Kyle Bell, Jesus Barrera Garcia, Ying Fan, Adam Kosofsky, Gabe Evans, Mason Tyndall

Homework 1

1.12

a) Take a = 4 and b = 2
   1) Set u =1, g = a = 4, x =0, and y = b= 2
   2) Y is not zero
   3) 4 = 2 * 2 + 0
   4) S = 1 – 2*0 = 1
   5) U = 0 and g = 2
   6) X = 1 and y = 0
   7) Y is zero, go v = (2-4*0)/2 = 1

   Therefore, au + bv = gcd(a, b) is true because 4*0 + 1*2 = 2

b) Implement with Java

c)

   i) (1258*13) + (527*-31) = 17; g = 17, u = 13, v = -31
   ii) (1056*8) + (228*-37) = 12; g = 12, u = 8, v = -37
   iii) (167181*-4430) + (163961 *4517) = 7; g = 7, u =-4430, v = 4517
   iv) (239847*59789) + (3892394*-970295) = 1; g = 1, u = 59789 ,v = -970295

d) If b = 0, then a is the gcd and u = 1 and v = 0.

e)

   i) (1258*-18) + (527*43) = 17; g = 17, u = -18, v = 43
   ii) (1056*51) + (228*-11) = 12; g = 12, u = 51, v = -11
   iii) (167181*4517) + (163961 *-4430) = 7; g = 7, u = 4517, v = -4430
   iv) (239847*59789) + (3892394*-970295) = 1; g = 1, u = 59789, v = -970295

1.23

a) X = 31
b) X = 5764
c) X = 221
d) X = a + my

   $a + mk \equiv b \pmod{n}$

   $a + mk – b = nj$

   $mk – nj = b – a$

   since gcd(m, n) = 1, then mu + nv = 1

   then, $mu(b - a) + nv(b - a) = b - a$

   $x = a + mu(b – a) = a + (1 – nv)(b – a) = b + nv(b – a)$

   This shows that $x \equiv a \bmod m$ and $x \equiv v \bmod n$

1.25

a).$17^{183}(mod\ 256)$

183 in binary = 10110111

X	17^{2^0}	17^{2^1}	17^{2^2}	17^{2^4}	17^{2^5}	17^{2^7}
X(mod 256)	17	33	65	1	1	1

17*33*65*1*1*1 (mod 256) = **113**

b.)2^{477}mod(1000)

477 in binary = 111011101

X	2^{2^0}	2^{2^2}	2^{2^3}	2^{2^4}	2^{2^6}	2^{2^7}	2^{2^8}
X(mod 256)	2	16	256	536	616	456	936

2*16*256*536*616*456*936 (mod 1000) = **272**

c.) 11^{507} (mod 1237)

507 in binary = 111111011

X	11^{2^0}	11^{2^1}	11^{2^3}	11^{2^4}	11^{2^5}	11^{2^6}	11^{2^7}	11^{2^8}
X(mod 256)	11	121	388	867	830	1128	748	380

11*121*388*867*830*1128*748*380 (mod 1237) = **322**