SHAURYA GAUI

11/14/17

# CS-182
## Homework 5

1. a) Since, $a|b$ there exists a $q \in Z$ such that $b = q.a$

Similarly as $c|d$ there exists $r \in Z$ such that $d = r.c$

$$\Rightarrow b+d = q.a + r.c$$
$$= ac\left(\frac{q}{c} + \frac{r}{a}\right)$$

Let us assume that $k \in Z$ such that $\frac{q}{c} = k$ and $s \in Z$ such that $s = \frac{r}{a}$

$\therefore$ $b+d = ac(k+l)$

$\therefore$ $ac | b+d$

Hence proved.

b) Since $a|c^2$, there exists $q \in \mathbb{Z}$ such that $c^2 = q.a$

$$ab = \frac{c^2}{q} \cdot \frac{c^2}{r} = \frac{1}{qr} c^4$$

$\Rightarrow ab | c^4$

$\therefore$ The statement is <u>false</u>

c) Let us assume that $p$ is not divisible by 3

$\Rightarrow$ as $p = 3k+1$ or $3k-1$, then
$p^2 = 3m_2+1$

$\Rightarrow$ $p^2+2$ will be divisible by 3 and composite

Hence, $p=3$ is the only option for $p^2+2$ to be prime.

$\therefore$ If $p=3$, then
$p^2+2 = (3)^2+2 = 11$ is prime

Similarly, $p^3+2 = (3)^3+2 = 27+2 = 29$ is prime too.

$\therefore$ When $p$ & $p^2+2$ are both prime
$\Rightarrow$ $p=3$ & $p^3+2$ are also prime. Hence proved.

2. a) Let $a = bq + r$ and $r = a \bmod b$.

Note that $x^k - 1 = (x-1)(x^{k-1} + x^{k-2} + x^{k-3} + \dots + 1)$

$\therefore$ For $\forall$ integers $k \geq 1$, $(x-1) \mid (x^k - 1)$

Let $x = 2^b$, we get

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

$\Rightarrow (2^a - 1) \bmod (2^b - 1) = 2^r - 1 = 2^{a \bmod b} - 1$

b) <u>By induction</u>:

Let $P(a)$ be the statement: $\forall\, 0 \leq b < a$ and

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

We know that $P(1)$ is true since for $a = 1$, $b = 0$ we get,

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

We assume that $P(i)$ is true, $1 \leq i \leq a$

We need to prove that $P(a+1)$ is also true.

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

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

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

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

in which the second inequality follows from Q1. and the third inequality from P(b) since $b \leq a$. The first & $4^{th}$ inequalities are derived from $\gcd(x,y) = \gcd(y, x \bmod y)$.

3. a) $21^{4600} \pmod{47}$

$\because$ 47 is prime and $21 \not\equiv 0 \pmod{47}$, we use Fermat's Theorem

$$\Rightarrow 21^{4600} \equiv (21^{46})^{100} \equiv \boxed{1} \pmod{47} \text{ --- } ①$$

b) $21^{4601} \pmod{47}$

$\because$ 47 is prime and $21 \not\equiv 0 \pmod{47}$, using Fermat's Theorem, we get:

$$21^{4601} = 21^{4600} \cdot 21 \text{ --- } ② \text{ (from ①)}$$
$$= \boxed{21}$$

c) $21^{4599} \pmod{47}$

from ① and ②, we get:

$$21^{4599} \equiv 21^{4600} \cdot \frac{1}{21} \equiv \boxed{\frac{1}{21}}$$

Now, we need to find the reciprocal of 21 (mod 47).
This requires us to solve the combo problem:

$$21x + 47y = 1$$

where, x = reciprocal.

We use Euclidean Algorithm in the usual way,
we get $x = 9$ and $y = -4$

Thus, $2^{4599} \equiv \boxed{9}$

4. $5x \equiv 14 \pmod{17}$ --- 1
$3x \equiv 2 \pmod{13}$ --- 2
We can rewrite 1 and 2 as:
$5x + 17y = 14$
$3x + 13y = 2$

Using 2, we get
$$x = \frac{2-13y}{3}$$

Substituting the value of $x$ in 1
$$5\left(\frac{2-13y}{3}\right) + 17y = 17$$

$$10 - 65y + 51y = 42$$

$$-14y = 32$$

$$y = -\frac{32}{14} = -\frac{16}{7}$$

$$\therefore \quad x = \frac{2 - 13\left(-\frac{16}{7}\right)}{3}$$

$$= \frac{14 + 208}{21} = \frac{222}{21}$$

$$\therefore \quad \boxed{x = \frac{222}{21}} \qquad \boxed{y = -\frac{16}{7}}$$

5. $x \equiv 1 \pmod{3}$ $\quad m_1 = 3$

$x \equiv 2 \pmod{5}$ $\quad m_2 = 5$

$x \equiv 3 \pmod{7}$ $\quad m_3 = 7$

$m = 105$

$M_1 = 35 \qquad M_2 = 21 \qquad M_3 = 15$

$a_1 = 1 \qquad a_2 = 2 \qquad a_3 = 3$

$$y_1 = 35^{-1} \pmod{3}$$

$$(35)(0) \equiv 0 \pmod{3}$$

$$(35)(1) \equiv 2 \pmod{3}$$

$$(35)(2) \equiv 1 \pmod{3}$$

So, $y_1 = 2$

$y_2 = 21^{-1} \pmod 5$

$(21)(0) \equiv 0 \pmod 5$
$(21)(1) \equiv 1 \pmod 5$
$\therefore y_2 = 1$

$y_3 = 15^{-1} \pmod 7$

$(15)(0) \equiv 0 \pmod 7$
$(15)(1) \equiv 1 \pmod 7$

$\therefore y_3 = 1$

$a_1 y_1 M_1 + a_2 y_2 M_2 + a_3 y_3 M_3$
$(1)(2)(35) + (2)(1)(21) + (3)(1)(15)$
$70 + 42 + 45$
$157 \equiv 52 \pmod{105}$
$\therefore \boxed{x = 52}$

6. Let $P_i$ (for $i \in I$) be the common primes dividing both $m$ and $n$.

Let $q_j$ (for $j \in J$) be the primes dividing $m$ but not $n$ & let $r_k$ (for $k \in K$) be the primes dividing $n$ but not $m$.

$$m = \prod p_i^{e_i} \prod q_j^{f_j}$$

and $$n = \prod p_i^{g_i} \prod r_k^{h_k}$$

Then, on calculating $\phi(m)$, $\phi(n)$ and $\phi(mn)$ we get

$$\frac{\phi(m)\,\phi(n)}{\phi(mn)} = \prod \left(1 - \frac{1}{p_i}\right)$$

Since, $1 - \frac{1}{p_i} < 1$, the only way the product $=1$ is if it is <u>empty</u>.

$\Rightarrow$ If there are no common primes dividing $m$ and $n$.

Hence, proved