**CS 3333 Mathematical Foundations Fall 2010**

**Homework 1 Solutions**

The following problems were graded. Total points: 30

Pages 208-210: 6, 16, 18, 20, 22, 26, 28

Pages 217, 218: 8, 12, 14, 20, 22, 24

**Division and Modular Arithmetic, Pages 208--210**

4. (2 points) Show that if a | b and b | c, then a | c.

Answer: Suppose a | b, so that b=at for some t, and b | c, so that c=bs for some s. Then substituting the first equation into the second, we obtain c=(at)s=a(ts). This means that a|c, as desired.

6. (2 points) Show that if a, b, c, and d are integers such that a | c and b | d, then ab | cd.

Answer: Under the hypotheses, we have c=ax and d=bt for some integers s and t. Multiplying we obtain cd=ab(st), which means that ab | cd, as desired.

10. (f). (1 point) what are the quotient and remainder when 0 is divided by 17.

Answer: 0 div 17=0 and 0 mod 17=0,

10. (h) (1 point) what are the quotient and remainder when -100 is divided by 101.

Answer: -100 = (-1)·101+1, we have -100 div 101= -1 and -100 mod 101 = 1

16(a) (1 point) Evaluate these quantities. -17 mod 2.

Answer: Since -17=2 · (-9)+1, the remainder is 1. That is, -17 mod 2 = 1.

16(b) (1 point) Evaluate these quantities. 144 mod 7.

Answer: Since 144=7\*20+4, the remainder is 4, that is, 144 mod 7=4.

18. (1 point) List five integers that are congruent to 4 modulo 12.

Answer: All such integers have the form 4+k · 12, where k is an integer. Among the infinite set of correct answers are 4, 16, -8, 1204, and -7016360.

20. (2 points) Show that if a ≡ b (mod m) and c ≡ d (mod m), where a, b, c, d and m are integers with m>=2, the a-c ≡ b-d (mod m).

Answer: From a ≡ b (mod m) we know that b = a+ sm for some integer s. Similarly, d = c+ tm. Subtracting, we have b-d= (a-c) + (s-t) m, which means that a-c ≡ b-d (mod m).

Alternative solution: a ≡ b (mod m) eq.1  
 c ≡ d (mod m) eq.2  
It is clear that -1 ≡ -1 (mod m) since m | (-1 - (-1)) or m | 0. eq.3

Using Theorem 5.ii, Section 3.4, and equations 2 and 3, we have –c ≡ -d (mod m) eq. 4  
Using Theorem 5.i, Section 3.4, and equations 1 and 4, we have a-c ≡ b-d (mod m).

22. (2 points) Show that if a, b, c and m are integers such that m>=2, c>0, and a ≡ b (mod m), then ac ≡ bc (mod mc).

Answer. From a ≡ b(mod m) we know that b = a+ sm for some integer s. Multiplying by c we have bc = ac+ s(mc) which means ac ≡ bc (mod mc).

24. (3 points) Prove that if n is an odd positive integer, then n²≡1(mod 8).

Answer: Write n=2k+1 for some integer k. Then n²=(2k+1)² = 4k²+4k+1 = 4k(k+1)+1. Since either k or k+1 is even, 4k(k+1) is a multiple of 8. Therefore n²-1 if a multiple of 8, so n²≡1(mod 8).

26. (2 points) Which memory locations are assigned by the hashing function h(k)=k mod 101 to the records of insurance company customers with these Social Security numbers?

Strategy: From the Division Algorithm, k = q m + r, where q = k div m = ⎣k/m⎦. Note: ⎣k/m⎦ is the integer part obtained when k is divided by m, say, using a scientific calculator.   
Now, find r = k mod m = k – q m = k - ⎣k/m⎦ · m

(c) k = 372201919, h(k) = k mod 11 = 372201919 - ⎣372201919/101⎦ · 101 = 52.

(d) k = 501338753, h(k) = 501338753 - ⎣501338753/101⎦ \* 101 = 3.

28. (2 points) What sequence of pseudorandom numbers is generated using the linear congruential generator xn+1 = (4 · n + 1) mod 7 with seed x0 = 3?

Answer: x1 = (4 · 3+1) mod 7 = 13 mod 7 = 6; x2 = (4 · 6+1 ) mod 7 = 25 mod 7 = 4;   
x3 = (4 · 4+1) mod 7 = 17 mod 7 = 3 = x0.   
So the sequence repeats 3, 6, 4, 3, 6, 4,….

32 (b). (1 points) Decrypt these messages encrypted using the Caesar cipher.

WHVW WRGDB

Answer: TEST TODAY.

**Primes, GCDs and LCMs, Pages 217, 218**

4. (3 points) Find the prime factorization of each of these integers.

(d) 143

Answer: We obtain the answer by trial division. The factorization is 143 = 11 · 13.

(e) 289

Answer: 289 = 17 · 17.

(f) 899

Answer: 899 = 29 · 31.

8. (3 points) Prove that for every positive integer n, there are n consecutive composite integers. [Hint: Consider the n consecutive integers starting with (n+1)!+2.]

Answer: Note that (n+1)! = 1 · 2 · 3 · … · (n+1), by definition. So (n+1)! is divisible by 2, 3, .. , (n+1).  
Consider the n consecutive numbers (n+1)! + 2, (n+1)! + 3, (n+1)! + 4,…, (n+1)! + (n+1).   
The first of these is composite because it is divisible by 2; the second is composite because it is divisible by 3; the third is composite because it is divisible by 4; … The last is composite because it is divisible by n+1. This gives us the desired n consecutive composite integers.

12. (2 points) Determine whether the integers in each of these sets are pairwise relatively prime.

(c) 25, 41, 49, 64

Answer: Since these numbers are small, the easiest approach is to find the prime factorization of each number and look for any common prime factors.

25=52, 41 is prime, 49=72, and 64=26. It is clear that any pair of them have no common divisors other than 1. Therefore these numbers are pairwise relative prime.

(d) 17, 18, 19, 23

Answer: Since 17, 19, and 23 are prime and 18=2 · 32, these are pairwise relative prime.

14(a) (2 points) We call a positive integer perfect if it equals the sum of its positive divisors other than itself. Show that 6 and 28 are perfect.

Answer:

The divisors of 6 other than itself are 1, 2, and 3. Since the sum of these divisors 1+2+3 =6, 6 is prefect by definition.   
The divisors of 28 other than itself are 1, 2, 4, 7, and 14. Since 1+ 2+ 4+ 7+ 14 = 28, 28 is a perfect number.

14(b) (4 points) Show that if N = 2p-1(2p-1) is a perfect number when 2p-1 is prime.

Answer. The divisors of N, other than itself, are:  
all powers of 2 up to 2p-1, which are given by 20, 21, …, 2p-1;  
and the integers obtained by multiplying the prime (2p-1) with a power of 2, up to 2p-2, which are given by  
20 · (2p-1), 21 · (2p-1), …, 2p-2 · (2p-1).

This pattern can be seen for 28 = 22 · 7, which has divisors 1 = 20, 2 = 21, 4 = 22, 7 = 20 · 7, 14 = 21 · 7.

[Not asked: To show that N is perfect, we need to find the sum of all of its positive divisors other than itself.

20 + 21 + … + 2p-1 + 20 · (2p-1) + 21 · (2p-1) + … + 2p-2 · (2p-1) = (2p-1)/(2-1) + (2p-1) · [(2p-1 -1)/(2-1)]  
 = (2p-1) · [1 + 2p-1 -1] = N.

]

16. (2 points) Determine whether each of these integers is prime, verifying some of Mersenne’s claims.

(b) 29-1.

Answer: Since 29-1=511 = 7 · 13, 29 -1 is not prime.

(d) 213-1=8191 has no prime divisor ≤ ⎣(8191)1/2⎦. So 213-1 is prime.

20. (2 points) What are the greatest common divisors of these pairs of integers?

(a) gcd(22 · 33 · 55, 25 · 33 · 52) = 22 · 33 · 52. [We form the greatest common divisors by finding the minimum exponent for each prime factor.]

(b)gcd( 2 · 3 · 5 · 7 · 11 · 13, 211 · 39 · 11 · 1714) = 2 · 3 · 11.

22. (2 points) What is the least common multiple of each pair in Exercise 20?

(a) lcm(22 · 33 · 55, 25 · 33 · 52) = 25 · 33 · 55. [We form the least common multiples by finding the maximum exponent for each prime factor.]

(b) gcd( 2 · 3 · 5 · 7 · 11 · 13, 211 · 39 · 11 · 1714) = 211 · 39 · 5 · 7 · 11 · 13 · 1714.

24. (2 points) Find gcd(1000, 625) and lcm(1000, 625) and verify that gcd( 1000, 625) · lcm(1000, 625)=1000 · 625.

Answer: We have 1000=23 · 53 and 625=54, so gcd(1000, 625)=53=125, and lcm(1000, 625)=23 · 54=5000. It can be verified that 125 · 5000 = 625000 = 1000 · 625.

26. (2 points) If the product of two integer is 273852711 and their gcd is 233451, what is their lcm?

Answer: Since a · b = gcd(a,b) · lcm(a,b), the required lcm is 273852711 / 23345 = 243451711.