ACOL 202

Lecture 16
(Relative Primality)

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

$n = 91$
$m = 287$

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

$7 = x(91) + y(287)$

$7 = 1(7) + 0(14)$
$= 1(91 - 6(14))$
$= 91 - 6(14)$
$= 91 - 6(287 - 3(91))$
$= 91 - 6(287) + 18(91)$

$7 = 19(91) - 6(287)$

$\gcd(12, 18) = \gcd(6, 12)$
$= 6$
$1(6) + 0(12)$

```
Extended-Euclid (n, m)                    (18, 30)
    if (m mod n = 0)
        return (1, 0, n)
    else
        x, y, r := Extended-Euclid (m mod n, n)
        return (y - ⌊m/n⌋ . x, x, r)
```

Extended-Euclid (91, 287) = (19, -6, 7)

x, y, r = Extended-Euclid (14, 91)

(y - ⌊287/91⌋ . x, x, r)

(1 - 3(-6), -6, 7)

x = -6
y = 1
r = 7

Extended-Euclid (14, 91)

x_1, y_1, r_1 = Extended-Euclid (7, 14)

$(y_1 - \lfloor \frac{91}{14} \rfloor \cdot x_1, x_1, r_1)$

Extended-Euclid (7, 14) = (1, 0, 7)

$x_1 = 1, \quad y_1 = 0, \quad r_1 = 7$

Extended-Euclid (14, 91) (0 - 6, 1, 7) = (-6, 1, 7)

Extended-Euclid (18, 30)

Claims For arbitrary positive integers n and m $(n \leq m)$, Extended-Euclid(n,m) returns three integers x, y, r such that $r = xn + ym$. and $r = \gcd(n,m)$.

Lemma Let p be a prime number and let a and b be integers. Then $p \mid ab$ iff $p \mid a$ or $p \mid b$.

Backward (Trivial) (Forward) $p \mid ab$ $p \nmid a$.

$$1 = px + ay$$
$$b = pbx + aby$$
$$b \bmod p = 0$$
$$\therefore p \mid b.$$

Proved

Proof of correctness of Extended-Euclid

If Extended-Euclid $(m \bmod n, n) = \langle x, y, r \rangle$
then Extended-Euclid (n, m)
$= \langle y - \lfloor \frac{m}{n} \rfloor \cdot x, x, r \rangle$

$$r = x(m \bmod n) + yn$$

then $r = \left(y - \left\lfloor \frac{m}{n} \right\rfloor x \right) \cdot n + x \cdot m$

$$= yn - \left\lfloor \frac{m}{n} \right\rfloor xn + xm$$

$$= yn - x\left(\left\lfloor \frac{m}{n} \right\rfloor \cdot n - m \right)$$

$$= yn - x\left(\frac{m - m \bmod n}{n} \cdot n - m \right)$$

$$= yn - x\left(m - m \bmod n - m \right)$$

$$= yn - x(-m \bmod n)$$

$$= yn + x(m \bmod n)$$

$$= r$$

Prime Factorization Theorem

Let $n \in \mathbb{Z}^{\geq 1}$ be any positive integer. There exist $k \geq 0$ prime numbers $p_1, \ldots, p_k$ such that

$$\prod_{i=1}^{k} p_i = n .$$

Further, up to reordering, the prime numbers $p_1, \ldots, p_k$ are unique.

B: Proof By strong induction on n.

Base case

$$1 = \prod_{i=1}^{0} p_i$$

product of zero prime numbers.

Inductive step $(n \geq 2)$

Assume every $n' < n$ has a unique prime factorization.

What about n ?

Case I n is prime. $\prod_{i=1}^{1} p_1$ $(p_1 = n)$.

$q_1 \cdot q_2 \cdots q_k$ $k \geq 2$

Each $q_i > 1$ and $< n$

$\therefore$ n cannot be prime.

Case II n is composite

$q_1 \cdot q_2 \cdots q_k$ $p_1 \; p_2 \cdots p_r$

$q_1 \leq q_2 \leq \ldots \leq q_k$ $p_1 \leq p_2 \leq \ldots \leq p_r$

Case II a $\boxed{p_1 = q_1}$

$n = n$

$p_1 \quad \overline{q_1}$

Case II (b)

$p_1 \neq q_1$

Assume $p_1 < q_1$ without loss of generality

We know that $p_1 \mid n$

$\Rightarrow p_1 \mid q_1 q_2 \ldots q_k$

$\Rightarrow p_1 \mid q_i$ for some i

but $p_1 > 1$

$p_1 \leq q_i$

$\Rightarrow q_i$ cannot be prime.

Contradiction

The Chinese Remainder Theorem

Knowing $n \bmod k$ for enough values of k will (almost) let you figure out the value of n exactly - at least if those values of k are all relatively prime.

$n \bmod 2 = 0$

$n \bmod 3 = 2$

$n \bmod 5 = 1$

$n \in \{0, 1, \ldots, 29\}$

~~1~~, ~~6~~, ~~11~~, ~~16~~, ~~21~~, 26

26 + 30 + 30 + - - -

Theorem Let n and m be any two relatively prime integers. For any $a \in \mathbb{Z}_n$ and $b \in \mathbb{Z}_m$ there exists one and only one integer $x \in \mathbb{Z}_{nm}$ such that $x \bmod n = a$ and $x \bmod m = b$.

(only one — exercise)

$\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$