**CS 3333 Mathematical Foundations Fall 2011**

**Homework 1 Solutions**

The following problems were graded. Total points: 70

Pages 208-210: 3, 5, 6, 10 c, d & e, 14, 16 c & d, 18, 20, 22, 24, 26 a & b, 28 (use seed 4), 32 c.

Additional problem: Find the smallest positive **a** such that **a ≡ 2a-5 (mod 3)** is satisfied.

Pages 217, 218: 2, 3, 5, 8, 10 (find integers < 50 that are relatively prime to 50), 13, 14 (for part b: list all positive divisors; do not have to prove), 16 b & d, 20 c & f, 22 c & f, 24, 26, 32, 34 (Hint: give a counterexample).

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

3. (2 points) Show that part (*ii*) of Theorem 1 is true.

Answer: If a|b, then we know that b = at for some integer t. Therefore bc = a(tc), so by definition a|bc.

5. (2 points) Show that if a | b and b | a, where a and b are integers, then a = b or a = -b.

Answer: The given conditions imply that there are integers s and t such that a = bs and b = at. Combining these, we obtain a = ats; since a != 0, we conclude that st = 1. Now the only way for this to happen is for s = t = 1 or s = t = -1. Therefore either a = b or a = -b.

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. (c). (1 point) what are the quotient and remainder when -123 is divided by 19.

Answer: As above, we can compute 123 div 19 = 6 and 123 mod 19 = 9. However, since the dividend is negative and the remainder is nonzero, the quotient is –(6 + 1) = -7 and the remainder is 19 – 9 = 10. To check that -123 div 19 = -7 and -123 mod 19 = 10, we note that -123 = (-7)(19) + 10.

10. (d) (1 point) what are the quotient and remainder when -1 is divided by 23.

Answer: Sincer 1 div 23 = 0 and 1 mod 23 = 1, we have -1 div 23 = -1 and -1 mod 23 = 22.

10. (e) (1 point) what are the quotient and remainder when -2002 is divided by 87.

Answer: Since 2002 div 87 = 23 and 2002 mod 87 = 1, we have -2002 div 87 = -24, -2002 mod 87 = 86.

14. (2 point) Show that if a is an integer and d is a positive integer greater than 1, then the quotient and remainder obtained when a is divided by d are ⎣a/d⎦ and a – d ⎣a/d⎦, respectively.

Answer: By Theorem 2 we have a = dq + r with 0 ≤ r < d, Dividing the equation by d we obtain a/d = q + (r/d), with 0 ≤ (r/d) < 1. Thus by definition it is clear that q is ⎣a/d⎦. The original equation show, of course, that r = a – dq, proving the second of the original statements.

16(c) (1 point) Evaluate these quantities: -101 mod 13.

Answer: Since -101 = 13 \* (-8) + 3, the remainder is 3. That is, -101 mod 13 = 3. Note that we do not write -101 = 13 \* (-7) -10; we can’t have -101 mod 13 = -10, because a mod b is always nonnegative.

16(d) (1 point) Evaluate these quantities: 199 mod 19.

Answer: Since 199 = 19 \* 10 + 9, the remainder is 9. That is, 199 mod 19 = 9.

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

(a) k = 104578690, h(k) = k mod 101 = 104578690- ⎣104578690/101⎦ · 101 = 58.

(b) k = 432222187, h(k) = k mod 101 = 432222187- ⎣432222187/101⎦ · 101 = 60.

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 = 4?

Answer: We are given x0 = 4. Then x1 = (4 · 4+1) mod 7 = 17 mod 7 = 3; x2 = (4 · 3+1) mod 7 = 13 mod 7 = 6; x3 = (4 · 6+1) mod 7 = 25 mod 7 = 4 = x0; x4 = (4 · 4+1) mod 7 = 17 mod 7 = 3 = x1.   
So the sequence repeats 4, 3, 6, 4, 3, 6, 4,….

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

HDW GLP VXP

Answer: EAT DIM SUM.

Additional problem: Find the smallest positive **a** such that **a ≡ 2a-5 (mod 3)** is satisfied.

Answer: according to the Theorem 4, **a = 2a – 5 + k · 3**, and k is an integer. So that **a = 5 – 3k**, and the smallest positive **a** is 2.

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

2. (6 points) Determine whether each of these integers is prime.

1. 19 Prime.
2. 27 Since 27 = 33, 27 is not prime.
3. 93 Since 93 = 31 · 3, 93 is not prime.
4. 101 Prime.
5. 107 Prime.
6. 113 Prime.

3. (6 points) Find the prime factorization of each of these integers.

1. 88. Since 2 is a factor of 88, and the quotient upon division by 2 is 44, We divide by 2 again then again, leaving a quotient of 11. Since 11 is prime, the prime factorization: 88 = 23 · 11.
2. 126. The prime factorization: 126 = 2 · 32 · 7
3. 729. The prime factorization: 729 = 36
4. 1001. The prime factorization: 1001 = 7 · 11 · 13
5. 1111. The prime factorization: 1111 = 11 · 101 (we know that 101 is prime because we have already tried all prime factors less than √101)
6. 909,090. The prime factorization: 909,090 = 2 · 33 · 5 · 7 · 13 · 37

5. (2 points) Find the prime factorization of 10!.

Answer: 10! = 10 · 9 · 8 · 7 · 6 · 5 · 4 · 3 · 2 = 28 · 34 · 52 · 7

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.

10. (2 points) Which positive integers less than 50 are relatively prime to 50.

Answer: We must find, by inspection with mental arithmetic, the greatest common divisors of the numbers from 1 to 49 with 50, and list those whose gcd is 1. There are 1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39, 41, 43, 47, 49. Note that 2 and 5 is not a prime factor of 50, we can try primes and composition of two primes less than 50.

13. (4 points) Determine whether the integers in each of these sets are pairwise relatively prime.

a) 11, 15, 19

Answer: Since gcd(11, 15) = 1, gcd (11, 19) = 1, and gcd(15, 19) = 1, these three numbers are pairwise relatively prime.

b) 14, 15, 21

Answer: Since gcd(15, 21) = 3 > 1, these three numbers are not pairwise relatively prime.

c) 12, 17, 31, 37

Answer: Since gcd(12, 17) = 1, gcd(12, 31) = 1, gcd (12, 37) = 1, gcd(17, 31) = 1, gcd(17, 37) = 1, and gcd(31, 37) = 1, these four numbers are pairwise relatively prime. (Indeed, the last three are primes, and the prime factors of the first are 2 and 3.)

d) 7, 8, 9, 11

Answer: Again, since no two of 7, 8, 9 and 11 have a common factor greater than 1, this set is pairwise relatively 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?

(c) gcd(17, 1717) = 17. (17 is a prime itself.)

(f)gcd( 2 · 3 · 5 · 7, 2 · 3 · 5 · 7) = 2 · 3 · 5 · 7. (They are both of the same value.)

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

(c) lcm(17, 1717) = 1717.

(f) gcd(2 · 3 · 5 · 7, 2 · 3 · 5 · 7) = 2 · 3 · 5 · 7. (They are both of the same value.)

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.

32. (2 points) Show that if a, b, and m are integers such that m ≥ 2 and a ≡ b (mod m), then gcd(a, m) = gcd(b, m).

Answer: From a ≡ b (mod m) we know that b = a + sm for some integer s. Now if d is a common divisor of a and m, then it divides the right-hand side of this equation, so it also divides b. We can rewrite the equation as a = b – sm, and then by similar reasoning, we see that every common divisor of b and m is also a divisor of a. This shows that the set of common divisors of an and m is equal to the set of common divisions of b and m, so certainly gcd(a, m) = gcd(b, m).

34. (3 points) Prove or disprove that p1p2 … pn+1 is prime for every positive integer n, where p1p2 … pn are the n smallest prime numbers.

Answer: We compute the first several of these: 2 + 1 = 3 (which is prime), 2 · 3 + 1 = 7(which is prime), 2 · 3 · 5 + 1 = 31(which is prime), 2 · 3 · 5 · 7 + 1 = 211(which is prime), 2 · 3 · 5 · 7 · 11 + 1 = 2311(which is prime), however 2 · 3 · 5 · 7 · 11 · 13 + 1 = 30031 = 59 · 509 , so the conjecture is false. Notice, however, that the prime factors in this last case were necessarily different from the primes being multiplied.