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| c2 and b| c2 then ab| c3. 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 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|c3. Therefore the statement is true.

c. If p and p2+2 are primes, show that p3 +2 is prime.

If p = 3, then p2+2 = 11, and so p3 + 2 = 29 which is prime

2) (30 pts.)

a. Show that if a and b are both positive integers, then (2a - 1) mod (2b - 1) = 2amodb - 1.

,

If a ≥ b then we can let a = bn + r, n ≥ 1, 0 ≤ r ≤ b

r = a mod (b)

xn – 1 = (x – 1)(xk-1 + xk-2 + … + 1); (x – 1)|(xn – 1)

choose x = 2b, then (2b - 1)|(2bn – 1)

(2a – 1) mod (2b – 1) = (2bn + 1) mod (2b – 1)

= (2bn ∙ 2r – 2r + 2r – 1) mod (2b – 1)

= ((2bn – 1) ∙ 2r + (2r – 1)) mod (2b – 1)

= (2r – 1) mod (2b – 1)

= 2r – 1 = 2amodb – 1

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

then gcd(2a − 1, 2b - 1) = 2gcd(a, b) -1.

If a = 1, b = 0, then gcd (21 – 1, 20 – 1) = gcd (1,0) = 1 and 2gcd (1,0) - 1 = 2 - 1 = 1.

Assume true for 1 ≤ n ≤ a

Consider n = a+1

gcd (2a+1 – 1, 2b – 1) = gcd ((2a+1 – 1) mod (2b – 1), 2b – 1)

= gcd ((2(a+1) mod (b) – 1), 2b – 1)

= 2gcd((a+1) mod (b), b) – 1

= 2gcd(a+1, b) – 1

3) (20 pts.) Solve the following:

a. Compute 214600 (mod 47)

47 is prime

21 ≡ 0 (mod 47)

Fermat’s Theorem

214600 ≡ (2146)100 ≡ 1 (mod 47)

b. Compute 214601 (mod 47)

214601 ≡ 214600 ∙ 21 ≡ 21

c. Compute 214599 (mod 47) [Hint: work on 3. (b) will be useful to solve this.]

214599 ≡ 214600 ∙ 21-1 ≡ 21-1 ≡ 1/21

21x + 41y = 1

x = 9

214599 ≡ 9

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

5x ≡ 14 (mod 17)

3x ≡ 2 (mod 13)

5x ≡ 14 (mod 17)

35x ≡ 98 (mod 17)

x ≡ 13 (mod 17)

3x ≡ 2 (mod 13)

27x ≡ 18 (mod 13)

x ≡ 5 (mod 13)

x = 13 + 17k

13 + 17k ≡ 5 (mod 13)

4k ≡ 5 (mod 13)

k ≡ 11 (mod 13)

x ≡ 13 + 17 ∙ 11 ≡ 200 (mod 221)

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

x ≡ 1 (mod 3)

x ≡ 2 (mod 5)

x ≡ 3 (mod 7)

gcd (3, 5) = 1

gcd (3, 7) = 1

gcd (5, 7) = 1

x = 5 ∙ 7 + 3 ∙ 7 + 3 ∙ 5

x = 35 + 21 + 15

x = 35 + 0 + 0 (mod 3)

x = 35 (mod 3)

x = 2 (mod 3)

x = 0 + 0 + 15 (mod 7)

x = 15 (mod 7)

x = 1 (mod 7)

1 ∙ 3 = 3 (mod 7)

x = 35 + 21 + 15 ∙ 3

x = 35 + 21 + 45

x = 0 + 21 + 0 (mod 5)

x = 21 (mod 5)

x = 1 (mod 5)

1 ∙ 2 = 2 (mod 5)

x = 35 + 21 ∙ 2 + 45

x = 35 + 42 + 45

x = 122

3 ∙ 5 ∙ 7 = 105

x = 17 (mod 105)

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

φ(mn)= φ(m)φ(n). Give a proof or counter example.

TRUE

If m = 1 or n = 1 then φ(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.

Φ(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 φ(n) integers coprime with n and therefore there are φ(m­­­) φ(n) integers in the array coprime with m and n.

So φ(mn) = φ(m) φ(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”.