CSCI 1900
Discrete Structures

Integers
Reading: Kolman, Section 1.4

Divisibility

- If one integer, n, divides into a second integer, m, without producing a remainder, then we say that "n divides m".
- Denoted n | m
- If one integer, n, does not divide evenly into a second integer, m, i.e., m÷n produces a remainder, then we say that "n does not divide m"
- Denoted $n \nmid m$

Some Properties of Divisibility

- If n | m, then there exists a q such that m = q×n
- The absolute values of both q and n are less than the absolute value of m, i.e., |n| < |m| and |q| < |m|
- Examples:
  4 | 24: 24 = 4×6 and both 4 and 6 are less than 24.
  5 | 135: 135 = 5×27 and both 5 and 27 are less than 135
- Simple properties of divisibility (proofs on page 21)
  - If a | b and a | c, then a | (b + c)
  - If a | b and a | c, where b > c, then a | (b - c)
  - If a | b or a | c, then a | bc
  - If a | b and b | c, then a | c

Prime Numbers

- A number *p* is called prime if the only positive integers that divide *p* are *p* and 1.
- Examples of prime numbers: 2, 3, 5, 7, 11, and 13.
- There is a science to determining prime numbers. The following slides present some computer algorithms that can be used to determine if a number n>1 is prime.

Basic Primer Number Algorithm

1. First, check if n=2. If it is, n is prime. Otherwise, proceed to step 2.
2. Check to see if each integer k is a divisor of n where $1<k\leq(n-1)$. If none of the values of k are divisors of n, then n is prime

Better Prime Number Algorithm

Note that if n=mk, then either m or k is less than √n. Therefore, we don't need to check for values of k greater than √n.

1. First check if n=2. If it is, n is prime. Otherwise, proceed to step 2.
2. Check to see if each integer k is a divisor of n where $1<k\leq\sqrt{n}$. If none of the values of k are divisors of n, then n is prime

Even Better Prime Number Algorithm

Note that if k | n, and k is even, then 2 | n. Therefore, if 2 does not divide n, then no even number can be a divisor of n. (If a | b and b | c, then a | c)

1. First check if n=2. If it is, n is prime. Otherwise, proceed to step 2.
2. Check if 2 | n. If so, n is not prime. Otherwise, proceed to step 3.
3. Check to see if each ***odd*** integer k is a divisor of n where $1<k\leq\sqrt{n}$. If none of the values of k are divisors of n, then n is prime.

$Even^2$ Better Prime Number Algorithm

Note that if k | n, and d | k, then d | n. Therefore, if d does not divide n, then no multiple of d can be a divisor of n.

1. First check if n=2. If it is, n is prime. Otherwise, proceed to step 2.
2. Use a sequence k = 2, 3, 5, 7, 11, 13, 17, … up to $\sqrt{n}$ to check if k | n. If none are the values of k are divisors of n, then n is prime. (Note that list is a list of prime numbers!)

Factoring a Number into its Primes

- Dividing a number into its multiples over and over again until the multiples cannot be divided any longer shows us that any number can eventually be broken down into prime numbers.
- Examples:
  $9 = 3 \cdot 3 = 3^2$
  $24 = 8 \cdot 3 = 2 \cdot 2 \cdot 2 \cdot 3 = 2^3 \cdot 3$
  $315 = 3 \cdot 105 = 3 \cdot 3 \cdot 35 = 3 \cdot 3 \cdot 5 \cdot 7 = 3^2 \cdot 5 \cdot 7$
- Basically, this means that any number can be broken into multiples of prime numbers.

Factoring into Primes (continued)

Each row of the table below presents a different number factored into its primes. The numbers in the columns represent the number of each particular prime can be factored out of each original value.

	2	3	5	7	11	13	17	
540	2	3	1	0	0	0	0	
85	0	0	1	0	0	0	1	
96	5	1	0	0	0	0	0	
315	0	2	1	1	0	0	0	

Factoring into Primes (continued)

- Every positive integer n > 1 can be broken into multiples of prime numbers.
- $n = p_1^{k1} p_2^{k2} p_3^{k3} p_4^{k4} \ldots p_s^{ks}$
  $p_1 < p_2 < p_3 < p_4 < \ldots < p_s$

Methods for Factoring

- 2 | n → If least significant digit of n is divisible by 2 (i.e., n is even), then 2 divides n
- 3 | n → If the sum of all the digits of n down to a single digit equals 3, 6, or 9, then 3 divides n. For example, is 17,587,623 divisible by 3?

  1 + 7 + 5 + 8 + 7 + 6 + 2 + 3 = 39
  3 + 9 = 12
  1 + 2 = 3 → YES! 3 divides 17,587,623

Methods for Factoring (continued)

- Does 7 divide n?
  - Remove least significant digit (one's place) from n and multiply it by two.
  - Subtract the doubled number from the remaining digits.
  - If result is divisible by 7, then original number was divisible by 7
  - Repeat if unable to determine from result.

Methods for Factoring (continued)

Examples of checking for divisibility by 7

- 1,876 → 187 – 12 = 175 → 17 – 10 = 7 ✓
- 4,923 → 492 – 6 = 486 → 48 – 12 = 36 ×
- 34,461 → 3,446 – 2 = 3,444 → 344 – 8 = 336 → 33 – 12 = 21 ✓

Methods for Factoring (continued)

- Does 11 divide n?
  - Starting with the most significant digit of n, adding the first digit, subtracting the next digit, adding the third digit, subtracting the fourth, and so on. If the result is 0 or a multiple of 11, then the original number is divisible by 11.
  - Repeat if unable to determine from result.

Methods for factoring (continued)

Examples of checking for divisibility by 11

- 285311670611 → 2 – 8 + 5 – 3 + 1 – 1 + 6 – 7 + 0 – 6 + 1 – 1 = –11 ✓
- 279048 → 2 – 7 + 9 – 0 + 4 – 8 = 0 ✓

Methods for Factoring (continued)

- Does 13 divide n?
  - Delete the last digit (one's place) from n.
  - Subtract nine times the deleted digit from the remaining number.
  - If what is left is divisible by 13, then so is the original number.
  - Repeat if unable to determine from result.

General Observation of Integers

- If n and m are integers and $n > 0$, we can write $m = qn + r$ for integers q and r with $0 \leq r < n$.
- For specific integers m and n, there is only one set of values for q and for r.
- If $r = 0$, then m is a multiple of n, i.e., $n \mid m$.

Examples of m = qn + r

- If n is 3 and m is 16, then 16 = 5(3) + 1 so q = 5 and r = 1
- If n is 10 and m is 3, then 3 = 0(10) + 3 so q = 0 and r = 3
- If n is 5 and m is –11, then – 11 = – 3(5) + 4 so q = – 3 and r = 4

Greatest Common Divisor

- If a, b, and k are in Z+, and k | a and k | b, we say that k is a ***common divisor***.
- If d is the largest such k, d is called the ***greatest common divisor*** (GCD).
- d is a multiple of every k, i.e., every k divides d.

GCD Example

Find the GCD of 540 and 315:

- $540 = 2^2 \cdot 3^3 \cdot 5$
- $315 = 3^2 \cdot 5 \cdot 7$
- 540 and 315 share the divisors 3, 3^2, 5, 3·5, and $3^2 \cdot 5$ (Look at it as the number of possible ways to combine 3, 3, and 5)
- The largest is the GCD → $3^2 \cdot 5 = 45$
- 315÷45 = 7 and 540÷45=12

Theorems of the GCD

Assume d is GCD(a, b)

- d = sa + tb for some integers s and t. (s and t are not necessarily positive.)
- If c is any other common divisor of a and b, then c | d
- If d is the GCD(a, b), then d | a and d | b
- Assume d is the GCD(a, b). If c | a and c | b, then c | d
- There is a horrendous proof of these theorems on page 22 of our textbook. You are not responsible for this proof!

GCD Theorem

- If a and b are in Z^+, a>b, then GCD(a,b) = GCD(a, a$\pm$b)
- If c divides a and b, it divides a$\pm$b (this is from the earlier “divides” theorems)
- Since b = a-(a-b) = -a+(a+b), then a common divisor of a and (a$\pm$b) also divides a and b
- Since all c that divide a or b must also divide b and b$\pm$a, then they have the same complete set of divisors and therefore the same GCD.

Euclidean Algorithm

- The Euclidean Algorithm is a recursive algorithm that can be used to find GCD (a, b)
- It is based on the fact that for any two integers, a > b, there exists a k and r such that:

$$a = k \cdot b + r$$

- Since if a | b and a | c, then a | (b + c), then we know that the GCD (a,b) must also divide r. Therefore, the GCD (a,b) = GCD(b,r)

Euclidean Algorithm Process

- For two integers a and b where a > b > 0
  $a = k_1 b + r_1$, where k_1 is in Z+ and $0 \leq r_1 < b$
- If $r_1 = 0$, then b | a and b the is GCD(a, b)
- If $r_1 \neq 0$, then if some integer n divides a and b, then it must also divide r_1. Similarly, if n divides b and r_1, then it must divide a.
- Go back to top substituting b for a and r_1 for b. Repeat until $r_n = 0$ and k_n will be GCD

Least Common Multiple

- If a, b, and k are in Z+, and a | k, b | k, we say that k is a common multiple of a and b.
- The smallest such k, call it c, is called the least common multiple or LCM of a and b
- We write c = LCM(a,b)

Deriving the LCM

- We can obtain LCM from a, b, and GCD(a,b)
- For any integers a and b, we can write $a = p_1^{a1} p_2^{a2} \ldots p_k^{ak}$ and $b = p_1^{b1} p_2^{b2} \ldots p_k^{bk}$
- $\text{GCD}(a,b) = p_1^{\min(a1,b1)} p_2^{\min(a2,b2)} \ldots p_k^{\min(ak,bk)}$
- $\text{LCM}(a,b) = p_1^{\max(a1,b1)} p_2^{\max(a2,b2)} \ldots p_k^{\max(ak,bk)}$
- Since, $\text{GCD}(a,b)\cdot\text{LCM}(a,b) = p_1^{(a1+b1)} p_2^{(a2+b2)} \ldots p_k^{(ak+bk)}$
  $= p_1^{a1} p_1^{b1} p_2^{a2} p_2^{b2} \ldots p_k^{ak} p_k^{bk}$
  $= a\cdot b$
- Therefore, LCM(a,b) = a·b/GCD(a,b)

Mod-n function

- If z is a nonnegative integer, the mod-n function, $f_n(z)$, is defined as $f_n(z) = r$ if $z = qn + r$
- For example:
  $f_3(14) = 2$ because $14 = 4\cdot 3 + 2$
  $f_7(153) = 6$ because $153 = 21\cdot 7 + 6$

Representation of integers

- We are used to decimal, but in reality, it is only one of many ways to describe an integer
- We say that a decimal value is the ***"base 10 expansion of n"*** or the ***"decimal expansion of n"***
- If b>1 is an integer, then every positive integer n can be uniquely expressed in the form:
  $n = d_k b^k + d_{k-1} b^{k-1} + d_{k-2} b^{k-2} + \ldots + d_1 b^1 + d_0 b^0$
  where $0 \leq d_i < b$, i = 0, 1, …, k

Proof that There is Exactly One Base Expansion

- Proof is on bottom of page 27
- Basis of proof is that $n = d_k b^k + r$
- If $d_k > b^k$, then k was not the largest non-negative integer so that $b^k \leq n$.
- If $r \geq b^k$, then d_k isn't large enough
- Go back to 1 replacing n with r. This time, remember that k = k-1, because r must be less than b^k
- Repeat until k=0.

Quick way to determine ***base b expansion of n***

- Note that d_0 is the remainder after dividing n by b.
- Note also that once n is divided by b, quotient is made up of:

  $(n-r)/b = (d_k b^{k-1}\ d_{k-1} b^{k-2} + d_{k-2} b^{k-3} + \ldots\ + d_1)$

  Therefore, we can go back to step 1 to determine d_1

Example: Determine base 5 expansion of decimal 432

- 432 = 86*5 + 2 (remainder is d_0 digit)
- 86 = 17*5 + 1 (remainder is d_1 digit)
- 17 = 3*5 + 2 (remainder is d_2 digit)
- 3 = 0*5 + 3 (remainder is d_3 digit)
- $432_{10} = 3212_5$
- Verify this using powers of 5 expansion:

  $3212_5 = 3\cdot5^3 + 2\cdot5^2 + 1\cdot5^1 + 2\cdot5^0$
  $= 3\cdot125 + 2\cdot25 + 1\cdot5 + 2\cdot1$
  $= 375 + 50 + 5 + 2$
  $= 423$

Example: Determine base 8 expansion of decimal 704

- 704 = 88*8 + 0 (remainder is d_0 digit)
- 88 = 11*8 + 0 (remainder is d_1 digit)
- 11 = 1*8 + 3 (remainder is d_2 digit)
- 1 = 0*8 + 1 (remainder is d_3 digit)
- $704_{10} = 1300_8$
- Verify this using powers of 8 expansion:

  $3212_5 = 1\cdot8^3 + 3\cdot8^2 + 0\cdot8^1 + 0\cdot8^0$
  $= 1\cdot512 + 3\cdot64 + 0\cdot8 + 0\cdot1$
  $= 512 + 192$
  $= 704_{10}$