Number Theory

Computer Science & Engineering 235: Discrete Mathematics

Christopher M. Bourke
cbourke@cse.unl.edu

Integer Division I

When talking about division over the integers, we mean division with no remainder.

Definition

Let $a, b \in \mathbb{Z}, a \neq 0$, we say that a *divides* b if there exists $c \in \mathbb{Z}$ such that $b = ac$. We denote this, $a \mid b$ and $a \nmid b$ when a does not divide b. When $a \mid b$, we say a is a *factor* of b.

Integer Division II

Theorem

Let $a, b, c \in \mathbb{Z}$ then

1. *If $a \mid b$ and $a \mid c$ then $a \mid (b + c)$.*
2. *If $a \mid b$, then $a \mid bc$ for all $c \in \mathbb{Z}$.*
3. *If $a \mid b$ and $b \mid c$, then $a \mid c$.*

proofs?

Integer Division III

Corollary

If $a, b, c \in \mathbb{Z}$ such that $a \mid b$ and $a \mid c$ then $a \mid mb + nc$ for $n, m \in \mathbb{Z}$.

Primes I

Definition

A positive integer $p > 1$ is called *prime* if its only positive factors are 1 and p. If a positive integer is not prime, it is called *composite*

Primes II

Theorem (Fundamental Theorem of Arithmetic)

Every positive integer $n > 1$ can be written uniquely as a prime or as the product of the powers of two or more primes written in nondecreasing size.

That is, for every $n \in \mathbb{Z}, n > 1$, can be written as

$$n = {p_1}^{k_1} {p_2}^{k_2} \cdots {p_l}^{k_l}$$

where each p_i is a prime and each $k_i \geq 1$ is a positive integer.

Sieve of Eratosthenes
Preliminaries

Given a positive integer, $n > 1$, how can we determine if n is prime or not?

The Seive of Eratosthenes ("siv of air-o-toss-ten-ees", Greek mathematician, 276 - 195 BCE) provides a brute-force primality test.

Lemma

If n is a composite integer, then n has a prime divisor $x \leq \sqrt{n}$.

Sieve of Eratosthenes
Preliminaries

Proof.

- Let n be a composite integer.
- By definition, n has a prime divisor a with $1 < a < n$, thus $n = ab$.
- Its easy to see that either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$. Otherwise, if on the contrary, $a > \sqrt{n}$ *and* $b > \sqrt{n}$, then

$$ab > \sqrt{n}\sqrt{n} = n$$

- Finally, either a or b is prime divisor or has a factor that is a prime divisor by the Fundamental Theorem of Arithmetic, thus n has a prime divisor $x \leq \sqrt{n}$.

□

Sieve of Eratosthenes
Algorithm

This result gives us an obvious algorithm. To determine if a number n is prime, we simple must test every prime number p with $2 \leq p \leq \sqrt{n}$.

SIEVE

```
   INPUT          : A positive integer n ≥ 4.
   OUTPUT         : true if n is prime.
1  FOREACH prime number p, 2 ≤ p ≤ √n DO
2      IF p | n THEN
3          output false
4      END
5  END
6  output true
```

Sieve of Eratosthenes
Efficiency?

- Sieve is old, but correct
- Efficiency?
- The outer for-loop runs for every prime $p \leq \sqrt{n}$.
- Assume that we get such a list *for free*. The loop still executes about

$$\frac{\sqrt{n}}{\ln \sqrt{n}}$$

  times (see distribution of primes; next topic).
- Assume also that division is our elementary operation.
- Then the algorithm is $\mathcal{O}(\sqrt{n})$
- Is this polynomial?
- What is the actual *input size*?

Sieve of Eratosthenes
Efficiency?

- Input is a *number*, input size is the *representation* of that number
- Number of bits to represent n: $\lceil \log(n) \rceil$
- Let $N = \log(n)$
- Then $n = 2^N$, so

$$\sqrt{n} = \sqrt{2^N}$$

- Thus the Sieve is exponential in the input size N.

The Sieve also gives an algorithm for determining the *prime factorization* of an integer. To date, no one has been able to produce an algorithm that runs in sub-exponential time. The hardness of this problem is the basis of *public-key cryptography*.

Sieve of Eratosthenes I
Primality Testing

Take note of the difference between the two problems—primality is a *decision* problem; we try to determine if the answer is "yes" or "no". However, factorization is a *functional* problem, we are actually trying to *find* a number; a factor.

Numerous algorithms for primality testing have been developed over the last 50 years, including randomized algorithms, probabilistic algorithms and algorithms based on unproven, but widely accepted conjectures.

Sieve of Eratosthenes II

Primality Testing

In 2002, three Indian computer scientists developed the first *deterministic polynomial-time* algorithm for primality testing, running in time $\mathcal{O}(\log^{12}(n))$.

M. Agrawal and N. Kayal and N. Saxena. PRIMES is in P. *Annals of Mathematics*, 160(2):781-793, 2004.

Available at http://projecteuclid.org/Dienst/UI/1.0/Summarize/euclid.annm/1111770735

How Many Primes?

How many primes are there?

Theorem

There are infinitely many prime numbers.

The proof is a simple proof by contradiction.

How Many Primes?

Proof

Proof.

- Assume to the contrary that there are a finite number of primes, $p_1, p_2, \ldots, p_n$.
- Let
$$Q = p_1 p_2 \cdots p_n + 1$$
- By the FTA, Q is either prime (in which case we are done) or Q can be written as the product of two or more primes.
- Thus, one of the primes p_j $(1 \leq j \leq n)$ must divide Q, but then if $p_j \mid Q$, it must be the case that
$$p_j \mid Q - p_1 p_2 \cdots p_n = 1$$
- Since this is not possible, we've reached a contradiction—there are not finitely many primes.

Distribution of Prime Numbers

Theorem

The ratio of the number of prime numbers not exceeding n and $\frac{n}{\ln n}$ approaches 1 as $n \to \infty$.

In other words, for a fixed natural number, n, the number of primes not greater than n is about

$$\frac{n}{\ln n}$$

Mersenne Primes I

A *Mersenne* prime is a prime number of the form

$$2^k - 1$$

where k is a positive integer. They are related to *perfect numbers* (if M_n is a Mersenne prime, $\frac{M_n(M_n+1)}{2}$ is perfect).

Perfect numbers are numbers that are equal to the sum of their proper factors, for example $6 = 1 \cdot 2 \cdot 3 = 1 + 2 + 3$ is perfect.

Mersenne Primes II

It is an open question as to whether or not there exist odd perfect numbers. It is also an open question whether or not there exist an infinite number of Mersenne primes.

Such primes are useful in testing suites for large super computers.

As of February 2013, 48 Mersennne primes have been found, largest:

$$2^{57,885,161} - 1$$

Distribution of Prime Numbers I

Extended Riemann Hypothesis

One of the most important open conjectures about primes is the *Riemann Hypothesis*.

In 1859, Riemann conjectured that the frequency of primes is closely related to the Riemann zeta function,

$$\zeta(s) = 1 + \left(\frac{1}{2}\right)^s + \left(\frac{1}{3}\right)^s + \left(\frac{1}{4}\right)^s + \cdots$$

His conjecture asserts that all non-trivial solutions to $\zeta(s) = 0$ lie on a *critical line*, $\frac{1}{2} + ti$ with i imaginary and $t \in \mathbb{R}$.

Distribution of Prime Numbers II

Extended Riemann Hypothesis

To date, no one has proven the conjecture, but it has been verified for very large numbers.

Because of this, it is one of the Clay Mathematics Institutes's *Millennium Problems*. Anyone who comes up with a correct, accepted proof will receive $1,000,000.

Future Work?

The study of primes continues to be an active research area. Recently, it was shown that the primes contain arbitrarily long arithmetic progressions; sequences of the form

$$\{p + kd\}_{k=1}^{\infty}$$

Ben Green and Terence Tao. The primes contain arbitrarily long arithmetic progressions. In arXiv: http://arxiv.org/abs/math.NT/0404188, April 2004.

Division

Theorem (The Division "Algorithm")

Let $a \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$ then there exists unique integers q, r with $0 \leq r < d$ such that

$$a = dq + r$$

Some terminology:

- d is called the *divisor*.
- a is called the *dividend*.
- q is called the *quotient*.
- r is called the *remainder*.

We use the following notation:

$$\begin{aligned} q &= a \ \mathbf{div}\ d \\ r &= a \ \mathbf{mod}\ d \end{aligned}$$

Greatest Common Divisor I

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. It is denoted

$$\gcd(a, b)$$

The $\gcd$ is always guaranteed to exist since the set of common divisors is finite. Recall that 1 is a divisor of any integer. Also, $\gcd(a, a) = a$, thus

$$1 \leq \gcd(a, b) \leq \min\{a, b\}$$

Definition

Greatest Common Divisor II

Two integers a, b are called *relatively prime* if

$$\gcd(a, b) = 1$$

Sometimes, such integers are called *coprime*.

Example

- $\gcd(60, 210) = 30$
- $\gcd(7, 49) = 7$
- $\gcd(7, 59) = 1$
- $\gcd(7, 60) = 1$

Greatest Common Divisor III

There is natural generalization to a set of integers.

Definition

Integers $a_1, a_2, \ldots, a_n$ are *pairwise relatively prime* if $\gcd(a_i, a_j) = 1$ for $i \neq j$.

Greatest Common Divisor

Computing

The $\gcd$ may be found by finding the prime factorization of two numbers.

Let

$$\begin{aligned} a &= p_1{}^{a_1} p_2{}^{a_2} \cdots p_n{}^{a_n} \\ b &= p_1{}^{b_1} p_2{}^{b_2} \cdots p_n{}^{b_n} \end{aligned}$$

Where each power is a nonnegative integer (if a prime is not a divisor, then the power is 0).

Then the $\gcd$ is simply

$$\gcd(a, b) = p_1^{\min\{a_1, b_1\}} p_2^{\min\{a_2, b_2\}} \cdots p_n^{\min\{a_n, b_n\}}$$

Greatest Common Divisor

Examples

Example

What is the $\gcd(6600, 12740)$?

The prime decompositions are

$$\begin{aligned} 6600 &= 2^3 3^1 5^2 7^0 11^1 13^0 \\ 12740 &= 2^2 3^0 5^1 7^2 11^0 13^1 \end{aligned}$$

So we have

$$\begin{aligned} \gcd(6600, 12740) &= 2^{\min\{2,3\}} 3^{\min\{0,1\}} 5^{\min\{1,2\}} 7^{\min\{0,2\}} \\ &\quad 11^{\min\{0,1\}} 13^{\min\{0,1\}} \\ &= 2^2 3^0 5^1 7^0 11^0 13^0 \\ &= 20 \end{aligned}$$

Least Common Multiple

Definition

The *least common multiple* of positive integers a, b is the smallest positive integer that is divisible by both a and b. It is denoted

$$\operatorname{lcm}(a, b)$$

The lcm may be computed similar to $\gcd$ using prime decomposition: use the $\max$ rather than the $\min$ of powers.

$$\operatorname{lcm}(a, b) = p_1^{\max\{a_1, b_1\}} p_2^{\max\{a_2, b_2\}} \cdots p_n^{\max\{a_n, b_n\}}$$

Least Common Multiple

Example

Example

What is the $\operatorname{lcm}(6600, 12740)$?

Again, the prime decompositions are

$$\begin{aligned} 6600 &= 2^3 3^1 5^2 7^0 11^1 13^0 \\ 12740 &= 2^2 3^0 5^1 7^2 11^0 13^1 \end{aligned}$$

So we have

$$\begin{aligned} \operatorname{lcm}(6600, 12740) &= 2^{\max\{2,3\}} 3^{\max\{0,1\}} 5^{\max\{1,2\}} 7^{\max\{0,2\}} \\ &\quad 11^{\max\{0,1\}} 13^{\max\{0,1\}} \\ &= 2^3 3^1 5^2 7^2 11^1 13^1 \\ &= 4,204,200 \end{aligned}$$

Intimate Connection

There is a very close connection between the $\gcd$ and lcm.

Theorem

Let $a, b \in \mathbb{Z}^+$, then

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

Proof?

Congruences
Definition

Often, rather than the quotient, we are only interested in the remainder of a division operation. We introduced the notation before, but we formally define it here.

Definition

Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. Then a is *congruent to b modulo m* if m divides $a - b$. We use the notation

$$a \equiv b (\mathrm{mod}\ m)$$

If the congruence does not hold, we write $a \not\equiv b (\mathrm{mod}\ m)$

Congruences
Another Characterization

An equivalent characterization can be given as follows.

Theorem

Let $m \in \mathbb{Z}^+$. Then $a \equiv b (\mathrm{mod}\ m)$ if and only if there exists $q \in \mathbb{Z}$ such that

$$a = qm + b$$

i.e. a quotient q.

Congruences
Properties

Theorem

Let $a, b \in \mathbb{Z}, m \in \mathbb{Z}^+$. Then,

$$a \equiv b (\mathrm{mod}\ m) \iff a \bmod m = b \bmod m$$

Theorem

Let $m \in \mathbb{Z}^+$. If $a \equiv b (\mathrm{mod}\ m)$ and $c \equiv d (\mathrm{mod}\ m)$ then

$$a + c \equiv b + d (\mathrm{mod}\ m)$$

and

$$ac \equiv bd (\mathrm{mod}\ m)$$

Modular Arithmetic
Example

Example

- $36 \equiv 1 (\mathrm{mod}\ 5)$ since the remainder of $\frac{36}{5}$ is 1.
- Similarly, $-17 \equiv -1 (\mathrm{mod}\ 2)$, $-17 \equiv 1 (\mathrm{mod}\ 2)$, $-17 \equiv 3 (\mathrm{mod}\ 2)$, etc.
- However, we prefer to express congruences in lowest positive terms: $0 \leq b < m$
- $64 \equiv 0 (\mathrm{mod}\ 2)$, $64 \equiv 1 (\mathrm{mod}\ 3)$, $64 \equiv 4 (\mathrm{mod}\ 5)$, $64 \equiv 4 (\mathrm{mod}\ 6)$, $64 \equiv 1 (\mathrm{mod}\ 7)$, etc.

Inverses I

Definition

An *inverse* of an element x modulo m is an integer x^{-1} such that

$$x x^{-1} \equiv 1 (\mathrm{mod}\ m)$$

Example: find the inverse of $a = 7$ modulo $m = 17$

Inverses do not always exist; example: $x = 5, m = 10$.

Verify for $b, 0 \leq b < m$

Inverses II

The following is a necessary and sufficient condition for an inverse to exist.

Theorem

Let a and m be integers, $m > 1$. A (unique) inverse of a modulo m exists if and only if a and m are relatively prime.

Intuition: if a, m are *not* coprime, then for $b = 0, \ldots m - 1$, the resulting congruences will be periodic, but never 1.