1. For more detailed solutions to problems like these, see the homework assignments and lecture notes.
   (a) For $7+2i$ it is $N(7+2i) = 53$ and for $\mathbb{F}_5[x]$ mod x^4+2 it is $5^4 = 625$.
   (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 $N(5+5i) = 50 = 2 \cdot 5^2$, testing factors yields $5+5i = (1+i)(2+i)(2-i)$, up to associates.
   (d) As $N(11+12i) = 245 = 5 \cdot 53$, testing factors yields $11+12i = i(2-i)(7-2i)$, up to associates.
   (e) 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.
   (f) As $999 = 3^3 \cdot 37$ and $37 = (6+i)(6-1)$ we get $999 = 3^3(6-i)(6+i)$, up to associates.
   (g) By Fermat's theorem, $104 = 10^2 + 2^2$ and $666 = 21^2 + 15^2$ can, 224 and 420 cannot.
   (h) 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 $450 = 15^2 + 15^2$.
   (i) Since $N(1+i) = 2$, $N(7) = 7^2$, $N(6+i) = 37$, take $(1+i)7(6+i) = 35 + 49i$, yielding $3626 = 35^2 + 49^2$.
   (j) 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.
   (k) Compute $\left(\frac{13}{2027}\right) = \left(\frac{2027}{13}\right) = \left(\frac{-1}{13}\right) = 1$ and $\left(\frac{26}{2027}\right) = \left(\frac{2}{2027}\right)\left(\frac{13}{2027}\right) = (-1)(1) = -1$ since $\left(\frac{2}{p}\right) = -1$ for $p \equiv 3, 5 \bmod 8$. So 13 is a QR but 26 is not.
   (l) Compute $\left(\frac{28}{71}\right) = \left(\frac{2}{71}\right)^2\left(\frac{7}{71}\right) = 1 \cdot -\left(\frac{71}{7}\right) = -\left(\frac{1}{7}\right) = -1$ and $\left(\frac{15}{71}\right) = -\left(\frac{71}{15}\right) = -\left(\frac{11}{15}\right) = \left(\frac{15}{11}\right) = \left(\frac{4}{11}\right) = 1$ using reciprocity for Jacobi symbols. So 15 is a QR but 28 is not.
   (m) 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.
   (n) We compute $\left(\frac{103}{307}\right) = -\left(\frac{307}{103}\right) = -\left(\frac{-2}{131}\right) = 1$ since $\left(\frac{-2}{p}\right) = -1$ for $p \equiv 5, 7 \bmod 8$, and $\left(\frac{141}{307}\right) = \left(\frac{307}{141}\right) = \left(\frac{25}{141}\right) = 1$.
   (o) We compute $\left(\frac{47}{245}\right) = \left(\frac{245}{47}\right) = \left(\frac{10}{47}\right) = \left(\frac{2}{47}\right)\left(\frac{5}{47}\right) = 1 \cdot \left(\frac{47}{5}\right) = 1 \cdot \left(\frac{2}{5}\right) = -1$ since $\left(\frac{2}{p}\right) = 1$ for $p \equiv 1, 7 \bmod 8$, and $\left(\frac{177}{245}\right) = \left(\frac{245}{177}\right) = \left(\frac{68}{177}\right) = \left(\frac{2}{177}\right)^2\left(\frac{17}{177}\right) = \left(\frac{177}{17}\right) = \left(\frac{7}{17}\right) = \left(\frac{17}{7}\right) = \left(\frac{3}{7}\right) = -1$.

---

2. Additional details can be found in the lecture notes.
   (a) 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.
   (b) 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.
   (c) This is an application of the Solovay-Strassen test: if $(\frac{a}{m}) \not\equiv a^{(m-1)/2} \pmod m$ then m must be composite.
   (d) 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.

3. Many problems of similar types were covered on the homework.

(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.

(d) 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.

(e) Compute $\left(\frac{11}{97}\right) = \left(\frac{97}{11}\right) = \left(\frac{9}{11}\right) = +1$ as 9 is a square. Since 97 is prime, the Legendre symbol being $+1$ means 11 is a quadratic residue.

(f) 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 $(x+3)^2 \equiv 23 \pmod{101}$.

(g) 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 $\left(\frac{3}{p}\right) = -1$.

(h) 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 $p \equiv 1 \pmod 3$.

(i) 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 $p \equiv 1, 4 \pmod 5$.

(j) 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 $p \equiv 1, 3 \pmod 8$.