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 November 29$^{\text{nd}}$, 23:59
The use of electronic calculators and computer algebra software is allowed.

Exercise 1 *November's not over yet!*

In this, we will solve the Pell-Fermat equation

$$x^2 - 11y^2 = 1$$

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

1. (30 pts) Determine the continued fraction expansion

$$\sqrt{11} = [a_0, a_1, \dots, a_r, \overline{b_1, \dots, b_s}]$$

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) $\sqrt{2}$

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.

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.*

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?*

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

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

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*

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

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

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

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.

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.

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

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