TRUE/FALSE. JUSTIFY AND/OR CORRECT.

(1) There is an isosceles right triangle with integer side lengths. FALSE

(2) Every triple of positive integers (a, b, c) with $a < b < c < a + b$ forms the side lengths of a triangle. TRUE

(3) If (a, b, c) are integers that form the side lengths of a right triangle, then there exists some integer n and some (u, v, w) pairwise coprime integers that form the side lengths of a right triangle with $a = nu$, $b = nv$, $c = nw$. TRUE

(4) If the GCD of a, b, c is 1, then some pair of the numbers a, b, c is coprime. FALSE

(5) If a, b are coprime and a divides bc, then a divides c. TRUE

(6) If $[a]_n \cdot [b]_n = [0]_n$, then $[a]_n = [0]_n$ or $[b]_n = [0]_n$. FALSE

(7) Every element of $\mathbb{Z}_{61}$ has a multiplicative inverse. FALSE

(8) 67 is a square in $\mathbb{Z}_{187}$. (Note that $187 = 11 \cdot 17$.) TRUE

(9) All but finitely many integers can be written as a difference of two squares. FALSE

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

(11) If n is odd, then exactly half of the elements of $\mathbb{Z}_p^\times$ are squares. FALSE

(12) If $\gcd(a, 60) = 1$ and $a^3 \equiv 1 \pmod{60}$, then $a \equiv 1 \pmod{60}$. TRUE

(13) If $p \geq 5$ is prime, then $p^2 - 1$ is a multiple of 24. TRUE

(14) If p is prime, every element of $\mathbb{Z}_p$ has either $0, 1$, or 3 cube roots. TRUE

(15) If $n = pq$ with p, q prime, every element of $\mathbb{Z}_n$ has at most 6 cube roots. FALSE

(16) There are infinitely many primes p that are congruent to 3 modulo 4. TRUE

(17) There are infinitely many primes p that are congruent to 2 modulo 4. FALSE

(18) There are infinitely many primes p that are congruent to 1 modulo 4. TRUE

(19) There are infinitely many triangular-pentagonal numbers. TRUE

(20) There is an element of order 52 in $\mathbb{Z}_{53}^\times$. TRUE

(21) There is an element of order 13 in $\mathbb{Z}_{53}^\times$. TRUE

(22) There is an element of order 51 in $\mathbb{Z}_{52}^\times$. FALSE

(23) There is an element of order 24 in $\mathbb{Z}_{52}^\times$. FALSE

(24) The set of units in $\mathbb{Z}[\sqrt{D}]$ for D a positive nonsquare integer forms a group under multiplication. TRUE

(25) Given D a positive nonsquare integer, the set of solutions (x, y) to the equation $x^2 - Dy^2 = 2$ has a group structure coming from identifying (x, y) with $x + y\sqrt{D}$. FALSE

(26) The set of positive solutions to any Pell's equation forms a group. FALSE

(27) Given D a positive nonsquare integer, the group operation on the solutions (x, y) to $x^2 - Dy^2 = 1$ has inverse operation $(x, y) \mapsto (-x, y)$. FALSE

(28) If n is an integer, the number $n^2 - 2$ can never have a prime factor of the form $p = 8k + 5$. TRUE

(29) Every $\mathbb{Z}_n^\times$ has a primitive root. FALSE

(30) An element $[a]_p$ cannot both be a primitive root and a quadratic residue. TRUE

(31) Every element of $\mathbb{Z}_{12}$ is a multiple of $[5]$. TRUE

(32) Every element of $\mathbb{Z}_{13}^\times$ has a 5th root. TRUE

(33) If $ab = c$, and none of a, b, c is a multiple of p then at least one of a, b, c has a square root modulo p. TRUE

(34) $[41]$ is not an element of $\mathbb{Z}_{40}$. FALSE

(35) If $x^2 + 2 = Dy^2$, for some positive integers x, y, D with $D \geq 10$ not a square, then $\frac{x}{y}$ occurs as a convergent in the continued fraction of $\sqrt{D}$. TRUE

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

(37) If D is a positive nonsquare integer, the equation $x^2 - Dy^2 = -2$ definitely has a solution. FALSE

(38) If r is an irrational number and $\left|\frac{p}{q} - r\right| < \frac{1}{q}$, then $\frac{p}{q}$ appears as a convergent in the continued fraction expansion of r. FALSE

(39) If r is an irrational number then there are infinitely many rational numbers p/q with $p/q < r < p/q + 1/q^2$. TRUE

(40) Every number has a finite continued fraction expansion. FALSE

(41) There is a rational number with denominator less than 100 that is closer to $\pi = [3; 7, 15, 1, 292, 1, \dots]$ than $355/113$ is. FALSE

(42) The group law on an elliptic curve is given by taking two points P, Q on E and setting $P \star Q$ to be the third point on the line between P and Q on E. FALSE

(43) The origin is the identity in the elliptic curve group. FALSE

(44) Every point on the y-axis of an elliptic curve has order 2. TRUE

(45) Every inflection point on a real elliptic curve has order 3. TRUE

(46) A real elliptic curve $\overline{E}$ can have infinitely many points of order 4. FALSE

(47) An elliptic curve $\overline{E}_p$ over $\mathbb{Z}_p$ can have more than $2p + 1$ points. FALSE

(48) An elliptic curve $\overline{E}_p$ with 26 points (including ∞) can have a point with order 4. FALSE

COMPUTATIONS

(1) Compute the GCD of 874 and 209, and express it as a linear combination of those numbers. $19 = -5 \cdot 874 + 21 \cdot 209$

(2) Compute the GCD of 305 and 204, and express it as a linear combination of those numbers. $1 = 101 \cdot 305 - 151 \cdot 204$

(3) Find the general integer solution to the equation $874x + 209y = 14$. $\varnothing$

(4) Find the general integer solution to the equation $874x+209y = 95$. $x = -25+11k$, $y = 105 - 46k$, $k \in \mathbb{Z}$

(5) Find the multiplicative inverse of $[204]_{305}$, if it exists. $[-151]_{305}$

(6) Find all solutions in $\mathbb{Z}_{874}$ to $[209]z - [120] = [13]$. $[147] + [19]k$, $0 \leq k < 46$

(7) Find all solutions in $\mathbb{Z}_7$ to the equation $x^3 + [2]x = [5]$. $x = [2], [3]$

(8) Find all solutions to the system $\begin{cases} x \equiv 3 \pmod{10} \\ x \equiv 5 \pmod{17} \end{cases}$ $73 + 173k$, $k \in \mathbb{Z}$

(9) Find all solutions to the system $\begin{cases} x \equiv 3 \pmod{10} \\ x \equiv 4 \pmod{16} \end{cases}$ $\varnothing$

(10) Find all square roots of -1 modulo 91. $\pm[1], \pm[27]$

(11) Compute $\phi(6!)$. 192

(12) Compute $7^{2023} \pmod{5}$. $3 \pmod{5}$

(13) Compute $7^{2023} \pmod{200}$. $143 \pmod{200}$

(14) Solve $x^{137} \equiv 17 \pmod{667(= 23 \cdot 29)}$ $191 \pmod{667}$

(15) Compute the index/discrete logarithm of $[9]$ with respect to the primitive root $[2]$ in $\mathbb{Z}_{11}$. 6

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

(17) Find the general solution to $x^2 - 63y^2 = 1$. $(\pm x_k, y_k)$, $k \in \mathbb{Z}$, where $x_k + y_k\sqrt{63} = (8 + \sqrt{63})^k$.

(18) Find the general solution to $x^2 - 55y^2 = 1$. $(\pm x_k, y_k)$, $k \in \mathbb{Z}$, where $x_k + y_k\sqrt{55} = (89 + 12\sqrt{55})^k$.

(19) Find three positive integer solutions to $x^2 - 2y^2 = 7$. $(3, 1)$, $(13, 9)$, $(75, 53)$

(20) Find the first four convergents (starting with $C_0 = 0$) in the continued fraction expansion of $\frac{2+\sqrt{2}}{5}$. $0/1$, $1/1$, $2/3$, $13/19$

(21) Evaluate the continued fraction $[2; 1, 2, 3]$. $30/11$

(22) Compute $\left(\frac{86}{163}\right)$. -1

(23) Determine how many roots the quadratic polynomial $x^2 - 3x + 8$ has modulo 41. 2

(24) For the points $P = (2, 4)$, $Q = (0, 4)$ in the real elliptic curve $\overline{E}$ given by $y^2 = x^3 - 4x + 16$, compute $P \star Q$, $P \star P$, and $Q \star Q$. $(-2, -4)$, $(-3, 1)$, $(0, -4)$

(25) Compute $([0], [0]) \star ([1], [2])$ in the elliptic curve $\overline{E}_7$ given by $y^2 = x^3 + 3x$ over $\mathbb{Z}_7$. $([3], [1])$

(26) Compute the order of every point in the elliptic curve $\overline{E}_7$ given by $y^2 = x^3 + x + [1]$ over $\mathbb{Z}_7$. ∞ has order 1 and $([0] \pm [1])$, $([2], \pm[2])$ all have order 5.