MTH6128 Number Theory

Solutions to exam

---

1 Question:

(a) Define the terms **algebraic integer**, **quadratic integer**, and **transcendental**. [Bookwork]

(b) Determine which of the following are quadratic integers. Explain which theorems you have used.

(i) $\frac{1+\sqrt{49}}{2}$;

(ii) $\frac{\sqrt{3}}{2} - \frac{7}{2}$;

(iii) $\frac{\sqrt{5}}{2} + \frac{\sqrt{-3}}{2}$;

(iv) $\frac{7}{2} + \frac{\sqrt{65}}{2}$.

[similar to coursework]

(c) Let D be a natural number which is not a square. Using minimal polynomials, show that $\frac{1+\sqrt{D}}{2}$ is an algebraic integer if and only if $D \equiv 1 \pmod 4$. [coursework]

Solution:

(a) The definitions are:

- $\alpha \in \mathbb{C}$ is an algebraic integer if there exists a monic polynomial $f(x)$ with integer coefficients such that $f(\alpha) = 0$.
- A quadratic integer is an algebraic integer whose minimal polynomial has degree 2 (our convention in the lectures is that the minimal polynomial is monic).
- $\alpha \in \mathbb{C}$ is a transcendental number if α is not an algebraic number.

(b) We had the following propositions in the lectures:

Proposition: $\alpha \in \mathbb{C}$ is a quadratic number if and only if $\alpha = u + v\sqrt{d}$ for some $u, v \in \mathbb{Q}$ and $1 \neq d \in \mathbb{Z}$ squarefree.

Proposition: A quadratic number α is a quadratic integer if and only if $\alpha = u + v\sqrt{d}$ for some $1 \neq d \in \mathbb{Z}$ squarefree and for u, v satisfying $u \in \mathbb{Z}$

and $v \in \mathbb{Z}$ or $u - \frac{1}{2} \in \mathbb{Z}$, $v - \frac{1}{2} \in \mathbb{Z}$ and $d \equiv 1 \pmod 4$. So all in all, $\alpha \in \mathbb{C}$ is a quadratic integer if and only if $\alpha = u + v\sqrt{d}$ for some $1 \neq d \in \mathbb{Z}$ squarefree and for u, v satisfying $u \in \mathbb{Z}$ and $v \in \mathbb{Z}$ or $u - \frac{1}{2} \in \mathbb{Z}$, $v - \frac{1}{2} \in \mathbb{Z}$ and $d \equiv 1 \pmod 4$.

(i) $\frac{1+\sqrt{49}}{2} = 4$. So it's an integer and not a quadratic integer.

(ii) We have $\frac{\sqrt{3}}{2} - \frac{7}{2} = u + v\sqrt{d}$. Here $u = -\frac{7}{2}$ and $v = \frac{1}{2}$. Since $d \equiv 3$ (mod 4) and $u, v \notin Z$, we know $\frac{\sqrt{3}}{2} - \frac{7}{2}$ is not a quadratic integer .

(iii) This is not of the form $u + v\sqrt{d}$ so it's not a quadratic number (and so isn't a quadratic integer).

(iv) This is of the form $u + v\sqrt{d}$ with $u = \frac{7}{2}$, $v = \frac{1}{2}$ and $d = 65 \equiv 1$ (mod 4). Since $u - \frac{1}{2}, v - \frac{1}{2} \in \mathbb{Z}$ we can conclude that $\frac{7}{2} - \frac{\sqrt{65}}{2}$ is a quadratic integer.

(c) Consider the polynomial $f(x) = x^2 - x - \frac{D-1}{4}$. We have

$$f\left(\frac{1+\sqrt{D}}{2}\right) = \frac{1+2\sqrt{D}+D}{4} - \frac{1+\sqrt{D}}{2} - \frac{D-1}{4} = \frac{D-1}{4} - \frac{D-1}{4} = 0.$$

This shows that f must be the minimal polynomial of $\frac{1+\sqrt{D}}{2}$ because if $\frac{1+\sqrt{D}}{2}$ were the root of a polynomial with degree 1, then it would have to be a rational number, which it is not.

We know that $\frac{1+\sqrt{D}}{2}$ is an algebraic integer if and only if all coefficients of f are integers. This, in turn, happens if and only if $\frac{D-1}{4}$ is an integer, which is equivalent to saying that 4 divides $D - 1$, i.e., $D \equiv 1 \pmod 4$.

2 Question:

(a) What is a **periodic continued fraction**? Give an example of an irrational number whose continued fraction expansion is not periodic. [Bookwork]

(b) Use the Euclidean algorithm to find a continued fraction expansion for $\frac{241}{113}$. [Similar to coursework/examples]

(c) Determine the value of the infinite continued fraction

$$[1; \overline{2, 1}].$$

Write your answer in the form $u + v\sqrt{d}$, where $u, v \in \mathbb{Q}$ and $d \in \mathbb{Z}$. [Similar to coursework/examples]

(d) Find the continued fraction expansion of $\sqrt{7}$. [Similar to coursework/examples]

Solution:

(a) Definition from the notes: The infinite continued fraction

$$[a_0; a_1, a_2, \ldots]$$

is *periodic* if there exist integers k, l with $k > 0$ such that

$$a_{n+k} = a_n \text{ for all } n \geq l.$$

We proved that a periodic continued fraction is a quadratic number. So the continued fraction of $2^{1/3}$ is not periodic. (Students will get full marks for writing down a correct answer without justification).

(b) Notice

$$[\overline{1;2}] = 1 + \frac{1}{2 + \frac{1}{[\overline{1;2}]}}$$

Let $x = [\overline{1;2}] > 0$. The above equation implies

$$2x^2 - 2x - 1 = 0 \Rightarrow x = \frac{1}{2} + \frac{\sqrt{3}}{2}.$$

(c) Apply the Euclidean algorithm to $241, 113$

$$\begin{aligned} 241 &= 2 \cdot 113 + 15 \\ 113 &= 7 \cdot 15 + 8 \\ 15 &= 1 \cdot 8 + 7 \\ 8 &= 1 \cdot 7 + 1 \\ 7 &= 7 \cdot 1 + 0 \end{aligned}$$

So the continued fraction is $[2; 7, 1, 1, 7]$. Note that $[2; 7, 1, 1, 6, 1]$ is also correct.

(d) Using the algorithm from the lectures

$$\begin{aligned} \sqrt{7} &= 2 + (\sqrt{7} - 2) \\ \frac{1}{\sqrt{7} - 2} &= \frac{\sqrt{7} + 2}{3} = 1 + \frac{\sqrt{7} - 1}{3} \end{aligned}$$

$$
\begin{aligned}
\frac{3}{\sqrt{7}-1} &= \frac{\sqrt{7}+1}{2} = 1 + \frac{\sqrt{7}-1}{2} \\
\frac{2}{\sqrt{7}-1} &= \frac{\sqrt{7}+1}{3} = 1 + \frac{\sqrt{7}-2}{3} \\
\frac{3}{\sqrt{7}-2} &= \sqrt{7}+2 = 4 + (\sqrt{7}-2)
\end{aligned}
$$

At this point notice that the fractional part in the last step equals the fractional part in the first step, hence this process will now repeat. This implies

$$\sqrt{7} = [2; \overline{1, 1, 1, 4}].$$

3 Question:

(a) Given that

$$\sqrt{29} = [5; \overline{2, 1, 1, 2, 10}]$$

find the fundamental solution to the equation

$$x^2 - 29y^2 = \pm 1.$$

Use your answer to write down all positive integer solutions to the equation $x^2 - 29y^2 = \pm 1$. Explain why you have found ALL solutions. [Similar to coursework]

(b) Given that $37^2 \equiv -1 \pmod{137}$ find integers x, y such that

$$x^2 + y^2 = 137.$$

[Similar to coursework]

(c) Suppose that $n \equiv 3 \pmod 4$. Show that $x^2 + y^2 = n$ has no integer solutions. [Bookwork]

Solution:

(a) From the notes: We define the *fundamental solution* to be the smallest solution of $x^2 - dy^2 = \pm 1$ in positive integers.

(b) In the lectures we saw that the the positive integer solutions (x, y) to the equation $x^2 - dy^2 = \pm 1$ are $(p_{\ell h-1}, q_{\ell h-1})$, $\ell = 1, 2, 3, \ldots$ where h is the period of $\sqrt{d}$ where p_n/q_n is the nth convergent of the continued fraction of

$\sqrt{d}$. Since the period is 5 the smallest solution will be (p_4, q_4). Computing we get that

$$\begin{aligned}
C_0 &= [5] = \frac{5}{1} \\
C_1 &= [5; 2] = \frac{11}{2} \\
C_2 &= \frac{p_2}{q_2} = \frac{1 \cdot 11 + 5}{1 \cdot 2 + 1} = \frac{16}{3} \\
C_3 &= \frac{p_3}{q_3} = \frac{1 \cdot 16 + 11}{1 \cdot 3 + 2} = \frac{27}{5} \\
C_4 &= \frac{p_4}{q_4} = \frac{2 \cdot 27 + 16}{2 \cdot 5 + 3} = \frac{70}{13}
\end{aligned}$$

So the fundamental solution is $(70, 13)$.

In the lectures we proved that if (x_1, y_1) is the fundamental solutions of $x^2 - dy^2 = \pm 1$ then all the positive integer solutions to $x^2 - dy^2 = \pm 1$ are the integers x_k, y_k, $k = 1, 2, \ldots$ defined by

$$x_k + y_k\sqrt{29} = (x_1 + y_1\sqrt{d})^k.$$

So the solutions are given by x_k, y_k defined by the formula

$$x_k + y_k\sqrt{29} = (70 + 13\sqrt{29})^k \qquad k = 1, 2, 3, 4, \ldots$$

Note that since the period of the continued fraction of $\sqrt{29}$ is odd

$$x_{2k+1}^2 - 29y_{2k+1}^2 = -1$$

and

$$x_{2k}^2 - 29y_{2k}^2 = +1$$

for $k = 0, 1, \ldots$.

(c) We run Hermite's algorithm from the lectures. Apply the Euclidean algorithm to 137 and 37

$$\begin{aligned}
137 &= 37 \cdot 3 + 26 \\
37 &= 26 \cdot 1 + 11 \\
26 &= 11 \cdot 2 + 4 \\
11 &= 4 \cdot 2 + 3 \\
4 &= 3 \cdot 1 + 1 \\
3 &= 1 \cdot 3 + 0
\end{aligned}$$

So the continued fraction of $37/137 = [0; 3, 1, 2, 2, 1, 3]$. We now compute convergent $C_n = p_n/q_n$ until we find m s.t. $q_m < \sqrt{137} < q_{m+1}$. We then know that $q_m^2 + (37 \cdot q_m - 137 \cdot p_m)^2 = 137$.

The convergents are:

$$C_0 = 0/1, C_1 = 1/3, C_2 = \frac{1 \cdot 1 + 0}{1 \cdot 3 + 1} = 1/4, C_3 = \frac{2 \cdot 1 + 1}{2 \cdot 4 + 3} = \frac{3}{11}, C_4 = \frac{2 \cdot 3 + 1}{2 \cdot 11 + 4} = 7/26$$

and we now stop since $26^2 > 137$. So $m = 3$ and

$$37 \cdot q_3 - 137 \cdot p_3 = 37 \cdot 11 - 137 \cdot 3 = -4.$$

So we conclude

$$4^2 + 11^2 = 137.$$

(Note: Finding the correct answer by brute force/guessing receives 2 points).

(d) Note that $x^2 \equiv 0, 1 \pmod 4$ and $y^2 \equiv 0, 1 \pmod 4$ so

$$x^2 + y^2 \equiv 0, 1, 2 \pmod 4$$

Hence if $n \equiv 3 \pmod 4$ then no solution exists.

Alternatively, suppose $n = f^2(x_1^2 + y_1^2)$ with $\gcd(x_1, y_1) = 1$ if $n \equiv 3 \pmod 4$ then $f^2 \equiv 1 \pmod 4$ so one of n's prime divisors p must be equivalent to 3 mod 4 and also divide $x_1^2 + y_1^2$. Also either x_1 or y_1 is co-prime to p (say x_1 is co-prime). So that

$$(y_1 \overline{x_1})^2 \equiv -1 \pmod p$$

where $x_1 \overline{x_1} \equiv 1 \pmod p$, but this is impossible, since -1 a quadratic non-residue $\pmod p$.

4 Question:

(a) Given a positive integer n define the **order of** $x \pmod n$. Define the term **primitive root** $\pmod p$. [Bookwork]

(b) Find a primitive root $\pmod{13}$. How many primitive roots $\pmod{13}$ are there? [Similar examples seen]

(c) Does there exist an integer n such that $n^4 \not\equiv 1 \pmod{17}$ and $n^5 \equiv 1 \pmod{17}$? Justify your answer by stating explicitly which theorems you use in the proof. [Unseen, similar to questions in previous exams]

(d) Compute $\varphi(280)$. (Hint: $280 = 2^3 \cdot 5 \cdot 7$.) [Similar examples seen]

(e) Show that $\varphi(n)$ is even for $n > 2$. [Coursework]

Solution:

(a) From the notes

(i) Let n be a positive integer. If there exists a positive integer d such that $x^d \equiv 1 \pmod{n}$, then the *order* of $x \pmod{n}$ is the smallest positive integer d such that $x^d \equiv 1 \pmod{n}$.

(ii) Let p be a prime number. An integer x is said to be a *primitive root* mod p if x has order $p-1 \pmod{p}$.

(b) By direct computation one can see that the order of each $2, 6, 7, 11$ is 12. To compute the order of 2, first note that the order of 2 divides 12. We need to check if any of $2^2, 2^3, 2^4, 2^6$ is $1 \pmod{13}$. We get that

$$2^2 \equiv 4 \pmod{13}, 2^3 \equiv 8 \pmod{13}, 2^4 \equiv 3 \pmod{13}, 2^6 \equiv 12 \pmod{13}.$$

Since none of these is $1 \pmod{13}$ 2 has order 12. There are $\varphi(13-1) = 4$ primitive roots.

(c) In the lectures we proved: For an integer x, there exists a positive integer d such that $x^d \equiv 1 \pmod{n}$ if and only if $\gcd(x, n) = 1$. If so, then the order of x divides $\phi(n)$.

Hence, the order of n must divide $\varphi(17) = 16$ so its order must be one of $1, 2, 4, 8, 16$. If its order is either $1, 2, 4$ then $n^4 \equiv 1 \pmod{17}$, the remaining options are $8, 16$, but in this case $n^5 \not\equiv 1 \pmod{17}$. So no such integer exists.

(d) $\varphi(280) = \varphi(8)\varphi(5)\varphi(7) = 4 \cdot 4 \cdot 6 = 96$.

(e) We saw that $\varphi(n) = \prod_{p^a || n} (p^a - p^{a-1})$, where the notation $p^a || n$ means that $p^a | n$ and p^{a+1} does not divide n. Notice that if $p > 2$ then $p^a - p^{a-1}$ is even so if $n \neq 2^b$ then $\varphi(n)$ is even. If $n = 2^b$ and $b = 0$ then $\varphi(n) = 1$ if $b \neq 0$ then $\varphi(n) = 2^b - 2^{b-1} = 2^{b-1}$ which is even unless $b = 1$.

5 Question:

(a) Define the term **quadratic residue**. Define the **Legendre symbol** $\left(\frac{a}{p}\right)$. State the **Law of Quadratic Reciprocity**. [Bookwork]

(b) Both 227 and 137 are primes. Compute $\left(\frac{137}{227}\right)$. You should clearly state any rules you use for calculating the Legendre symbol. [Similar to coursework/examples]

(c) Let p be an odd prime. Suppose that $p+2$ is also prime. Show that p is a quadratic residue $\pmod{(p+2)}$ if and only if

$$p \equiv \pm 1 \pmod 8.$$

[Unseen]

Solution

(a) From the coursenotes: An integer a is a *quadratic residue* $\pmod p$ if there exists an integer x with $x^2 \equiv a \pmod p$.

The *Legendre symbol* $\left(\frac{a}{p}\right)$ is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a, \\ +1 & \text{if } p \nmid a \text{ and } a \text{ is a quadratic residue } \pmod p, \\ -1 & \text{if } p \nmid a \text{ and } a \text{ is a quadratic non-residue } \pmod p \end{cases}$$

Quadratic reciprocity is: For any two distinct odd primes p and q,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$$

(b) We will now repeatedly use quadratic reciprocity along with other properties of the Legendre symbol.

$$\begin{aligned}
\left(\frac{137}{227}\right) &= \left(\frac{227}{137}\right) && \text{Quad. Recip.} \\
&= \left(\frac{-47}{137}\right) && \text{Periodicity} \\
&= \left(\frac{-1}{137}\right)\left(\frac{47}{137}\right) && \text{Multiplicativity} \\
&= 1 \cdot \left(\frac{137}{47}\right) && \text{Quad. Recip.} \\
&= \left(\frac{-4}{47}\right) && \text{Periodicity} \\
&= \left(\frac{-1}{47}\right) \cdot \left(\frac{2}{47}\right)^2 && \text{Mult.} \\
&= -1 \cdot 1 = -1.
\end{aligned}$$

(c) Observe

$$\left(\frac{p}{p+2}\right) = \left(\frac{p+2}{p}\right)$$

since either p or $p+2$ must be $\equiv 1 \pmod 4$.

Also

$$\left(\frac{p+2}{p}\right) = \left(\frac{2}{p}\right) = 1$$

where the last equality holds if and only if $p \equiv \pm 1 \pmod 8$.