

This quiz is intended to give you some practice with modular math and RSA. There are 10 questions, each worth 2 points, for a total of 20 points. You will submit your answers in Canvas for evaluation.

When a question asks for the value $\text{mod } n$, the answer is always given in the range 0 to $n-1$. For all open response questions, your answer should be a single integer value (do not include any units).

Question #1:

What is $2^{345} \text{ mod } 31$?

Answer: 1

$$2^{345} = 2^{5 \cdot 69} = 32^{69} \equiv 1^{69} \equiv 1 \text{ mod } 31$$

OR (using Fermat's Little Theorem):

$$\begin{aligned} 2^{30} &\equiv 1 \text{ mod } 31 \Rightarrow 2^{345} = (2^{30})^{11} \times 2^{15} \equiv 1^{11} \times 2^{15} \text{ mod } 31 \\ &\equiv 2^{15} \text{ mod } 31 \\ &= 2^5 \times 2^5 \times 2^5 \text{ mod } 31 \\ &\equiv 1 \times 1 \times 1 \text{ mod } 31 \\ &= 1 \text{ mod } 31 \end{aligned}$$

Question #2:

A new Computer Science algorithms course takes 32 weeks to complete. The CS teacher offers to assign you just one second of homework the first week of school, two seconds the second week, four seconds the third, and so on.

How long would the homework take for the last week of school?

Provide your answer in seconds mod 11.

Answer: 2

$$2^{31} \text{ seconds} = (2^{10})^3 \times 2^1 \equiv (1)^3 \times 2 \text{ mod } 11 \equiv 2 \text{ mod } 11 = 2 \text{ seconds mod } 11$$

Question #3:

What is the value $3^{2003} \text{ mod } 5$

Answer: 2

Using Fermat's Little Theorem,

$$3^{2003} \equiv (3^4)^{500} \times 3^3 \equiv (1)^{500} \times 27 \equiv 2 \text{ mod } 5$$

Question #4:

What is $13^{-1} \bmod 22$? (provide an integer value)

Answer: 17

$d = ax + by = 3 \times 22 - 5 \times 13 \equiv 1 \bmod 22$ (this fits the condition for Extended Euclid).

Since $(3 \times 22) \bmod 22 \equiv 0 \bmod 22$, we have $-5 \times 13 \equiv 1 \bmod 22$

So, $13^{-1} \bmod 22 = -5$ which means that 17 is the answer

A step by step calculation:

$$22 = 1(13) + 9$$

$$13 = 1(9) + 4$$

$$9 = 2(4) + 1$$

$$E1: 9 - 2(4) = 1$$

$$E2: 13 - 1(9) = 4$$

$$E3: 22 - 1(13) = 9$$

$$\text{Using E1: } 9 - 2(4) = 1$$

$$\text{Then substituting for 4 in E1, using E2: } 9 - 2(13 - 1(9)) = 1$$

$$\text{Then collecting common terms: } 3(9) - 2(13) = 1$$

$$\text{Then substituting for 9 here using E3: } 3(22 - 1(13)) - 2(13) = 1$$

$$\text{And collecting common terms: } 3(22) - 5(13) = 1$$

Taking mod 22: $3(22) - 5(13) \bmod 22 = -5(13) \bmod 22 \Rightarrow -5 = 13^{-1} \bmod 22$,
so the answer is 17

Question #5:

Find $(2^{20} + 4^{40} + 5^{50} + 6^{60}) \bmod 7$.

Answer: 6 mod 7

Here, we can use Fermat's Little Theorem:

$$2^{20} = 2^2 \times (2^6)^3 \equiv 4 \bmod 7$$

$$4^{40} = 4^4 \times (4^6)^6 \equiv 4 \bmod 7$$

$$5^{50} = 5^2 \times (5^6)^8 \equiv 4 \bmod 7$$

$$6^{60} = (6^6)^{10} \equiv 1 \bmod 7$$

$$\text{So, } (2^{20} + 4^{40} + 5^{50} + 6^{60}) \bmod 7 \equiv (4 + 4 + 4 + 1) \bmod 7 = 6 \bmod 7$$

Question #6:

How many numbers in the range 1...143 are relatively prime with 143?

Answer: 120

As $143 = 11 \times 13$, the product of two prime numbers, we can use Euler's Totient Function where $\phi(N) = (p - 1)(q - 1)$, giving
 $(11 - 1)(13 - 1) = (10)(12) = 120$

Question #7:

A red ribbon spool has 22,608 inches of ribbon and a blue ribbon spool has 10,206 inches of ribbon. The ribbons on both spools are to be evenly divided (with no leftover) into pieces of the same length so that the pieces are as long as possible. What is the length of each piece? (Provide an integer value without any units)

Answer: This is the same as $\gcd(22608, 10206)$ which is 18

Using Euclid's algorithm:

Euclid's Gcd	Call $\gcd(a,b)$	$a = b \times \text{factor} + \text{rem } (a \bmod b)$	
Initial call	$\gcd(22608, 10206)$	$22608 = 10206 \times 2 + 2196$	$22608 = 2196 \bmod 10206$
2 nd level	$\gcd(10206, 2196)$	$10206 = 2196 \times 4 + 1422$	$10206 = 1422 \bmod 2196$
3 rd level	$\gcd(2196, 1422)$	$2196 = 1422 \times 1 + 774$	$2196 = 774 \bmod 1422$
4 th level	$\gcd(1422, 774)$	$1422 = 774 \times 1 + 648$	$1422 = 648 \bmod 774$
5 th level	$\gcd(774, 648)$	$774 = 648 \times 1 + 126$	$774 = 126 \bmod 648$
6 th level	$\gcd(648, 126)$	$648 = 126 \times 5 + 18$	$648 = 18 \bmod 126$
7 th level	$\gcd(126, 18)$	$126 = 18 \times 7 + 0$	$126 = 0 \bmod 18$
8 th level	$\gcd(18, 0)$	returns 18	

Using factorization:

Number	
22608	10206
2×11304	2×5103
$2 \times 2 \times 5652$	$2 \times 3 \times 1701$
$2 \times 2 \times 2 \times 2826$	$2 \times 3 \times 3 \times 567$
$2 \times 2 \times 2 \times 2 \times 1413$	$2 \times 3 \times 3 \times 3 \times 189$
$2 \times 2 \times 2 \times 2 \times 3 \times 471$	$2 \times 3 \times 3 \times 3 \times 3 \times 63$
$2 \times 2 \times 2 \times 2 \times 3 \times 3 \times 157$	$2 \times 3 \times 3 \times 3 \times 3 \times 3 \times 21$
	$2 \times 3 \times 3 \times 3 \times 3 \times 3 \times 3 \times 7$

Question #8: (RSA Algorithm)

Your younger brother posts his RSA public key ($N = 133$, $e = 7$). You decide to show him that he needs to pick a stronger key. Find your brother's private key (the value of d). (Provide an integer value)

Answer: 31

The prime factorization of N is $N = 133 = 7 \times 19$. We calculate $(p-1)(q-1) = 6 \times 18 = 108$. The candidate private key is $d = e^{-1} \bmod 108 = 7^{-1} \bmod 108$, and we find it using Euclid:

$$108 = 15(7) + 3$$

$$7 = 2(3) + 1$$

$$1 = 7 - 2(3)$$

$$1 = 7 - 2(108 - 15(7))$$

$$1 = 31(7) - 2(108), \text{ so } d = 31 \text{ is a suitable decryption exponent.}$$

Question #9: (RSA Algorithm)

Using your brother's RSA Public Key ($N=133, e=7$), one of his friends sends him the encrypted message "5" (the number 5 is the complete message). Decrypt the message to your brother. (Provide an integer value)

Answer: 131

From Q8, you calculated that $d=31$. So you need to compute $y^d \bmod N = 5^{31} \bmod 133$, so the following may be helpful:

$$5^2 \equiv 25 \pmod{133}$$

$$5^4 = 25^2 \equiv 93 \pmod{133}$$

$$5^8 = 93^2 \pmod{133} \equiv 4 \pmod{133}$$

$$5^{16} = 4^2 \pmod{133} \equiv 16 \pmod{133}$$

First, we write d as a sum of powers of 2: $d = 31 = 16 + 8 + 4 + 2 + 1$

$$5^d = 5^{16+8+4+2+1} = 5^{16} 5^8 5^4 5^2 5^1 \equiv (16)(4)(93)(25)(5) \pmod{133}$$

$$\equiv 744,000 \pmod{133} \equiv 131 \pmod{133}$$

We conclude that the decrypted message is 131.

Question #10: (RSA Algorithm)

Using $p = 3$, $q = 11$, $d = 7$ and $e = 3$ in the RSA algorithm, provide the result of encrypting the number 5. (Provide an integer value)

Answer: 26

The encryption of $x = 5$ is $x^e \bmod (p * q) = 5^3 \bmod (3 * 11) = 125 \bmod 33 = 26$