Kipling Gillespie
CS 315

Homework 3

Problem 1

3^{220}mod221 = 55 following our modulus exponentiation algorithm. 220_{10}=11011100_2

Z=1

W=3

b0=0

Z=1

W=(3*3)mod221=9

b1=0

Z=1

W=(9*9)mod221=81

b2=1

Z=(1*81)mod221=81

W=(81*81)mod221=152

b3=1

Z=(81*152)mod221=157

W=(152*152)mod221=120

b4=1

Z=(157*120)mod221=55

W=(120*120)mod221=35

b5=0

Z=55

W=(35*35)mod221=120

b6=1

Z=(55*120)mod221=191

W=(120*120)mod221=35

b7=1

Z=(191*35)mod221=55

W=(35*35)mod221=120

55

Kipling Gillespie
CS 315

Problem 2
$3^{101}+8^{101}$ is evenly divisible by 11.

Z=1 W=3 b0=1 Z=(1*3)mod11=3 W=(3*3)mod11=9 b1=0 Z=3 W=(9*9)mod11=4 b2=1 Z=(3*4)mod11=1 W=(4*4)mod11=5 b3=0 Z=1 W=(5*5)mod11=3 b4=0 Z=1 W=(3*3)mod11=9 b5=1 Z=(1*9)mod11=9 W=(9*9)mod11=4 b6=1 Z=(9*4)mod11=3 W=(4*4)mod11=5 3 Thus, 3^{101}mod11 = 3	Z=1 W=8 b0=1 Z=(1*8)mod11=8 W=(8*8)mod11=9 b1=0 Z=8 W=(9*9)mod11=4 b2=1 Z=(8*4)mod11=10 W=(4*4)mod11=5 b3=0 Z=10 W=(5*5)mod11=3 b4=0 Z=10 W=(3*3)mod11=9 b5=1 Z=(10*9)mod11=2 W=(9*9)mod11=4 b6=1 Z=(2*4)mod11=8 W=(4*4)mod11=5 8 Thus, 8^{101}mod11 = 8

Based on the substitution rule of modular congruence which says if for integers A, B, C, D, N, if A≡C mod N and B≡D mod N, then A+B ≡ C+D mod N. I have shown that 3^{101}≡3 mod 11 and that 8^{101}≡8 mod 11. So $3^{101}+8^{101}$≡3+8 mod 11 or 11 mod 11 which is 0 and $11|3^{101}+8^{101}$ with no remainder.

Problem 3
The greatest common divisor of x=392 and y=105 can be calculated with Euclid's Algorithm.
gcd(392, 105) = gcd (105, 392 mod 105) = gcd(105, 77) = gcd(77, 105 mod 77) = gcd(77, 28) = gcd(28, 77 mod 28) = gcd(28, 21) = gcd(21, 28 mod 21) = gcd(21, 7) = gcd(7, 21 mod 7) = gcd(7, 0) -> thus 7 is the greatest common divisor of both 392 and 105.

Part 1.
Does 105^{-1} mod 392 exist? gcd(392, 105) = 7. Thus 392 and 105 are not relatively prime, so no inverse exists for 105^{-1}≡1mod392.

Kipling Gillespie
CS 315

Part 2.
Since the greatest common divisor isn’t 1 we can do this simply without using the extended Euclid’s algorithm. $X = 105/7 = 15$. -> $392y + 105*15 = 7$ -> $392y = 7 - 105*15$ -> $y = (7 - 105*15)/392 = -4$
Thus $105*15 + (-4)392 = 7$. $X = 15$, and $Y = -4$.

Part 3.
According to Bezout’s identity, the greatest common divisor of a and b is also the smallest positive linear combination of the form $ax+by = d$ where d is the greatest common divisor. Since the $\gcd(392, 105) = 7$ and $1<7$, there are no integers x, and y where $105x+392y=1$.