ACOL 202

Lecture 15

(Modular Arithmetic)

Theorem Let $K \geq 1$ and n be integers. Then there exist integers q and r such that

i) $0 \leq r < K$

ii) $n = Kq + r$

Furthermore, the value of q and r satisfying (i) and (ii) are unique.

$K = 7, \quad n = 54$

$q = 7, \quad r = 5$

Consider a fixed integer $K \geq 1$

$P(n)$ denote the fact that

$\exists\, q, r \in \mathbb{Z}$ such that

(i) and (ii) hold.

Case I $\quad (n \geq 0)$

Proof by strong induction on n.

Base case(s) $\quad (0 \leq n < K)$

Select $q = 0, \quad r = n$

$n = K \cdot 0 + n = n$

Inductive step $\quad (n \geq K)$

Consider $n - K$ (call it m)

$m \geq 0, \quad m < n$

From the inductive hypothesis,

$m = Kq' + r'$

$m + K = Kq' + K + r'$

$= K(q' + 1) + r'$

$n \qquad\qquad q \qquad\quad r$

Case II ($n < 0$)

$$-n = kq_1 + r_1$$

$$n = -kq_1 - r_1$$

If $r_1 = 0$

$$n = k(-q_1) + 0$$

If $r_1 \neq 0$

$$n = \underline{-kq_1 - k} + (k - r_1)$$

$$= k(-q_1 - 1) + r$$

Proved

What about uniqueness ?

Assume

$$n = kq_1 + r_1 = kq_2 + r_2$$

Without loss of generality, assume $(r_2 > r_1)$

$$k(q_1 - q_2) = r_2 - r_1$$

$r_2 - r_1$ is a multiple of k but is also less than k (and greater than 0) $< k$

$\therefore$ $r_2 - r_1$ must be 0

$\therefore$ q_1 must be equal to q_2

$\therefore$ $r_1 = r_2$. Proved

$$q = \left\lfloor \frac{n}{k} \right\rfloor$$

$$r = n \bmod k$$

mod - and - div (n, k)

{ $r = n$
while $(r > k)$
$r = r - k$, $q = q + 1$

return q, r

Properties of modular arithmetic

$$k \bmod k = 0$$

$$(a+b) \bmod k = (a \bmod k + b \bmod k) \bmod k$$

$$ab \bmod k = [(a \bmod k) \cdot (b \bmod k)] \bmod k$$

$$a^b \bmod k = [(a \bmod k)^b] \bmod k.$$

Congruence Two integers a and b are congruent mod k, $a \equiv_k b$, if $a \bmod k = b \bmod k$.

For two integers $k > 0$ and n, we write $k \mid n$ to denote the proposition that k divides n.

$k \nmid n$ (k does not divide n).

Properties

- $a \mid 0$
- $1 \mid a$
- $a \mid a$
- $a \mid b$ and $b \mid c \Rightarrow a \mid c$
- $a \mid b$ and $b \mid a \Rightarrow a = b$ or $a = -b$
- $a \mid b$ and $a \mid c \Rightarrow a \mid (b+c)$
- $a \mid b \Rightarrow a \mid bc$
- $ab \mid c \Rightarrow a \mid c$ and $b \mid c$

Exercise (prove these)

The greatest common divisor of two positive integers n and m, $\gcd(n, m)$, is the largest $d \in \mathbb{Z}^{\geq 1}$ such that

$d \mid n$ and $d \mid m$.

"Obvious" way of computing the gcd

$\gcd(12, 18)$

$\{1, 2, 3, 4, 5, 6, \ldots, 12\}$ $\min(n, m)$

Euclid-gcd (n, m)

$n, m > 0$

$m \geq n$

if $m \bmod n = 0$

return n

else return Euclid-gcd ($m \bmod n$, n)

gcd (17, 42)

= gcd (8, 17)

= gcd (1, 8)

= 1.

gcd (12, 18)

= gcd (6, 12)

= 6

Lemma Let n and m be positive integers, such that $n \leq m$ and $n \nmid m$.

Let $d \mid n$ be an arbitrary divisor of n. Then $d \mid m$ iff $d \mid (m \bmod n)$.

Corollary $\gcd(n, m) = \gcd(m \bmod n, n)$

Since d divides n, $n = kd$

$m = k'd$

$d \mid m \Rightarrow d \mid m \bmod n$

$$m = qn + r$$

$$= q(kd) + r$$

$$r = m - q(kd)$$

$$= k'd - qkd$$

$$= d(k' - qk)$$

$$\therefore \quad d \mid r$$

($\Leftarrow$)

$$n = dk$$
$$r = dk''$$

$$nq + r = dkq + dk''$$

$$= d(kq + k'')$$

$$\therefore \quad d \mid m .$$

Claim (correctness of Euclid-gcd)

For arbitrary positive integers n and m with $n \leq m$, we have

$$\text{Euclid-gcd}(n, m) = \gcd(n, m) .$$

Proof by strong induction on the smaller input n.

$P(n)$:= for any $m \geq n$, Euclid-gcd(n,m) = gcd(n,m)

$(\forall n \geq 1)$

Base case ($n = 1$)

Euclid-gcd ($1, m$) $= 1$

$= \gcd(1, m)$

Inductive step

case I $n \mid m$

$\gcd(n, m) = n$

$=$ Euclid-gcd (n, m)

case II $n \nmid m$

$=$ Euclid-gcd (n, m)

$=$ Euclid-gcd $(m \bmod n, n)$

$= \gcd(m \bmod n, n)$ (inductive hypothesis)

$= \gcd(m, n)$ (corollary)

Proved

Recall primes and composites

Prime Number Theorem

Let $\pi(n)$ denote the number of primes $\leq n$

$$\lim_{n \to \infty} \frac{\pi(n)}{\left(\frac{n}{\log_e n}\right)} = 1$$

Relative primality

Two positive integers n and m are relatively prime if $\gcd(n, m) = 1$.

$\gcd$ (prime, not a multiple of that prime) $= 1$

Lemma Let n and m be positive integers, and let $r = \gcd(n, m)$. Then there exist integers x and y such that $r = nx + my$.

n	m	r	x	y
5, 6		1	−1	1
17, 35		1	−2	1
16, 48		16	1	0