Assignment 5

Due: Wednesday, November 15th, 2017, upload before 11:59pm

1) (15 pts.) Answer the following:

a. Prove or disprove: For all integers a, b, c, d, if a|b and c|d, then (ac)|(b+d).

Let a = 5, b = 10, c = 2, d = 6

a|b = 5|10 = 2

c|d = 2|6 = 3

(ac)|(b+d) = (5*2)|(10+6) = 10|16

10 does not divide 16 so this disproves it.

b. True or false: if a| c^2 and b| c^2 then ab| c^3. Give a proof or counter example.

There is s, t ϵ Z such that

$$1 = as + bt$$

Assume a|c and b|c then there are k, j ϵ Z such that

$$c = ka \text{ and } c = jb$$

Multiply by c

c = cas + cbt = (jb)as + (ka)bt = (js)ab + (kt)ab = (js + kt)ab

Proves that ab|c

and if ab|c then ab|c^3. Therefore the statement is true.

c. If p and p^2+2 are primes, show that p^3 +2 is prime.

If p = 3, then p^2+2 = 11, and so p^3 + 2 = 29 which is prime

2) (30 pts.)

a. Show that if a and b are both positive integers, then $(2^a - 1) \bmod (2^b - 1) = 2^{amodb} - 1$.

,

If $a \geq b$ then we can let $a = bn + r$, $n \geq 1$, $0 \leq r \leq b$

$r = a \bmod (b)$

$x^n - 1 = (x - 1)(x^{k-1} + x^{k-2} + \ldots + 1)$; $(x - 1)|(x^n - 1)$

choose $x = 2^b$, then $(2^b - 1)|(2^{bn} - 1)$

$$
\begin{aligned}
(2^a - 1) \bmod (2^b - 1) &= (2^{bn + 1}) \bmod (2^b - 1) \\
&= (2^{bn} \cdot 2^r - 2^r + 2^r - 1) \bmod (2^b - 1) \\
&= ((2^{bn} - 1) \cdot 2^r + (2^r - 1)) \bmod (2^b - 1) \\
&= (2^r - 1) \bmod (2^b - 1) \\
&= 2^r - 1 = 2^{amodb} - 1
\end{aligned}
$$

b. Using the above question, show that if a and b are both positive integers,

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

If $a = 1$, $b = 0$, then $\gcd(2^1 - 1, 2^0 - 1) = \gcd(1,0) = 1$ and $2^{\gcd(1,0)} - 1 = 2 - 1 = 1$.

Assume true for $1 \leq n \leq a$

Consider $n = a+1$

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

3) (20 pts.) Solve the following:

a. Compute 21^{4600} (mod 47)

47 is prime

$21 \equiv 0 \pmod{47}$

Fermat's Theorem

$21^{4600} \equiv (21^{46})^{100} \equiv 1 \pmod{47}$

b. Compute 21^{4601} (mod 47)

$21^{4601} \equiv 21^{4600} \cdot 21 \equiv 21$

c. Compute 21^{4599} (mod 47) [Hint: work on 3. (b) will be useful to solve this.]

$21^{4599} \equiv 21^{4600} \cdot 21^{-1} \equiv 21^{-1} \equiv 1/21$

$21x + 41y = 1$

$x = 9$

$21^{4599} \equiv 9$

4) (10 pts.) Solve the system of congruences using Substitution method:

$5x \equiv 14 \pmod{17}$

$3x \equiv 2 \pmod{13}$

$5x \equiv 14 \pmod{17}$

$35x \equiv 98 \pmod{17}$

$x \equiv 13 \pmod{17}$

$3x \equiv 2 \pmod{13}$

$27x \equiv 18 \pmod{13}$

$x \equiv 5 \pmod{13}$

$x = 13 + 17k$

$13 + 17k \equiv 5 \pmod{13}$

$4k \equiv 5 \pmod{13}$

$k \equiv 11 \pmod{13}$

$x \equiv 13 + 17 \cdot 11 \equiv 200 \pmod{221}$

5) (10 pts.) Solve the system of congruences using Chinese Remainder Theorem:

$x \equiv 1 \pmod{3}$
$x \equiv 2 \pmod{5}$
$x \equiv 3 \pmod{7}$

$\gcd(3, 5) = 1$
$\gcd(3, 7) = 1$
$\gcd(5, 7) = 1$

$x = 5 \cdot 7 \quad + 3 \cdot 7 \quad + 3 \cdot 5$
$x = 35 \quad + 21 \quad + 15$
$x = 35 \quad + 0 \quad + 0 \pmod{3}$
$x = 35 \pmod{3}$
$x = 2 \pmod{3}$

$x = 0 \quad + 0 \quad + 15 \pmod{7}$
$x = 15 \pmod{7}$
$x = 1 \pmod{7}$
$1 \cdot 3 = 3 \pmod{7}$
$x = 35 \quad + 21 \quad + 15 \cdot 3$
$x = 35 \quad + 21 \quad + 45$

$x = 0 \quad + 21 \quad + 0 \pmod{5}$
$x = 21 \pmod{5}$
$x = 1 \pmod{5}$
$1 \cdot 2 = 2 \pmod{5}$
$x = 35 \quad + 21 \cdot 2 \quad + 45$

$x = 35 \quad + 42 \quad + 45$
$x = 122$
$3 \cdot 5 \cdot 7 = 105$

$x = 17 \pmod{105}$

6) (15 pts.) True or False: two positive integers m and n are coprime if and only if

$\varphi(mn) = \varphi(m)\varphi(n)$. Give a proof or counter example.

TRUE

If m = 1 or n = 1 then $\varphi(1) = 1$, so $m > 1$ and $n > 1$

We shall arrange integers from 1, 2, …, mn in an array, a, of n rows and m columns.

Since m and n are coprime gcd(a, mn) = 1 if a and m are coprime and a and n are coprime.

$\Phi(m)$ of the columns contain integers coprime with m.

Column c of integers coprime with m is in the form

C, m + c, 2m + c, …, (n-1)m + c

Since m and n are coprime all answers are different mod n. Therefore the column contains $\varphi(n)$ integers coprime with n and therefore there are $\varphi(m)\ \varphi(n)$ integers in the array coprime with m and n.

So $\varphi(mn) = \varphi(m)\ \varphi(n)$

Note: Provide justifications for your solutions.

Note: Late submissions will not be accepted. You are allowed a maximum of 3 attempts to submit your assignment. Link for Submission is on Blackboard under ”Homework5” and save the file as ”FirstName. LastName.Assignment5”.