COL 202: DISCRETE MATHEMATICAL STRUCTURES

LECTURE 15

QUIZ 2

FEB 02, 2024 | ROHIT VAISH

Problem 1 (24 points)
Let a and b be any pair of positive integers.

(a) [**8 points**] Show that $2^a - 1 \equiv 2^{\text{rem}(a,b)} - 1 \pmod{(2^b - 1)}$,
where $\text{rem}(a, b)$ is the remainder obtained in the Division Theorem when a is divided by b.
Hint: You may use the fact that for any real-valued x and any positive integer k, $x - 1$ divides $x^k - 1$.

(b) [**16 points**] Show that $\gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a,b)} - 1$.
Hint: You may use part (a).

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

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

Thus, $rem(a,b) = r$.

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 $2^a - 1 \equiv 2^{\text{rem}(a,b)} - 1 \pmod{2^b - 1}$

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 $k = q$.

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

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

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

$\blacksquare$

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

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

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

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

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

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

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

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

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

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

$\left\{ \begin{array}{l} \text{From Part (a)} \\ 2^a-1 \equiv 2^{a \pmod b} - 1 \pmod{2^b-1} \end{array} \right.$

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

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

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

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

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

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

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

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

Remainder Lemma

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

$b \leq a$ $\quad$ $< b \leq a$

From Part (a)

$2^a-1 \equiv 2^{a \pmod b}-1 \pmod{2^b-1}$

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

Induction hypothesis

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

relies on <u>strong</u> induction

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

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

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

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

Remainder Lemma

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

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" $= a+1 \ (\mathrm{mod}\ b)$

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

again, Remainder Lemma

PROBLEM 1

(a) TOTAL = 8 prints

Using division theorem to simplify objective [3 pts]

Correctly using the hint [3 pts]

Correctly simplifying the congruence [2 pts]

PROBLEM 1

(b) TOTAL = 16 points

Identifying proof by strong induction		[1 pt]
Correctly framing the induction hypothesis		[4 pts]
Base case		[3 pts]
Inductive step —	Remainder Lemma (first)	[3 pts]
	Using part (a)	[1 pt]
	Using induction hypothesis	[2 pts]
	Remainder Lemma (second)	[2 pt]