MAU22103/33101 - Introduction to Number Theory

Exercise Sheet 6

Trinity College Dublin

Course homepage

This is an entirely optional homework. If submitted, the best 5 out of 6 homeworks will be considered for your continuous assessment. Answers are due for Friday December 5th$^{\text{nd}}$, 23:59
The use of electronic calculators and computer algebra software is allowed.

Exercise 1 *Should've used this last year!*

In this, we will solve the Pell-Fermat equation

$$x^2 - 7y^2 = 1$$

for $x, y \in \mathbb{Z}$.

1. (30 pts) Determine the continued fraction expansion
$$\sqrt{7} = [a_0, a_1, \ldots, a_r, \overline{b_1, \ldots, b_s}]$$
2. (30 pts) Hence, determine the fundamental solution of the above Pell-Fermat equation
3. (30 pts) Determine a solution (x, y) to the Pell-Fermat equation with $y > 100$

4. (10 pts) Prove that there exists an infinite family of solutions (x_n, y_n) such that $3|y_n$

   Hint: Binomial expansion

This was the only exercise that is required for your submission to be considered. All remaining exercises are entirely optional and are not worth any points

However, I strongly encourage you to give them a try, as the best way to learn number theory is through practice.

The exercises are arranged by theme, and roughly in order of difficulty within each theme, with the first few working as good warm-ups, and the remainder being of similar difficulty to the main exercise. You are welcome to email me if you have any questions about them. The solutions will be made available with the solution to the main exercise.

Exercise 2 *Computing continued fraction expansions*

Compute the complete continued fraction expansions of the following quadratic irrationals

i) $\sqrt{13}$

ii) $\sqrt{17}$

iii) $\frac{11+\sqrt{7}}{2}$

iv) $\frac{3+\sqrt{8}}{2}$

v) $\sqrt{2}$

Solution 2

We know all these will be eventually periodic, so we just need to compute until we loop around

i) $a_0 = \lfloor \sqrt{13} \rfloor = 3$, and so

$$\begin{aligned}
x_1 &= \frac{1}{\sqrt{13}-3} = \frac{\sqrt{13}+3}{4} \\
a_1 &= 1 \\
x_2 &= \frac{1}{\frac{\sqrt{13}+3}{4}-1} = \frac{4}{\sqrt{13}-1} = \frac{\sqrt{13}+1}{3} \\
a_2 &= 1 \\
x_3 &= \frac{3}{\sqrt{13}-2} = \frac{\sqrt{13}+2}{3} \\
a_3 &= 1 \\
x_4 &= \frac{3}{\sqrt{13}-1} = \frac{\sqrt{13}+1}{4} \\
a_4 &= 1 \\
x_5 &= \frac{4}{\sqrt{13}-3} = \sqrt{13}+3 \\
a_5 &= 6 \\
x_6 &= \frac{1}{\sqrt{13}-3} = \frac{\sqrt{13}+3}{4} = x_1
\end{aligned}$$

and so we have entered the loop. Thus

$$\sqrt{13} = [3, \overline{1, 1, 1, 1, 1, 6}].$$

ii) $a_0 = 4$, and so

$$\begin{aligned}
x_1 &= \frac{1}{\sqrt{17}-4} = \sqrt{17}+4 \\
a_1 &= 8 \\
x_2 &= \frac{1}{\sqrt{17}-4} = \sqrt{17}+4 = x_1
\end{aligned}$$

and so

$$\sqrt{17} = [4, \overline{8}].$$

iii) We compute $a_0 = 6$, and so

$$\begin{aligned}
x_1 &= \frac{2}{\sqrt{7}-1} = \frac{\sqrt{7}+1}{3} \\
a_1 &= 1 \\
x_2 &= \frac{3}{\sqrt{7}-2} = \sqrt{7}+2 \\
a_2 &= 4 \\
x_3 &= \frac{1}{\sqrt{7}-2} = \frac{\sqrt{7}+2}{3} \\
a_3 &= 1 \\
x_4 &= \frac{3}{\sqrt{7}-1} = \frac{\sqrt{7}+1}{2} \\
a_4 &= 1 \\
x_5 &= \frac{2}{\sqrt{7}-1} = \frac{\sqrt{7}+1}{3} = x_1
\end{aligned}$$

and so

$$\frac{11+\sqrt{7}}{2} = [6, \overline{1,4,1,1}]$$

iv) $a_0 = 2$, and

$$\begin{aligned}
x_1 &= \frac{2}{\sqrt{8}-1} = \frac{2\sqrt{8}+2}{7} \\
a_1 &= 1 \\
x_2 &= \frac{7}{2\sqrt{8}-5} = 2\sqrt{8}+5 \\
a_2 &= 10 \\
x_3 &= \frac{1}{2\sqrt{8}-5} = \frac{2\sqrt{8}+5}{7} \\
a_3 &= 1 \\
x_4 &= \frac{7}{2\sqrt{8}-2} = \frac{2\sqrt{8}+2}{4} = \frac{\sqrt{8}+1}{2} \\
a_4 &= 1
\end{aligned}$$

$$x_5 = \frac{2}{\sqrt{8}-1} = \frac{2\sqrt{8}+2}{7} = x_1$$

and so

$$\frac{3+\sqrt{8}}{2} = [2, \overline{1, 10, 1, 1}].$$

v) We have that $a_0 = 1$ and

$$\begin{aligned} x_1 &= \frac{1}{\sqrt{2}-1} = \sqrt{2}+1 \\ a_1 &= 2 \\ x_2 &= \frac{1}{\sqrt{2}-1} = \sqrt{2}+1 = x_1 \end{aligned}$$

and so

$$\sqrt{2} = [1, \overline{2}].$$

Exercise 3 *The battle of Hastings*

The battle of Hastings, took place on October 14, 1066, is referred to in the following fictional historical text, taken from *Amusement in Mathematics* (H. E. Dundeney, 1917), refers to it:

"The men of Harold stood well together, as their wont was, and formed thirteen squares, with a like number of men in every square thereof. (. . .) When Harold threw himself into the fray the Saxons were one mighty square of men, shouting the battle cries 'Ut!', 'Olicrosse!', 'Godemite!'."

Use continued fractions to determine the minimal number of soldiers this fictional historical text suggests Harold II had at the battle of Hastings.

Solution 3

Prior to Harold joining the battle, there are thirteen squares of men, so $13y^2$ men overall, for some $y > 0$. After Harold joins, there is one big square, so x^2 for some $x > 0$. Since Harold was the only mentioned addition, we must have

$$13y^2 + 1 = x^2 \quad \Leftrightarrow \quad x^2 - 13y^2 = 1$$

Thus, it suffices to find the fundamental solution to this Pell-Fermat equation. Using the continued fraction expansion computed in the previous exercise, we compute the convergents of $\sqrt{13}$:

$$\begin{aligned}(p_0, q_0) &= (3, 1)\\ (p_1, q_1) &= (4, 1)\\ (p_2, q_2) &= (7, 2)\\ (p_3, q_3) &= (11, 3)\\ (p_4, q_4) &= (18, 5)\\ (p_5, q_5) &= (119, 33)\\ (p_6, q_6) &= (137, 38)\\ (p_7, q_7) &= (256, 71)\\ (p_8, q_8) &= (393, 109)\\ (p_9, q_9) &= (649, 180)\end{aligned}$$

Checking all of these, we find that the first solution is

$$649^2 - 13(180)^2 = 1$$

Hence, $(x, y) = (649, 180)$ is the minimal solution. We could have gotten there slightly faster by noting that

$$18^2 - 13(5)^2 = -1$$

and deducing that a solution (a fundamental solution) must therefore correspond to

$$(18 + 5\sqrt{13})^2.$$

Either way, Harold had $13(180)^2 = 421,200$ soldiers other than himself, roughly a fifth of the population of England at the time!

Exercise 4 *Negative Pell Equations*

Let $d \in \mathbb{N}$ be a non-square. Can we find integers $x, y \in \mathbb{Z}$ such that

$$x^2 - dy^2 = -1?$$

i) Show that if (x, y) is a solution to the negative Pell-Fermat equation, then $(z, w) = (x^2 + dy^2, 2xy)$ is a solution to the usual Pell-Fermat equation

$$z^2 - dw^2 = 1$$

Hint: Norm

ii) Let (a, b) be the fundamental solution of

$$x^2 - dy^2 = 1.$$

Show that there exists a solution to

$$x^2 - dy^2 = -1$$

if and only if

$$\sqrt{a + b\sqrt{d}} \in \mathbb{Z}[\sqrt{d}].$$

Hint: For the $\Leftarrow$ implication, find a nice polynomial satisfied by the square root. How many real roots does this have?

iii) Hence determine a solution to

$$x^2 - 17y^2 = -1$$

You may use that

$$33^2 - 17(8)^2 = 1$$

Remark 1. *In practice, computing the square root of a fundamental solution is not the best way to compute a solution to the negative Pell-Fermat equation. A solution exists if and only if the continued fraction of $\sqrt{d}$ has odd period, and if such a solution exists, it will be (p_n, q_n) for some convergent before that corresponding to the fundamental solution. As such, computing the square root is only useful if you are given the fundamental solution - otherwise you'll solve the negative Pell-Fermat equation along the way to solving the positive Pell-Fermat equation.*

Solution 4

i) If (x, y) is a solution to the negative Pell-Fermat equation, that means that

$$\mathrm{N}(x + y\sqrt{d}) = -1$$

and hence

$$\mathrm{N}((x + y\sqrt{d})^2) = \Big(\mathrm{N}(x + y\sqrt{d})\Big)^2 = (-1)^2 = 1$$

and so taking (z, w) defined by

$$z + w\sqrt{d} = (x + y\sqrt{d})^2 = x^2 + dy^2 + 2xy\sqrt{d}$$

gives a solution to the usual Pell-Fermat equation.

ii) If (x, y) is a solution to the negative Pell-Fermat equation, then $(x + y\sqrt{d})^2$ is a unit in $\mathbb{Z}[\sqrt{d}]$ and hence

$$(x + y\sqrt{d})^2 = \pm(a + b\sqrt{d})^n$$

for some $n \in \mathbb{Z}$. We can assume, without loss of generality, that $x, y \geq 0$, and hence we must have

$$(x + y\sqrt{d})^2 = (a + b\sqrt{d})^n$$

for some $n \geq 0$. Then, if $n = 2m$

$$x + y\sqrt{d} = (a + b\sqrt{d})^m$$

and so $x^2 - dy^2 = 1 \neq -1$, and so $n = 2m + 1$ must be odd. Thus

$$x + y\sqrt{d} = (a + b\sqrt{d})^m \sqrt{a + b\sqrt{d}}$$

and so

$$\sqrt{a + b\sqrt{d}} = \frac{x + y\sqrt{d}}{(a + b\sqrt{d})^m} = (x + y\sqrt{d})(a - b\sqrt{d})^m \in \mathbb{Z}[\sqrt{d}]$$

In contrast, suppose that there exists $\alpha = x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ such that

$$\alpha^2 = (x + y\sqrt{d})^2 = a + b\sqrt{d}.$$

Considering norms, we see that we must have

$$\mathrm{N}(\alpha) = x^2 - dy^2 = \pm 1.$$

If $\mathrm{N}(\alpha) = 1$, then we must have that there exists $n \in \mathbb{Z}$ such that

$$\alpha = \pm(a + b\sqrt{d})^n = \pm\alpha^{2n}$$

and so $f(\alpha) = 0$ for $f(z) = z^{2n} + z$ or $f(z) = z^{2n} - z$. Since $\alpha \neq 0$, this means that α is a root of

$$g(z) = z^{2n-1} \pm 1$$

which have at exactly one real root of $z = \pm 1$. Since $\alpha \neq \pm 1$, we cannot have that $\mathrm{N}(\alpha) = 1$ and hence $\mathrm{N}(\alpha) = -1$, giving a solution to the negative Pell-Fermat equation.

iii) We will determine $x, y \in \mathbb{N}$ such that

$$(x + y\sqrt{17})^2 = 33 + 8\sqrt{17}$$

or equivalently, such that

$$x^2 + 17y^2 = 33 \quad \text{and} \quad 2xy = 8.$$

Since $2xy = 8$, $xy = 4$ and so we have that

$$(x, y) \in \{(1, 4), (2, 2), (4, 1)\}.$$

Checking these, we see that $x = 4$, $y = 1$ is a desired pair. And we can easily check that

$$4^2 - 17(1)^2 = -1.$$

Exercise 5 *Fractions to series*

Let $x \in (0, 1)$ be an irrational real, and denote by $[a_0, a_1, \ldots, a_n] = \frac{p_n}{q_n}$ the convergents of x. Show that

$$x = \sum_{n=0}^{\infty} \frac{(-1)^n}{q_n q_{n+1}}$$

Hint: Can we write $(-1)^n$ in terms of convergents?

Solution 5

Recall that $q_{n+1}p_n - p_{n+1}q_n = (-1)^{n+1}$ and hence

$$(-1)^n = p_{n+1}q_n - q_{n+1}p_n.$$

Then, for every $N \geq 0$, we must have that

$$\sum_{n=0}^{N} \frac{(-1)^n}{q_n q_{n+1}} = \sum_{n=0}^{N} \frac{p_{n+1}q_n - q_{n+1}p_n}{q_n q_{n+1}} = \sum_{n=0}^{N} \frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n} = \frac{p_{N+1}}{q_{N+1}} - \frac{p_0}{q_0}.$$

Thus

$$\sum_{n=0}^{\infty} \frac{(-1)^n}{q_n q_{n+1}} = \lim_{N\to\infty} \frac{p_{N+1}}{q_{N+1}} - \frac{p_0}{q_0} = x - \frac{p_0}{q_0}.$$

But $\frac{p_0}{q_0} = a_0 = \lfloor x \rfloor = 0$ and $x \in (0, 1)$.

Exercise 6 *Pellish equations modulo p*

If we want to find integer solutions to something like $x^2 - 11y^2 = 14$, continued fractions are less helpful to us. We could use a same norm argument construct a solution from solutions to

$$x^2 - 11y^2 = 2 \quad \text{and} \quad x^2 - 11y^2 = 7$$

but solving these is non-trivial. Working modulo various primes, at least lets us check whether an integer solution is even possible. In fact, we can reduce it to checking finitely many primes.

i) Show that, modulo any prime $p \neq 11$, there exist $x, y \in \mathbb{Z}$ such that

$$x^2 - 11y^2 \equiv 14 \pmod{p}$$

Hint: How many possible values in $\mathbb{Z}/p\mathbb{Z}$ can x^2 take? How many possible values can $11y^2 + 14$ take? Must the two sets of possible values overlap?

ii) Give a necessary and sufficient condition for there to exist $x, y \in \mathbb{Z}$ such that

$$x^2 - 11y^2 \equiv 14 \pmod{7}.$$

Determine if such a pair exist.

iii) Show that, for any integers $d, n \in \mathbb{Z}$ and $p \nmid d$, there exist $x, y \in \mathbb{Z}$ such that

$$x^2 - dy^2 \equiv n \pmod{p}$$

Remark 2. *Using a variation on Hensel's Lemma (from the second problem sheet), you can show that for all odd primes $p \nmid d$ and $p \nmid n$, there exists a solution to*

$$x^2 - dy^2 \equiv n \ (mod\ p^k)$$

for all $k \geq 1$. If there exist solutions to

$$x^2 - dy^2 \equiv n \ (mod\ p^k)$$

for all primes p and all $k \geq 1$, a result called the Hasse principle says that there exist $x, y \in \mathbb{Q}$ such that

$$x^2 - dy^2 = n$$

Combined with the results from above and some variations on Hensel's Lemma, you can reduce showing the existence of rational solutions to checking for "nice" solutions in $\mathbb{Z}/p\mathbb{Z}$ for the finitely many odd primes p such that $p|dn$, and a "nice" solution in $\mathbb{Z}/2^k\mathbb{Z}$ for some hopefully small k. Usually $k = 3$ is good enough.

Solution 6

1. We know that the map

$$\begin{aligned}(\mathbb{Z}/p\mathbb{Z})^\times &\to (\mathbb{Z}/p\mathbb{Z})^\times \\ x &\mapsto x^2\end{aligned}$$

is 2-to-1, and hence takes $\frac{p-1}{2}$ values. If we include $\overline{0}$, we see that the map

$$\begin{aligned}\mathbb{Z}/p\mathbb{Z} &\to \mathbb{Z}/p\mathbb{Z} \\ x &\mapsto x^2\end{aligned}$$

takes $\frac{p+1}{2}$ distinct values as x ranges over $\mathbb{Z}/p\mathbb{Z}$.

As 11 is invertible modulo $p \neq 11$, multiplication by 11 gives a bijection

$$\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$$

and hence $11y^2$ takes $\frac{p+1}{2}$ distinct values as y ranges over $\mathbb{Z}/p\mathbb{Z}$. Similarly, addition of 14 is also a bijection, and so $11y^2 + 14$ takes $\frac{p+1}{2}$ distinct values as y ranges over $\mathbb{Z}/p\mathbb{Z}$.

If the $\frac{p+1}{2}$ distinct possible values of x^2 and the $\frac{p+1}{2}$ distinct possible values of $11y^2+14$ in $\mathbb{Z}/p\mathbb{Z}$ did not have any common values, this would implies there are $\frac{p+1}{2} + \frac{p+1}{2} = p + 1$ distinct elements in $\mathbb{Z}/p\mathbb{Z}$. But $\mathbb{Z}/p\mathbb{Z}$ is a set of size p, so this is impossible. Hence there must exist a choice of $x, y \in \mathbb{Z}/p\mathbb{Z}$ such that

$$x^2 \equiv 11y^2 + 14 \pmod{p}$$

2. The existence of such x, y is equivalent to being able to solve

$$x^2 \equiv 14 \equiv 3 \pmod{7}$$

which is in turn equivalent to

$$\left(\frac{3}{11}\right) = 1$$

We can easily compute

$$\left(\frac{3}{11}\right) = -\left(\frac{7}{3}\right) = -\left(\frac{-1}{3}\right) = 1$$

so a solution does indeed exist.

3. Similarly to before, x^2 $\frac{p+1}{2}$ distinct values as x ranges over $\mathbb{Z}/p\mathbb{Z}$. As $p \nmid d$, multiplication by d is a bijection, and so dy^2+n takes $\frac{p+1}{2}$ distinct values as y ranges over $\mathbb{Z}/p\mathbb{Z}$.

Thus, by the same reasoning as in part (i), there must exist $x, y \in \mathbb{Z}$ such that

$$x^2 \equiv dy^2 + n \pmod{p}$$

for every $p \nmid d$.

Exercise 7 *Approximations*

Without computing the convergents of the irrational in question, determine whether the following rational approximations are convergents of the given irrational α

1. $\sqrt{2} \approx \frac{3}{2}$
2. $\sqrt{40} \approx \frac{20}{3}$
3. $\sqrt{72} \approx \frac{17}{2}$
4. $\pi \approx \frac{22}{7}$
5. $e \approx \frac{27}{10}$

Hint: Try to bound the true value of $|q\alpha - p|$ above or below by taking a close bound to α.

Solution 7

We will use that if $|q\alpha - p| < \frac{1}{2q}$, then $\frac{p}{q}$ is a convergent.

i) We need to check what $|2\sqrt{2} - 3|$ is to the accuracy of $\frac{1}{4} = 0.25$.. As $\sqrt{2} \approx 1.414 > 1.4$,

$$3 - 2\sqrt{2} < 3 - 2.8 = 0.2 < 0.25$$

and so $\frac{3}{2}$ is a convergent.

ii) We need to check whether

$$|3\sqrt{40} - 20| < \frac{1}{6}$$

We have that

$$\sqrt{40} \approx 6.324555 < \frac{19}{3}$$

and so

$$20 - 3\sqrt{40} > 20 - 19 = 1 > \frac{1}{6}$$

so $\frac{20}{3}$ is not a convergent.

iii) We have that $\sqrt{72} \approx 8.48$, and so $8.4 < \sqrt{72} < 8.5$. Hence

$$0.2 = 17 - 16.8 > 17 - 2\sqrt{72} > 17 - 17 = 0$$

and $0.2 < \frac{1}{4}$, so $\frac{17}{2}$ is a convergent.

iv) We know that $\pi \approx 3.14$, so $3.1 < \pi < 3.2$. Hence

$$0.4 = 7(3.2) - 22 > |7\pi - 22| < 22 - 7(3.1) = 0.7$$

neither of give a tight enough bound for us to say either way. Lets try the bound of

$$|7\pi - 22| < 7(3.15) - 22 = 0.05 < 0.07 < \frac{1}{14}$$

and so $\frac{22}{7}$ is a convergent.

v) I know that $e \approx 2.718$, so $2.71 < e$ and hence

$$|10e - 27| > 0.1 > \frac{1}{20}$$

so $\frac{27}{10}$ is not a convergent of e.

Exercise 8 *Continued fractions for near-squares*

We will now prove a formula for the continued fraction of $n^2 + 1$, and more generally certain quadratic irrationals

i) Prove that $\sqrt{n^2 + 1}$ is irrational for all $n \geq 1$

ii) Prove that if $x^2 = n^2 + 1$ and $x > 0$, then

$$x = [n, x + n]$$

iii) Hence show that

$$\sqrt{n^2 + 1} = [n, \overline{2n}].$$

iv) Suppose that

$$x^2 + bx + c = 0$$

has irrational roots $\beta < 0 < \alpha$, and

$$x^2 + bx + c - 1$$

has integer roots $t < 0 < s \in \mathbb{Z}$, then

$$\alpha = [s, \overline{s - t}]$$

Solution 8

i) If $\sqrt{n^2+1}$ is rational, it must be an integer m. Then

$$m^2 - n^2 = 1$$

and so

$$(m-n)(m+n) = 1.$$

Since ± 1 are the only divisors of 1, and m, n are integers, we must have

$$m - n = m + n = \pm 1$$

and hence $n = -n$, which implies $n = 0$. Hence, $\sqrt{n^2+1}$ is irrational for all $n \geq 1$

ii) If $x^2 = n^2 + 1$, then

$$\begin{aligned} x^2 - n^2 &= 1, \\ (x-n)(x+n) &= 1, \\ x - n &= \frac{1}{x+n}, \\ x &= n + \frac{1}{x+n}. \end{aligned}$$

Since $x > 0$, $x + n \geq 1$, and so we can use the extended notation for continued fractions to write

$$x = [n, x+n]$$

iii) $x = \sqrt{n^2+1}$ is the positive solution to $x^2 = n^2 + 1$, and as such satisfies

$$x = [n, x+n]$$

Hence

$$x + n = n + \frac{1}{x+n} + n = 2n + \frac{1}{x+n}$$

and so

$$x + n = [2n, x+n]$$

which we can iterated to get

$$x + n = [2n, x+n] = [2n, 2n, x+n] = \cdots [\overline{2n}]$$

and hence

$$x = [n, x+n] = [n, \overline{2n}].$$

iv) Similarly to above, if $x^2 + bx + c = 0$, we must have that

$$(x - s)(x - t) = 1$$

and hence

$$x = s + \frac{1}{x - t} = [s, x - t] = [s, s - t, x - t] = [s, s - t, s - t, x - t] = \cdots = [s, \overline{s - t}]$$

is a continued fraction expansion for one of the roots of $x^2 + bx + c$, as $s - t > 0$. Since $\beta < 0$, and $[s, \overline{s - t}] > 0$, we must have

$$\alpha = [s, \overline{s - t}]$$