{\min(3,4)} = 2^0 \times 5^3 = 5^3 = 125$

524

Relatively Prime Integers

- Definition: Positive integers a and b are *relatively prime* if $\gcd(a, b) = 1$.
- Definition: Positive integers $a_1, a_2, \ldots, a_n$ are *pairwise relatively prime* if $\gcd(a_i, a_j) = 1$ whenever $1 \le i < j \le n$.

525

Least Common Multiples

- Definition: Let a and b be positive integers. The *least common multiple* of a and b is the smallest positive integer that is divisible by both a and b.
  It is denoted by $\mathrm{lcm}(a, b)$.
  - If $a = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n}$,
    $b = p_1^{b_1} p_2^{b_2} \ldots p_n^{b_n}$, then
    $\mathrm{lcm}(a, b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \ldots p_n^{\max(a_n,b_n)}$
- Find lcm(1000,625)
  - $1000 = 2 \times 2 \times 2 \times 5 \times 5 \times 5 = 2^3 \times 5^3$
  - $625 = 5 \times 5 \times 5 \times 5 = 5^4 = 2^0 \times 5^4$
  - $\mathrm{lcm}(1000,625) = 2^{\max(0,3)} \times 5^{\max(3,4)} = 2^3 \times 5^4 = 5000$

526

Observation

- We computed that:
  - $\gcd(1000,625) = 2^{\min(0,3)} \times 5^{\min(3,4)} = 2^0 \times 5^3 = 5^3 = 125$
  - $\mathrm{lcm}(1000,625) = 2^{\max(0,3)} \times 5^{\max(3,4)} = 2^3 \times 5^4 = 5000$
  - Note that:
    - $\gcd(1000,625) \times \mathrm{lcm}(1000,625) = 125 \times 5000 = 625000$
  - Any observation?

527

gcd and lcm relationship

- Theorem: $\forall a \in Z^+ \; \forall b \in Z^+$
  $$a \times b = \gcd(a, b) \times \mathrm{lcm}(a, b)$$
- Proof:
  - Just use the expressions for gcd and lcm using prime factorizations of a and b.

528

Modulo inverse

- Definition: Let n and $m > 1$ be integers. If there is an integer s such that $n \times s \equiv 1 \pmod{m}$, then we say s is an *inverse* of n.
  - Example:
    - 12 is an inverse of 3 modulo 7 because $12 \times 3 \equiv 1 \pmod{7}$
    - What is inverse of 12 modulo 6?
      - It does not exist

529

Inverse ....

- Theorem: Let n and $m > 1$ be integers. An inverse of n exists *if and only if* n and m are relatively prime.
- Proof outline: Use the theorem that there are integers s and t such that
  $sn + tm = \gcd(m,n) = 1$, or
  $sn + tm \equiv 1 \bmod m$
  Since $tm \equiv 0 \bmod m$, it implies that $sn \equiv 1 \bmod m$.
  Thus n has an inverse.

530

Example

- Find an inverse of 101 modulo 4620
- Solution:
  - Check that gcd(101, 4620) = 1
  - Then find s, and t such that
    - $s101 + t4620 = \gcd(101, 4620) = 1$
    - It turns out that $s = 1601$ and $t = -35$ would work
    - Thus $s = 1601$ is an invers of 101 modulo 4620
      - $1601 \times 101 = 35 \times 4620 + 1$

531

Solving congruence equalities

- Find n, in terms of k, r, and m, that satisfies the following congruence equality,
- $kn \equiv r \pmod{m}$
- $kn = qm + r$
- Find inverse of k modulo m, that is $\bar{k}$, where $k \cdot \bar{k} \equiv 1 \pmod{m}$. This implies $k \cdot \bar{k} \equiv q'm + 1$
- $\bar{k}kn = \bar{k}qm + r\bar{k}$
- $(q'm + 1)n = \bar{k}qm + r\bar{k}$
- $n = \bar{k}qm - q'mn + r\bar{k} \equiv r\bar{k} \pmod{m}$

532

Example

- Find n, in terms of k, r, and m, that satisfies the following congruence equality,
- $4n \equiv 5 \pmod{9}$
  - What is the *solution space* for this problem?
    - $9q + 5$
    - First find an inverse of 4 modulo 9, which is 7.
  - $7 \times 4 \times n \equiv 7 \times 5 \pmod{9}$
  - $n \equiv 8$

533

