PMATH 340 Number Theory, Solutions to the Exercises for Chapter 7

1: (a) Express the (finite) continued fraction $[2,1,3,1,2]$ as a rational number, in reduced form.

Solution: We have

$$[2,1,3,1,2] = 2 + \cfrac{1}{1+\frac{1}{3+\frac{1}{1+\frac{1}{2}}}} = 2 + \cfrac{1}{1+\frac{1}{3+\frac{2}{3}}} = 2 + \cfrac{1}{1+\frac{3}{11}} = 2 + \tfrac{11}{14} = \tfrac{39}{14}.$$

(b) Express that rational number $\frac{64}{47}$ as a (finite) continued fraction.

Solution: Applying the Euclidean Algorithm gives

$$64 = 1\cdot 47 + 17\ ,\ 47 = 2\cdot 17 + 13\ ,\ 17 = 1\cdot 13 + 4\ ,\ 13 = 3\cdot 4 + 1\ ,\ 4 = 4\cdot 1 + 0$$

so, using the quotients as in Theorem 7.2, we have $\frac{64}{47} = [1,2,1,3,4]$.

2: (a) Express the (periodic) continued fraction $[1,\overline{1,3}\cdots]$ as a quadratic irrational.

Solution: Let $x = [1,\overline{1,3}]$ and $u = [\overline{1,3}]$. Then $u = 1 + \frac{1}{3+\frac{1}{1+\frac{1}{3+\cdots}}} = 1 + \frac{1}{3+\frac{1}{u}}$ and $x = 1 + \frac{1}{1+\frac{1}{3+\cdots}} = 1 + \frac{1}{u}$. Since $u = 1 + \frac{1}{3+\frac{1}{u}} = 1 + \frac{u}{3u+1} = \frac{4u+1}{3u+1}$ we have $u(3u+1) = 4u+1$, that is $3u^2 - 3u - 1 = 0$, and hence $u = \frac{3\pm\sqrt{21}}{6}$. Since $u > 1$ we must have $u = \frac{3+\sqrt{21}}{6}$ and hence $x = 1 + \frac{1}{u} = 1 + \frac{6}{\sqrt{21}+3} = 1 + \frac{6(\sqrt{21}-3)}{12} = \frac{\sqrt{21}-1}{2}$.

(b) Express the quadratic irrational $\frac{3+\sqrt{7}}{2}$ as a (periodic) continued fraction.

Solution: Using the recursion $x_0 = \frac{3+\sqrt{7}}{2}$, $a_k = \lfloor a_k \rfloor$ and $x_{k+1} = \frac{1}{x_k - a_k}$ we have

k	x_k	a_k
0	$\frac{\sqrt{7}+3}{2}$	2
1	$\frac{2}{\sqrt{7}-1} = \frac{\sqrt{7}+1}{3}$	1
2	$\frac{3}{\sqrt{7}-2} = \frac{\sqrt{7}+2}{1}$	4
3	$\frac{1}{\sqrt{7}-2} = \frac{\sqrt{7}+2}{3}$	1
4	$\frac{3}{\sqrt{7}-1} = \frac{\sqrt{7}+1}{2}$	1
5	$\frac{2}{\sqrt{7}-1} = \frac{\sqrt{7}+1}{3}$	

Since $x_5 = x_1$ the sequences x_k and a_k become periodic and we have $\frac{3+\sqrt{7}}{2} = [a_0, a_1, a_2, \cdots] = [2, \overline{1,4,1,1}]$.

3: (a) Express $\sqrt{7}$ as a continued fraction and find the the k^{th} convergents $c_k = \frac{p_k}{q_k}$ for $0 \leq k \leq 7$. Let $u_k = p_k + q_k\sqrt{7} \in \mathbf{Z}[\sqrt{7}\,]$ for $0 \leq k \leq 7$ and calculate $u_3 u_k \in \mathbf{Z}[\sqrt{7}\,]$ for $0 \leq k \leq 3$. What do you notice?

Solution: The following table lists the data used to calculate the continued fraction for $\sqrt{7}$ and the convergents $c_k = \frac{p_k}{q_k}$ for $0 \leq k \leq 7$. The values of x_k a_k, p_k and q_k are given recursively by $x_0 = \sqrt{7}$, $a_k = \lfloor x_k \rfloor$, $x_{k+1} = \frac{1}{x_k - a_k}$, $p_0 = a_0$, $p_1 = a_1 a_0 + 1$, $p_k = a_k p_{k-1} + p_{k-2}$, $q_0 = 1$, $q_1 = a_1$ and $q_k = a_k q_{k-1} + q_{k-2}$.

k	x_k	a_k	p_k	q_k
0	$\sqrt{7}$	2	2	1
1	$\frac{1}{\sqrt{7}-2} = \frac{\sqrt{7}+2}{3}$	1	3	1
2	$\frac{3}{\sqrt{7}-1} = \frac{\sqrt{7}+1}{2}$	1	5	2
3	$\frac{2}{\sqrt{7}-1} = \frac{\sqrt{7}+1}{3}$	1	8	3
4	$\frac{3}{\sqrt{7}-2} = \frac{\sqrt{7}+2}{1}$	4	37	14
5	$\frac{1}{\sqrt{7}-2} = \frac{\sqrt{7}+2}{3}$	1	45	17
6	$\frac{3}{\sqrt{7}-1} = \frac{\sqrt{7}+1}{2}$	1	82	31
7	$\frac{2}{\sqrt{7}-1} = \frac{\sqrt{7}+1}{3}$	1	127	48

From the table, we see that $\sqrt{7} = [2, \overline{1, 1, 1, 4}]$ and the first few convergents are

$$(c_0, c_1, \cdots, c_7) = \left(\tfrac{2}{1}, \tfrac{3}{1}, \tfrac{5}{2}, \tfrac{8}{3}, \tfrac{37}{14}, \tfrac{45}{17}, \tfrac{82}{31}, \tfrac{127}{48}\right).$$

The first few values of $u_k = p_k + q_k\sqrt{7} \in \mathbf{Z}[\sqrt{7}\,]$ are

$$(u_0, u_1, \cdots, u_7) = \left(2+\sqrt{7}\,, 3+\sqrt{7}\,, 5+2\sqrt{7}\,, 8+3\sqrt{7}\,, 37+14\sqrt{7}\,, 45+17\sqrt{7}\,, 82+31\sqrt{7}\,, 127+48\sqrt{7}\right)$$

and we have

$$\begin{aligned} u_3 u_0 &= (8 + 3\sqrt{7})(2 + \sqrt{7}) = 37 + 14\sqrt{7} = u_0, \\ u_3 u_1 &= (8 + 3\sqrt{7})(3 + \sqrt{7}) = 45 + 17\sqrt{7} = u_5, \\ u_3 u_2 &= (8 + 3\sqrt{7})(5 + 2\sqrt{7}) = 82 + 31\sqrt{7} = u_6 \text{ and} \\ u_3 u_3 &= (8 + 3\sqrt{7})(8 + 3\sqrt{7}) = 127 + 48\sqrt{7}. \end{aligned}$$

We notice that $u_3 u_k = u_{k+3}$ for $0 \leq k \leq 3$.

(b) Express $\sqrt{2}$ as a continued fraction, then show that the k^{th} convergent is given by $c_k = \frac{p_k}{q_k}$ with

$$p_k = \tfrac{1}{2}\Big((1+\sqrt{2})^{k+1} + (1-\sqrt{2})^{k+1}\Big) \quad \text{and} \quad q_k = \tfrac{1}{2\sqrt{2}}\Big((1+\sqrt{2})^{k+1} - (1-\sqrt{2})^{k+1}\Big).$$

Solution: The following table lists the data used to obtain the continued fraction for $\sqrt{2}$ and the convergents $c_k = \frac{p_k}{q_k}$.

k	x_k	a_k	p_k	q_k
0	$\sqrt{2}$	1	1	1
1	$\frac{1}{\sqrt{2}-1} = \frac{\sqrt{2}+1}{1}$	2	3	2
2	$\frac{1}{\sqrt{2}-1} = \frac{\sqrt{2}+1}{1}$	2	7	5

We see that $\sqrt{2} = [1, \overline{2}]$ and that p_k and q_k are given recursively by $p_0 = 1$, $p_1 = 3$, $p_{k+1} = 2p_k + p_{k-1}$, $q_0 = 1$, $q_1 = 2$ and $q_{k+1} = 2q_k + q_{k-1}$.

Recall (or prove by induction) that when a sequence x_k is given by the linear recursion $x_{k+1} = ax_k + bx_{k-1}$ (where $a, b \in \mathbf{C}$) the solution is of the form $x_k = Au^k + Bv^k$ for some $A, B \in \mathbf{C}$, where u and v are the (complex) roots of the polynomial $g(x) = x^2 - ax - b$, provided that the roots are distinct. The values of A and B can be determined from two initial values of the sequence, say x_0 and x_1.

The sequence p_k is given by $p_0 = 2$, $p_1 = 3$ and $p_k = 2p_k + p_{k-1}$. The polynomial $g(x) = x^2 - 2x - 1$ has roots $1 \pm \sqrt{2}$ and so the sequence p_k is given by $p_k = A(1+\sqrt{2}) + B(1-\sqrt{2})$ for some constants A, B. To get $p_0 = 2$ we need $A + B = 2$ and to get $p_1 = 3$ we need $A(1+\sqrt{2}) + B(1-\sqrt{2}) = 3$ Solving these two linear equations gives $A = \frac{1}{2}(1+\sqrt{2})$ and $B = \frac{1}{2}(1-\sqrt{2})$ and so we have $p_k = \frac{1}{2}(1+\sqrt{2})^{k+1} + \frac{1}{2}(1-\sqrt{2})^{k+1}$, as required.

The sequence q_k is given by the same recursion formula so it is given by $q_k = D(1+\sqrt{2}) + E(1-\sqrt{2})$ for some constants D, E, but it has different initial values. To get $q_0 = 1$ we need $D + E = 1$ and to get $q_1 = 2$ we need $D(1+\sqrt{2}) + E(1-\sqrt{2}) = 2$. Solving these two linear equations gives $D = \frac{1}{2\sqrt{2}}(1+\sqrt{2})$ and $E = -\frac{1}{\sqrt{2}}(1-\sqrt{2})$ and so we obtain $q_k = \frac{1}{2\sqrt{2}}(1+\sqrt{2})^{k+1} - \frac{1}{2\sqrt{2}}(1-\sqrt{2})^{k+1}$, as required.

4: (a) Express $\sqrt{57}$ as a continued fraction and find the smallest unit $u>1$ in $\mathbf{Z}\big[\sqrt{57}\,\big]$.

Solution: The following table lists the data used to obtain the continued fraction for $\sqrt{57}$.

k	0	1	2	3	4	5	6
a_k	7	1	1	4	1	1	14
x_k	$\frac{\sqrt{57}+0}{1}$	$\frac{\sqrt{57}+7}{8}$	$\frac{\sqrt{57}+1}{7}$	$\frac{\sqrt{57}+6}{3}$	$\frac{\sqrt{57}+6}{7}$	$\frac{\sqrt{57}+1}{8}$	$\frac{\sqrt{57}+7}{1}$
p_k	7	8	15	68	83	151	
q_k	1	1	2	9	11	20	
${p_k}^2-57\,{q_k}^2$	-8	7	-3	7	-8	1	

From the table we see that $\sqrt{57}=[7,\overline{1,1,4,1,1,14}]$ and the smallest unit is $u>1$ in $\mathbf{Z}[\sqrt{57}\,]$ is $u=151+20\sqrt{57}$.

(b) Determine whether 5 is irreducible in the ring $\mathbf{Z}[\sqrt{57}\,]$.

Solution: We use the field norm defined in $\mathbf{Q}(\sqrt{57})$ by $N(x+y\sqrt{57})=x^2-57\,y^2$. We know that this norm is multiplicative. Note that $N(5)=25$. It follows that if 5 was reducible, then it would have to factor into two elements of norm ±5. We claim that there are no elements of norm ±5 in $\mathbf{Z}[\sqrt{57}\,]$. Suppose, for a contradiction, that $x,y\in\mathbf{Z}^+$ and $x^2-57\,y^2=\pm5$. Since $5<\sqrt{57}$ it follows, from Corollary 7.11 in the Lecture Notes, that we can choose $k\in\mathbf{Z}^+$ so that $\frac{x}{y}=\frac{p_k}{q_k}$. Since $\gcd(p_k,q_k)=1$ we must have $x=tp_k$ and $y=tq_k$ for some $t\in\mathbf{Z}^+$. This implies that $\pm5=x^2-57\,y^2=t^2({p_k}^2-57{q_k}^2)$ and so we must have $t=1$ and ${p_k}^2-57{q_k}^2=\pm5$. But from the above table (whose final row repeats), we see that there is no value of $k\in\mathbf{Z}^+$ for which ${p_k}^2-57{q_k}^2=\pm5$. Thus there are no elements of norm ±5 in $\mathbf{Z}[\sqrt{57}]$, as claimed, and hence 5 is irreducible.

We remark that it is also possible (but it requires a fair amount of trial and error) to show that there are no elements of norm ±5 by working in $\mathbf{Z}_n$ for various values of n. For example, you can verify that there are no solutions to the equation $x^2-57y^2=+5$ in $\mathbf{Z}_3$ and no solutions to $x^2-57y^2=-5$ in $\mathbf{Z}_{19}$. Alternatively, you can verify that there are no solutions to $x^2-57y^2=\pm5$ in $\mathbf{Z}_{25}$.

5: (a) Let $x=[a_0,a_1,a_2,\cdots]$ with $a_0\in\mathbf{Z}$ and $a_i\in\mathbf{Z}^+$ for $i\geq 2$. Show that

$$-x=\begin{cases}\big[-a_0-1,a_2+1,a_3,a_4,a_5,\cdots\big] & \text{, if } a_1=1\\ \big[-a_0-1\,,\,1\,,\,a_1-1,a_2,a_3,a_4,\cdots\big] & \text{, if } a_1>1.\end{cases}$$

Solution: Suppose first that $a_1=1$. Let $n\geq 3$ and let $u=[a_3,a_4,a_5,\cdots,a_n]$. Then

$$\begin{aligned}[a_0,a_1,a_2,\cdots,a_n]+[-a_0-1,a_2+1,a_3,a_4,\cdots,a_n]&=a_0+\frac{1}{1+\frac{1}{a_2+\frac{1}{u}}}-a_0-1+\frac{1}{(a_2+1)+\frac{1}{u}}\\ &=\frac{1}{1+\frac{u}{a_2u+1}}-1+\frac{u}{a_2u+u+1}=\frac{a_2u+1}{a_2u+u+1}-\frac{a_2u+u+1}{a_2u+u+1}+\frac{u}{a_2u+u+1}=0\end{aligned}$$

and so we have $-[a_0,a_1,\cdots,a_n]=[-a_0-1,a_2+1,a_3,a_4\cdots,n]$. Taking the limit as $n\to\infty$ gives

$$-x=[-a_0-1,a_2+1,a_3,a_4,a_5,\cdots].$$

Now suppose that $a_1>1$. For $n\geq 2$ let $v=[a_2,a_3,\cdots,a_n]$. Then

$$\begin{aligned}[a_0,a_1,a_2,\cdots,a_n]+[-a_0-1,1,a_1-1,a_2,a_3,\cdots,a_n]&=a_0+\frac{1}{a_1+\frac{1}{v}}-a_0-1+\frac{1}{1+\frac{1}{(a_1-1)+\frac{1}{v}}}\\ &=\frac{v}{a_1v+1}-1+\frac{1}{1+\frac{v}{a_1v-v+1}}=\frac{v}{a_1v+1}-\frac{a_1v+1}{a_1v+1}+\frac{a_1v-v+1}{a_1v+1}=0\end{aligned}$$

and so we have $-[a_0,a_1,a_2,\cdots,a_n]=[-a_0-1,1,a_1-1,a_2,a_3,\cdots,a_n]$. Taking the limit as $n\to\infty$ gives

$$-x=[-a_0-1,1,a_1-1,a_2,a_3,a_4,\cdots].$$

(b) Let $x=\sqrt{d}$, where $d\in\mathbf{Z}^+$ is a non-square, so we have $x=\big[a_0,\overline{a_1,a_2,\cdots,a_{\ell-1},2a_0}\,\big]$ where ℓ is the minimum period of the sequence $\{a_k\}$. Show that $\{a_k\}$ is symmetric in the sense that $a_k=a_{\ell-k}$ for $0<k<\ell$.

Solution: Let $y=\lfloor\sqrt{d}\rfloor+\sqrt{d}=a_0+x=[\,\overline{2a_0,a_1,a_2,\cdots,a_{\ell-1}}\,]$. By Theorem 7.20, $-\frac{1}{\overline{y}}=[\,\overline{a_{\ell-1},\cdots,a_2,a_1,2a_0}\,]$ and so $-\overline{y}=[0,\overline{a_{\ell-1},\cdots,a_2,a_1,2a_0}\,]$. On the other hand, $-\overline{y}=-\big(\lfloor\sqrt{d}\rfloor-\sqrt{d}\big)=\sqrt{d}-\lfloor\sqrt{d}\rfloor=x-a_0=[0,\overline{a_1,a_2,\cdots,a_{\ell-1},2a_0}\,]$. Since

$$-\overline{y}=[0,\overline{a_1,a_2,\cdots,a_{\ell-1},2a_0}\,]=[0,\overline{a_{\ell-1},\cdots,a_1,2a_0}\,]$$

we see that $a_k=a_{\ell-k}$ for $0<k<\ell$.