---

1. Determine / calculate / find the following:

   (a) Integers x, y with $688x + 164y = \gcd(688, 164)$.

   (b) The remainder when $7^{29} \cdot 28!$ is divided by 29.

   (c) The values of $\varphi(121)$ and $\varphi(5^3 7^5)$.

   (d) The value $0.1\overline{49}$ as a rational number.

   (e) All units and zero divisors modulo 12.

   (f) Multiplicative inverses of 5 and 7 modulo 97.

   (g) The orders of 3 and 7 modulo 22.

   (h) All n with $n \equiv 2 \pmod 9$ and $n \equiv 7 \pmod{14}$.

   (i) A Fermat factorization of 851, noting $\sqrt{851} \approx 29.17$.

   (j) Polynomials p, q with $(x^3+1)p + (x^2+2)q = \gcd(x^3+1, x^2+1)$ in $\mathbb{F}_3[x]$.

   (k) Gaussian integers p, q with $(11+24i)p + (13-i)q = \gcd(11+24i, 13-i)$ in $\mathbb{Z}[i]$.

   (l) The multiplicative inverse of $x+3$ modulo x^3+5 in $\mathbb{R}[x]$.

   (m) The solution to $(1+i)x \equiv 3 \pmod{8+i}$ in $\mathbb{Z}[i]$.

   (n) All units and zero divisors in $\mathbb{F}_3[x]$ modulo x^2+2x.

   (o) The number of primitive roots modulo 17, 18, 19, 20, and 21.

   (p) The number of residue classes in $\mathbb{Z}[i]$ mod $7+2i$ and $\mathbb{F}_5[x]$ mod x^4+2.

   (q) The irreducible factorizations of x^2+x+1 in $\mathbb{F}_3[x]$, $\mathbb{F}_5[x]$, and $\mathbb{F}_7[x]$.

   (r) The number of monic irreducible polynomials in $\mathbb{F}_5[x]$ of degrees 3, 4, 5.

   (s) Gaussian prime factorizations of 51 and $-3+11i$ in $\mathbb{Z}[i]$.

   (t) Which of 104, 224, 420, and 666 are the sum of two squares.

   (u) Two ways of writing $450 = 2 \cdot 3^2 \cdot 5^2$ as the sum of two squares.

   (v) Two Pythagorean right triangles with a side length 29.

   (w) Whether 13 and 26 are quadratic residues modulo the prime 2027.

   (x) Whether 28 and 15 are quadratic residues modulo the prime 71.

   (y) The values of the Legendre symbols $\left(\frac{103}{307}\right)$ and $\left(\frac{141}{307}\right)$.

   (z) The values of the Jacobi symbols $\left(\frac{47}{245}\right)$ and $\left(\frac{177}{245}\right)$.

---

2. Give brief responses justifying the following statements:

   (a) Rabin encryption is provably equivalent to factorization, but is not suitable for modern use.

   (b) A zero-knowledge protocol can be used to establish knowledge of secret information without revealing useful information about it.

   (c) It is possible to establish that large integers are prime, or composite, very quickly.

   (d) A polynomial may have a nontrivial factorization even if has no roots.

   (e) There is a faster way to solve the congruence $x^2 \equiv 3 \pmod{11291867}$ than simply checking each possible residue class modulo 11291867 to see if it is a solution.

   (f) Because $\left(\frac{31}{6601}\right) = -1$ but $31^{(6601-1)/2} \equiv +1 \pmod{6601}$, that means 6601 must be composite.

---

3. Solve the following:

(a) Prove that $1 + \frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{2^n} = 2 - \frac{1}{2^n}$ for every positive integer n.

(b) Show that 5 is a primitive root modulo 18.

(c) Show that 3 has order 12 modulo 73.

(d) Show that $a^4 \equiv 0$ or $1 \pmod 5$ for every integer a. Deduce that 2024 is not the sum of three fourth powers.

(e) Prove that 101 is the smallest prime divisor of $99! - 1$.

(f) Show that $\mathbb{F}_5[x]$ modulo $x^3 + 4x + 2$ is a field.

(g) Show that $\mathbb{F}_7[x]$ modulo $x^3 + 4x + 2$ is not a field.

(h) Prove that there are no elements of norm 2 or -2 in $\mathbb{Z}[\sqrt{26}]$. [Hint: Consider $a^2 - 26b^2 = \pm 2$ modulo 13.]

(i) Prove that $2 + \sqrt{26}$ is irreducible but not prime in $\mathbb{Z}[\sqrt{26}]$. [Hint: Use (g) for irreducibility.]

(j) Verify Euler's Theorem for the residue class of $x + 2$ in $\mathbb{F}_3[x]$ modulo $x^2 + x$.

(k) Show that x is a primitive root in $\mathbb{F}_2[x]$ modulo $x^3 + x + 1$.

(l) Prove that there exists a solution to $x^2 \equiv 11 \pmod{97}$. Note 97 is prime.

(m) Prove that there exists a solution to $x^2 + 6x \equiv 14 \pmod{101}$. Note 101 is prime.

(n) If $p > 3$ is a prime, prove that 3 is a quadratic residue modulo p if and only if $p \equiv 1, 11 \pmod{12}$.

(o) If $p > 3$ is a prime, prove that -3 is a quadratic residue modulo p if and only if $p \equiv 1 \pmod 3$.

(p) Characterize the primes dividing an integer of the form $n^2 + 4n - 1$, for n an integer.

(q) Characterize the primes dividing an integer of the form $n^2 + 6n + 11$, for n an integer.