Jennifer Cafiero

CS 135 Homework 9

6 May 2015

I pledge my honor that I have abided by the Stevens Honor System.

Section 4.1

1. 1. 10
2. 0
3. 6
4. 16, 28, 40, 52, & 64

Section 4.2

1. 1. Sum = 1022  
      Product = 101220
   2. Sum = 21210  
      Product = 111020122
2. (644)10 = (10 1000 0100)2  
   a = 1010000100  
   i = 0 – 9  
   x = 1  
   i = 0. a0­­ = 0, x = 1 and power = 112 mod 645 = 121  
   i = 1. a­­1 = 0, x = 1 and power = 1212 mod 645 = 451  
   i =2. a2 = 1, x = (1 \* 451) mod 645 = 451 and power = 4512 mod 645 = 226  
   i =3. a3 = 0, x = 451 and power = 2262 mod 645 = 121  
   i = 4. a4 = 0, x = 451 and power = 1212 mod 645 = 451  
   i =5. a5 = 0, x = 451 and power = 4512 mod 645 = 226  
   i =6. a6 = 0, x = 451 and power = 2262 mod 645 = 121  
   i = 7. a7 = 1, x = (451 \* 121) mod 645 = 391 and power = 1212 mod 645 = 451  
   i = 8. a8 = 0, x = 391 and power = 4512 mod 645 = 226  
   i = 9. a9 = 1, x = (391 \* 226) mod 645 = 1, x =1

Section 4.4

1. 15 \* 7 = 105 1 (mod 26)
3. 89 = 2 \* 34 + 21  
   34 = 1 \* 21 + 13  
   21 = 1 \* 13 + 8  
   13 = 1 \* 8 + 5  
   8 = 1 \* 5 + 3  
   5 = 1 \* 3 + 2  
   3 = 1\* 2 + 1  
   2 = 2 \* 1   
   Retrace:  
   1 = 1\*3 + (-1) \* 2 = (-1) \* 5 + 2 \* 3 = 2 \* 8 + (-3) \* 5 = (-3) \* 13 + 5 \* 8   
    = 5 \* 21 + (-8) \* 12 = (-8) \* 34 + 13\*21 = 13 \* 89 + (-34) \* 34   
   Answer: -34 55 mod 89
4. 1. x = 52 mod 89
5. All values of k that fit the following: k = 53 mod 60, x = 60\*k +53
6. gcd(23, 41) = 1  
   2340 = 1 mod 41  
   231002 = 2340^25 \*232 = 1250 \* 529 = 37 mod 41

Section 4.6 (Assume A = 0, B = 1, … Z = 25)

* 2. GR QRW SDVV JR

1. 1. SURRENDER NOW
2. 1913 mod (43 \* 59) = 2299  
    190013 mod (43 \* 59) = 1317  
    21013 mod (43 \* 59) = 2117  
   2299 1317 2117
3. SQUIRREL
4. First, Alice and Bob have to agree to use a prime number p(101) and a primitive root a(2) of p(101). Then, Alice has to choose a secret integer k1(7) and sends Bob ak1 = 27 = 27 (mod 101). Bob then has to choose his secret integer k­2(9) and sends Alice ak2 = 29 = 7 (mod 101). Alice uses the 7 to compute 77 = 90 (mod 101). Bob uses the 27 to compute 279 = 90 (mod 101). Each key equals 90 so it’s a success.