EECS 203-1 Homework 10 Solutions

Total Points: 30

Page 126:

12) How many zeros are there at the end of 100!

4 points

To find the number of 0's at the end of 100! ,we need to find the total number of factors of 5 and the total number of factors of 2 in all the numbers from 1 to 100; the smaller of those two numbers will be the number of 0's at the end of 100!

The number of factors of 5 contained in the numbers 1 to 100 inclusive

100/5 = 20

20/5 = 4

4/5 =0

----

total = 24

The number of factors of 2 contained in the numbers 1 to 100 inclusive

100/2 = 50

50/2 = 25

25/2 =12

12/2 = 6

6/2 = 3

3/2 = 1

1/2 = 0

----

total = 97

Thus there are 24 zeros at the end of 100!

22) Show that n is prime if and only if $\Phi(n) = n-1$

(The value of the **Euler Φ-function** at the positive integer n is defined to be the number of positive integers less than or equal to n that are relatively prime to n.)

4 points

Case a: Assume that n is prime, to show that Φ (n) =n-1.

Since n is prime, by definition of prime numbers, n is divisible by only 1 and n. Thus, all numbers that are less than n are relatively prime to n

Thus, by definition of Euler Function,

$\Phi(n) = n-1$

Case b: Assume that Φ (n) =n-1, to prove that n is prime.

Lets assume that n is composite; i.e.; it is divisible by 1 and n as well as by atleast one more number less than n.

Thus, all numbers that are less than n are not relatively prime with n.

Which implies, that Φ (n) < (n-1).

This is a contradiction to our initial assumption. Hence n must be prime.

Hence proved!

38) Show that if a, b and m are integers such that $m \geq 2$ and $a \equiv b \pmod{m}$, then gcd(a, m) = gcd(b, m).

4 points

From $a \equiv b \pmod{m}$ then a,b $\in$ $[r]_m$ for some r positive and less than m. So $a = r + m.k_1$ and $b = r + mk_2$ for some integer k_1, k_2. This means that a mod m =r = b mod m. we proved in class that gcd(a,m) = gcd(m,a mod m). So gcd(a,m) = gcd(m,r) = gcd(b,m). Thus proved that
gcd(a, m) = gcd(b, m).

Page 135:

Do 2abf using the extended Euclidean algorithm to come up with s and t such that gcd (m, n) = sm + tn in each case.
(***2)****Use Euclidean Algorithm to find the gcd(m, n)*)

6 points

a) gcd (5, 1) = 1

(m,n)	**Quotient**	**(t,s)**
(5,1)	5	(0,1)
(1,0)	-	(1,0)

Here s = 1 and t = 0

b) gcd (100, 101) = 1

(m,n)	**Quotient**	**(t,s)**
(101,100)	1	(1, -1)
(100,1)	100	(0,1)
(1,0)	-	(1,0)

Here s = -1 and t = 1

f) gcd (11111, 111111) = 1
The Euclidean algorithm uses the following divisions

(m,n)	**Quotient**	**(t,s)**
(111111,11111)	10	(1, -10)
(11111,1)	11111	(0,1)
(1,0)	-	(1,0)

Here s = -10 and t=1

Page 149:

4) Show that 937 is an inverse of 13 modulo 2436

2 points

To show that 937 is the solution of the congruence 13x = 1 mod 2436. From the Euclid's algorithm, we find gcd(13,2436) =1 and s = 937 and t = -5. This means 937*13- 5*2436 = 1. Or 937*13 = 1 mod 2436. **Therefore, 937 is an inverse of 13 modulo 2436**.

6) Find an inverse of 2 modulo 17

2 points

Since gcd(2,17) =1, an inverse of 2 modulo 17 exists.
17 = 2*8 + 1
17+(-8)*2 =1
therefore, -8 ≡ 9 is an inverse of 2 modulo 17.

12) Solve the congruence $2x \equiv 7(\text{mod}17)$

2 points

We note that 9 is an inverse of 2 modulo 17 (9*2 =18 ≡ 1 (mod 17)). Thus $9*2x \equiv 9*7(\text{mod } 17)$. After simplifying we have $x \equiv 12(\text{mod } 17)$. The set of all solutions = {x : x = 12 + 17*n* where n is an integer}

14) **a)** Show that the positive integers less than 11, except 1 and 10, can be split into pairs of integers such that each pair consists of integers that are inverses of each other modulo 11.
b) Use part (a) to show that 10! ≡ -1 (mod 11).

6 points

a) We know that each of the integers 1, 2, 3 … 10 has an inverse modulo 11 (because 11 is prime). One can easily check that the inverse of 2 is 6, the inverse of 3 is 4, the inverse of 5 is 9, and the inverse of 7 is 8.

b) 10! = 1. (2.6).(3.4).(5.9).(7.8).10 ≡ 1.1.1.1.1.10 ≡ -1(mod 11).