COL 202: DISCRETE MATHEMATICAL STRUCTURES

LECTURE 16

MINOR-I DISCUSSION & GRAPH THEORY

FEB 10, 2023 | ROHIT VAISH

MINOR-I DISCUSSION

PROBLEM 1: Let k, n be positive integers.

Prove that if k is cancellable $(\bmod n)$, then

$$\gcd(k, n) = 1.$$

Cancellability $(\bmod n) \Rightarrow \gcd(k, n) = 1$

By contradiction.

Suppose, for contradiction, that $\gcd(k, n) = d > 1$.

That is, $k = d \cdot \alpha$

$n = d \cdot \beta$

for some integers α and β

Cancellability $(\bmod n) \Rightarrow \gcd(k,n) = 1$

Consider integers $a = \beta$ and $b = 0$.

$k = d\alpha$

$n = d\beta$

Then, $(a-b) \cdot k = \beta \cdot d\alpha = n\alpha$

Therefore, $ka \equiv kb \pmod n$

By cancellability, we must have $a \equiv b \pmod n$.

However, $a - b = \beta$ and n does NOT divide β

$(\because 0 < \beta < n)$.

Contradiction! Thus, cancellable $\Rightarrow \gcd(k,n) = 1$ ∎

PROBLEM 1

TOTAL = 10 points

Identifying proof by contradiction [1 pt]

Writing k and n in terms of gcd [1 pt]

Coming up with correct 'a' and 'b' [6 pts]

Demonstrating the contradiction [2 pts]

Problem 2 :

(a) Prove that $\forall\, n > 2$, $\phi(n)$ is even

(b) List all n's where $\phi(n) = 2$.

(a) $\forall n > 2$ $\phi(n)$ is even

* If n has an odd prime factor, say p, then (e.g., 3, 5, 7, 11, ---)

$$\phi(n) = \phi(p^k)\,\phi(\text{rest}) = \underbrace{(p^k - p^{k-1})}_{\text{even}}\,\phi(\text{rest})$$

* Otherwise, n only has even prime factors, i.e., $n = 2^k$.

$$\phi(n) = 2^k - \frac{2^k}{2} = 2^{k-1} \quad \text{which is even for } n > 2.$$

(b) List all n's where $\phi(n) = 2$.

$\phi(2) = 1$

$\phi(3) = 2$

$\phi(4) = 2$

$\phi(5) = 4$

$\phi(6) = 2$

Aside:

$\phi(1) := 1$

$\phi(0) := 1$

modified defn:

$$\phi(n) = \left| \left\{ \begin{array}{l} \text{integers less than or} \\ \text{EQUAL TO } n \text{ that} \\ \text{are co-prime to } n \end{array} \right\} \right|$$

Any $n \geq 6$ either has an odd prime factor or is itself a "sufficiently large" power of 2.

PROBLEM 2

(a) TOTAL = 6 points

Argument for n having odd prime factors [4 pts]

_____ only even _____ [2 pts]

(b) TOTAL = 4 points

Identifying the three values of n correctly [3 pts]

Explanation for other values of n [1 pt]

Problem 3 : Let a, b be positive integers.

(a) Show that $2^a - 1 \equiv 2^{a \pmod b} - 1 \pmod{2^b - 1}$

(b) Show that $\gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a,b)} - 1$

(a) Show that $2^a - 1 \equiv 2^{a \pmod b} - 1 \pmod{2^b - 1}$

By division theorem, $a = qb + r$.

Thus, $a \pmod b = r$.

So, we need to show that

$$2^{bq+r} - 1 \equiv 2^r - 1 \pmod{2^b - 1}$$

or $$2^{bq+r} \equiv 2^r \pmod{2^b - 1}$$

(a) Show that $2^a - 1 \equiv 2^{a \pmod b} - 1 \pmod{2^b - 1}$

Want: $2^{bq+r} \equiv 2^r \pmod{2^b - 1}$

Using the hint $(x-1) \mid (x^k - 1)$ for $x = 2^b$ and $k = q$.

$$(2^b - 1) \mid 2^{bq} - 1$$

$$\Rightarrow \quad 2^{bq} \equiv 1 \pmod{2^b - 1}$$

$$\Rightarrow \quad 2^{bq+r} \equiv 2^r \pmod{2^b - 1}.$$

∎

(b) Show that $\gcd(2^a-1, 2^b-1) = 2^{\gcd(a,b)} - 1$

Proof by strong induction.

★ $P(a)$: $\forall\ 0 < b \leq a \quad \gcd(2^a-1, 2^b-1) = 2^{\gcd(a,b)} - 1$.

Base case: $P(1)$ is TRUE because only $a=1$ $b=1$ are feasible.

So, $\gcd(2^1-1, 2^1-1) = \gcd(1,1) = 1 = 2^{\gcd(1,1)} - 1$.

Induction step: $\forall\ a \in \mathbb{N} \quad P(1) \wedge P(2) \cdots \wedge P(a) \Rightarrow P(a+1)$.

(b) Show that $\gcd(2^a-1, 2^b-1) = 2^{\gcd(a,b)} - 1$

$P(a+1)$: $\forall\ 0 < b \leq a+1$

$$\gcd(2^{a+1}-1, 2^b-1) \stackrel{?}{=} 2^{\gcd(a+1,\,b)} - 1$$

If $b = a+1$, the above equality holds

So, let us assume $b \leq a$ from here onwards.

(b) Show that $\gcd(2^a-1, 2^b-1) = 2^{\gcd(a,b)} - 1$

$P(a+1)$: $\forall\ 0 < b \le a+1$

$$\gcd(2^{a+1}-1, 2^b-1) \stackrel{?}{=} 2^{\gcd(a+1,\,b)} - 1$$

$$\text{LHS} = \gcd(2^b-1,\ 2^{a+1} - 1 \pmod{2^b-1})$$

Remainder Lemma

$$= \gcd(2^b-1,\ 2^{a+1 \pmod b} - 1)$$

{ From Part (a)
$2^a - 1 \equiv 2^{a \pmod b} - 1 \pmod{2^b-1}$

If $a+1 \pmod b = 0$, then

$\text{LHS} = \gcd(2^b-1, 2^0-1) = 2^b-1$

$\text{RHS} = 2^{\gcd(a+1,b)} - 1 = 2^b - 1$

requires that $a+1 \pmod b > 0$

(b) Show that $\gcd(2^a-1, 2^b-1) = 2^{\gcd(a,b)} - 1$

$P(a+1)$: $\forall\ 0 < b \le a+1$

$$\gcd(2^{a+1}-1, 2^b-1) \stackrel{?}{=} 2^{\gcd(a+1,\,b)} - 1$$

$$\text{LHS} = \gcd\left(2^b-1,\ 2^{a+1}-1 \pmod{2^b-1}\right)$$

Remainder Lemma

$$= \gcd\left(2^b-1,\ 2^{a+1\,(\mathrm{mod}\,b)}-1\right)$$

$b \le a$; $0 < b \le a$

From Part (a):
$2^a - 1 \equiv 2^{a\,(\mathrm{mod}\,b)} - 1 \pmod{2^b-1}$

$$= 2^{\gcd(b,\ a+1\,(\mathrm{mod}\,b))} - 1$$

Induction hypothesis
"a" $= b$, "b" $= a+1 \pmod b$

relies on strong induction

(b) Show that $\gcd(2^a-1, 2^b-1) = 2^{\gcd(a,b)} - 1$

$P(a+1)$: $\forall\ 0 < b \le a+1$

$$\gcd(2^{a+1}-1, 2^b-1) \stackrel{?}{=} 2^{\gcd(a+1,\,b)} - 1$$

$$\text{LHS} = \gcd\left(2^b-1,\ 2^{a+1}-1 \pmod{2^b-1}\right)$$

Remainder Lemma

$$= \gcd\left(2^b-1,\ 2^{a+1\,(\mathrm{mod}\,b)}-1\right)$$

$b \le a$; $0 < b \le a$

{ From Part (a)
$2^a - 1 \equiv 2^{a\,(\mathrm{mod}\,b)} - 1 \pmod{2^b-1}$

$$= 2^{\gcd(b,\ a+1\,(\mathrm{mod}\,b))} - 1$$

{ Induction hypothesis
"a" = b, "b" = $a+1 \pmod b$

$$= 2^{\gcd(a+1,\ b)} - 1$$

again, Remainder Lemma

∎

Problem 3

(a) Total = 8 points

Using division theorem to simplify objective [3 pts]

Correctly using the hint [3 pts]

Correctly simplifying the congruence [2 pts]

Problem 3

(b) Total = 12 points

Identifying proof by strong induction [1 pt]

Correctly framing the induction hypothesis [3 pts]

Base case [2 pts]

Inductive step — Remainder Lemma (first) [2 pts]

Using part (a) [1 pt]

Using induction hypothesis [2 pts]

Remainder Lemma (second) [1 pt]