Homework #3 Key

1.18

a Factorization

$210 = 2 \cdot 3 \cdot 5 \cdot 7$ and $588 = 2 \cdot 2 \cdot 3 \cdot 7 \cdot 7$. Since they have 2, 3, and 7 in common, the greatest common divisor is $2 \cdot 3 \cdot 7 = 42$.

b Euclidean Algorithm

$$\begin{aligned} 588 &= 2(210) + 168 \\ 210 &= 1(168) + 42 \\ 168 &= 4(42) + 0 \end{aligned}$$

The last nonzero remainder, 42, is the greatest common divisor.

1.20

For each of these you can just find the numbers by hand using the extended euclid algorithm as we did in class. Alternatively, you can walk through them as shown on page 22 of the text, which is the way demonstrated below.

a

$$\begin{aligned} 79 &= 3(20) + 19 \\ 20 &= 1(19) + 1 \\ 1 &= 20 - 19 \\ 1 &= 20 - (79 - 3(20)) = 4(20) - 79 \end{aligned}$$

So $4 \cdot 20 \equiv 1 \pmod{79}$ and $20^{-1} = 4$.

b

$$\begin{aligned} 62 &= 20(3) + 2 \\ 3 &= 1(2) + 1 \\ 1 &= 3 - 2 \\ 1 &= 3 - (62 - 20(3)) = 21(3) - 62 \end{aligned}$$

So $21 \cdot 20 \equiv 1 \pmod{62}$ and $3^{-1} = 21$.

c

$$\begin{aligned} 91 &= 4(21) + 7 \\ 21 &= 3(7) + 0 \end{aligned}$$

Since the greatest common divisor is 7 (and not 1), 21 has no multiplicative inverse $\pmod{91}$.

d

$$\begin{aligned} 23 &= 4(5) + 3 \\ 5 &= 1(3) + 2 \\ 3 &= 1(2) + 1 \\ 1 &= 3 - 2 \\ 1 &= 3 - (5 - 3) = 2(3) - 5 \\ 1 &= 2(23 - 4(5)) - 5 = 2(23) - 9(5) \end{aligned}$$

So $-9 \cdot 5 \equiv 1 \pmod{23}$ and $5^{-1} = -9 \equiv 14 \pmod{23}$.

1.27

First calculate $(p-1)(q-1) = 16 \cdot 22 = 352$. We use the extended Euclid algorithm to compute the $\gcd(a,b) = \gcd(352,3)$ and get the inverse d of $e \pmod{352}$.

Table 1:

a	b	x'	y'	waffle	r_1	r_2	r_3
352	3	0	1	1	1	$0 - \lfloor \frac{352}{3} \rfloor (1) = -117$	1
3	1	1	0	1	0	$1 - \lfloor \frac{3}{1} \rfloor (0) = 0$	1
1	0				1	0	1

We obtain $e \cdot d \equiv 1 \pmod{352}$ which implies $d \equiv -117 \equiv 235 \pmod{352}$.

The encryption of the message $M = 41$ is then

$$\begin{aligned} y &= M^e \pmod{391} \\ &= 41^3 \pmod{391} \\ &\equiv 105 \pmod{391} \end{aligned}$$

And the decryption of $y = 105$ is

$$\begin{aligned} x &= y^d \pmod{391} \\ &= 105^{235} \pmod{391} \\ &\equiv 41 \pmod{391} \end{aligned}$$