Tom Hopkins
HW 3
1.18, 1.20, 1.27

1.18) gcd(210, 588)

a)

210 = 2 · 105
105 = 3 · 35
35 = 7 · 5

588 = 2 · 294
294 = 2 · 147
147 = 3 · 49
49 = 7 · 7

588 = 2 · 3 · 7 = 42

b)

X		Y		mod
~~588~~	%	210	=	168
210	%	168	=	42
168	%	42	=	0

1.20) inverse of: 20 mod 79

~~79 = 20 · 3 + 19~~
20 = 19 · 1 + 1
1 = 20 − 19
1 = 20 − (79 − (20 · 3))
1 = 20 − 79 + 20(3)
1 = 20(4) ~~− 79~~
$\frac{1}{20} = 4 \pmod{79}$ ~~$20^{-1} \pmod{79} = 4 \pmod{79}$~~

b) 3 mod 62

62 = 3 × 20 + 2
3 = 2 × 1 + 1
1 = 3 − 2 × 1
2 = 62 − (3 × 20)
1 = 3 − (62 − (3 × 20))
1 = 3 − 62 + 3 × 20
1 = 3(21) ~~= 63~~
$\frac{1}{3}$ = 21 mod 62

c) 21 mod 91

91 = 21 × 4 + 7
21 = 7 × 3 + 0

There is no inverse because gcd = 7

d) 5 mod 23

23 = 5 × 4 + 3
5 = 3 × 1 + 2
3 = 2 × 1 + 1
1 = 3 − 2 × 1
2 = 5 − 3 × 1
1 = 3 − (5 − 3)
3 = 23 − 5 × 4
1 = 3 − (5 − (23 − (5 × 4)))
1 = 3 − (5 − 23 + (5 × 4))
1 = 3 − 5 + 23 − 5 × 4
1 = (23 − 5 × 4) + 23 − 5 × 5
1 = (23 × 2) + (5 × 9)
1 = 5(9) 23 = 14
$\frac{1}{5}$ = 14 mod 23

1.27) (p−1)(q−1) = 352 e = 3

352 = 3 × 117 + 1
1 = 352 − 3 × 117
1 = −3 × 117
$\frac{1}{3}$ = 235 (mod 352) (−117 → 235)

So d = 235 (mod 352)

E(m) = 41^e % N = 41^3 % 391 ≠ 105 (mod 391)