1. Each item is 2 points.
   (a) By the Euclidean algorithm, $23 \cdot 12 - 11 \cdot 25 = 1$ so the inverse is $\overline{23}$.
   (b) Since $\varphi(25) = 20$, we have $6^{20} \equiv 1 \pmod{25}$ by Euler's theorem.
   (c) Plug in $n = 3 + 20a$ to $n \equiv 4 \pmod{19}$ to get $n \equiv 23 \pmod{380}$.
   (d) If $x = 0.1\overline{25}$ then $990x = 1000x - 10x = 125.\overline{25} - 1.\overline{25} = 124$, so $x = 124/990$.
   (e) Take the smallest power of each irreducible factor: gcd is $3(2-i)$.
   (f) The classes are represented by polynomials of degree ≤ 2, so there are 7^3 residue classes.

---

2. Induct on n. Base case $n = 1$ has $F_1 + F_3 = 3 = F_4$. Inductive step: if $F_1 + \cdots + F_{2n+1} = F_{2n+2}$ then $F_1 + \cdots + F_{2n+1} + F_{2n+3} = [F_1 + \cdots + F_{2n+1}] + F_{2n+3} = F_{2n+2} + F_{2n+3} = F_{2n+4}$.

---

3. Note $3^1 \equiv 3$, $3^2 \equiv 9$, $3^4 \equiv 81 \equiv 20$, $3^8 \equiv 400 \equiv 34$. So $3^{10} \equiv 3^8 \cdot 3^2 \equiv 34 \cdot 9 \equiv 1$ so the order divides 10. But $3^5 \equiv 3^4 \cdot 3 \equiv 60$ and $3^2 \equiv 9$, so the order does not divide 2 or 5, so it is 10.

---

4. Since $125 = 5^3$ we can use $\mathbb{F}_5[x]$ modulo an irreducible polynomial of degree 3. For $p(x) = x^3 + x + 1$ we have $p(0) = p(2) = p(3) = 1$, $p(1) = 3$, $p(4) = 4 \bmod 5$, so p has no roots. Since it has degree 3 it is irreducible.

---

5. Each part is worth 3 points.
   (a) Inverse of $1 + i$ is $-4 + 3i$ so solution is $n \equiv 3(-4 + 3i) \pmod{8 + i}$.
   (b) Total number of primitive roots is $\varphi(\varphi(2 \cdot 3^{2026})) = 2 \cdot 3^{2024}$.
   (c) Total is $\frac{1}{10}(2^{10} - 2^5 - 2^2 + 2^1) = 99$.
   (d) Number of residue classes mod $7 + 2i$ is $N(7 + 2i) = 53$.
   (e) 2 is a QR modulo a prime p when $p \equiv 1, 7 \bmod 8$. Since $67 \equiv 3$ and $71 \equiv 7 \bmod 8$, 2 is a QR mod 71 but not mod 67.

---

6. Part (a) is 3 points and (b), (c) are each 4 points.
   (a) $12445 = 2 \cdot 5567 + 1311$, $5567 = 4 \cdot 1311 + 323$, $1311 = 4 \cdot 323 + 19$, $323 = 17 \cdot 19$ so the gcd is 19. It is a zero divisor, and $\overline{5567} \cdot \overline{12445/19} = \overline{0}$.
   (b) $7 - 8i = (-2i)(3 + 4i) + (-1 - 2i)$, $3 + 4i = -2(-1 - 2i) + 1$, $-1 - 2i = (-1 - 2i) \cdot 1$ so gcd is 1. It is a unit, and backsolving gives $(1 + 4i)(3 + 4i) + 2(7 - 8i) = 1$ so inverse of $3 + 4i$ is $1 + 4i$.
   (c) $\overline{x^4 + 1} = \overline{(x^2 + x + 1)(x^2 + x)} + (x + 1)$, $x^2 + 1 = (x + 1)(x + 1)$ so gcd is $x + 1$. It is a zero divisor, and $\overline{x^2 + x} \cdot \overline{(x^4 + 1)/(x + 1)} = \overline{0}$.

---

7. Each part is worth 3 points.
   (a) As $5 = (2 + i)(2 - i)$ and $17 = (4 + i)(4 - i)$ we get $85 = (2 + i)(2 - i)(4 + i)(4 - i)$, up to associates.
   (b) Since $N(1 + i) = 2$, $N(7) = 7^2$, $N(6 + i) = 37$, take $(1 + i)7(6 + i) = 35 + 49i$, yielding $3626 = 35^2 + 49^2$.
   (c) For leg 29 need $k(s + t)(s - t) = 29$ yielding $k = 1$, $s + t = 29$, $s - t = 1$ so $(k, s, t) = (1, 15, 14)$ giving 29-420-421. For hypotenuse 29 need $k(s^2 + t^2) = 29$ so $(k, s, t) = (1, 5, 2)$ giving 20-21-29.
   (d) We have $\left(\frac{141}{307}\right) = \left(\frac{307}{141}\right) = \left(\frac{25}{141}\right) = 1$.
   (e) $\left(\frac{47}{245}\right) = \left(\frac{245}{47}\right) = \left(\frac{10}{47}\right) = \left(\frac{2}{47}\right)\left(\frac{5}{47}\right) = 1 \cdot \left(\frac{47}{5}\right) = 1 \cdot \left(\frac{2}{5}\right) = -1$as $\left(\frac{2}{p}\right) = 1$ for $p \equiv 1, 7 \bmod 8$.

---

8. Each part is worth 4 points.

   (a) Since $N(a+b\sqrt{26}) = a^2 - 26b^2$ it suffices to decide whether $a^2 - 26b^2 = \pm 2$ has any solutions. Reducing both sides mod 13 yields $a^2 \equiv \pm 2 \pmod{13}$, but since $\left(\frac{2}{13}\right) = \left(\frac{-2}{13}\right) = -1$ since $13 \equiv 5 \pmod 8$, there are no solutions to this congruence. Therefore there are no elements of norm 2 or -2.

   (b) If we had a factorization $2 + \sqrt{26} = bc$ then $N(b)N(c) = N(bc) = N(2+\sqrt{26}) = -22$. But $N(b), N(c)$ cannot equal ± 2 by (a), so the only possible values would have one of $N(b)$, $N(c)$ equal to ± 1 hence b or c would be a unit. Thus $2 + \sqrt{26}$ is irreducible.

   (c) Note that $(2+\sqrt{26}) | (-2)\cdot(11)$ since $-22 = N(2+\sqrt{26}) = (2+\sqrt{26})(2-\sqrt{26})$, but $2+\sqrt{26}$ does not divide -2 or 11 since its norm -22 does not divide $N(-2) = 4$ or $N(11) = 121$. Thus $2+\sqrt{26}$ is not prime.

---

9. We want to compute $\left(\frac{3}{p}\right)$. If $p \equiv 1 \pmod 4$, then $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = +1$ only when $p \equiv 1 \pmod 3$ which together say $p \equiv 1 \pmod{12}$. Likewise, if $p \equiv 3 \pmod 4$, then $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = +1$ only when $p \equiv 2 \pmod 3$, which together say $p \equiv 11 \pmod{12}$. If $p \equiv 5, 7 \pmod{12}$ then the calculations show $\left(\frac{3}{p}\right) = -1$.

---

10. Completing the square gives $n^2 + 6n + 11 = (n+3)^2 + 2$, so we want primes p such that there is a solution to $(n+3)^2 \equiv -2 \pmod p$, which is equivalent to solving $x^2 \equiv -2 \pmod p$. Clearly there is a solution for $p = 2$. For other p we know $\left(\frac{-2}{p}\right) = +1$ precisely when $p \equiv 1, 3 \pmod 8$. So p divides some $n^2 + 6n + 11$ iff $p = 2$ or $p \equiv 1, 3 \pmod 8$.

---

11. Each item is worth 3 points.

   (a) The Euclidean algorithm is very efficient for computing gcds even for large numbers. (Finding gcds via prime factorization, on the other hand, is very slow.)

   (b) Using primality/compositeness tests like the Fermat test, the Lucas primality criterion, Miller-Rabin, AKS, or Solovay-Strassen allow for rapid and accurate testing of primality even for very large integers.

   (c) Polynomials of degree greater than 3 could have a factorization where each of the irreducible factors has degree greater than 1. For instance, $x^4 + 3x^2 + 2$ factors over the real numbers as $(x^2+1)(x^2+2)$, and both factors are irreducible since they have no real roots.

   (d) We can use Berlekamp's root-finding algorithm to solve $q(x) \equiv 0 \pmod p$ much more quickly than using a brute-force search: by computing $\gcd(x^{(p-1)/2} - 1, q(x-a))$ using successive squaring and the Euclidean algorithm, if q has a root then each value of a we try has at least a 50% chance of yielding a partial factorization. This procedure is very efficient even for large p.

   (e) Our study of factorization in $\mathbb{Z}[i]$ allowed us to characterize the integers that are the sums of two squares and find all the Pythagorean triples, and our study of factorization in $\mathbb{F}_p[x]$ helped us prove that there is a primitive root modulo p for every prime p.

---

1. Each item is 2 points.
   (a) $520 = 2 \cdot 256 + 8$, $258 = 32 \cdot 8$ so gcd is 8, then lcm is $256 \cdot 520/8$.
   (b) Units are $\{1, 3, 5, 9, 11, 13\}$, zero divisors are $\{2, 4, 6, 7, 8, 10, 12\}$.
   (c) $\varphi(5^5 7^{10}) = (5^5 - 5^4)(7^{10} - 7^9)$.
   (d) Cancel 5 to get $n \equiv 24 \pmod{38}$.
   (e) Since 47 is prime, we have $2^{47} \equiv 2 \pmod{47}$ by Fermat's little theorem.

---

2. Induct on n with base cases $n = 1$ and $n = 2$. Inductive step: if $d_n = 2^n$ and $d_{n-1} = 2^{n-1}$ then $d_{n+1} = 2^n + 2(2^{n-1}) = 2^n + 2^n = 2^{n+1}$ as required.

---

3. By Euler, $a^4 \equiv 1 \pmod 5$ for every unit, and $0^4 \equiv 0 \pmod 5$. Then the sum of three fourth powers is 0, 1, 2, or 3 mod 5, hence cannot be 2024 since 2024 is 4 mod 5.

---

4. 3 is a primitive root modulo 7 since its order divides $\varphi(7) = 6$ but $3^2, 3^3 \not\equiv 1 \pmod 7$ so its order mod 7 is 6. We then compute $3^6 \equiv 43 \pmod{49}$: thus 3 is a primitive root mod 7^2 hence mod 7^d for all $d \geq 2$.

---

5. Part (a) is 2 points and parts (b), (c), (d), (e) are each 3 points.
   (a) The residue classes are represented by polynomials of degree less than 3: $\overline{0}, \overline{1}, \overline{x}, \overline{x+1}, \overline{x^2}, \overline{x^2+1}, \overline{x^2+x}, \overline{x^2+x+1}$.
   (b) We have $\overline{x^2} + \overline{x^2+1} = \overline{1}$, $\overline{x^2} \cdot \overline{x^2+1} = \overline{x^2+1}$, and $\overline{x^2+1}^2 = \overline{0}$.
   (c) The units are the polynomials relatively prime to the modulus: $\overline{1}, \overline{x}, \overline{x^2}, \overline{x^2+x+1}$.
   The zero divisors are the nonzero polynomials not relatively prime to the modulus: $\overline{x+1}$, $\overline{x^2+1}$, $\overline{x^2+x}$.
   (d) There are 4 units and indeed $\overline{x^2+x+1}^4 = \overline{x^2}^2 = \overline{1}$ as required.
   (e) Multiply by the inverse of $\overline{x^2}$, which is $\overline{x^2}$ again, to see $q(x) \equiv x^2(x+1) \equiv x+1$.

---

6. Each part is worth 2 points.
   (a) $N(7 + 4\sqrt{3}) = 1$ so it is a unit and since the norm is 1, the inverse is the conjugate $7 - 4\sqrt{3}$.
   (b) $(19 + 3i)/(4 + i) = (79 - 7i)/17$ so quotient 5, remainder $-1 - 2i$.
   (c) Units are degree less than 2 and relatively prime to the modulus $x(x+2)$: they are $\overline{1}$, $\overline{2}$ $\overline{x+1}$, $\overline{2x+2}$.
   (d) Total is $\frac{1}{7}(2^7 - 2) = 18$.
   (e) By Fermat's theorem, $104 = 10^2 + 2^2$ and $666 = 21^2 + 15^2$ can, 224 and 420 cannot.

---

7. $4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$, not equivalent since only units are ± 1. As $N(2) = N(1 \pm \sqrt{-3}) = 4$ and $N(a + b\sqrt{-3}) = a^2 + 3b^2$ there are no elements of norm 2, so any element of norm 4 is irreducible. Euclidean domains have unique factorization so $\mathbb{Z}[\sqrt{-3}]$ cannot be Euclidean.

---

8. Completing the square by adding 9 gives $(x+3)^2 \equiv 23 \pmod{101}$. (Alternatively, the quadratic formula says to compute $\sqrt{23}$.) We have $\left(\frac{23}{101}\right) = \left(\frac{101}{23}\right) = \left(\frac{9}{23}\right) = +1$ so 23 is a quadratic residue modulo 101 hence there is a solution to $(x+3)^2 \equiv 23 \pmod{101}$.

---

9. Each item is worth 3 points.

   (a) Solving second congruence gives $z = 3 + (4+5i)w$, then first congruence yields $3 + (4+5i)w \equiv 2 - i \pmod{3+i}$ so that $w \equiv 1 + i \pmod{3+i}$. Solution is $z \equiv 2 + 9i \pmod{7+19i}$.

   (b) The fundamental region (the square with vertices 0, β, $i\beta$, $(1+i)\beta$) has vertices 0, $2-i$, $1+2i$, $3+i$. Drawing this and then picking inequivalent points, we get representatives 0, 1, 2, $1+i$, $2+i$.

   (c) As $N(11+12i) = 245 = 5 \cdot 53$, testing factors yields $11 + 12i = i(2-i)(7-2i)$, up to associates.

   (d) $\left(\frac{103}{307}\right) = -\left(\frac{307}{103}\right) = -\left(\frac{-2}{131}\right) = 1$ since $\left(\frac{-2}{p}\right) = -1$ for $p \equiv 5, 7 \bmod 8$.

   (e) $\left(\frac{177}{245}\right) = \left(\frac{245}{177}\right) = \left(\frac{68}{177}\right) = \left(\frac{2}{177}\right)^2 \left(\frac{17}{177}\right) = \left(\frac{177}{17}\right) = \left(\frac{7}{17}\right) = \left(\frac{17}{7}\right) = \left(\frac{3}{7}\right) = -1$.

---

10. We want to compute $\left(\frac{-3}{p}\right)$. If $p \equiv 1 \pmod 4$, then $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = +1 \cdot \left(\frac{p}{3}\right) = +1$ only when $p \equiv 1 \pmod 3$. Likewise, if $p \equiv 3 \pmod 4$, then $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = -1 \cdot -\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right) = +1$ only when $p \equiv 1 \pmod 3$. So in either case, $\left(\frac{-3}{p}\right) = +1$ only when $p \equiv 1 \pmod 3$.

---

11. Completing the square gives $n^2 + 4n - 1 = (n+2)^2 - 5$, so we want primes p such that there is a solution to $(n+2)^2 \equiv 5 \pmod p$, which is equivalent to solving $x^2 \equiv 5 \pmod p$. Clearly there is a solution for $p = 2, 5$. For other p we compute $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$ which is $+1$ for $p \equiv 1, 4 \pmod 5$ and -1 for $p \equiv 2, 3 \pmod 5$. So p divides some $n^2 + 4n - 1$ iff $p = 2, 5$ or $p \equiv 1, 4 \pmod 5$.

---

12. Each part is worth 3 points.

   (a) RSA is believed difficult to break on a general message. Finding a general decryption exponent is essentially equivalent in most cases to calculating $\varphi(N)$ which as shown on the homework is equivalent to factoring N.

   (b) Using a zero-knowledge protocol like the Rabin protocol described in class, where Peggy proves to an arbitrarily high probability that she knows the square root of a particular value s^2 modulo $N = pq$, will allow Peggy to convince Victor that she knows the secret s without revealing useful information.

   (c) Because the ring $\mathbb{Z}[i]$ of Gaussian integers is a Euclidean domain, as proven in class, the Euclidean algorithm can be used to compute greatest common divisors. The norm of the remainder at each step is at most half the norm of the value being divided by, so the algorithm is very efficient.

   (d) We can use quadratic reciprocity to calculate the Legendre symbol $\left(\frac{3}{11291867}\right) = -\left(\frac{11291867}{3}\right) = -\left(\frac{2}{3}\right) = +1$, so in fact there is a solution.

   (e) This is an application of the Solovay-Strassen test: if $\left(\frac{a}{m}\right) \not\equiv a^{(m-1)/2} \pmod m$ then m must be composite.
