Discrete Math for Computing

Ch 4.3 Primes and Greatest Common Divisors

- Primes
- What is a prime number?

Positive integers that have exactly two different positive integer factors are called primes

- A positive integer p > 1 is called prime

  if the only positive factors of p are 1 and p

- A positive integer > 1 and is not prime is called composite

Primes and Greatest Common Divisors

- Example: Is integer 5 prime?
- Yes
- Because its only positive factors are 1 and 5

- What about integer 9?
- No
- Because it is divisible by 3

Primes and Greatest Common Divisors

- The Fundamental Theorem of Arithmetic
- Every positive integer > 1

  - can be written uniquely as a prime

  - or as the product of two or more primes

  - where the prime factors are written

  - in order of non-decreasing size

Primes and Greatest Common Divisors

- Example: What is the prime factorization of 100, 641, 999, and 1024
- 100

  $= 2.2.5.5 = 2^2.5^2$
- 641

  $= 641$
- 999

  $= 3.3.3.37 = 3^3.37$
- 1024

  $= 2.2.2.2.2.2.2.2.2.2 = 2^{10}$

Primes and Greatest Common Divisors

- If n is a composite integer, then n has a prime factor less than or equal to $\sqrt{n}$.
- Example - Show that 101 is prime.
- The square root of is ≈ 10.05. The primes ≤ 10.05 are 2, 3, 5, and 7. But 101 is not evenly divisible by 2, 3, 5, or 7. Thus, 101 must itself be a prime number.

UTD

Distribution of Primes

- Mathematicians have been interested in the distribution of prime numbers among the positive integers
- In the nineteenth century, the *prime number theorem* was proved which gives an asymptotic estimate for the number of primes not exceeding *x*.

Distribution of Primes

- The Prime Number Theorem

The ratio of the number of primes not exceeding x and x/ln x approaches 1 as x grows without bound

If a random number nearby some large number N is selected,

the chance of it being prime is about 1 / ln(N),

where ln(N) denotes the natural logarithm of N

Distribution of Primes

- The Prime Number Theorem

  Example:

  Near N = 10,000

  about one in every ln(10000) = 9 numbers is prime

  Near N = 1,000,000,000

  one in every ln(1000000000) = 21 numbers is prime

  The average gap between prime numbers near N is roughly ln(N)

Primes and Greatest Common Divisors

- Claims about Primes
- Marin Mersenne – France
- In 1644, claimed that $2^p - 1$ (Mersenne Primes)

  is prime for p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257

  is composite for all other primes less than 257
- Took over 300 years to disprove him

  Not prime for p = 67, 257

  Prime for p = 61, 87, 107

Primes and Greatest Common Divisors

- Do you know what is the largest known prime number?
- The 49th Mersenne prime, $2^p - 1$

Twin Prime Conjecture

Conjectures about Primes – Even though primes have been studied extensively for centuries, many conjectures about them are unresolved

- Twin primes are primes that differ by 2

  3 and 5, 5 and 7, 11 and 13

- Twin Prime Conjecture – asserts that there are infinitely many twin primes

- What is the world's record for twin primes (early 2006)?

- $16{,}869{,}987{,}339{,}975.2^{171{,}960} \pm 1$

  numbers with 51,779 digits

UTD

Primes and Greatest Common Divisors

- Greatest Common Divisors
- Let a and b be integers, $a \neq 0$, $b \neq 0$
- Greatest Common Divisor

  - The largest integer d such that $d \mid a$ and $d \mid b$
- Denoted by gcd(a, b)
- To find the gcd of two integers, find all the positive common integers of both integers
- Take the largest divisor

Primes and Greatest Common Divisors

- Example: What is the greatest common divisor of 24 and 36?
- The positive common divisors of 24 and 36 are:
- 1, 2, 3, 4, 6, and 12

$\therefore$ gcd(24, 36) = 12

What is the greatest common divisor of 5 and 7?

There are no positive common divisors other than 1

$\therefore$ gcd(5, 7) = 1

UTD

Primes and Greatest Common Divisors

- Two integers a and b are relatively prime

  if their greatest common divisor is 1

  Example: Integers 5 and 7

- The integers a_1, a_2, ..., an are pairwise relatively prime

  if $\gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$

Primes and Greatest Common Divisors

- Example: Determine whether the integers 10, 17, and 21 are pairwise relatively prime.
- gcd(10, 17) = 1
- gcd(17, 21) = 1
- gcd(10, 21) = 1

Integers 10, 17, and 21 are pairwise relatively prime

Primes and Greatest Common Divisors

Example: Are 10, 19, 24 pairwise relatively prime?

gcd(10, 19) = 1

gcd(19, 24) = 1

gcd(10, 24) = 2

Since gcd(10, 24) = 2, these numbers are *not* pairwise relatively prime.

Primes and Greatest Common Divisors

- To find greatest common divisor of two integers use the prime factorization of these integers.
- For any two integers 'a' and 'b', a ≠ 0, b ≠ 0

$$a = p_1^{a1} p_2^{a2} \ldots p_n^{an}, \quad b = p_1^{b1} p_2^{b2} \ldots p_n^{bn}$$

each exponent is a nonnegative integer, all primes are included

The gcd(a,b) = $p_1^{\min(a1,b1)} p_2^{\min(a2,b2)} \ldots p_n^{\min(an,bn)}$

min(x, y) = the minimum of two numbers x and y

Primes and Greatest Common Divisors

- Find gcd(120, 500).
- Let's solve this in two ways. First method:
- The positive divisors of 120 are: 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60
- The positive divisors of 500 are: 2, 4, 5, 10, 20, 25, 50, 100, 125, 250
- The common divisors of 120 and 150 are: 2, 4, 5, 10, and 20
- The greatest common divisor is 20

Primes and Greatest Common Divisors

- Find gcd(120, 500).
- $120 = 2^3.3.5$
- $500 = 2^2.5^3$
- gcd(120, 500)

  $= 2^{\min(3,\ 2)}3^{\min(1,0)}5^{\min(1,\ 3)}$

  $= 2^2 3^0 5^1 = 20$

Primes and Greatest Common Divisors

- Least Common Multiple
- Let a and b be integers, $a \neq 0$, $b \neq 0$
- Least common multiple

  - The smallest integer ‘d’ divisible by both ‘a’ and ‘b’
- Denoted by lcm(a, b)

Primes and Greatest Common Divisors

- Least Common Multiple

Example: What is the lcm of 6 and 15?

Certainly 90 (6 x 15) is divisible by both 6 and 15

but is there a smaller number divisible by both?

Yes: 30

Primes and Greatest Common Divisors

- To find least common multiple of two integers use the prime factorization of these integers.
- For any two integers 'a' and 'b', a ≠ 0, b ≠ 0

$$a = p_1^{a1} p_2^{a2} \dots p_n^{an}, \quad b = p_1^{b1} p_2^{b2} \dots p_n^{bn}$$

each exponent is a nonnegative integer, all primes are included

The lcm(a,b) = $p_1^{\max(a1,b1)} p_2^{\max(a2,b2)} \dots p_n^{\max(an,bn)}$

max(x, y) = the maximum of two numbers x and y

Primes and Greatest Common Divisors

- Example: What is the least common multiple of $2^3 3^5 7^2$ and $2^4 3^3$?
- $\text{lcm}(2^3 3^5 7^2, 2^4 3^3)$

  $= 2^{\max(3,\ 4)} 3^{\max(5,\ 3)} 7^{\max(2,\ 0)}$

  $= 2^4 3^5 7^2$

Relationship between gcd and lcm

- If *a* and *b* are positive integers, then

$$ab = \gcd(a,b) \bullet \operatorname{lcm}(a,b)$$

- Example:

$$\gcd(120, 500) \bullet \operatorname{lcm}(120, 500)$$

$$= 20 \bullet 3000$$

$$= 60000$$

$$= 120 \bullet 500$$

Integers and Algorithms

- The Euclidean Algorithm
- More efficient – greatest common divisor
- Time consuming to find prime factorization
- Greek mathematician Euclid, ancient times

Let $a = bq + r$, where a, b, q, r are integers.

$$\gcd(a, b) = \gcd(b, r)$$

where ‘r’ is the last nonzero remainder

$O(\log b)$ divisions

Euclidean Algorithm

- The Euclidean algorithm is an efficient method for computing the greatest common divisor of two integers. It is based on the idea that gcd(a,b) is equal to gcd(a,c) when $a > b$ and c is the remainder when a is divided by b.

Example: Find gcd(91, 287):

- $287 = 91 \cdot 3 + 14$ Divide 287 by 91
- $91 = 14 \cdot 6 + 7$ Divide 91 by 14
- $14 = 7 \cdot 2 + 0$ Divide 14 by 7

Stopping condition

gcd(287, 91) = gcd(91, 14) = gcd(14, 7) = 7

Integers and Algorithms

- ALGORITHM: The Euclidean Algorithm

```
procedure gcd(a, b: positive integers)
x := a
y := b
while y ≠ 0
begin
    r := x mod y
    x := y
    y := r
end {gcd(a, b) is x}
```

Integers and Algorithms

- Example: Find the greatest common divisor of 414 and 662 using the Euclidean algorithm.

  662 = 414.1 + 248

  414 = 248.1 + 166

  248 = 166.1 + 82

  166 = 82.2 + 2

  82 = 2.41

gcd(414, 662) = 2, last nonzero remainder

gcds as Linear Combinations

Bézout's Theorem: If a and b are positive integers, then there exist integers s and t such that gcd(a,b) = $sa + tb$.

Definition: If a and b are positive integers, then integers s and t such that gcd(a,b) = $sa + tb$ are called *Bézout coefficients* of a and b. The equation gcd(a,b) = $sa + tb$ is called *Bézout's identity.*

- By Bézout's Theorem, the gcd of integers a and b can be expressed in the form $sa + tb$ where s and t are integers. This is a *linear combination* with integer coefficients of a and b.

  gcd(6,14) = $(-2)\cdot 6 + 1\cdot 14$

Finding gcds as Linear Combinations

Example: Express gcd(252,198) = 18 as a linear combination of 252 and 198.

Solution: First use the Euclidean algorithm to show gcd(252,198) = 18

i. $252 = 1 \cdot 198 + 54$
ii. $198 = 3 \cdot 54 + 36$
iii. $54 = 1 \cdot 36 + 18$
iv. $36 = 2 \cdot 18$

- Now working backwards, from iii and i above
  - $18 = 54 - 1 \cdot 36$
  - $36 = 198 - 3 \cdot 54$
- Substituting the 2nd equation into the 1st yields:
  - $18 = 54 - 1 \cdot (198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198$
- Substituting $54 = 252 - 1 \cdot 198$ (from i)) yields:
  - $18 = 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198$

- This method illustrated above is a two pass method. It first uses the Euclidean algorithm to find the gcd and then works backwards to express the gcd as a linear combination of the original two integers.