Chapter 5 Number Theory II

Date:

Death by Induction:

- Story: Bruce is given a 3-gallon jug and a 6-gallon jug & must measure out exactly 4 gallons.

aim: w/ Inductive proof to show that Bruce can ∄ product exactly 4 gallons using 3-gallon & 6-gallon jug.

Note: Induction requires n natural variable.
that some statement holds for all values of a natural variable n.
⇓
let n, be a number of steps or operations.
, n, be the number of times water is poured.

→ try to prove that for all $n \geq 0$, neither jug contains exactly 4 gallons of water after n steps.

P(n): "neither jug contains 4 gallons after n steps"

P(0) is true as both jugs are empty.

, assume P(n) is true in order to prove P(n+1).
P(n+1): neither jug contains 4 gallons after n+1 steps
⇓
but, each jug after n steps might contain 2 gallons.
⇓
then combining their contents in the 6 gallon = 4 gallons

$P(n) \not\Rightarrow P(n+1)$.

→ solution After n steps, both jugs contain a multiple of 3 gallons.

Scanned by CamScanner

A General Theorem.

Suppose that we have jugs w/ capacities a and b

The state of the system at each step: a pair of numbers (x, y).

x: the amount of water in a

y: the amount of water in b.

$(0,0) \to (a,0)$ fill first jug

$\to (a-b, b)$ fill second jug from first

$\to (a-b, 0)$ empty second jug

$\to (a-2b, b)$ fill second jug from first

$\to (a-2b, 0)$ empty second jug

$\to (0, a-2b)$ empty first jug into second

$\to (a, a-2b)$ fill first jug

$\to (2a-3b, b)$ fill second jug from first

at every step the amount of water in each jug

$s \cdot a + t \cdot b$ for some integers s & t.

Lemma 33. Suppose that we have water jugs w/ capacities a & b. The the amount of water in each jug is always a linear combination of a & b and at least one jug is either empty or full.

Proof: $P(n)$: after n steps, the amount of water in each jug is a linear combination of a & b and at least one jug is either empty or full.

$P(0) = 0 \cdot a + 0 \cdot b = 0$

$P(n)$ is true and prove the claim for $P(n+1)$.

Scanned by CamScanner

P(n) is after n steps, the amount of water in each jug is a linear combination of a x b and at least one jug is either empty or full

P(n+1). is true. There are two cases.

if we fill a jug from the fountain or empty a jug into the fountain.

↓

The jug is empty or full.

↓

the amount in the other jug remains a linear combination of a x b & P(n+1) holds.

we pour water from one jug to another until one is empty or the other is full

↓

$J_1 = s_1 \cdot a + t_1 \cdot b$

$J_2 = s_2 \cdot a + t_2 \cdot b$

↓

after pouring, one jug is either empty (contain 0 gallons) or full (contains a or b gallons)

↓

the other jug contains either

$J_1 + J_2$, $J_1 + J_2 - a$ or $J_1 + J_2 - b$.

a linear combinations of a x b

Scanned by CamScanner

Proof: Bruce dies

Since Bruce has water jugs w/ capacities 3 & 6.
the amount in each jug is always of the form $3s+6t$.

$3s+6t$ is always a multiple of 3, so he can't measure out 4 p

The Greatest Common Divisor (GCD)

gcd of a, b is the largest number that is a divisor of both a & b
gcd (a,b) for example gcd (18, 24) = 6

$18 = 2 \cdot 3^2$
$24 = 2^3 \cdot 3$
$GCD = 2 \cdot 3 = 6$

Theorem 35. The greatest common divisor of a & b is equal to the smallest positive linear combination of a & b

e.g. gcd (52, 44) is 4.

4 is a linear combination of $6 \cdot 52 + (-7) 44 = 4$.

$52 = 2^2 \cdot 13$
$44 = 2^2 \cdot 11$
$\boxed{2^2} = 4$.

Proof: Let m be the smallest positive linear combination of a & b
$m = \gcd(a,b)$ by showing both $\gcd(a,b) \le m$
$m \le \gcd(a,b)$

$\gcd(a,b) \le m$, $\gcd(a,b) \mid a$ and $\gcd(a,b) \mid b$.

$\Downarrow$

for every pair of integers s & t: $\gcd(a,b) \mid sa + tb$.

Thus in particular gcd(a,b) divides m, so $\gcd(a,b) \le m$.

Scanned by CamScanner

Date: No.

Now, we show that $m \leq \gcd(a,b)$.

$\Downarrow$

$m \mid a$ & $m \mid b$.

$\Downarrow$

m is a common divisor of a and b.

Thus $m \leq \gcd(a,b)$.

$m \mid a$, by division algorithm

$a = Q \cdot m + r \quad (0 \leq r < m)$.

$m = sa + tb$ for some integers s & t.

$a = q(sa + tb) + r$

$r = (1 - qs)a + (-qt) \cdot b$

r is a linear combination of a & b.

However m is the smallest positive linear combination $0 \leq r < m$.

This implies $m \mid a$.

Every linear combination of a & b is a multiple of $\gcd(a,b)$ and vice versa.

$\Rightarrow$ Suppose that we have water jugs w/ capacities a & b. Then the amount of water in each jug is always a multiple of $\gcd(a,b)$ and at least one jug is either empty or full.

Scanned by CamScanner

Properties of Greatest Common Divisor

Date: No.

1). Every common divisor of a & b divides $\gcd(a,b)$.

2) $\gcd(ka, kb) = k.\gcd(a,b)$ for all $k > 0$.

3) If $\gcd(a,b) = 1$ and $\gcd(a,c) = 1$, then $\gcd(a, bc) = 1$.

4) If $a \mid bc$ and $\gcd(a,b) = 1$, then $a \mid c$.

5). $\gcd(a,b) = \gcd(a \text{ rem } b, b)$.

Proof 3.

$\gcd(a,b) = 1$ and $\gcd(a,c) = 1$, then $\gcd(a, bc) = 1$.

$$sa + tb = 1$$
$$ua + vc = 1.$$

$$(sa+tb)(ua+vc) = 1.$$

$$a^2su + svac + uab + vtbc = 1.$$
$$a(asu + svc + utb) + bc(tv) = 1$$

$\Downarrow$

this is a linear combination of a and $bc = 1$.

So $\gcd(a, bc) = 1$.

4)

$a \mid ac$ and $a \mid bc$, assumption

a divides every linear combination of ac & bc.

$\gcd(ac, bc) = 1$ such linear combination

therefore a divides $\gcd(ac, bc) = c.\gcd(a,b) = c$

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

Scanned by CamScanner

Date: No.

2. $\gcd(1001, 777) = \gcd(\underbrace{1001 \text{ rem } 777}_{224}, 777)$

$= \gcd(\underbrace{777 \text{ rem } 224}_{105}, 224)$

$= \gcd(\underbrace{224 \text{ rem } 105}_{14}, 105)$

$= \gcd(\underbrace{105 \text{ rem } 14}_{7}, 14)$

$= \gcd(14, 7)$.

$= \underline{\underline{7}}$.

Scanned by CamScanner

The Fundamental Theorem of Arithmetic.

Date: No.

Theorem 39 (Fundamental Theorem of Arithmetic)

Every positive integer n can be written in a unique way as a product of primes

$$n = p_1 \cdot p_2 \cdots p_j \qquad (p_1 \leq p_2 \leq \cdots \leq p_j)$$

Note: the theorem $\Rightarrow$ fails if 1 were considered a prime

e.g $15 = 3 \cdot 5 \vee 1 \cdot 3 \cdot 5$ or $1 \cdot 1 \cdot 3 \cdot 5$.

Standard convention.

- the product of an empty set of numbers is defined to be 1.
- the sum of an empty set of numbers defined to be 0.

Lemma 40. if p is a prime and $p \mid ab$ then $p \mid a$ or $p \mid b$

Proof: the greatest common divisor of a, b must be either 1 or p.

Lemma 41. Let p be a prime. if $p \mid a_1 a_2 \cdots a_n$, then p divides some a_i

Proof
- every positive integer can be expressed as a product of primes
- this expression is unique.

Base case, $n = 1$ is the product of the empty set of primes.

For the inductive step, suppose that every $k < n$ is a product of primes.

n is also a product of primes.

if n is a prime, then this is true.

otherwise $n = a \cdot b$ for some $a, b < n$.

By the induction assumption, $a \times b$ are both products of primes

, Therefore $a \cdot b = n$ is also a product of primes.

Scanned by CamScanner

Arithmetic modulo:

Relative Primality & Phi.

- Integers a & b are relatively prime if $\gcd(a,b)=1$

e.g 8 & 15 are relatively prime since $\gcd(8,15)=1$

Note: every integer is relatively prime to a genuine prime number p, except for multiples of p

Let n be a positive integer
$\phi(n)$ denotes the number of integers in $\{1, 2, \ldots n-1\}$, that are relatively prime to n

e.g: $\phi(7)=6$ since 1, 2, 3, 4, 5, 6 are all relatively prime to 7.
$\phi(12)=4$ since only 1, 5, 7, 11 are relatively prime to 12.

Note: If you know the prime factorization of n
$\Downarrow$
$\phi(n)$ is easy.

The function ϕ obeys the following relationships:

1) if a & b are relatively prime then $\phi(ab)=\phi(a)\phi(b)$.

2) if p is a prime, then $\phi(p^k)=p^k-p^{k-1}$ for $k \geq 1$

300
2 150
2 75
3 25
5 5

$$\phi(300)=\phi(2^2.3.5^2)$$
$$=\phi(2^2).\phi(3).\phi(5^2)$$
$$=(2^2-2).(3^1-3^0).(5^2-5)$$
$$=2 \cdot 2 \cdot 20$$
$$=\boxed{80}.$$

12
2 6
2 3

$$\phi(12)=\phi(2^2.3)$$
$$=\phi(2^2).\phi(3)$$
$$=(2^2-2^1).(3^1-3^0)$$
$$=2.2=\boxed{4}.$$

Scanned by CamScanner

$$1+x+x^2+x^3+\cdots = \frac{1}{1-x}.$$

$$\begin{aligned} 1+x+x^2+x^3+\cdots &= y. \\ x+x^2+x^3+\cdots &= xy \\ \hline 1 &= y-xy \\ 1 &= y(1-x) \\ y &= \frac{1}{1-x}. \end{aligned}$$

Generalizing to an Arbitrary Modulus.

~~Arim~~ arithmetic modulo a prime.

→ modulo an arbitrary positive integer n.

$\Downarrow$

Arithmetic modulo n may be complicated but the integers relatively prime to n → well-behaved

e.g. If k is relatively prime to n, then k has a multiplicative inverse modulo n:

Lemma 43

→ let n be a positive integer. if k is relatively prime to n, then there exists an integer k^{-1} such that

$$k \cdot k^{-1} \equiv 1 \pmod{n}.$$

Proof. There exist integers s & t such that $sk + tn = \gcd(k,n) = 1$

$= tn = 1 - sk.$

$n \mid 1 - sk.$

and $sk \equiv 1 \pmod{n}$.

$s = k^{-1}$.

Scanned by CamScanner

Euler's Theorem.

Lemma 9.

Suppose n is a positive integer and k is relatively prime to n. Let $k_1, \dots, k_r$ denote all the integers relatively prime to n in the range $0 \le k_i < n$. Then the sequence

1*) $(k_1 \cdot k) \text{ rem } n, (k_2 \cdot k) \text{ rem } n, (k_3 \cdot k) \text{ rem } n, \dots (k_r \cdot k) \text{ rem } n$

is a permutation of the sequence

2*) $k_1, k_2, \dots k_r$

Proof:

1). In equation 1* they are all distinct

Suppose that $k_i k \text{ rem } n = k_j k \text{ rem } n$

$$k_i k \equiv k_j k \pmod{n}$$
$$k_i \equiv k_j \pmod{n}$$
$$k_i = k_j \text{ since both are between } 1 \text{ and } n-1$$
$$\Downarrow$$

Thus a term in the first sequence is only equal to itself

2). each number in the first sequence appears in the second.

$\gcd(k_i, n) = 1$ and $\gcd(k, n) = 1$

$$\gcd(k_i k, n) = \gcd(k_i k \text{ rem } n, n) = 1$$

Scanned by CamScanner

Date: No.

Euler's Theorem.

- Suppose n is a positive integer and k is relatively prime to n

$$k^{\phi(n)} \equiv 1 \pmod{n}$$

Proof: Let $k_1, \ldots k_r$ denote all integers relatively prime to n such that $0 \leq k_i < n$.

then $r = \phi(n)$

$$\equiv k_1 \cdot k_2 \cdot k_3 \ldots k_r$$

$$\equiv (k_i \cdot k \text{ rem } n) \cdot (k_2 \cdot k \text{ rem } n) \cdot (k_3 \cdot k \text{ rem } n) \ldots (k_r \cdot k \text{ rem } n) \pmod{n}$$

$$\equiv (k_1 \cdot k) \cdot (k_2 \cdot k) \cdot (k_3 \cdot k) \ldots (k_r \cdot k) \bmod n.$$

$$\equiv (k_1 \cdot k_2 \cdot k_3 \ldots k_r)\, k^r \pmod{p}.$$

Multiplicative inverse of k modulo n : $k^{\phi(n)-1}$.

Scanned by CamScanner