Question 1

3.5 / 3.5 pts

The extended GCD algorithm learned in class calculates a sequence of remainders, and each remainder can be expressed as a linear combination of the original two inputs. Fill in the blanks with the sequence of remainders that are computed when calculating egcd(40,15) and the linear combination of 40's and 15's that gives you each remainder. To help, I've filled in the last row for you.

Double check your work because an error in any row will propagate to the next and cause additional incorrect answers.

Remainder	40's	15's
10	1	-2
5	-1	3
0	3	-8

egcd(40, 15)

$\text{egcd}(15, \underbrace{40 \% 15}_{10})$

$$40 = 15 \cdot 2 + 10$$
$$\Rightarrow 10 = 40 \cdot 1 + 15 \cdot (-2)$$

$\text{egcd}(10, \underbrace{15 \% 10}_{5})$

$$15 = 10 \cdot 1 + 5$$
$$\Rightarrow 5 = 15 \cdot 1 + 10 \cdot (-1)$$
$$\Rightarrow 5 = 15 \cdot 1 + [40 \cdot 1 + 15 \cdot (-2)] \cdot (-1)$$
$$\Rightarrow 5 = 15 \cdot 1 + 40 \cdot (-1) + 15 \cdot (2)$$
$$\Rightarrow 5 = 40 \cdot (-1) + 15 \cdot (3)$$

$\text{egcd}(5, \underbrace{10 \% 5}_{0})$

$$10 = 5 \cdot 2 + 0$$
$$\Rightarrow 0 = 10 \cdot (1) + 5 \cdot (-2)$$
$$\Rightarrow 0 = [40 \cdot 1 + 15 \cdot (-2)] \cdot (1) + [40 \cdot (-1) + 15 \cdot (3)] \cdot (-2)$$
$$\Rightarrow 0 = 40 \cdot 1 + 15 \cdot (-2) + 40 \cdot (2) + 15 \cdot (-6)$$
$$\Rightarrow 0 = 40 \cdot 3 + 15 \cdot (-8)$$

Question 2

1.5 / 1.5 pts

Let's say you are generating RSA keys and you choose p=63 and q=67. What is the smallest value of e that qualifies as an encryption exponent?

You may use https://www.wolframalpha.com to aid with this problem. Some useful queries might be things like "gcd(50,35)" or "inverse of 7 mod 13".

5

$p = 63 \quad q = 67 \quad e = ?$

$\phi(n) = (p-1)(q-1) = (62)(66) = 4092$

$e = 5$

$\gcd(5, 4092) = 1$

Question 3

1.5 / 1.5 pts

Let's say you are generating RSA keys and you choose p=19, q=29 and encryption exponent e=11. What value d do you choose for the decryption exponent?

You may use https://www.wolframalpha.com to aid with this problem. Some useful queries might be things like "gcd(50,35)" or "inverse of 7 mod 13".

275

$p = 19 \quad q = 29 \quad e = 11$

$$\phi(n) = (p-1)(q-1)$$
$$= (18)(28)$$
$$= 504$$

let $d = e^{-1} \bmod \phi(n)$

$d = 11^{-1} \bmod 504$

$d = 275$

Question 4

0 / 1.5 pts

On the homework you saw that 3^5 could be expressed as a sequence of squaring and multiplying: `(((1^2*3)^2)^2*3)`

Using this same notation write the sequence of squaring and multiplying for 7^{29}. Begin with 1^2 as your first squaring operation, and include a close-parenthesis after each step (SQ or SQ-MULT), as demonstrated in the example. Do not include any spaces. Note: 7 in binary is 111 and 29 in binary is 11101. Your answer should have 5 open-parenthesis and 5 close-parenthesis.

You may paste your text into https://www.wolframalpha.com and it should give you the correct answer (3219905755813179726837607).

(((((1^2*7))^2*7)^2*7)^2)^2*7

7^{29} $\quad$ $29 = 1\ 1\ 1\ 0\ 1$

pow (x, y):

let $y = y_1 y_2 \cdots y_n$ where $y_i \in \{0, 1\}$

```
acc = 1
for i = 1 to n
    acc = acc * acc
    if yi == 1
        acc = acc * x
return acc
```

$(1^2 \cdot 7)$ $\quad$ 1

$(1^2 \cdot 7)^2 \cdot 7$ $\quad$ 1 1

$((1^2 \cdot 7)^2 \cdot 7)^2 \cdot 7$ $\quad$ 1 1 1

$(((1^2 \cdot 7)^2 \cdot 7)^2 \cdot 7)^2$ $\quad$ 1 1 1 0

$(((((1^2 \cdot 7)^2 \cdot 7)^2 \cdot 7)^2)^2 \cdot 7)$ $\quad$ 1 1 1 0 1

Question 5

2 / 2 pts

In lecture you saw an algorithm for testing if p is prime. In it, x is chosen at random so that 1 < x < p. Some x's are compatible with p being prime and some immediately indicate that p is not prime. When p = 2465, what is the smallest x that indicates p is not prime? In other words, what is the smallest x that, if randomly chosen, would cause the algorithm immediately to report p not prime?

You may use https://www.wolframalpha.com to aid with these problems. Some useful queries might be things like "11^3 mod 11", "gcd(50,35)" or "inverse of 7 mod 13".

5

When $p = 2465$

$x^{\frac{p-1}{2}} \bmod p$

$5^{\frac{2465-1}{2}} \bmod 2465 = 1480 \neq 1$

increment x by 1 until the result doesn't equal 1