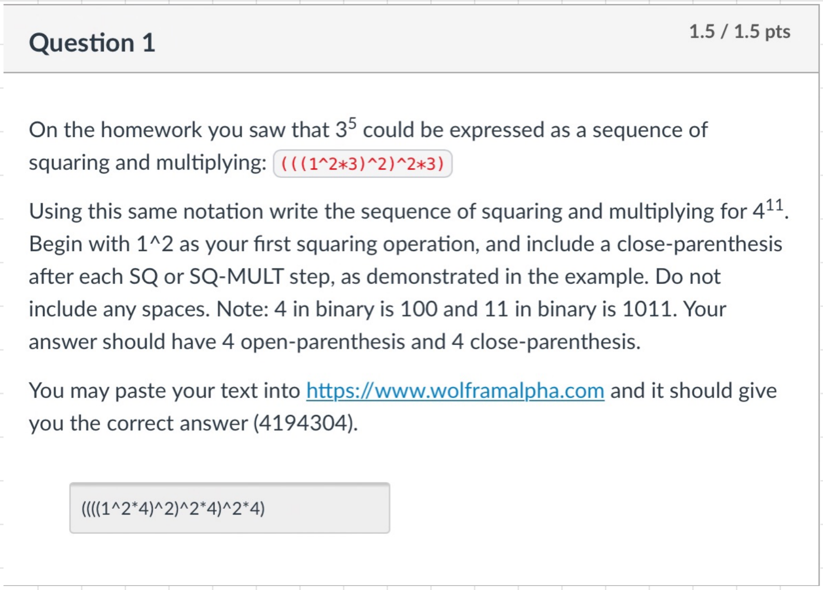


Question 1

1.5 / 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 4^{11}. Begin with 1^2 as your first squaring operation, and include a close-parenthesis after each SQ or SQ-MULT step, as demonstrated in the example. Do not include any spaces. Note: 4 in binary is 100 and 11 in binary is 1011. Your answer should have 4 open-parenthesis and 4 close-parenthesis.

You may paste your text into https://www.wolframalpha.com and it should give you the correct answer (4194304).

((((1^2*4)^2)^2*4)^2*4)

$(4)^{11} \leftarrow \underline{1}011$

Step 1: Convert exponent to binary

11 => 1011

Step 2: 4^{0}

1^2

Step 3: 4^{01}

$1^2 \cdot 4$

Step 4: 4^{010}

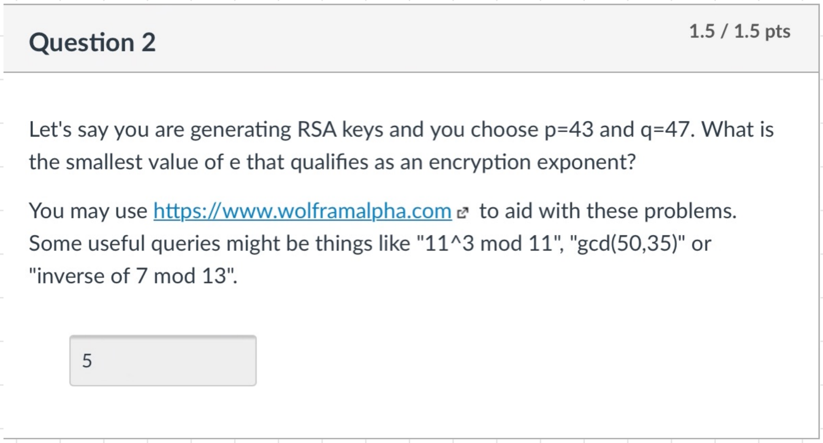
$(1^2 \cdot 4)^2$

Step 5: 4^{0101}

$((1^2 \cdot 4)^2)^2 \cdot 4$

Step 6: 4^{01011}

$((((1^2 \cdot 4)^2)^2 \cdot 4)^2 \cdot 4)$



Question 2

1.5 / 1.5 pts

Let's say you are generating RSA keys and you choose p=43 and q=47. What is the smallest value of e that qualifies as an encryption exponent?

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

$p = 43 \quad q = 47 \quad e = ?$

$n = pq = (43)(47) = 2021$

$\phi(n) = (p-1)(q-1) = (42)(46) = 1932$

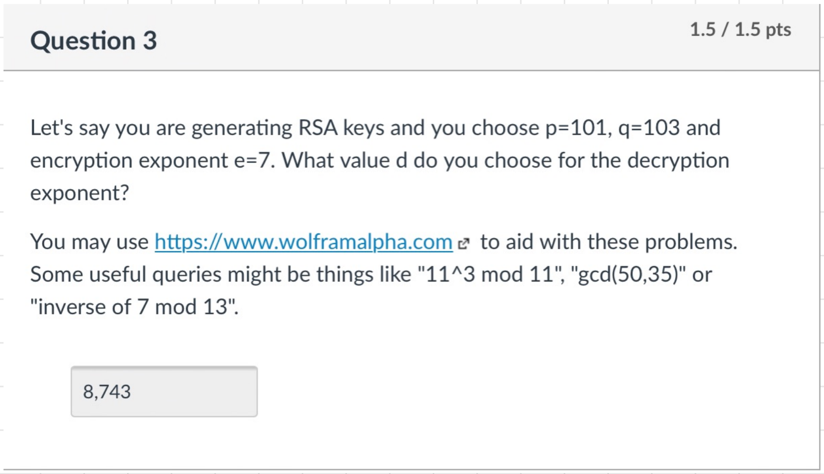
$e = 5$

$1 < e < n$

$1 < e < 1932$

$\gcd(e, 1932) = 1$

$\gcd(5, 1932) = 1$



Question 3

1.5 / 1.5 pts

Let's say you are generating RSA keys and you choose p=101, q=103 and encryption exponent e=7. What value d do you choose for the decryption exponent?

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".

8,743

$p = 101 \quad q = 103 \quad e = 7$

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

$d = 7^{-1} \bmod 10{,}200$

$d = 8743$

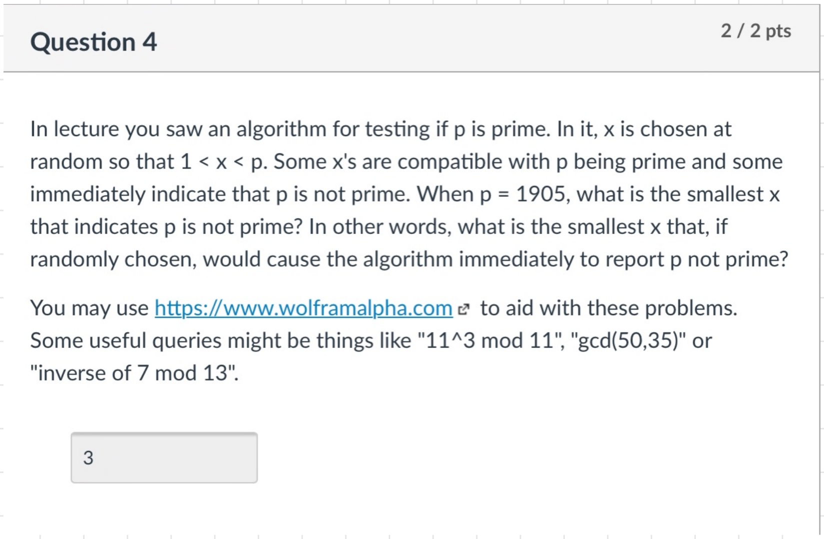
Let $n = pq$

$n = (101)(103) = 10{,}403$

$\phi(n) = (p-1)(q-1)$

$= (100)(102)$

$= 10{,}200$



Question 4

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 = 1905, 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".

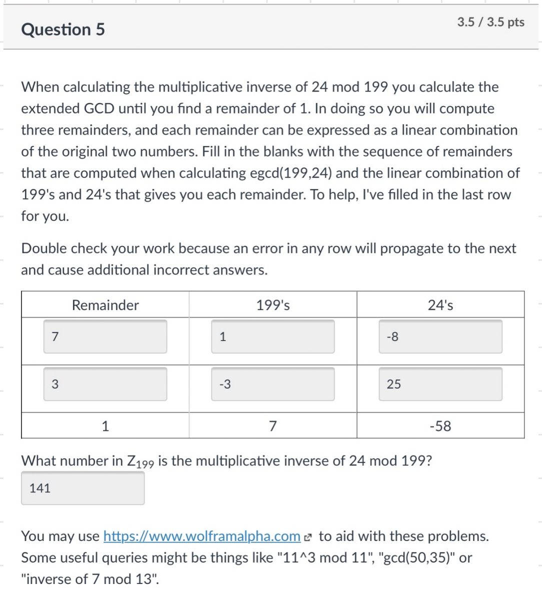
3

When $p = 1905$

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

$$3^{\frac{1905-1}{2}} \bmod 1905 = 861 \neq 1$$

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



Question 5 3.5 / 3.5 pts

When calculating the multiplicative inverse of 24 mod 199 you calculate the extended GCD until you find a remainder of 1. In doing so you will compute three remainders, and each remainder can be expressed as a linear combination of the original two numbers. Fill in the blanks with the sequence of remainders that are computed when calculating egcd(199,24) and the linear combination of 199's and 24'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	199's	24's
7	1	-8
3	-3	25
1	7	-58

What number in Z_{199} is the multiplicative inverse of 24 mod 199?

141

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".

$\text{egcd}(199,\ 24)$

$\text{egcd}(24,\ \underbrace{199 \% 24}_{7})$

$$199 = 24 \cdot 8 + 7$$
$$\Rightarrow 7 = 199 \cdot 1 + 24 \cdot (-8)$$

$\text{egcd}(7,\ \underbrace{24 \% 7}_{3})$

$$24 = 7 \cdot 3 + 3$$
$$\Rightarrow 3 = 24 \cdot 1 + 7 \cdot (-3)$$
$$\Rightarrow 3 = 24 \cdot 1 + [199 \cdot 1 + 24 \cdot (-8)] \cdot (-3)$$
$$\Rightarrow 3 = 24 \cdot 1 + 199 \cdot (-3) + 24 \cdot (24)$$
$$\Rightarrow 3 = 199 \cdot (-3) + 24 \cdot (25)$$

$\text{egcd}(3,\ \underbrace{7 \% 3}_{1})$

$$7 = 3 \cdot 2 + 1$$
$$\Rightarrow 1 = 7 \cdot 1 + 3 \cdot (-2)$$
$$\Rightarrow 1 = [199 \cdot 1 + 24 \cdot (-8)] \cdot 1 + [199 \cdot (-3) + 24 \cdot (25)] \cdot (-2)$$
$$\Rightarrow 1 = 199 \cdot 1 + 24 \cdot (-8) + 199 \cdot (6) + 24 \cdot (-50)$$
$$\Rightarrow 1 = 199 \cdot 7 + 24 \cdot (-58)$$

$1 = 199 \cdot 7 + 24 \cdot (-58) \pmod{199}$ $\quad 199x + 24y = 1 \pmod{199}$

$1 = 24x \bmod 199$ $\quad 24y \bmod 199 = 1$

$x = 141$ $\quad 24^{-1} \bmod 199 = ?$

type " inverse of 24 mod 199 " into Wolfram Alpha

$24^{-1} \bmod 199 = 141$