EECS 203-1 Homework –11 Solutions

Total Points: 34

Page 149:

22) Which integers are divisible by 5 but leave a remainder of 1 when divided by 3?

2 points

By the Chinese remainder theorem, the integers 10+15n are divisible by 5 and congruent to 1 modulo 3. Note that to use the Chinese Remainder Theorem, we must check first that the numbers m_1 and m_2 are relatively prime. In this case they are, so we can apply the theorem.

26) Find the non-negative integer *a* less than 28 represented by each of the following pairs, where each pair represents (*a* mod 4, *a* mod 7)

4 points

e) (2,2)

First method

By the Chinese remainder theorem, we can see that the number ***a* = 2**. Note that to use the Chinese Remainder Theorem, we must check first that the numbers m_1 and m_2 are relatively prime. In this case they are, so we can apply the theorem.

Second method

This gives us

$a = 4n + 2$ …(1)

$a = 7m + 2$ …(2)

From (1) and (2) we get

$4n + 2 = 7m + 2$

$\therefore m/n = 4/7$ …(3)

Now looking at (1) and (2), one solution is m=0 and n=0.

Now looking at (3), one of the solutions could be m = 4 and n=7.

But we need $a < 28$ => $4n + 2 < 28$ and $7m + 2 < 28$

=> $n \leq 4$ and $m \leq 3$. This contradicts what we got from (3).

Hence m =0 and n=0.

$\therefore$ *a* = 2 …(from (1) and (2))

h) (3,5)

First method

By the Chinese remainder theorem, we can see that the number ***a* = 19**. Note that to use the Chinese Remainder Theorem, we must check first that the numbers m_1 and m_2 are relatively prime. In this case they are, so we can apply the theorem.

Second method

This gives us

$a = 4n + 3$ ..(1)

$a = 7m + 5$ ..(2)

From (1) and (2) we get

$4n + 3 = 7m + 5$

$\therefore n = (7m + 2)/4$ ..(3)

We need $a < 28$ => $4n + 3 < 28$ and $7m + 5 < 28$

$\therefore n \leq 6$ and $m \leq 3$

By trial and error, we get n = 4, and m= 2

$\therefore a = 19$

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

10 points

Looks like there are a number of ways of doing this. One solution is the following.

Case 1)

a < b. In this case it is trivial. So a **mod** b = a. Also $2^a-1 < 2^b-1$, so 2^a-1 **mod** $2^b-1 = 2^a-1 = 2^{a \bmod b}-1$.

Case 2)

a ≥ b. So now a can be written as a = nb + r where n ≥ 1 and $0 \leq r < b$. First let us prove that when a = n*b, $2^a-1 \bmod 2^b - 1 = 0$, that is $2^b - 1$ divides numbers of the form $2^{nb}-1$. Using the fact that (x-1) is a factor of (x^n-1), (n ≥ 1) we get this result, but nb **mod** b = 0 and $2^0 - 1 = 0$. So when a = nb, 2^a-1 **mod** $2^b - 1 = 2^{a \bmod b} - 1$. Call this result (1)

When a = nb + r (0 < r < b), (note that r = a **mod** b)

2^a-1 **mod** $2^b - 1 = (2^{nb + r} - 1)$ **mod** $(2^b - 1)$

$= (2^{nb}.2^r - 2^r + 2^r - 1)$ **mod** $(2^b - 1)$ [Adding $0 = 2^r - 2^r$]

$= ((2^{nb} - 1).2^r + (2^r - 1))$ **mod** $(2^b - 1)$

$= (2^r - 1)$ **mod** $(2^b - 1)$ [Using result (1)]

$= 2^r - 1 = 2^{a \bmod b} - 1$.

So in all cases, the identity holds. **Hence proved.**

36) Encrypt the message ATTACK using the RSA system with n = 43.59 and e = 13, translating each letter into integers and grouping together pairs of integers as done in example 10.

10 points

(AT) (TA) (CK) is written as 0019 1900 0210. To encrypt we must compute $0019^{13} \equiv 2299 \pmod{2537}$, $1900^{13} \equiv 1317 \pmod{2537}$ and $0210^{13} \equiv 2117 \pmod{2537}$. The encrypted message is **2299 1317 2117**.

Pg 164:

18) Show that the system of congruences $x \equiv 2 \pmod 6$ and $x \equiv 3 \pmod 9$ has no solutions.

2 points

$x \equiv 3 \pmod 9 \Rightarrow x = 3 + 9t$ for some integer t. So, $3|x$.
On the other hand, $x \equiv 2 \pmod 6 \Rightarrow x = 2+6s = 2+ 3(2s)$ for some integer s. hence $x \bmod 3 = 2$ which contradicts the conclusion obtained above that $3|x$.
Therefore, there is no solution of the given system of congruences**.**
Another way you can do this is using the next problem. So in case you proved the next problem before you did this, then since gcd(6,9) = 3 does not divide 2-3 = -1, this system of congruences has no solution.

20a) Show that the system of congruences $x \equiv a_1 \pmod{m_1}$ and $x \equiv a_2 \pmod{m_2}$ has a solution if and only if $\gcd(m_1, m_2) \mid a_1 - a_2$.

6 points

$\Rightarrow$)
Let $d = \gcd(m_1, m_2)$. The fact that the system of linear congruences has a solution means that $\exists\ x = a_1 + m_1y = a_2 + m_2z$. Thus $a_1 - a_2 = m_2z - m_1y$. Since $d \mid m_1$ and $d \mid m_2$, $d \mid (m_2z - m_1y)$. Thus $d \mid (a_1 - a_2)$.
$\Leftarrow$)
Let $d = \gcd(m_1, m_2)$. By the hypothesis, $d \mid (a_1 - a_2)$.
By the '*sm+tn*' theorem, we know there are 2 integers s and t such that $sm_1 + tm_2 = d$.
Thus $(a_1 - a_2) = d*k = (sm_1 + tm_2)*k$. Rearranging terms in this equation, we get $a_1 + (-s*k)m_1 = a_2 + (t*k)m_2$. Thus there is a number x such that $x \equiv a_1 \pmod{m_1}$ and $x \equiv a_2 \pmod{m_2}$. This means that the system of linear congruences has a solution.
Hence proved.