PMATH 340 Number Theory, Solutions to the Exercises for Chapter 8

1: For each of the following integers n, determine whether n is a sum of two squares, and if so then find the number of pairs $(x,y)\in\mathbf{Z}^2$ for which $n=x^2+y^2$.

(a) $n=1081$

Solution: We have $1081=23\cdot 47$, which is not a sum of 2 squares because $23=3\bmod 4$ (and $47=3\bmod 4$).

(b) $n=3{,}185{,}000$

Solution: We have $3\,185\,000=2^3\cdot 5^4\cdot 7^2\cdot 13$, which is a sum of 2 squares because $13=1\bmod 4$. The number of pairs $(x,y)\in\mathbf{Z}^2$ for which $n=x^2+y^2$ is equal to $4\,\tau(5^4\cdot 13)=4\cdot 5\cdot 2=40$.

(c) $n=\binom{100}{11}=\frac{100!}{11!\,89!}$

Solution: We have $\binom{100}{11}=\frac{100\cdot 99\cdot 98\cdot 97\cdot 96\cdot 95\cdot 94\cdot 93\cdot 92\cdot 91\cdot 90}{11\cdot 10\cdot 9\cdot 8\cdot 7\cdot 6\cdot 5\cdot 4\cdot 3\cdot 2\cdot 1}=14\cdot 97\cdot 95\cdot 94\cdot 93\cdot 92\cdot 91\cdot 15=2^4\cdot 3^2\cdot 5^2\cdot 13\cdot 19\cdot 23\cdot 31\cdot 47\cdot 97$, which is not a sum of two squares because $19=23=31=47=3\bmod 4$.

2: Let $n=99450$.

(a) Write n as a product of irreducible elements in $\mathbf{Z}[i]$.

Solution: $n=99450=2\cdot 3^2\cdot 5^2\cdot 13\cdot 17=(1+i)(1-i)(3)^2(2+i)^2(2-i)^2(3+2i)(3-2i)(4+i)(4-i)$.

(b) List all of the pairs $(x,y)\in\mathbf{Z}^2$ with $0\le x\le y$ such that $n=x^2+y^2$.

Solution: We have $n=x^2+y^2$ if and only if $n=z\,\overline{z}$ where $z=x+y\,i$. We can write $n=z\,\overline{z}$ when $z=u(1+i)(3)(2+i)^j(2-i)^{2-j}(3+2\,i)^k(3-2\,i)^{1-k}(4+i)^\ell(4-i)^{1-\ell}$ where u is a unit and $j=0$, 1 or 2 and $k=0$ or 1 and $\ell=0$ or 1. We note that there are $4\cdot 3\cdot 2\cdot 2=48$ possibilities for z. We list some of the possible values for z.

$$(1+i)(3)(2+i)(3+2\,i)(4+i)=(3+3\,i)(3+4\,i)(10+11\,i)=(-3+21\,i)(10+11\,i)=-261+177\,i$$
$$(1+i)(3)(2+i)^2(3+2\,i)(4-i)=(-3+21\,i)(14+5\,i)=-147+279\,i$$
$$(1+i)(3)(2+i)^2(3-2\,i)(4+i)=(-3+21\,i)(14-5\,i)=63+309\,i$$
$$(1+i)(3)(2+i)^2(3-2\,i)(4-i)=(-3+21\,i)(10-11\,i)=201+243\,i$$
$$(1+i)(3)(2+i)(2-i)(3+2\,i)(4+i)=(3+3\,i)(5)(10+11\,i)=(15+15\,i)(10+11\,i)=-15+315\,i$$
$$(1+i)(3)(2+i)(2-i)(3+2\,i)(4-i)=(15+15\,i)(14+5\,i)=135+285\,i$$

At this stage we can stop listing values for z because each of the above 6 values $z=x+y\,i$ determines 8 of the 48 possible values, namely $\pm x\pm y\,i$ and $\pm y\pm x\,i$. Thus there are 6 pairs $(x,y)\in\mathbf{Z}^2$ with $0\le x\le y$ such that $n=x^2+y^2$, namely $(x,y)=(15,315)$, $(63,309)$, $(135,285)$, $(147,279)$, $(177,261)$ and $(201,243)$.

3: (a) Solve Pell's equation $x^2 - 22y^2 = 1$.

Solution: The following table lists the data used to calculate the continued fraction for $\sqrt{22}$ and the first few convergents $c_k = \frac{p_k}{q_k}$ along with the norms $N_k = N(p_k + q_k\sqrt{22}) = p_k^2 - 22\,q_k^2$.

k	x_k	a_k	p_k	q_k	N_k
0	$\sqrt{22}$	4	4	1	-6
1	$\frac{1}{\sqrt{22}-4} = \frac{\sqrt{22}+4}{6}$	1	5	1	3
2	$\frac{6}{\sqrt{22}-2} = \frac{\sqrt{22}+2}{3}$	2	14	3	-2
3	$\frac{3}{\sqrt{22}-4} = \frac{\sqrt{22}+4}{2}$	4	61	13	3
4	$\frac{2}{\sqrt{22}-4} = \frac{\sqrt{22}+4}{3}$	2	136	29	-6
5	$\frac{3}{\sqrt{22}-2} = \frac{\sqrt{22}+2}{6}$	1	197	42	1
6	$\frac{6}{\sqrt{22}-4} = \frac{\sqrt{22}+4}{1}$	8			

We have $\sqrt{22} = [4, \overline{1,2,4,2,1,8}]$ with period $\ell = 6$. Writing $u_k = p_k + q_k\sqrt{22} \in \mathbf{Z}[\sqrt{22}]$, the smallest unit in $\mathbf{Z}[\sqrt{22}\,]$ with $u > 1$ is $u = u_{\ell-1} = u_5 = 197 + 42\sqrt{22}$, and we have $N(u) = 1$. The set of all units is the set of elements of the form $\pm u^k = \pm u_{k\ell-1}$ with $k \in \mathbf{Z}$, and all of these units have norm 1. If we write $u^k = (197 + 42\sqrt{22})^k = r_k + s_k\sqrt{22}$, then the solutions to Pell's equation $x^2 - 22y^2 = 1$ are given by $(x, y) = (\pm r_k, \pm s_k)$ where $k \in \mathbf{Z}$ with $k \geq 0$. We also remark that since

$$(r_{k+1}, s_{k+1}\sqrt{22}) = u^{k+1} = u^k \cdot u = (r_k + s_k\sqrt{22})(197 + 42\sqrt{22}) = (197r_k + 924s_k) + (42r_k + 197s_k)\sqrt{22},$$

it follows that the sequences $\{r_k\}$ and $\{s_k\}$ are given recursively for $k \geq 0$ by

$$r_0 = 1\ ,\ s_0 = 0\ ,\ r_{k+1} = 197r_k + 924s_k\ ,\ s_{k+1} = 42r_k + 197s_k\ .$$

It is also possible to solve the recursion to obtain explicit (but ugly) closed-form formulas for r_k and s_k.

(b) Solve Pell's equation $x^2 - 13y^2 = 1$.

Solution: The following table lists the data used to calculate the continued fraction for $\sqrt{13}$ and the first few convergents $c_k = \frac{p_k}{q_k}$ along with the norms $N_k = N(p_k + q_k\sqrt{13}) = p_k^2 - 13\,q_k^2$.

0	$\sqrt{13}$	3	3	1	-4
1	$\frac{1}{\sqrt{13}-3} = \frac{\sqrt{13}+3}{4}$	1	4	1	3
2	$\frac{4}{\sqrt{13}-1} - \frac{\sqrt{13}+1}{3}$	1	7	2	-3
3	$\frac{3}{\sqrt{13}-2} = \frac{\sqrt{13}+2}{3}$	1	11	3	4
4	$\frac{3}{\sqrt{13}-1} = \frac{\sqrt{13}+1}{4}$	1	18	5	-1
5	$\frac{4}{\sqrt{13}-3} = \frac{\sqrt{13}+3}{1}$	6			

We have $\sqrt{13} = [3, \overline{1,1,1,1,6}\,]$ with periosd $\ell = 5$. Writing $u_k = p_k + q_k\sqrt{13} \in \mathbf{Z}[\sqrt{13}\,]$, the smallest unit u in $\mathbf{Z}[\sqrt{13}\,]$ with $u > 1$ is $u = u_{\ell-1} = u_4 = 18 + 5\sqrt{13}$, and we have $N(u) = -1$. The smallest unit v in $\mathbf{Z}[\sqrt{13}\,]$ with $v > 1$ and $N(v) = 1$ is $v = u^2 = (18+5\sqrt{13})^2 = 649+180\sqrt{13}$. If we write $v^k = (649+180\sqrt{13})^k = r_k + s_k\sqrt{13}$, then the solutions to Pell's equation $x^2 - 13y^2 = 1$ are given by $(x, y) = (\pm r_k, \pm s_k)$ where $k \in \mathbf{Z}$ with $k \geq 0$.

4: (a) Let $d \in \mathbf{Z}^+$ be a non-square and let $0 \neq n \in \mathbf{Z}$. Show that the Diophantine equation $x^2 - dy^2 = n$ either has no solution or infinitely many solutions.

Solution: Suppose that the Diophantine equation $x^2 - dy^2 = n$ has at least one solution. Let (x, y) be a solution. Let $a = |x|$ and $b = |y|$, and note that (a, b) is another solution with $a, b \geq 0$. Let $w = a + b\sqrt{d}$ and note that $N(w) = a^2 - db^2 = n$. Since $n \neq 0$ we have $(a, b) \neq (0, 0)$ and so $w = a + b\sqrt{d} \geq 1$. Let u be the smallest unit in $\mathbf{Z}[\sqrt{d}]$ with $u > 1$. Since $u > 1$ and $w \geq 1$ we have $w < wu < wu^2 < wu^3 < \cdots$. Write $wu^k = r_k + s_k\sqrt{d}$ for $k \geq 0$. For each $k \geq 0$ we have $r_k^2 - ds_k^2 = N(wu^k) = N(w)N(u)^k = n \cdot 1^k = n$ and so (r_k, s_k) is a solution to the Diophantine equation $x^2 - dy^2 = n$.

(b) For which $n \in \mathbf{Z}$ with $-3 \leq n \leq 10$ do there exist $x, y \in \mathbf{Z}$ with $x^2 - 31\,y^2 = n$?

Solution: We calculate the continued fraction for $\sqrt{31}$.

k	a_k	$x_k = \frac{1}{x_k - a_k} = \frac{r_k + \sqrt{31}}{s_k}$	p_k	q_k	${p_k}^2 - 31{q_k}^2$
0	5	$\sqrt{31} = \frac{0+\sqrt{31}}{1}$	5	1	-6
1	1	$\frac{1}{\sqrt{31}-5} = \frac{\sqrt{31}+5}{6}$	6	1	5
2	1	$\frac{6}{\sqrt{31}-1} = \frac{\sqrt{31}+1}{5}$	11	2	-3
3	3	$\frac{5}{\sqrt{31}-4} = \frac{\sqrt{31}+4}{3}$	39	7	2
4	5	$\frac{3}{\sqrt{31}-5} = \frac{\sqrt{31}+5}{2}$	206	37	-3
5	3	$\frac{2}{\sqrt{31}-5} = \frac{\sqrt{31}+5}{3}$	657	118	5
6	1	$\frac{3}{\sqrt{31}-4} = \frac{\sqrt{31}+4}{5}$	863	155	-6
7	1	$\frac{5}{\sqrt{31}-1} = \frac{\sqrt{31}+1}{6}$	1520	273	1
8	10	$\frac{6}{\sqrt{31}-5} = \frac{\sqrt{31}+5}{1}$			

Note first that the solutions to $x^2 - 31y^2 = 1$ are given by $(x, y) = (p_k, q_k)$ with $k = 7 \bmod 8$, and there are no solutions to $x^2 - 31y^2 = -1$. When $n = -3$ a solution to the equation $x^2 - 31y^2 = n$ is given by $(x, y) = (p_2, q_2) = (11, 2)$, when $n = 0$ a solution is given by $(x, y) = (0, 0)$, when $n = 2$ a solution is given by $(x, y) = (p_3, q_3) = (39, 7)$, when $n = 5$ a solution is given by $(x, y) = (p_1, q_1) = (6, 1)$, and when $n = -6$ a solution is given by $(x, y) = (p_0, q_0) = (5, 1)$.

For $x, y \in \mathbf{Q}$, let us write $N(x + y\sqrt{31}) = x^2 - 31y^2$ (with no absolute value sign). Let $u_{-6} = 5 + \sqrt{31}$, $u_{-3} = 11 + 2\sqrt{31}$, $u_1 = 1520 + 273\sqrt{31}$, $u_2 = 39 + 7\sqrt{31}$ and $u_5 = 6 + \sqrt{31}$ so that for each $n = -6, -3, 1, 2, 5$ we have $u_n \in \mathbf{Z}[\sqrt{31}]$ with $N(u_n) = n$. Let $u_4 = (u_2)^2$, $u_8 = (u_2)^3$, $u_9 = (u_3)^3$ and $u_{10} = u_2 u_5$. Then for $n = 4, 8, 9, 10$ we have $N(u_n) = n$, and so the equation $x^2 - 31y^2 = n$ does have a solution (indeed if we write $u_n = x + y\sqrt{31}$ then $n = N(u_n) = x^2 - y\sqrt{31})$.

We claim that when $n \in \{-1, -2, 3\}$ there is no solution. Suppose, for a contradiction that $x^2 - 31y^2 = n$ with $x, y \in \mathbf{Z}^+$ and $n \in \{-1, -2, 3\}$. Since $|n| < \sqrt{31}$, we know that $\frac{x}{y}$ must be equal to some convergent $c_k = \frac{p_k}{q_k}$. Note that $\gcd(x, y) = 1$ since if p was prime with $p|x$ and $p|y$ then we would have $p^2 | (x^2 - 31y^2) = n$, but -1, -2 and 3 have no square prime factors. Also note that $\gcd(p_k, q_k) = 1$ because of the identity $p_{k+1}q_k - q_{k+1}p_k = (-1)^k$. It follows that we must have $x = p_k$ and $y = q_k$. But then, from our table, and from the periodic nature of the values ${p_k}^2 - 31{q_k}^2$, we must have $x^2 - 31y^2 = {p_k}^2 - 31{q_k}^2 \in \{-6, -3, 1, 2, 5\}$.

Finally, we claim that when $n \in \{-1, 3, 6, 7\}$ there can be no solution. To see this we work modulo 8. Modulo 8, we have $x^2 \in \{0, 1, 4\}$ and so $x^2 - 31y^2 = x^2 + y^2 \in \{0, 1, 2, 4, 5\}$, and hence $x^2 - 31y^2 \notin \{-1, 3, 6, 7\}$. To summarize, there is a solution for $n \in \{-3, 0, 1, 2, 4, 5, 8, 9, 10\}$ but no solution for $n \in \{-2, -1, 3, 6, 7\}$.

5: (a) Find the first 2 smallest positive solutions to the Diophantine equation $x^2 - 2y^4 = -1$.

Solution: We solve Pell's equation $x^2 - 2z^2 = -1$ with $z = y^2$. By inspection, the smallest unit $u \in \mathbf{Z}[\sqrt{2}]$ with $u > 1$ is $u = 1 + \sqrt{2}$ and we have $N(u) = -1$. The units $v > 1$ with $N(v) = 1$ are the elements u^k with k even and the units $v > 1$ with $N(v) = -1$ are the elements u^k with k odd. If we write $u^{2k+1} = r_k + s_k\sqrt{2}$, then the positive solutions to Pell's equation $x^2 - 2z^2 = -1$ are the pairs $(x, z) = (r_k, s_k)$ with $k \geq 0$. We have

$$r_{k+1} + s_{k+1}\sqrt{2} = u^{2k+3} = u^{2k+1} \cdot u^2 = (r_k + s_k\sqrt{2})(3 + 2\sqrt{2}) = (3r_k + 4s_k) + (2r_k + 3s_k)\sqrt{2}$$

and so $\{r_k\}$ and $\{s_k\}$ are given recursively by $r_0 = 1$, $s_0 = 1$, $r_{k+1} = 3r_k + 4s_k$ and $s_{k+1} = 2r_k + 3s_k$. The first few values of r_k and s_k are listed below:

k	r_k	s_k
0	1	1
1	7	5
2	41	29
3	237	169

The first 2 values of s_k which are perfect squares are $s_0 = 1$ and $s_3 = 169$. Thus the first 2 positive solutions to Pell's equation $x^2 - 2z^2 = -1$ with z equal to a perfect square are $(x, z) = (1, 1)$ and $(237, 169)$, and hence the first 2 positive solutions to the Diophantine equation $x^2 - 2y^4 = -1$ are $(x, y) = (1, 1)$ and $(237, 13)$. We remark that these might be the *only* two positive solutions.

(b) Find the first 4 smallest positive solutions to the Diophantine equation $x(x + 1) = 2y^2$.

Solution: Note that $x(x+1) = 2y^2 \iff \left(x + \frac{1}{2}\right)^2 - \frac{1}{4} = 2y^2 \iff (2x+1)^2 - 8y^2 = 1$. We find the continued fraction for $\sqrt{8}$.

k	a_k	x_k	p_k	q_k	${p_k}^2 - 8{q_k}^2$
0	2	$\sqrt{8}$	2	1	-4
1	1	$\frac{1}{\sqrt{8}-2} = \frac{\sqrt{8}+2}{4}$	3	1	1
2	4	$\frac{4}{\sqrt{8}-2} = \frac{\sqrt{8}+2}{1}$			

We see that the smallest unit $u > 1$ in $\mathbf{Z}[\sqrt{8}]$ is $u = 3 + \sqrt{8}$. The smallest 4 units $v > 1$ are

$$u^1 = 3 + \sqrt{8}\ ,\ u^2 = 17 + 6\sqrt{8}\ ,\ u^3 = 99 + 35\sqrt{8}\ ,\ u^4 = 577 + 204\sqrt{8}.$$

The positive pairs (x, y) with $(2x + 1)^2 - 8y^2 = 1$ correspond to the units $(2x + 1) + y\sqrt{8}$, so the smallest 4 such pairs (x, y) are $(1, 1)$, $(8, 6)$, $(49, 35)$ and $(288, 204)$.