MTH6128 Number Theory

Solutions to exam

---

1 Question:

(a) Define the terms

(i) *algebraic number*;

(ii) *algebraic integer*;

(iii) *transcendental number.*

[bookwork]

(b) Which of the following numbers are algebraic integers? Explain, stating explicitly which theorems you use.

(i) $\frac{1+\sqrt{11}}{2}$;

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

(iii) $\frac{3+\sqrt{45}}{6}$.

[similar to coursework]

(c) Let a be an algebraic number, and suppose that $a \neq 0$. Show that $\frac{1}{a}$ is an algebraic number. [unseen]

(d) Give an example of an algebraic integer which is not approximable by rationals up to order 6. Explain why the example you gave has the desired properties. [unseen]

Solution:

(a) (i) $\alpha \in \mathbb{C}$ is an algebraic number if there exists a non-zero polynomial $f(x)$ with rational coefficients such that $f(\alpha) = 0$.

(ii) $\alpha \in \mathbb{C}$ is an algebraic integer if there exists a monic polynomial $f(x)$ with integer coefficients such that $f(\alpha) = 0$.

(iii) $\alpha \in \mathbb{C}$ is a transcendental number if α is not an algebraic number.

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

Theorem: $\alpha \in \mathbb{C}$ 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.

Theorem: 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) $\frac{1+\sqrt{11}}{2} = \frac{1}{2} + \frac{1}{2}\sqrt{11}$. So in this case, $u = \frac{1}{2}$, $v = \frac{1}{2}$ and $d = 11$. As $u \notin \mathbb{Z}$ and $d = 11 \not\equiv 1 \pmod 4$, we conclude that $\frac{1+\sqrt{11}}{2}$ is not an algebraic integer.

(ii) $\frac{2}{3+\sqrt{7}} = \frac{2(3-\sqrt{7})}{(3+\sqrt{7})(3-\sqrt{7})} = \frac{6-2\sqrt{7}}{2} = 3 - \sqrt{7}$. So in this case, $u = 3$ and $v = -1$. We have $u \in \mathbb{Z}$ and $v \in \mathbb{Z}$, so $\frac{2}{3+\sqrt{7}}$ is an algebraic integer.

(iii) $\frac{3+\sqrt{45}}{6} = \frac{3(1+\sqrt{5})}{6} = \frac{1+\sqrt{5}}{2} = \frac{1}{2} + \frac{1}{2}\sqrt{5}$. So in this case, $u = \frac{1}{2}$, $v = \frac{1}{2}$ and $d = 5$. As $u - \frac{1}{2} = 0 \in \mathbb{Z}$, $v - \frac{1}{2} = 0 \in \mathbb{Z}$ and $d = 5 \equiv 1 \pmod 4$, we conclude that $\frac{3+\sqrt{45}}{6}$ is an algebraic integer.

Remark: The long explanation in (b) is only included for the convenience of the checker. Students are not required to give this explanation for full marks; it is enough to cite the relevant results from the lectures.

(c) If α is an algebraic number, then there are $a_n, a_{n-1}, \ldots, a_1, a_0 \in \mathbb{Q}$, at least one of which is non-zero, such that $a_n\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0$. As $\alpha \neq 0$, we may divide by α^n to obtain $a_0(\frac{1}{\alpha})^n + a_1(\frac{1}{\alpha})^{n-1} + \ldots + a_{n-1}\frac{1}{\alpha} + a_n = 0$. This shows that $\frac{1}{\alpha}$ is the root of a non-zero polynomial with rational coefficients, hence an algebraic number.

(d) We had a theorem in the lectures saying that a root of a polynomial f is not approximable by rationals to order $\deg(f) + 1$. Therefore, $\sqrt[5]{2}$ is not approximable by rationals to order 6 since it is the root of $f(x) = x^5 - 2$.

2 Question:

(a) Calculate the value of the infinite continued fraction $[3; 4, \overline{2, 1}]$. [similar to coursework]

(b) You are given that

$$[10; \overline{1, 1, 1, 2, 2, 1, 1, 1, 20}]$$

is the continued fraction for $\sqrt{113}$. Using this, find positive integers x and y such that $x^2 + y^2 = 113$. [similar to coursework]

(c) You are given that

$$[9; \overline{1, 2, 1, 18}]$$

is the continued fraction for $\sqrt{95}$. Using this, find all the integer solutions of the equation $x^2 - 95y^2 = \pm 1$. [similar to coursework]

Solution:

(a) Let y be the value of $[\overline{2; 1}]$. Then $y = [2; 1, y] = 2 + \frac{1}{1+\frac{1}{y}}$. So

$$y - 2 = \frac{y}{y+1}.$$

Thus

$$\begin{aligned} & y^2 - y - 2 = y \\ \Leftrightarrow\quad & y^2 - 2y - 2 = 0 \\ \Leftrightarrow\quad & y = 1 + \sqrt{3} \text{ or } y = 1 - \sqrt{3}. \end{aligned}$$

As $y > 2$, we must have $y = 1 + \sqrt{3}$.

Now let x be the value of $[3; 4, \overline{2, 1}]$. Then $x = 3 + \frac{1}{4+\frac{1}{y}}$, and thus

$$x = 3 + \frac{1}{4 + \frac{1}{y}} = 3 + \frac{1}{4 + \frac{1}{1+\sqrt{3}}} = 3 + \frac{1}{4 + \frac{\sqrt{3}-1}{2}} = 3 + \frac{2}{7 + \sqrt{3}}$$
$$= 3 + \frac{2(7 - \sqrt{3})}{46} = 3 + \frac{7 - \sqrt{3}}{23} = \frac{76 - \sqrt{3}}{23}.$$

Remark: 4 points for calculating y correctly, 2 points for determining x correctly.

(b) As $p = 113$ is a prime with $p \equiv 1 \pmod 4$, we know from lectures that

$$\sqrt{p} = [a_0; \overline{a_1, \ldots, a_m, a_m, \ldots, a_1, 2a_0}]$$

for some $m \geq 0$ and positive integers $a_0, \ldots, a_m$. Let x_i be the real numbers appearing in the algorithm for finding the continued fraction of $\sqrt{p}$, i.e., $x_0 = \sqrt{p}$ and $a_i = \lfloor x_i \rfloor$, $x_{i+1} = \frac{1}{x_i - a_i}$. Then there are unique integers P_{m+1} and Q_{m+1} with $x_{m+1} = \frac{P_{m+1}+\sqrt{p}}{Q_{m+1}}$. Then $x = P_{m+1}$ and $y = Q_{m+1}$ satisfy $x^2 + y^2 = p$.

In this case, $m = 4$, so we have to find x_5 from the continued fraction algorithm. We run the algorithm from the lectures: Starting with $x_0 = \sqrt{113}$, we get

$$\begin{aligned}
a_0 &= \lfloor x_0 \rfloor = 10,\ x_1 = \frac{1}{x_0 - a_0} = \frac{10 + \sqrt{113}}{13} \\
a_1 &= \lfloor x_1 \rfloor = 1,\ x_2 = \frac{1}{x_1 - a_1} = \frac{3 + \sqrt{113}}{8} \\
a_2 &= \lfloor x_2 \rfloor = 1,\ x_3 = \frac{1}{x_2 - a_2} = \frac{5 + \sqrt{113}}{11} \\
a_3 &= \lfloor x_3 \rfloor = 1,\ x_4 = \frac{1}{x_3 - a_3} = \frac{6 + \sqrt{113}}{7} \\
a_4 &= \lfloor 4_3 \rfloor = 2,\ x_5 = \frac{1}{x_4 - a_4} = \frac{8 + \sqrt{113}}{7}.
\end{aligned}$$

So $P_5 = 8$, $Q_5 = 7$, and indeed, $8^2 + 7^2 = 64 + 49 = 113$.

Remark: A detailed explanation of the procedure is not required, but the strategy should become clear. 2 points for the correct strategy, 4 points for the computation.

(c) Assume that we are given a positive integer n which is not a square, and that the continued fraction for $\sqrt{n}$ is given by $[a_0; \overline{a_1, \ldots, a_N}]$. Let $x_1 = [a_0, \ldots, a_{N-1}]$, $y_1 = [a_1, \ldots, a_{N-1}]$ so that x_1/y_1 is the $(N-1)$-th convergent of $\sqrt{n}$. For every positive integer m, define integers x_m and y_m by setting $x_m + y_m\sqrt{n} = (x_1 + y_1\sqrt{n})^m$. We know that $x_1^2 - ny_1^2 = (-1)^N$, so there are two cases:

If $x_1^2 - ny_1^2 = 1$, then there exists no solution of the equation $x^2 - ny^2 = -1$. Moreover, every integer solution x, y of $x^2 - ny^2 = 1$ is given by $x = x_m, y = y_m$ or $x = x_m, y = -y_m$ or $x = -x_m, y = y_m$ or $x = -x_m, y = -y_m$ for some positive integer m.

If $x_1^2 - ny_1^2 = -1$, then every integer solution x, y of $x^2 - ny^2 = 1$ is given by $x = x_m, y = y_m$ or $x = x_m, y = -y_m$ or $x = -x_m, y = y_m$ or $x = -x_m, y = -y_m$ for some even integer $m \geq 2$, and every integer solution x, y of $x^2 - ny^2 = -1$ is given by $x = x_m, y = y_m$ or $x = x_m, y = -y_m$ or $x = -x_m, y = y_m$ or $x = -x_m, y = -y_m$ for some odd integer $m \geq 1$.

We may now apply this general procedure: $n = 95$ is not a square, so we can use the procedure described above. The period of the continued fraction of $\sqrt{95}$ is $N = 4$. We compute $x_1 = [9, 1, 2, 1]$ and $y_1 = [1, 2, 1]$:

$$\begin{aligned} [1] &= 1 \\ [2, 1] &= 3 \\ [1, 2, 1] &= 1 \cdot 3 + 1 = 4 \\ [9, 1, 2, 1] &= 9 \cdot 4 + 3 = 39. \end{aligned}$$

So $x_1 = 39$, $y_1 = 4$. We have $x_1^2 - ny_1^2 = 39^2 - 95 \cdot 4^2 = (-1)^4 = 1$. Moreover, let x_m and y_m be given by $x_m + y_m\sqrt{95} = (39 + 4\sqrt{95})^m$, for positive integers m. Then every integer solution x, y of $x^2 - 95y^2 = 1$ is given, up to signs, by $x = x_m, y = y_m$ for some integer $m \geq 1$, and there is no integer solution x, y of $x^2 - 95y^2 = -1$.

Remark: 4 points for the explanation, 4 points for the computation.

Remark: The long explanations in (b) and (c) are only included for the convenience of the checker. Students are not required to give these explanations for full marks; it is enough to cite the relevant results from the lectures.

3 Question:

(a) Let p be a prime. What is a *primitive root* (mod p)? What is the *order* (mod p) of an integer x with $1 \leq x \leq p - 1$? [bookwork]

(b) Find a primitive root (mod 13). [similar to coursework]

(c) What are the possible orders (mod 13) of an integer x with $1 \leq x \leq 12$? For each possible order, find a natural number x with $1 \leq x \leq 12$ which has exactly that order (mod 13). [unseen]

(d) Let p be a prime and g a primitive root (mod p). Show that for every integer x with $1 \leq x \leq p-1$, there is a natural number i with $x \equiv g^i \pmod{p}$. [unseen]

Solution:

(a) A primitive root (mod p) is an integer g which has order $p-1$ mod p, i.e., $g^k \not\equiv 1\,(mod\,p)$ for all $1 \leq k \leq p-2$. The order (mod p) of an integer x with $1 \leq x \leq p-1$ is the smallest integer $i > 0$ such that $x^i \equiv 1\,(mod\,p)$.

(b) We have to find an element with order 12. We compute modulo 13: $2^2 = 4$, $2^3 = 8$, $2^4 \equiv 3$, $2^5 \equiv 6$, $2^6 \equiv 12$. As the order of 2 has to divide 12, this computation shows that 2 is a primitive root.

(c) The possible orders (mod 13) are precisely the divisors of 12, i.e., 1, 2, 3, 4, 6 and 12. In general, we know that if g is a primitive root (mod p), then the order of g^i (mod p) is given by $\frac{12}{\gcd(i,12)}$. In our case, we can take $g = 2$. Then 2^{12} (which is congruent to 1 modulo 13) has order 1, 2^6 has order 2, 2^4 has order 3, 2^3 has order 4, 2^2 has order 6 and 2 has order 12.

(d) Assume the contrary, i.e., there exists x with $1 \leq x \leq p-1$ such that $x \not\equiv g^i \pmod{p}$ for all i. As $g^i \pmod{p}$ only depends on $i \pmod{p-1}$, we can have at most $p-2$ elements in $\{g^i \pmod{p} : 1 \leq i \leq p-1\}$. Thus there must exist two distinct integers i and j with $1 \leq i, j \leq p-1$ such that $g^i \equiv g^j \pmod{p}$. Assuming that $i < j$, we conclude that $g^{j-i} \equiv 1 \pmod{p}$. But this is a contradiction since the order of g is $p-1$, and $0 < j-i < p-1$.

4 Question:

(a) Let p be an odd prime, and let a be an integer. Define the *Legendre symbol* $\left(\frac{a}{p}\right)$. [bookwork]

(b) Calculate the value of $\left(\frac{21}{67}\right)$. You should state clearly any rules for computing Legendre symbols that you use, but are not required to prove them. [similar to coursework]

(c) Let p be an odd prime. Show that we have $\left(\frac{5}{p}\right) = -1$ if and only if $p \equiv 2 \pmod 5$ or $p \equiv 3 \pmod 5$. [unseen]

(d) Show that there are infinitely many primes congruent to 1 mod 4. [seen in lectures]

Solution:

(a)

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

(b)

$$\left(\frac{21}{67}\right) \overset{R1}{=} \left(\frac{3}{67}\right)\left(\frac{7}{67}\right) \overset{R4}{=} (-1)\left(\frac{67}{3}\right)(-1)\left(\frac{67}{7}\right) \overset{R0}{=} \left(\frac{1}{3}\right)\left(\frac{4}{7}\right) = +1.$$

(c) We have

$$\left(\frac{5}{p}\right) \overset{R4}{=} \left(\frac{p}{5}\right),$$

and as $1^2 = 1$, $2^2 = 4$, $3^2 = 9 \equiv 4 \pmod 5$, $4^2 = 16 \equiv 1 \pmod 5$, we have that

$$\left(\frac{p}{5}\right) = -1$$

if and only if $p \equiv 2 \pmod 5$ or $p \equiv 3 \pmod 5$.

(d) We argue by contradiction. Suppose that $p_1, \ldots, p_r$ were all the primes congruent to $1 \pmod 4$. Now let

$$x = 2p_1p_2 \cdots p_r, \qquad N = x^2 + 1.$$

Let q be a prime divisor of N. Then q is odd. We have

$$x^2 \equiv -1 \pmod q,$$

so -1 is a quadratic residue mod q. By R2, $q \equiv 1 \pmod 4$. Hence by assumption, q must be one of the primes $p_1, \ldots, p_r$. But this is a contradiction, since N leaves remainder 1 when divided by each of these primes.

5 Question:

(a) What is a *quadratic form* over the integers? [bookwork]

(b) In each of the following cases, state whether the quadratic form is positive definite, negative definite, indefinite, or degenerate:

(i) $7x^2 + 3xy + 4y^2$;

(ii) $5x^2 + 4xy - 3y^2$.

[similar to coursework]

(c) Find a reduced positive definite quadratic form which is equivalent to

$$5x^2 + 2xy + y^2.$$

[similar to coursework]

(d) Show that equivalent quadratic forms have the same discriminant. [seen in lectures]

(e) Give examples of two positive definite quadratic forms with the same discriminant, which are not equivalent. Explain why the examples you gave have the desired properties. [unseen]

Solution:

(a) A quadratic form over the integers is a function $f(x, y) = ax^2 + bxy + cy^2$ with $a, b, c \in \mathbb{Z}$.

(b) (i) The discriminant is $3^2 - 4 \cdot 7 \cdot 4 = 9 - 112 = -103$, hence negative. Moreover, the coefficient in front of x^2 is positive. Hence this quadratic form is positive definite.

(ii) The discriminant is $4^2 - 4 \cdot 5 \cdot (-3) = 16 + 60 = 76$, hence positive. Thus the quadratic form is indefinite.

(c) We run the algorithm from the lectures:

The coefficients of the given quadratic form are $a_0 = 5$, $b_0 = 2$ and $a_1 = 1$. We want to find q_1 and b_1 with $2 = 2q_1 - b_1$ and $-1 < b_1 \leq 1$. The solution is $q_1 = 1$, $b_1 = 0$, and $f_1(x, y) = x^2 + a_2 y^2$, where $a_2 = 5 - 2 \cdot 1 + 1 = 4$, that is, $f_1(x, y) = x^2 + 4y^2$, which is reduced.

(d) Let f and g be equivalent quadratic forms. Then for their matrices M and N, we must be able to find a unimodular matrix P with integer coefficients such that $N = P^\top M P$. Therefore, the discriminant of g is given by $-\det(N)$, hence by $-\det(P^\top M P) = -\det(P^\top)\det(M)\det(P) = -\det(P)\det(M)\det(P) = -\det(M)$, which is the discriminant of f.

(e) Consider the quadratic forms $f(x, y) = x^2 + 3y^2$ and $g(x, y) = 2x^2 + 2xy + 2y^2$. Their discriminants are both -12. As their coefficients in front of x^2 are positive, they are both positive definite. However, they are not equivalent: f represents the integer 1 as $f(1, 0) = 1$. However, $g(x, y) = x^2 + (x + y)^2 + y^2$ is always strictly bigger than 1, as $g(x, y) = 1$ would imply that two out of the three terms x, $x + y$ and y would have to vanish, but then, the remaining term would also have to vanish, forcing $x = y = 0$.