TRUE/FALSE. JUSTIFY AND/OR CORRECT.

(1) If a is coprime to n, then there is a unique integer b such that b is the inverse to a modulo n.

(2) For p prime and $[a] \in \mathbb{Z}_p^\times$, we have $[a]$ is a quadratic residue if and only if $[a]^{-1}$ is a quadratic residue.

(3) If $n \equiv 1 \pmod 4$ then n is a sum of two squares.

(4) For any integers a, n, we have $a^{n-1} \equiv 1 \pmod n$.

(5) If $a > n$, then $[a]_n$ is not an element of $\mathbb{Z}_n$.

(6) If p is an odd prime, and a is coprime to p, then $a^{(p-1)/2} \equiv \pm 1 \pmod p$.

(7) If a, b are coprime, the equation $ax + by = n$ has at most one integer solution (x_0, y_0).

(8) The number $[46]$ is a fifth power in $\mathbb{Z}_{307}$.

(9) If a, b are coprime, the equation $ax + by = n$ has at least one integer solution (x_0, y_0).

(10) There are infinitely many primes p that are congruent to 4 modulo 6.

(11) If p is an odd prime, then exactly half of the elements of $\mathbb{Z}_p^\times$ are quadratic residues.

(12) $77 \in \mathbb{Z}_{120}^\times$.

(13) If a, b are coprime and ab is a perfect cube, then a is a perfect cube.

(14) If n is an integer, the number $n^2 - 2$ can never have a prime factor of the form $p = 8k + 3$.

(15) Every quadratic over $\mathbb{Z}_p$, for p prime, has either zero or two roots.

(16) The notions "even" and "odd" are well-defined in $\mathbb{Z}_{203}$.

(17) The notions "even" and "odd" are well-defined in $\mathbb{Z}_{204}$.

(18) There exist integers m, n, a, b such that $\begin{cases} a \equiv b \pmod{m} \\ a \equiv b \pmod{n} \end{cases}$ but $a \not\equiv b \pmod{mn}$.

(19) The number 445 is a sum of three cubes.

(20) If p, q are distinct primes, then $a^{(p-1)(q-1)+1} \equiv a \pmod{pq}$ for all integers a.

(21) All but finitely many numbers are sums of three squares.

(22) For any $g \in \mathbb{Z}_{100}^{\times}$, either g is a primitive root, $g^{20} = [1]$, or $g^8 = [1]$.

(23) If n is an integer, then at least $2/5$ of the numbers between 0 and n are coprime to n.

(24) There exist integers m, n, a, b, c, d, with $m.n$ coprime, such that

$$\begin{cases} a \equiv c \pmod{m} \\ a \equiv d \pmod{n} \end{cases} \quad \text{and} \quad \begin{cases} b \equiv c \pmod{m} \\ b \equiv d \pmod{n} \end{cases}$$

but $[a] \neq [b]$ in $\mathbb{Z}_{mn}$.

Computations

(1) Find the GCD of 672 and 399.

(2) Find the GCD of 310 and 206, and express this GCD as a linear combination of these numbers.

(3) Find the general integer solution to the equation $310x + 206y = 14$.

(4) Find all solutions in $\mathbb{Z}_{72}$ to the equation $[30]x + [4] = [10]$.

(5) Find all solutions in $\mathbb{Z}_6$ to the equation $x^3 + [5]x^2 = [2]$.

(6) Find all solutions to the system
$$\begin{cases} x \equiv 4 \pmod{10} \\ x \equiv 7 \pmod{17} \end{cases}$$

(7) Find all solutions to the system
$$\begin{cases} x \equiv 4 \pmod{10} \\ x \equiv 7 \pmod{16} \end{cases}$$

(8) Compute $3^{2023} \pmod{5}$.

(9) Compute $3^{2023} \pmod{25}$.

(10) Compute the last digit of $3^{3^{3^3}}$.

(11) Compute the index/discrete logarithm of $[7]$ with respect to the primitive root $[2]$ in $\mathbb{Z}_{11}$.

(12) Determine how many primitive roots there are in $\mathbb{Z}_{37}$.

(13) Compute $\left(\frac{27}{503}\right)$. ($503$ is prime.)

(14) Compute $\left(\frac{107}{173}\right)$. ($107$ and 173 are prime.)

(15) Determine how many roots the quadratic polynomial $x^2 + [3]x + [13]$ has in $\mathbb{Z}_{101}$.

(16) Find a formula for all of the rational points on the circle $x^2 + y^2 = 5$.