TRUE/FALSE. JUSTIFY AND/OR CORRECT.

answers + hints

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

F : there is a unique congruence class mod n comprising the inverses to a mod 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.

T

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

F : $n=21$ is not

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

F : $a=0$ $n=2$

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

F

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

T : Euler criterion

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

F

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

T : $[46] = g^k$ want $[46] = a^5 = g^{5l}$; $g^{306} \equiv 1$, $[5]$ unit mod 306 $\Rightarrow 5l \equiv k \bmod 306$ has sol'n for any k

$a = g^l$ primitive

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

T

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

F : $\Rightarrow p$ even

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

T : even index vs odd index

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

F : $[77] \in \mathbb{Z}_{120}^\times$

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

T

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

T : $2 \equiv n^2 \bmod p \Rightarrow \left(\frac{2}{n}\right) = 1$

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

F : could have $[b^2 - 4ac] = [0]$

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

F

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

T

(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 $a \not\equiv b \pmod{mn}$.

T $m = n = 2$, $a = 1, b = 3$

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

F (go mod 9... Only cubes are $[0], [1], [8], \ldots$)

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

T (go mod p, mod q, show holds for both & apply CRT)

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

F (go mod 8... $n \equiv 7 \bmod 8 \Rightarrow n \neq a^2 + b^2 + c^2$)

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

T (g not prim. $\Rightarrow \operatorname{ord}(g) \mid 40 \Rightarrow \operatorname{ord}(g) \mid 20$ or $\operatorname{ord}(g) \mid 8$)

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

F ($n = 30$ works)

(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 $\mathbb{Z}_{mn}$.

F : CRT

COMPUTATIONS

answers

(1) Find the GCD of 672 and 399. 21

(2) Find the GCD of 310 and 206, and express this GCD as a linear combination of these numbers. $2 = 2 \cdot 310 - 3 \cdot 206$

(3) Find the general integer solution to the equation $310x + 206y = 14$. $(26+103k, -42-155k)$, $k \in \mathbb{Z}$

(4) Find all solutions in $\mathbb{Z}_{72}$ to the equation $[30]x + [4] = [10]$. $\{[5], [17], [29], [41], [53], [65]\}$

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

(6) Find all solutions to the system

$$\begin{cases} x \equiv 4 \pmod{10} \\ x \equiv 7 \pmod{17} \end{cases}$$

$24 + 170k$, $k \in \mathbb{Z}$

(7) Find all solutions to the system

$$\begin{cases} x \equiv 4 \pmod{10} \\ x \equiv 7 \pmod{16} \end{cases}$$

$\emptyset$

(8) Compute $3^{2023} \pmod 5$. 2

(9) Compute $3^{2023} \pmod{25}$. 2

(10) Compute the last digit of 3^{3^3}. 7

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

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

(13) Compute $\left(\frac{27}{503}\right)$. (503 is prime.) 1

(14) Compute $\left(\frac{107}{173}\right)$. (107 and 173 are prime.) -1

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

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

$\left(2 - \frac{2m+4}{m^2+1}, 1 + m\left(\frac{2m+4}{m^2+1}\right)\right)$ $m \in \mathbb{Q}$