1. For explicit examples of the Euclidean algorithm, see problem 4 from homework 7. Note that depending on your calculations, you may end up with an associate of the listed answer, which would also be correct.

   (a) GCD is $x^2 + x$, with linear combination $1 \cdot (x^4 + x) + x \cdot (x^3 + x) = x^2 + x$.

   (b) GCD is $4 + i$, with linear combination $-1 \cdot (11 + 24i) + (1 + 2i)(13 - i) = 4 + i$.

   (c) GCD is $x - 1$, with linear combination $\frac{1}{6}(x^3 - x) - \frac{1}{6}(x + 3)(x^2 - 3x + 2) = x - 1$.

   (d) GCD is 1, with linear combination $(1 - 2i)(9 - 5i) + (4 + 5i)(3 + 2i) = 1$.

---

2. Note that $\overline{a}$ is a unit precisely when a, p are relatively prime (and we can compute the inverse x of a using the Euclidean algorithm to find x, y with $xa + ya \equiv 1 \bmod p$), while $\overline{a}$ is a zero divisor when a, p are not relatively prime (in which case $b = p/\gcd(a, p)$ has $ab \equiv 0 \bmod p$).

   (a) Zero divisor since gcd is $2 - i$, have $(2 - i) \cdot (1 + 3i) = 0 \bmod p$.

   (b) Unit since gcd is 1, have $\frac{1}{7}(-x + 3)(x + 3) + \frac{1}{7}(x^2 - 2) = 1$ so inverse is $\frac{1}{7}(-x + 3)$.

   (c) Unit since gcd is 1, have $(1 + 4i)(3 + 4i) + 2(7 - 8i) = 1$ so inverse is $1 + 4i$.

   (d) Zero divisor since gcd is $x + 1$, have $(x^2 + x) \cdot (x^3 + x^2 + x + 1) = 0 \bmod p$.

   (e) Unit since gcd is 1, have $(2x^2 + 2x + 4)(x^2 + x) + (3x + 1)(x^3 + 3x + 1) = 1$ so inverse is $2x^2 + 2x + 4$.

---

3. Most of these problem types were covered on at least one homework (and in most cases, also the notes).

   (a) Need $a^2 + 2b^2 = 9$ yielding ± 3 and $\pm 1 \pm 2\sqrt{-2}$.

   (b) Quotient 5, remainder $-1 - 2i$.

   (c) Quotient $x^2 - 1$, remainder x.

   (d) Inverse of $1 + i$ is $-4 + 3i$ so solution is $n \equiv 3(-4 + 3i) \pmod{8 + i}$.

   (e) Solution is $z \equiv 2 + 9i \pmod{7 + 19i}$.

   (f) Solution is $p \equiv x + 2x^2 \pmod{x^3 - 2x^2}$.

   (g) The classes are represented by polynomials of degree ≤ 2, so there are 7^3 residue classes.

   (h) Units are $\overline{1}$, $\overline{2}$ $\overline{x+1}$, $\overline{2x+2}$; zero divisors are $\overline{x}$, $\overline{x+2}$, $\overline{2x}$, $\overline{2x+1}$.

   (i) Units are $\overline{ax+b}$ where $b \neq 0$ (20 total); zero divisors are $\overline{x}$, $\overline{2x}$, $\overline{3x}$, $\overline{4x}$.

   (j) Searching for roots produces factorizations $x(x+1)$, $(x + 1)^2$, and $(x + 2)^2$.

   (k) Total is $\frac{1}{7}(2^7 - 2) = 18$.

   (l) Total is $\frac{1}{4}(7^4 - 7^2) = 588$.

   (m) Total is $\frac{1}{10}(2^{10} - 2^5 - 2^2 + 2^1) = 99$.

   (n) There are primitive roots mod 34 and 37 but not mod 35 or mod 36.

   (o) 2 is a primitive root mod 3^2 hence mod 3^{2023}. Total number is $\varphi(\varphi(3^{2023})) = 2 \cdot 3^{2021}$.

   (p) 2 is a prim root mod 3^{2023} so $2 + 3^{2023}$ is a prim root mod $2 \cdot 3^{2023}$. Total number is $\varphi(\varphi(2 \cdot 3^{2023})) = 2 \cdot 3^{2021}$.

   (q) The number of residue classes is $N(7 - 5i) = 49 + 25 = 74$.

   (r) By drawing the fundamental region (square with vertices 0, β, $i\beta$, $(1+i)\beta = 0$, $2-i$, $1+2i$, $3+i$), and picking inequivalent points, we get 0, 1, 2, $1 + i$, $2 + i$.

   (s) $5 + 5i = (1 + i)(2 + i)(2 - i)$, up to associates.

   (t) $11 + 12i = i(2 - i)(7 - 2i)$, up to associates.

   (u) $999 = 3^3(6 - i)(6 + i)$, up to associates.

   (v) By Fermat's theorem, $104 = 10^2 + 2^2$ and $666 = 21^2 + 15^2$ can, 224 and 420 cannot.

   (w) Since $N(1+i) = 2$, $N(2 \pm i) = 5$, $N(3 \pm 2i) = 13$, take $(1 + i)^2(2 + i)(3 + 2i) = -14 + 8i$ yielding $260 = 8^2 + 14^2$, and also $(1 + i)^2(2 + i)(3 - 2i) = 2 + 16i$ yielding $260 = 2^2 + 16^2$.

   (x) Since $N(1+i) = 2$, $N(3) = 3^2$, $N(2 \pm i) = 5$, take $(1 + i)3(2 + i)^2 = 21 - 3i$ yielding $450 = 21^2 + 3^2$, and also $(1 + i)3(2 + i)(2 - i) = 15 + 15i$ yielding $450 = 15^2 + 15^2$.

   (y) Solving $k(s^2 + t^2) = 65$ in cases gives $(k, s, t) = (1, 8, 1), (1, 7, 4), (5, 3, 2), (13, 2, 1)$ yielding triangles $(2kst, k(s^2 - t^2), k(s^2 + t^2))$ as 16-63-65, 25-60-65, 33-56-65, 39-52-65.

   (z) Solving $k(s^2 - t^2) = 49$ in cases gives $(k, s, t) = (1, 50, 49), (7, 4, 3)$ yielding the triangles 49-1200-1201, 49-168-175.

---

4. This problem is similar to problems 1, 2, 3 from homework 8.
   (a) The residue classes are $\overline{0}, \overline{1}, \overline{x}, \overline{x+1}, \overline{x^2}, \overline{x^2+1}, \overline{x^2+x}, \overline{x^2+x+1}$.
   (b) $\overline{x^2} + \overline{x^2+1} = \overline{1}$, $\overline{x^2} \cdot \overline{x^2+1} = \overline{x^2+1}$, and $\overline{x^2+1}^2 = \overline{0}$.
   (c) Units are $\overline{1}, \overline{x}, \overline{x^2}, \overline{x^2+x+1}$, zero divisors are $\overline{x+1}$, $\overline{x^2+1}$, $\overline{x^2+x}$.
   (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 $q(x) \equiv x^2(x+1) \equiv x+1$.

---

5. Problems like these appear on homework 10. Note $\left(\frac{-1}{p}\right) = 1$ for $p \equiv 1 \bmod 4$, $\left(\frac{2}{p}\right) = 1$ for $p \equiv 1, 7 \bmod 8$.
   (a) $1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, 9^2 \equiv 1, 4, 9, 16, 6, 17, 11, 7, 5 \bmod 19$.
   (b) Mod 43 there are $(43-1)/2 = 21$ quadratic residues since 43 is prime.
   (c) We have $\left(\frac{7}{43}\right) = -\left(\frac{43}{7}\right) = -\left(\frac{1}{7}\right) = -1$, $\left(\frac{11}{43}\right) = -\left(\frac{43}{11}\right) = -\left(\frac{-1}{11}\right) = 1$, and $\left(\frac{14}{43}\right) = \left(\frac{2}{43}\right)\left(\frac{7}{43}\right) = (-1)(-1) = 1$. So 11 and 14 are QRs mod 43 but 7 is not.
   (d) We have $\left(\frac{13}{2027}\right) = \left(\frac{2027}{13}\right) = \left(\frac{-1}{13}\right) = 1$ and $\left(\frac{26}{2027}\right) = \left(\frac{2}{2027}\right)\left(\frac{13}{2027}\right) = (-1)(1) = -1$ so 13 is a QR but 26 is not.
   (e) Get $\left(\frac{28}{71}\right) = \left(\frac{2}{71}\right)^2\left(\frac{7}{71}\right) = -\left(\frac{71}{7}\right) = -\left(\frac{1}{7}\right) = -1$ and $\left(\frac{15}{71}\right) = \left(\frac{3}{71}\right)\left(\frac{5}{71}\right) = -\left(\frac{71}{3}\right)\left(\frac{71}{5}\right) = -\left(\frac{2}{3}\right)\left(\frac{1}{5}\right) = 1$. So 15 is a QR but 28 is not.
   (f) We get $\left(\frac{103}{307}\right) = -\left(\frac{307}{103}\right) = -\left(\frac{-2}{131}\right) = 1$ and $\left(\frac{141}{307}\right) = \left(\frac{307}{141}\right) = \left(\frac{25}{141}\right) = 1$.

---

6. Many problems of similar types were covered on at least one homework.
   (a) Note $N(7+4\sqrt{3}) = 1$ so it is a unit since the norm is ± 1. The inverse is the conjugate $7 - 4\sqrt{3}$.
   (b) Note $N[(1+\sqrt{5})^{2023}] = N(1+\sqrt{5})^{2023} = (-4)^{2023}$ so it is not a unit. But $N[(2+\sqrt{5})^{2023}] = N(2+\sqrt{5})^{2023} = (-1)^{2023} = -1$ so it is a unit.
   (c) Note $N(4+5i) = 4^2 + 5^2 = 41$ is a prime integer so as $\mathbb{Z}[i]$ is Euclidean, $4+5i$ is irreducible and prime.
   (d) Note $N(2+\sqrt{-7}) = 11$ is a prime integer, so $2+\sqrt{-7}$ is irreducible.
   (e) Note $N(1+\sqrt{-7}) = 8$ so if we had a nontrivial factorization, it would have to be the product of an element of norm 2 with an element of norm 4. But since $N(a+b\sqrt{-7}) = a^2 + 7b^2$ there are no elements of norm 2 or 4, so there is no possible factorization.
   (f) Note that $(1+\sqrt{-7})(1-\sqrt{-7}) = 8 = 2 \cdot 4$ so $1+\sqrt{-7}$ divides $2 \cdot 4$ but it divides neither 2 nor 4, since $2/(1+\sqrt{-7}) = (1-\sqrt{-7})/4$ and $4/(1+\sqrt{-7}) = (1-\sqrt{-7})/2$. This means $1+\sqrt{-7}$ is not prime.
   (g) x^2+x+1 has no roots in $\mathbb{F}_2$ by a direct check, so since it has degree 2, it is irreducible hence also prime since $F[x]$ is Euclidean.
   (h) It is not hard to list all the units to see that there are 4 of them (they are the polynomials with constant term 1). We then calculate $\overline{x^2+1}^4 = \overline{x^4+2x^2+1}^2 = \overline{1}^2 = \overline{1}$ so Euler's theorem holds.
   (i) There are $N(3+2i) = 13$ residue classes and $i^{13} \equiv i \pmod{3+2i}$ as required (indeed, i^{13} just equals i).
   (j) 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, so $\mathbb{F}_5[x]$ modulo x^3+x+1 is a field.
   (k) Searching yields a root $x = 3$, so the polynomial is reducible so $\mathbb{F}_5[x]$ modulo x^4+x+1 is not a field.
   (l) Note that x^2+2x+8 has no real roots (its roots are $-1 \pm i\sqrt{7}$). Since it has degree 2 it is irreducible, so $\mathbb{R}[x]$ modulo x^2+2x+8 is a field.
   (m) Since $125 = 5^3$ we can use $\mathbb{F}_5[x]$ modulo an irreducible polynomial of degree 3. We actually just identified such a polynomial, namely x^3+x+1, in part (j).
   (n) There are $N(4+i) = 17$ residue classes hence 16 units since $4+i$ is irreducible. Then $(1+i)^2 \equiv 2i$, so $(1+i)^4 \equiv (2i)^2 \equiv -4 \equiv i$, $(1+i)^8 \equiv i^2 \equiv -1$, and finally $(1+i)^{16} \equiv (-1)^2 \equiv 1$ as required.
   (o) We compute $\left(\frac{11}{97}\right) = \left(\frac{97}{11}\right) = \left(\frac{9}{11}\right) = +1$, so the Legendre symbol is $+1$. This means 11 is a quadratic residue mod 97 so $x^2 \equiv 11 \pmod{97}$ has a solution.
   (p) Completing the square gives $(x+3)^2 \equiv 5 \pmod{101}$ so we must determine whether 5 is a quadratic residue modulo 101. We compute $\left(\frac{5}{101}\right) = \left(\frac{101}{5}\right) = \left(\frac{1}{5}\right) = 1$, so 5 is a QR and thus there are solutions.
