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

13.
    a. 10
    c. 0
    e. 6

26. 16, 28, 40, 52, & 64

Section 4.2

22.
    a. Sum = 1022
       Product = 101220
    b. Sum = 21210
       Product = 111020122

26.

$(644)_{10} = (10\ 1000\ 0100)_2$

a = 1010000100

i = 0 – 9

x = 1

i = 0. a_0 = 0, x = 1 and power = 11^2 mod 645 = 121

i = 1. a_1 = 0, x = 1 and power = 121^2 mod 645 = 451

i =2. a_2 = 1, x = (1 * 451) mod 645 = 451 and power = 451^2 mod 645 = 226

i =3. a_3 = 0, x = 451 and power = 226^2 mod 645 = 121

i = 4. a_4 = 0, x = 451 and power = 121^2 mod 645 = 451

i =5. a_5 = 0, x = 451 and power = 451^2 mod 645 = 226

i =6. a_6 = 0, x = 451 and power = 226^2 mod 645 = 121

i = 7. a_7 = 1, x = (451 * 121) mod 645 = 391 and power = 121^2 mod 645 = 451

i = 8. a_8 = 0, x = 391 and power = 451^2 mod 645 = 226

i = 9. a_9 = 1, x = (391 * 226) mod 645 = 1, x =1

Section 4.4

1. 15 * 7 = 105 ≡ 1 (mod 26)
6.

b. $89 = 2 * 34 + 21$
$34 = 1 * 21 + 13$
$21 = 1 * 13 + 8$
$13 = 1 * 8 + 5$
$8 = 1 * 5 + 3$
$5 = 1 * 3 + 2$
$3 = 1* 2 + 1$
$2 = 2 * 1$
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: $-34 \equiv 55 \bmod 89$

12.

a. $x = 52 \bmod 89$

20. All values of k that fit the following: $k = 53 \bmod 60$, $x = 60*k +53$

34. $\gcd(23, 41) = 1$
$23^{40} = 1 \bmod 41$
$23^{1002} = 23^{40\wedge 25} *23^2 = 1^{250} * 529 = 37 \bmod 41$

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

1.

a. GR QRW SDVV JR

5.

a. SURRENDER NOW

24. $19^{13} \bmod (43 * 59) = 2299$
$1900^{13} \bmod (43 * 59) = 1317$
$210^{13} \bmod (43 * 59) = 2117$
2299 1317 2117

26. SQUIRREL

30. 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 $k_1(7)$ and sends Bob $a^{k}{}_{1} = 2^7 = 27 \pmod{101}$. Bob then has to choose his secret integer $k_2(9)$ and sends Alice $a^{k}{}_{2} = 2^9 = 7 \pmod{101}$. Alice uses the 7 to compute $7^7 = 90 \pmod{101}$. Bob uses the 27 to compute $27^9 = 90 \pmod{101}$. Each key equals 90 so it’s a success.