Number Theory

June 23, 2014

Primes

Definition

A positive integer p is **prime** if $p \geq 2$ and its only positive factors are itself and 1. Otherwise, if $p \geq 2$, then p is **composite**.

Theorem/Definition (Fundamental theorem of arithmetic)

Every integer greater than 1 can be written as the product of one or more prime factors, and except for the order in which we write the prime factors, this product is unique. The product is the integer's **prime factorization**.

Example: $600 = 2^3 \times 3 \times 5^2$. Proof later in the course...

Greatest common divisor

- $\gcd(a, b)$ is the largest integer that divides a and b
- Example: GCD of 140 and 48 is 4.
- If $\gcd(a, b) = 1$, then a and b are **relatively prime**. (Notation: $a \perp b$.)

Euclid's Algorithm

Assume $a \geq b$.

EuclidAlg(a,b)

- If $b = 0$
  - Return a
- Else
  - Return EuclidAlg(b, a mod b)

Reminder: a mod b is the remainder when a is divided by b.
Example: $\gcd(662, 414) = 2$.

Euclid's Algorithm, Correctness

EuclidAlg(a,b)

- If $b = 0$
  - Return a.
- Else
  - Return EuclidAlg(b, a mod b)

Theorem

If $a, b \in \mathbb{N}$ and $b \neq 0$, then $\gcd(a, b) = \gcd(b, a \bmod b)$.

Proof: Show that common divisors of a and b are the same as the common divisors of b and a mod b.

Euclid's Algorithm, Termination

EuclidAlg(a,b)

- If $b = 0$
  - Return a.
- Else
  - Return EuclidAlg(b, a mod b)

Theorem

For every two recursive calls, the first argument a is halved.

Proof: By cases. Either $b \leq a/2$ or $b > a/2$...

Bézout's Identity, Euclid's Lemma

Theorem (Bézout's Identity)

If a and b are positive integers, then there exist integers s and t such that $sa + tb = gcd(a, b)$.

Example: $2 = 8(414)$ - $5(662)$ "Proof": Use Euclid's Algorithm...

Corollary (*)

Two positive integers a and b are relatively prime if and only if there exist integers s and t such that $sa + tb = 1$.

Example: 35 and 12 are relatively prime and $3(12) + (-1)(35) = 1$
Proof: Use above theorem.

Euclid's Lemma

Corollary (Euclid's Lemma)

If a, b, and c are integers, a and b are relatively prime, and $a \mid bc$, then $a \mid c$.

Example: $15 \mid (77)(45)$ and $15 \mid 45$ Proof: Use previous corollary.

Proposition

For all primes p and integers a, if $p \nmid a$, then $\gcd(p, a) = 1$.

Proof: By contrapositive.

Corollary (also called Euclid's lemma)

If a and b are integers, p is a prime, $p \mid ab$, and $p \nmid a$, then $p \mid c$.

Example: $5 \mid (12)(15)$ and $5 \mid 15$. Proof: Use above corollary.

Clock arithmetic

- 5 hours after 3 o'clock is 8 o'clock, so $\mathbf{3 + 5 = 8}$.
- 6 hours after 10 o'clock is 4 o'clock, so $16 = \mathbf{6 + 10 = 4}$.
- 8 hours before 5 o'clock is 9 o'clock, so -3 $= \mathbf{5 - 8 = 9}$.

We can add or subtract multiples of 12...

Congruences

Definition

If a and b are integers, m is a positive integer, and $m \mid (a - b)$, then a and b are **congruent modulo** m, denoted $a \equiv b \pmod{m}$

Alternatively, $a \equiv b \pmod{m}$ if there is an integer k such that $a - b = km$.

Example: $4 \equiv 18 \pmod{7}$, $7 \equiv 7 \pmod{87}$, $-7 \equiv 8 \pmod{15}$.

Modular arithmetic

Theorem

Suppose $a, b, c, d \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

- $a + c \equiv b + d \pmod{m}$
- $ac \equiv bd \pmod{m}$.

Corollary

If a and b are integers, m and n are positive integers, and $a \equiv b \pmod{m}$, then $a^n \equiv b^n \pmod{m}$.

Proof:

Modular arithmetic example

$$11^{999} \equiv 1^{999} \equiv 1 \pmod{10} \tag{1}$$

$$9^{999} \equiv (-1)^{999} \equiv -1 \equiv 9 \pmod{10} \tag{2}$$

$$7^{999} \equiv 49^{499} \cdot 7 \equiv (-1)^{499} \cdot 7 \equiv -7 \equiv 3 \pmod{10} \tag{3}$$

mod m versus $(\text{mod } m)$

- $a = b \bmod m$ means that a is the remainder when b is divided by m.
- $a \equiv b \pmod{m}$ means that $a - b$ is a multiple of m.

Proposition

$a \bmod m = b \bmod m \leftrightarrow a \equiv b \pmod{m}$.

Proof: $(\rightarrow)$: Let $r = a \bmod m = b \bmod m$. There exist integers q_1 and q_2 such that $a = q_1 m + r$ and $b = q_2 m + r$. $(\leftarrow)$: There exists an integer q such that $mq = a - b$. Thus $a = b + mq$.

Modular arithmetic example

Suppose we want to know $11^{999} \bmod 10$, $9^{999} \bmod 10$, and $7^{999} \bmod 10$.

- $11^{999} \equiv 1 \pmod{10}$, so $11^{999} \bmod 10 = 1 \bmod 10 = 1$.
- $9^{999} \equiv 9 \pmod{10}$, so $9^{999} \bmod 10 = 9$.
- $7^{999} \equiv 3 \pmod{10}$, so $7^{999} \bmod 10 = 3$.

Repeated squaring

Find 7^{100} mod 11.

Modular arithmetic example

Proposition

If n is odd, then $n^2 \equiv 1 \pmod 8$.

Proof: Let $r = n \bmod 8$. Since $n = 8q + r$ for some q, r is odd. By the above proposition, $n^2 \equiv r^2 \pmod 8$. Now look at cases.

Inverses

Corollary (*)

Two positive integers a and b are relatively prime if and only if there exist integers s and t such that $sa + tb = 1$.

Proof: You've already seen this.

Theorem

If a and m are positive integers, then there exists a positive integer b such that $ab \equiv 1 \pmod{m}$ if and only if $\gcd(a, m) = 1$.

Proof: Use above proposition.

Definition

In the above, b is the **modulo** m **multiplicative inverse** of a.

Inverses

Theorem

If a and m are positive integers, then there exists a positive integer b such that $ab \equiv 1 \pmod{m}$ if and only if $\gcd(a, m) = 1$.

Corollary

If a and p are positive integers, p is prime, and $p \nmid a$, then there exists a positive integer b such that $ab \equiv 1 \pmod{m}$.

Example: If we have the congruence $xy \equiv xz \pmod{m}$ and $m \nmid x$, then $y \equiv z \pmod{m}$.
How do we find the inverse?