Q1 FLT (twice)
3 Points

Make sure you don't include any whitespace in your answers, and make sure you do not include the modulus in your answers: in other words, if the problem is in $(\mathrm{mod}\ m)$, your answer should be an integer from 0 to $m-1$.

Q1.1
1 Point

What is $5^6 \pmod 7$?

1

Explanation

Fermat's little theorem: $a^{p-1} \equiv 1 \pmod p$ with $a = 5, p = 7$.

Q1.2
1 Point

What is $5^{32} \pmod{31}$?

25

Explanation

Fermat's little theorem: $a^{p-1} \equiv 1 \pmod p$ with $a = 5, p = 31$; then we have $5^{30} \cdot 5^2 \equiv 1 \cdot 5^2 = 25 \pmod{31}$.

Q1.3
1 Point

If p is prime and $a \not\equiv 0 \pmod{p}$, then $\{a \pmod{p}, 2a \pmod{p}, \ldots, (p-1)a \pmod{p}\} = \{1, 2, \ldots, p-1\}$ always.

- (●) True
- ( ) False

Explanation

This is the sequence $\{ax \pmod{p} : x = 1, 2, \ldots, p-1\}$, which is a bijection with $\{0, 1, \ldots, m-1\}$ if $\gcd(a, p) = 1$.

Q2 RSA Practice

3 Points

Alice and Bob wish to communicate secretly and employ the RSA algorithm to do this. Alice and Bob choose primes, $p = 7$ and $q = 13$, and exponent $e = 5$. Answer the following 3 questions about their communication protocol.

Q2.1

1 Point

What is N in the public key (N, e)?

- ○ $N = 49$
- ○ $N = 77$
- ◉ $N = 91$
- ○ $N = 143$

Explanation

N, the modulus under which encoding and decoding are done, is the product of the primes $pq = 7 \times 13 = 91$.

Q2.2

1 Point

What is the public key (N, e)?

- ○ (77, 7)
- ○ (49, 5)
- ◉ (91, 5)
- ○ (143, 8)

Explanation

$N = 91$ and $e = 5$.

Q2.3
1 Point

Suppose that we know:
$1 = 1 \times 91 + (-18) \times 5.$
$1 = 3 \times 72 + (-43) \times 5.$
$1 = -3 \times 72 + 31 \times 7.$
$1 = (-1) \times 13 + 2 \times 7.$
What is d?

- 73
- 29
- 31
- 2

Explanation

$d \equiv e^{-1} \pmod{(p-1)(q-1)} = e^{-1} \pmod{72}$. Thus $d \equiv 5^{-1} \equiv -43 \equiv 29 \pmod{72}$.