CSE 015: Discrete Mathematics
Homework #10 Solutions

Chapter 4.3

- 31: Let d = gcd(a,b) and l = lcm(a,b). Notice that $\frac{ab}{d}$ is a common multiple of both a and b, since $\frac{a}{d}$ and $\frac{b}{d}$ are integers, by definition. By euclidean algorithm, $\frac{a}{d}$ and $\frac{b}{d}$ are relatively prime. Now assume n is a common multiple of a and b; then we can find integers k and k' such that $n = ka$ and $n = kb'$, so $ka = k'b$. We divide both sides by d to get $k'\frac{b}{d} = k\frac{a}{d}$. Hence, $\frac{a}{d}$ divides $\frac{b}{d}k'$ and since $\frac{a}{d}$ and $\frac{b}{d}$ are relatively prime then $\frac{a}{d}$ divides k'. Hence $n = k'b = q\frac{ab}{d}$ for some integer q. So $\frac{ab}{d}$ divides n. Hence, lcm(a,b) $= \frac{ab}{d} = \frac{ab}{gcd(a,b)}$.

- 32(c): gcd(123, 277) = gcd(123, 31) = gcd(31, 30) = gcd(30, 1) = gcd(1, 0) = 1

- 32(d): gcd(1529, 14039) = gcd(1529, 278) = gcd(278, 139) = gcd(139, 0) = 139

- 42:We take a = 356 and b = 252 to avoid a needless first step. When we apply the Euclidean algorithm we obtain the following quotients and remainders: $q_1 = 1$, $r_2 = 104$, $q_2 = 2$, $r_3 = 44$, $q_3 = 2$, $r_4 = 16$, $q_4 = 2$, $r_5 = 12$, $q_5 = 1$, $r_6 = 4$, $q_6 = 3$. Note that n = 6. Thus we compute the successive s's and t's as follows, using the given recurrences:

  $s_2 = s_0 - q_1 s_1 = 1 - 1.0 = 1,$ $\quad t_2 = t_0 - q_1 t_1 = 0 - 1.1 = -1$
  $s_3 = s_1 - q_2 s_2 = 0 - 2.1 = -2,$ $\quad t_3 = t_1 - q_2 t_2 = 1 - 2.(-1) = 3$
  $s_4 = s_2 - q_3 s_3 = 1 - 2.(-2) = 5,$ $\quad t_4 = t_2 - q_3 t_3 = -1 - 2.3 = -7$
  $s_5 = s_3 - q_4 s_4 = -2 - 2.5 = -12,$ $\quad t_5 = t_3 - q_4 t_4 = 3 - 2.(-7) = 17$
  $s_6 = s_4 - q_5 s_5 = 5 - 1.(-12) = 17,$ $\quad t_6 = t_4 - q_5 t_5 = -7 - 1.17 = -24$
  Thus we have $s_6 a + t_6 b = 17.356 + (-24).252 = 4$, which is gcd(356,252)

- 50: 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 a and m is equal to the set of common divisors of b and m, so certainly gcd(a,m) = gcd(b,m) .

Chapter 4.4

- 6(a): The first step of the procedure in Example 1 yields 17 = 8.2 + 1, which means that 17 - 8.2 = 1, so -8 is an inverse. We can also report this as 9, because -8 ≡ 9 (mod 17).

- 6(b):We need to find s and t such that 34s + 89t = 1. Then s will be the desired inverse, since 34s.1 (mod 89) (i.e., 34s-1 = -89t is divisible by 89). To do so, we proceed as in Example 2. First we go through the Euclidean algorithm computation that gcd(34,89) = 1:

  89 = 2.34+21
  34 = 21+13

21 = 13+8
13 = 8 + 5
8 = 5 + 3
5 = 3+2
3 = 2+1

Then we reverse our steps and write 1 as the linear combination:

1 = 3-2
= 3 - (5-3) = 2.3 - 5
= 2.(8-5) - 5 = 2.8 - 3.5
= 2.8 - 3.(13-8) = 5.8 - 3.13
= 5.(21-13) - 3.13 = 5.21 - 8.13
= 5.21 - 8.(34-21) = 13.21 - 8.34
= 13.(89 - 2.34) - 8.34 = 13.89 - 34.34

Thus s = -34, so an inverse of 34 modulo 89 is -34, which can also be written as 55.

- 10: We know that 9 is an inverse of 2 modulo 17. Therefore, if we multiply both sides of this equation by 9 we will get x≡9.7 (mod 17). Since 63 mod 17 = 12, the solutions are all integers congruent to 12 modulo 17, such as 12, 29, and -5. We can check, for example, that 2.12 = 24≡7 (mod 17). This answer can also be stated as all integers of the form 12 + 17k for k ∈ Z.

- 12(a):We know that 55 is an inverse of 34 modulo 89, so x≡77.55 = 4235 ≡ 52 (mod 89). Check: 34.52 = 1768 ≡ 77 (mod 89).

Chapter 4.5

- 2(a):58

- 2(b):60

- 6:We just calculate using the formula. We are given $x_0 = 3$. Then $x_1 = (4.3 + 1)$ mod 7 = 13 mod 7 = 6; $x_2 = (4.6 + 1)$ mod 7 = 25 mod 7 = 4; $x_3 = (4.4 + 1)$ mod 7 = 17 mod 7 = 3. At this point the sequence must continue to repeat 3, 6, 4, 3, 6, 4, . . . forever.

Chapter 4.6

- 2(a) WXST TSPPYXMSR

- 2(b) NOJK KJHHPODJI