# PMATH 340 Number Theory, Solutions to the Exercises for Chapter 6

**1:** (a) For $x, y \in \mathbf{Q}$, let $E(x + y\sqrt{2}) = \left|x^2 - 2y^2\right|$ and recall that $E$ is a Euclidean norm in $\mathbf{Z}[\sqrt{2}\,]$. Let $a = 17 + 26\sqrt{2} \in \mathbf{Z}[\sqrt{2}\,]$ and $b = 5 + 3\sqrt{2} \in \mathbf{Z}[\sqrt{2}\,]$. Find $q, r \in \mathbf{Z}[\sqrt{2}\,]$ with $a = qb + r$ and $E(r) < E(b)$.

Solution: We have $\frac{a}{b} = \frac{17+26\sqrt{2}}{5+3\sqrt{2}} = \frac{17+26\sqrt{2}}{5+3\sqrt{2}} \cdot \frac{5-3\sqrt{2}}{5-3\sqrt{2}} = \frac{-68+79\sqrt{2}}{7} \cong -10 + 11\sqrt{2}$ (with $-10$ being the integer nearest to $-\frac{68}{7}$ and 11 being the integer nearest to $\frac{79}{7}$), so we take $q = -10 + 11\sqrt{2}$ and then we take $r = a - qb = (17 + 26\sqrt{2}) - (-10 + 11\sqrt{2})(5 + 3\sqrt{2}) = (17 + 26\sqrt{2}) - (16 + 25\sqrt{2}) = 1 + \sqrt{2}$.

(b) Let $a = -20 + 30\,i \in \mathbf{Z}[i]$ and $b = -5 + 14\,i$ in $\mathbf{Z}[i]$. Use the Euclidean Algorithm to find $d = \gcd(a, b) \in \mathbf{Z}[i]$ then use Back-Substitution to find $s, t \in \mathbf{Z}[i]$ such that $as + bt = d$.

Solution: We have $\frac{a}{b} = \frac{-20+3\,i}{-5+14\,i} = \frac{-20+30\,i}{-5+14\,i} \cdot \frac{-5-14\,i}{-5-14\,i} = \frac{520+130\,i}{221} = \frac{520+130\,i}{221} \cong 2 + i$, so we take $q_1 = 2 + i$ and $r_1 = a - q_1 b = (-20+30\,i) - (2+i)(-5+14\,i) = 4 + 7\,i$. Next we have $\frac{b}{r_1} = \frac{-5+14\,i}{4+7\,i} = \frac{78+91\,i}{65} \cong 1 + i$ so we take $q_2 = 1 + i$ and $r_2 = b - q_2 r_1 = (-5 + 14\,i) - (1 + i)(4 + 7\,i) = -2 + 3\,i$. Finally we have $\frac{r_1}{r_2} = \frac{4+7\,i}{-2+3\,i} = 1 - 2\,i$ so we take $q_3 = 1 - 2\,i$ and $r_3 = 0$. Thus $d = \gcd(a, b) = r_2 = -2 + 3\,i$.

Back-Substitution gives the sequence $(s_0, s_1, s_2) = \big(1\ ,\ -(1 + i)\ ,\ (2 + i)(1 + i) + 1 = 2 + 3i\big)$ so we can take $s = s_1 = -(1 + i)$ and $t = s_2 = 2 + 3\,i$ to get $as + bt = d$.

**2:** (a) Find the smallest unit $u > 1$ in $\mathbf{Z}[\sqrt{18}\,]$.

Solution: We use the method described in Example 6.12 of the Lecture Notes. We have

| | | | | |
|---|---|---|---|---|
| $b$ | 1 | 2 | 3 | 4 |
| $18b^2$ | 18 | 76 | 162 | 288 |

We see that the smallest value of $b \in \mathbf{Z}^+$ for which $18b^2$ differs from a square by $\pm 1$ is $b = 4$ and, in this case, we have $18b^2 = 288 = a^2 - 1$ for $a = 17$. Thus the smallest unit $u \in \mathbf{Z}[\sqrt{18}\,]$ with $u > 1$ is $u = 17 + 4\sqrt{18}$.

(b) Show that $\mathbf{Z}[\sqrt{10}\,]$ is not a unique factorization domain.

Solution: In $\mathbf{Z}[\sqrt{10}\,]$ we have $(2 + \sqrt{10})(-2 + \sqrt{10}) = 6 = 2 \cdot 3$. We claim that each of the elements 2, 3 and $\pm 2 + \sqrt{10}$ is irreducible in $\mathbf{Z}[\sqrt{10}\,]$. We use the field norm in $\mathbf{Q}[\sqrt{10}\,]$ given by $N(x + y\sqrt{10}) = x^2 - 10y^2$. Note that $N(2) = 4$, $N(3) = 9$ and $N(\pm 2 + \sqrt{10}) = -6$. If 2 was reducible, it would factor as a product of two non-units, say $2 = zw$. Then we would have $N(z)N(w) = N(zw) = N(2) = 4$ so that either $N(z) = 2 = N(w)$ or $N(z) = -2 = N(w)$. Similarly, if 3 was reducible it would factor into two elements of norms $\pm 3$ and if $\pm 2 + \sqrt{10}$ were reducible then it would factor into two elements with one of norm $\pm 2$ and the other of norm $\mp 3$. To show that the elements 2, 3 and $\pm 2 + \sqrt{10}$ are irreducible, it suffices to show that there are no elements in $\mathbf{Z}[\sqrt{10}\,]$ of norm $\pm 2$ or $\pm 3$. We can see this by working modulo 10. Note that for $x, y \in \mathbf{Z}$ we have $N(x + y\sqrt{10}) = x^2 - 10y^2 \equiv x^2 \bmod 10$. But in $\mathbf{Z}_{10}$ we have

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| $x$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| $x^2$ | 0 | 1 | 4 | 9 | 6 | 5 | 6 | 9 | 4 | 1 |

so there are no elements $x \in \mathbf{Z}_{10}$ with $x^2 = \pm 2, \pm 3$. Thus the elements 2, 3 ad $\pm 2 + \sqrt{10}$ are all irreducible in $\mathbf{Z}[\sqrt{10}\,]$.

Finally, note that 2 is not an associate of either of the two elements $\pm 2 + \sqrt{10}$ because (working in the field $\mathbf{Q}[\sqrt{10}\,]$) we have $\frac{\pm 2+\sqrt{10}}{2} = \pm 1 + \frac{1}{2}\sqrt{10} \notin \mathbf{Z}[\sqrt{10}\,]$ (if they were associates then we would have $\frac{\pm 2+\sqrt{10}}{2} = u$ for some unit $u \in \mathbf{Z}[\sqrt{10}\,]$). Similarly, 3 is not an associate of $\pm 2 + \sqrt{10}$ because $\frac{\pm 2+\sqrt{10}}{3} = \pm\frac{2}{3} + \frac{1}{3}\sqrt{10} \notin \mathbf{Z}[\sqrt{10}\,]$.

**3:** Let $w = e^{i\,\pi/3} = \frac{1+\sqrt{3}\,i}{2}$ and let $\mathbf{Z}[w] = \big\{a + bw \,\big|\, a, b \in \mathbf{Z}\big\}$ and $\mathbf{Q}[w] = \big\{a + bw \,\big|\, a, b \in \mathbf{Q}\big\}$.

(a) Show that $\mathbf{Z}[\sqrt{3}\,i] \subsetneqq \mathbf{Z}[w]$ and $\mathbf{Q}[\sqrt{3}\,i] = \mathbf{Q}[w]$.

Solution: For $a, b \in \mathbf{Z}$ we have $a + b\sqrt{3}\,i = (a-b) + 2b\big(\frac{1+\sqrt{3}\,i}{2}\big) = (a-b) + 2b\,w$, and so $\mathbf{Z}[\sqrt{3}\,i] \subseteq \mathbf{Z}[w]$. Since $w = \frac{1}{2} + \frac{1}{2}\sqrt{3}\,i \notin \mathbf{Z}[\sqrt{3}\,i]$ we have $\mathbf{Z}[\sqrt{3}\,i] \subsetneqq \mathbf{Z}[w]$. We remark that we made use of the fact that elements in $\mathbf{Q}[\sqrt{3}\,i]$ can be *uniquely* written in the form $x + y\sqrt{3}\,i$ with $x, y \in \mathbf{Q}$, hence when $x, y \in \mathbf{Q}$ we have $x + y\sqrt{3}\,i \in \mathbf{Z}[\sqrt{3}\,i]$ if and only if $x \in \mathbf{Z}$ and $y \in \mathbf{Z}$.

For $a, b \in \mathbf{Q}$ we have $a + b\sqrt{3}\,i = (a-b) + 2b\big(\frac{1+\sqrt{3}\,i}{2}\big) = (a-b) + 2b\,w \in \mathbf{Q}[w]$ and so $\mathbf{Q}[\sqrt{3}\,i] \subseteq \mathbf{Q}[w]$. Also, for $a, b \in \mathbf{Q}$ we have $a + bw = a + b\big(\frac{1+\sqrt{3}\,i}{2}\big) = \big(a + \frac{b}{2}\big) + \frac{b}{2}\sqrt{3}\,i \in \mathbf{Q}[\sqrt{3}\,i]$ so we have $\mathbf{Q}[w] \subseteq \mathbf{Q}[\sqrt{3}\,i$.

(b) Find all the units in $\mathbf{Z}[w]$.

Solution: The field norm in $\mathbf{Q}[w] = \mathbf{Q}[\sqrt{3}\,i]$ is given by $N(u) = \|u\|^2$ that is by $N(a + b\sqrt{3}\,i) = a^2 + 3b^2$ when $a, b \in \mathbf{Q}$. For $a, b \in \mathbf{Q}$ we have

$$N(a + bw) = N\big(a + b\big(\tfrac{1+\sqrt{3}\,i}{2}\big)\big) = N\big(\big(a + \tfrac{b}{2}\big) + \tfrac{b}{2}\sqrt{3}\,i\big) = \big(a + \tfrac{b}{2}\big)^2 + 3\big(\tfrac{b}{2}\big)^2 = a^2 + ab + b^2.$$

We know that the field norm is multiplicative (meaning that $N(uv) = N(u)N(v)$ and the above formula shows that when $a, b \in \mathbf{Z}$ we have $N(a + bw) \in \mathbf{Z}$. It follows that the units in $\mathbf{Z}[w]$ are the elements of field norm $\pm 1$ or equivalently, the elements of complex norm 1. It is easy to see from a picture of the set $\mathbf{Z}[w]$ (which consists of the vertices in a grid of equilateral triangles of unit side length) that there are exactly 6 elements in $\mathbf{Z}[w]$ of complex norm 1, namely the $6^{\text{th}}$ roots of unity $\pm 1, \pm w, \pm w^2$. To be rigorous, let us verify this algebraically.

Note that $\|\pm 1\| = \|\pm w\| = \|w^2\| = 1$. We claim that these are the only 6 elements in $\mathbf{Z}[w]$ of complex norm 1. Note that these 6 elements, represented in the form $a + bw$ with $a, b \in \mathbf{Z}$ are given by

$$1 = 1 + 0w\,,\ -1 = -1 + 0w\,,\ w = 0 + 1w\,,\ -w = 0 - 1w\,,\ w^2 = \tfrac{-1+\sqrt{3}\,i}{2} = -1 + 1w \ \text{ and } \ -w^2 = 1 - 1w.$$

Let $a, b \in \mathbf{Z}$ and suppose that $N(a + bw) = \|a + bw\|^2 = 1$, that is $a^2 + ab + b^2 = 1$. If $a = 0$ then we have $1 = a^2 + ab + b^2 = b^2$, hence $b = \pm 1$. If $a = 1$ then we have $1 = a^2 + ab + b^2 = 1 + b + b^2$, that is $b(b+1) = 0$, hence $b = 0$ or $b = -1$. If $a = -1$ then we have $1 = a^2 + ab + b^2 = 1 - b + b^2$, that is $b(b-1) = 0$, and hence $b = 0$ or $b = 1$. If $\|a\| \geq 2$, then since the minimum value of $f(x) = x(x - |a|)$ is equal to $-\frac{\|a\|^2}{4}$ $\big($occurring when $x = \frac{\|a\|}{2}\big)$ we have

$$N(a + bw) = a^2 + ab + b^2 \geq \|a\|^2 - \|a\|\,\|b\| + \|b\|^2 = \|a\|^2 + \|b\|\big(\|b\| - \|a\|\big) \geq \|a\|^2 - \tfrac{\|a\|^2}{4} = \tfrac{3\|a\|^2}{4} \geq 3.$$

Thus the only 6 elements in $\mathbf{Z}[w]$ of norm 1 are indeed the $6^{\text{th}}$ roots of unity $\pm 1$, $\pm w$ and $\pm w^2$.

(c) Show that $\mathbf{Z}[w]$ is a unique factorization domain (indeed a Euclidean domain) but $\mathbf{Z}[\sqrt{3}\,i]$ is not.

Solution: For $u \in \mathbf{Z}[w]$, let $E(u) = N(u) = \|u\|^2$. Note that $E$ is multiplicative (that is $E(uv) = E(u)E(v)\big)$ and $E$ satisfies Properties E1-E4 in the definition of a Euclidean norm. We need to show that $E$ satisfies Property E5, that is the Division Algorithm Property. Let $u, v \in \mathbf{Z}[w]$ with $v \neq 0$. Working in $\mathbf{Q}[w]$, say $\frac{u}{v} = x + yw$ with $x, y \in \mathbf{Q}$. Choose $a, b \in \mathbf{Z}$ with $|a - x| \leq \frac{1}{2}$ and $|b - y| \leq \frac{1}{2}$. Let $q = a + bw \in \mathbf{Z}[w]$ and let $r = u - qv$ so that $u = qv + r$. Then we have

$$\begin{aligned} N(r) = \|r\|^2 = \|u - qv\|^2 &= \big\|\tfrac{u}{v} - q\big\|\,\|v\|^2 = \big\|(a-x) + (b-y)w\big\|\,\|v\|^2 \\ &\leq \Big(|a-x|^2 + |b-y|^2\|w\|^2\Big)\|v\|^2 \leq \big(\tfrac{1}{4} + \tfrac{1}{4}\|w\|^2\big)\|v\|^2 = \tfrac{1}{2}E(v). \end{aligned}$$

Thus $\mathbf{Z}[w]$ is a Euclidean domain with Euclidean norm $E$.

We claim that $\mathbf{Z}[\sqrt{3}\,i]$ is not a unique factorization domain. Note that in $\mathbf{Z}[\sqrt{3}\,i]$ we have $(1 + \sqrt{3}\,i)(1 - \sqrt{3}\,i) = 4 = 2\cdot 2$. We claim that the elements $1 \pm \sqrt{3}\,i$ and 2 are irreducible. Note tha $N(1 \pm \sqrt{3}\,i) = N(2) = 4$. It follows that if either 2 or $1 \pm \sqrt{3}\,i$ was a product of two nonunits, then those two nonunits would each have field norm equal to 2. But there are no elements in $\mathbf{Z}[\sqrt{3}\,i]$ with field norm equal to 2 because for $x, y \in \mathbf{Z}$, we have $N(x + y\sqrt{3}\,i) = x^2 + 3y^2$ so if $y = 0$ then $N(x + y\sqrt{3}\,i) = x^2 \neq 2$ and if $y \neq 0$ then $N(x + y\sqrt{3}\,i) = x^2 + 3y^2 \geq 3y^2 \geq 3$. Thus the elements $1 \pm \sqrt{3}\,i$ and 2 are all irreducible, as claimed. Finally note that 2 is not an associate of either of the elements $1 \pm \sqrt{3}\,i$ because $\frac{1\pm\sqrt{3}\,i}{2} \notin \mathbf{Z}[\sqrt{3}\,i]$. Thus $\mathbf{Z}[\sqrt{3}\,i]$ is not a unique factorization domain.

**4:** (a) Find the association classes in $\mathbf{Z}_{18}$.

Solution: It helps to make a multiplication table for $\mathbf{Z}_{18}$. Using the fact that $(a)(-b) = -(ab) = (-a)(b)$ and $(-a)(-b) = ab$ we can save a bit of trouble by displaying only the upper-left quarter of the multiplication table and writing the elements in $\mathbf{Z}_{18}$ as $\pm k$ with $0 \leq k \leq 9$.

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 2 | 0 | 2 | 4 | 6 | 8 | $-8$ | $-6$ | $-4$ | $-2$ | 0 |
| 3 | 0 | 3 | 6 | 9 | $-6$ | $-3$ | 0 | 3 | 6 | 9 |
| 4 | 0 | 4 | 8 | $-6$ | $-2$ | 2 | 6 | $-8$ | $-4$ | 0 |
| 5 | 0 | 5 | $-8$ | $-3$ | 2 | 7 | $-6$ | $-1$ | 4 | 9 |
| 6 | 0 | 6 | $-6$ | 0 | 6 | $-6$ | 0 | 6 | $-6$ | 0 |
| 7 | 0 | 7 | $-4$ | 3 | $-8$ | $-1$ | 6 | $-5$ | 2 | 9 |
| 8 | 0 | 8 | $-2$ | 6 | $-4$ | 4 | $-6$ | 2 | $-8$ | 0 |
| 9 | 0 | 9 | 0 | 9 | 0 | 9 | 0 | 9 | 0 | 9 |

Let use the table to help determine which elements are associates of each other. Recall that for $a \in \mathbf{Z}_{18}$, we define $[a] = \{x \in \mathbf{Z}_{18} \big| x \sim a\}$, and we call the set $[a]$ the association class of $a$ in $\mathbf{Z}_{18}$. From the table, we can find all the association classes. For example, to find the associates of 2, we look on row 2 to find all the multiples of 2, namely $0, \pm 2, \pm 4, \pm 6, \pm 8$, then we look along each of the rows $0, 2, 4, 6, 8$ to see whether $\pm 2$ occurs as a multiple, and we find that $\pm 2$ occurs on rows $2, 4, 8$ but not on rows $0, 6$, so the associates of 2 are $\pm 2, \pm 4, \pm 8$. We find that $[0] = \{0\}$, $[1] = \{\pm 1, \pm 5, \pm 7\} = \{1, 5, 7, 11, 13, 17\}$, $[2] = \{\pm 2, \pm 4, \pm 8\} = \{2, 4, 8, 10, 14, 16\}$, $[3] = \{\pm 3\} = \{3, 15\}$, $[6] = \{\pm 6\} = \{6, 12\}$ and $[9] = \{9\}$.

We now redisplay our multiplication table by considering multiplication to act on association classes.

| | [0] | [1] | [2] | [3] | [6] | [9] |
|---|---|---|---|---|---|---|
| [0] | [0] | [0] | [0] | [0] | [0] | [0] |
| [1] | [0] | [1] | [2] | [3] | [6] | [9] |
| [2] | [0] | [2] | [2] | [6] | [6] | [0] |
| [3] | [0] | [3] | [6] | [9] | [0] | [9] |
| [6] | [0] | [6] | [6] | [0] | [0] | [0] |
| [9] | [0] | [9] | [0] | [9] | [0] | [9] |

We shall use this table for Parts (b) and (c).

(b) Find all the units and all the zero divisors in $\mathbf{Z}_{18}$.

Solution: The units in $\mathbf{Z}_{18}$ are the associates of 1, namely the elements in $[1] = \{1, 5, 7, 11, 13, 17\}$. To find the zero-divisors, we look for the [0] entries in the multiplication table which do not occur in the first row or column (as multiples of [0]). We see that $[2][9] = [9][2] = [0]$, $[3][6] = [6][3] = [0]$, $[6][6] = [0]$ and $[6][9] = [9][6] = [0]$ and so the zero divisors are the elements in $[2] \cup [3] \cup [6] \cup [9] = \{2, 3, 4, 6, 8, 9, 10, 12, 14, 15, 16\}$ (in this ring, all of the non-zero non-units are zero divisors).

(c) Find all the irreducible elements and all the prime elements in $\mathbf{Z}_{18}$.

Solution: The reducible and irreducible elements (by definition) are the nonzero non-units, that is the elements in $[2] \cup [3] \cup [6] \cup [9]$. To find the reducible elements we find all the non-zero entries in the table which do not occur in the first or second row or column (as multiples of [0] or [1]), namely [2], [6] and [9] (for example $[2] = [2][2]$, $[6] = [2][3]$ and $[9] = [3][3]$). Thus the reducible elements are the elements in $[2] \cup [6] \cup [9]$ and the irreducible elements are the elements in $[3] = \{3, 15\}$.

Finally, let us determine the primes. Since primes are nonzero non-units, the only possible primes are the elements in $[2] \cup [3] \cup [6] \cup [9]$. Since $[9] = [3][3]$ but [9] does not divide [3], it follows that the elements in [9] are not prime. Since $[6] = [2][3]$ but [6] divides neither [2] nor [3], it follows that the elements in [6] are not prime. If $[3] = [a][b]$ with $a, b \in \mathbf{Z}_{18}$ then (from the table) we have $([a], [b]) = ([1], [3])$ or $([a], [b]) = ([3], [1])$ and, in either case, [3] divides $[a]$ or [3] divides $[b]$, and so the elements in [3] are prime. If $[2] = [a][b]$ with $a, b \in \mathbf{Z}_{18}$ then (from the table) we have $([a], [b]) \in \{([1], [2]), ([2], [1]), ([2], [2])\}$, and in all cases $[2] \big| [a]$ or $[2] \big| [b]$, and so the elements in [2] are prime. Thus the primes are the elements in $[2] \cup [3] = \{2, 3, 4, 8, 10, 14, 15, 16\}$.

**5:** (a) Use the method of the Sieve of Eratosthenes to find all irreducible elements $u \in \mathbf{Z}[\sqrt{2}\,i]$ with $\|u\| \leq 10$ (where $\|u\|$ denotes the complex norm of $u$). Begin by drawing a grid which shows all the elements $u \in \mathbf{Z}[\sqrt{2}\,i]$ with $\|u\| \leq 10$ and crossing off 0 and $\pm 1$. At each step, circle the remaining elements of smallest complex norm and cross off their multiples: if you have circled $u$ then cross off the elements $uv$ with $v \in \mathbf{Z}[\sqrt{2}\,i] \setminus \{\pm 1\}$. To locate the multiples $uv$ on your grid, it helps to make use of the fact that to multiply $u$ and $v$ you must multiply their lengths and add their angles.

Solution: It helps to draw a picture of the grid. At the first step, circle the elements $\pm\sqrt{2}i$. The multiples of $\sqrt{2}i$ are the elements $(\sqrt{2}i)(s+t\sqrt{2}i) = -2t + s\sqrt{2}i$ with $s,t \in \mathbf{Z}$, or equivalently the elements $a + b\sqrt{2}i$ where $a,b \in \mathbf{Z}$ with $a$ even. Cross these elements off in your picture of the grid. At the second step, circle the elements $\pm 1 \pm \sqrt{2}i$. If we write $1+\sqrt{2}i = re^{i\theta}$ (where $r = \sqrt{3}$ and $\theta = \tan^{-1}\sqrt{2}$) then multiplication of an element $u \in \mathbf{Z}[\sqrt{2}i]$ by $1+\sqrt{2}i$ is given, geometrically, by scaling the length of $u$ by $\sqrt{3}$ and rotating $u$ counterclockwise about the origin by the angle $\theta$. It follows that the multiples of $1+\sqrt{2}i$ are the points on the grid obtained by scaling the entire grid $\mathbf{Z}[\sqrt{2}i]$ by $\sqrt{3}$ and rotating it by $\theta$, This geometric interpretation helps to locate all the multiples of $1+\sqrt{3}i$ and cross them off. You should find that the multiples of $1+\sqrt{2}i$ which lie in the circle $\|u\| \leq 10$, and are in the first quadrant, and have not already been crossed off in Step 1, are the elements $3$, $1+4\sqrt{2}i$, $3+3\sqrt{2}i$, $5+2\sqrt{2}i$, $7+\sqrt{2}i$, $9$, $1+7\sqrt{2}i$, $3+6\sqrt{2}i$, $5+5\sqrt{2}i$, $7+4\sqrt{2}i$ and $9+3\sqrt{2}i$. The multiples of $1-\sqrt{2}i$ should also be crossed off, and you should find that the multiples of $1-\sqrt{2}i$ which lie in the circle $\|u\| \leq 10$ and in first quadrant and have not already been crossed off in Step 1 are the elements $9$, $3$, $5+\sqrt{2}i$, $7+2\sqrt{2}i$, $9+3\sqrt{2}i$, $1+2\sqrt{2}i$, $3+3\sqrt{2}i$, $5+4\sqrt{2}i$, $7+5\sqrt{2}i$, $1+5\sqrt{2}i$ and $3+6\sqrt{2}i$. At the third step, we circle the smallest remaining elements $\pm 3 \pm \sqrt{2}i$. Because $N(3+\sqrt{2}i) > 10$ we may stop and all the remaining elements inside the circle $\|u\| \leq 10$ are irreducible (and prime). Thus the irreducible elements $u$ in $\mathbf{Z}[\sqrt{2}i]$ with $\|u\| \leq 10$ are the elements

$$\pm 5\,,\ \pm 7\,,\ \pm\sqrt{2}\,i\,,\ \pm 1 \pm \sqrt{2}\,i\,,\ \pm 3 \pm \sqrt{2}i\,,\ \pm 9 \pm \sqrt{2}i\,,\ \pm 3 \pm 2\sqrt{2}i\,,\ \pm 9 \pm 2\sqrt{2}i\,,$$
$$\pm 1 \pm 3\sqrt{2}i\,,\ \pm 5 \pm 3\sqrt{2}i\,,\ \pm 7 \pm 3\sqrt{2}i\,,\ \pm 3 \pm 4\sqrt{2}i\,,\ \pm 3 \pm 5\sqrt{2}i\,,\ \pm 1 \pm 6\sqrt{2}i\,,\ \pm 5 \pm 6\sqrt{2}\,i\,.$$

(b) Let $p$ be an odd prime in $\mathbf{Z}^+$. Show that $p$ is reducible in $\mathbf{Z}\big[\sqrt{2}\,i\big]$ if and only if $p = x^2 + 2y^2$ for some $x, y \in \mathbf{Z}$.

Solution: Suppose first that $p$ is reducible. Choose non-units $u, v \in \mathbf{Z}\big[\sqrt{2}\,i\big]$ such that $p = uv$. Since $N(u), N(v) \in \mathbf{Z}^+$ and we have $N(u)N(v) = N(uv) = N(p) = p^2$, it follows that $N(u) = N(v) = p$. Write $u = a + b\sqrt{2}\,i$ with $a, b \in \mathbf{Z}$ and let $x = |a|$ and $y = |b|$. Then we have $p = N(u) = a^2 + 2b^2 = x^2 + 2y^2$. Finally note that $x \neq 0$ since $p$ is odd so that $p \neq 2y^2$, and $y \neq 0$ since $p$ is prime so that $p \neq x^2$, and so we have $x, y \in \mathbf{Z}^+$.

Conversely, suppose that $p = x^2 + 2y^2$ with $x, y \in \mathbf{Z}^+$. Let $u = x + y\sqrt{2}\,i$ and $v = \overline{u} = x - i\sqrt{2}\,i$ and note that $u, v \in \mathbf{Z}\big[\sqrt{2}\,i\big]$. Then $N(u) = N(v) = x^2 + 2y^2 = p$ so that $u$ and $v$ are non-units and we have $uv = x^2 + 2y^2 = p$ so that $p$ is reducible in $\mathbf{Z}\big[\sqrt{2}\,i\big]$.