MTH6128 **Number Theory**

Solutions to 2020 May exam

---

1 Question:

(a) Define the terms **algebraic integer** and **quadratic integer**. State the Fundamental Theorem of Arithmetic. [bookwork]

(b) Determine which of the following numbers are quadratic integers. Explicitly state any results from the lectures that you use. [similar to coursework/examples]

(i) $\dfrac{2+\sqrt{52}}{4}$;

(ii) $\dfrac{\sqrt{43}}{2} - \dfrac{7}{2}$.

(c) Show that $\sqrt{3+\sqrt{11}}$ is an algebraic integer. [similar to coursework]

(d) Find all integer solutions to the equation [similar to coursework/examples]

$$17x \equiv 4 \pmod{71}.$$

Solution:

(a) We had the following definitions from the lectures

Definition Let α be a complex number. Then:

- α is an *algebraic number* if there is a non-zero polynomial $f(x)$ with rational coefficients such that $f(\alpha) = 0$;
- α is a *transcendental number* if α is not an algebraic number. Moreover,
- α is an *algebraic integer* if there is a non-zero *monic* polynomial $f(x)$ with *integer* coefficients such that $f(\alpha) = 0$. (2 marks)

Definition An algebraic number is a quadratic number if its minimal polynomial is of degree 2.

An algebraic number is a quadratic integer if its minimal polynomial is of degree 2 and has integer coefficients. (2 marks)

Remark. The extra definitions are included for the convenience of the checker.

(The Fundamental Theorem of Arithmetic) Any natural number greater than 1 can be written as a product of prime numbers, and this product expression is unique apart from re-ordering the factors. (2 marks)

(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) $\frac{2+\sqrt{52}}{4} = \frac{1}{2} + \frac{1}{2}\sqrt{13}$. So in this case, $u = \frac{1}{2}$, $v = \frac{1}{2}$ and $d = 13$. As $u - \frac{1}{2}, v - \frac{1}{2} \in \mathbb{Z}$ and $d = 13 \equiv 1 \pmod{4}$, we conclude that $\frac{2+\sqrt{52}}{4}$ is a quadratic integer (2 marks).

(ii) $\frac{\sqrt{43}}{2} - \frac{7}{2}$. So in this case, $u = -\frac{7}{2} \notin \mathbb{Z}$ and $d = 43 \not\equiv 1 (\text{mod} 4)$. We conclude that $\frac{\sqrt{43}}{2} - \frac{7}{2}$ is not a quadratic integer (2 marks).

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. It's also possible to just find the minimal polynomials and this would receive full marks.

(c) Let $\alpha = \sqrt{3 + \sqrt{11}}$. Then

$$\begin{aligned}
\alpha^2 &= 3+\sqrt{11} \\
(\alpha^2-3) &= \sqrt{11} \\
(\alpha^2-3)^2 &= 11 \\
\alpha^4-6\alpha^2+9 &= 11 \\
\alpha^4-6\alpha^2-2 &= 0.
\end{aligned}$$

(3 marks) Hence α is a root of $f(x) = x^4 - 6x^2 - 2$ (1 mark). Since $f(x)$ is a monic polynomial with integer coefficients, α is an algebraic integer (1 mark).

(d) Apply the extended Euclidean algorithm to get that

$$\begin{aligned}
71 &= 17\cdot 4+3 \\
17 &= 3\cdot 5+2 \\
3 &= 2\cdot 1+1
\end{aligned}$$

so that

$$\begin{aligned}
1 &= 3-2 \\
&= 3-(17-3\cdot 5) = 6\cdot 3-17 \\
&= 6(71-17\cdot 4)-17 = 6\cdot 71-25\cdot 17.
\end{aligned}$$

(3 marks). Hence $-25\cdot 17\equiv 1 \pmod{71}$ (1 mark). So that

$$x\equiv -100\equiv 42 \pmod{71}$$

(1 mark).

2 Question:

(a) Use the Euclidean algorithm to find a continued fraction expansion of $\dfrac{1723}{505}$. [similar to coursework/examples]

(b) Let $a_0, a_1, \ldots, a_n$ be positive integers. Let $c_k = p_k/q_k$ be the kth convergent of the continued fraction $[a_0; a_1, \ldots, a_n]$. [similar to coursework/examples]

(i) Prove for each $1\le k\le n$ that

$$\frac{p_k}{p_{k-1}} = a_k + \frac{p_{k-1}}{p_{k-2}}.$$

(ii) Use part (i) to prove for each $1\le k\le n$ that

$$\frac{p_k}{p_{k-1}} = [a_k; a_{k-1}, \ldots, a_1, a_0].$$

Solution:

(a) We apply the Euclidean algorithm and get

$$\begin{aligned} 1723 &= 505 \cdot 3 + 208 \\ 505 &= 208 \cdot 2 + 89 \\ 208 &= 89 \cdot 2 + 30 \\ 89 &= 30 \cdot 2 + 29 \\ 30 &= 29 \cdot 1 + 1 \\ 29 &= 1 \cdot 29 + 0 \end{aligned}$$

So we get that

$$\frac{1723}{505} = [3; 2, 2, 2, 1, 29]$$

(b) Given real numbers $a_0, a_1, \ldots, a_n$, we defined the numbers p_k, q_k in the lectures as follows

$$\begin{aligned} p_0 &= 1, p_0 = a_0 \\ q_{-1} &= 0, q_0 = 1 \end{aligned}$$

and for $1 \leq k \leq n$

$$p_k = a_k p_{k-1} + p_{k-2}, q_k = a_k q_{k-1} + q_{k-2}.$$

(i) Using the definition of p_k above we get that for each $1 \leq k \leq n$

$$\frac{p_k}{p_{k-1}} = \frac{a_k p_{k-1} + p_{k-2}}{p_{k-1}} = a_k + \frac{p_{k-2}}{p_{k-1}}.$$

(2 marks).

(ii) The proof is by induction on k. The base case is $k = 1$ which is

$$\frac{p_1}{p_0} = \frac{a_1 a_0 + 1}{a_0} = a_1 + \frac{1}{a_0} = [a_1; a_0].$$

(2 marks) To complete the induction step we use part (i) and the induction hypothesis to see that

$$\frac{p_{k+1}}{p_k} = a_{k+1} + \frac{p_{k-1}}{p_{k-2}} = a_{k+1} + \frac{1}{[a_k; a_{k-1}, \ldots, a_0]} = [a_{k+1}; a_k, \ldots, a_0]$$

(3 marks).

3 Question:

(a) Find the continued fraction expansion of $\dfrac{1+\sqrt{37}}{2}$.[similar to coursework]

(b) You are given that

$$\sqrt{53} = [7; \overline{3, 1, 1, 3, 14}].$$

Find all solutions in positive integers x, y to the following equation

$$x^2 - 53y^2 = -1.$$

Explain why you have found ALL solutions. [similar to coursework]

Solution:

(a) We run the algorithm from the lectures: Starting with $x_0 = \frac{1+\sqrt{37}}{2}$, we get

$$\begin{aligned}
a_0 = \lfloor x_0 \rfloor = 3,\ x_1 &= \frac{1}{x_0 - a_0} = \frac{5+\sqrt{37}}{6} \\
a_1 = \lfloor x_1 \rfloor = 1,\ x_2 &= \frac{1}{x_1 - a_1} = \frac{1+\sqrt{37}}{6} \\
a_2 = \lfloor x_2 \rfloor = 1,\ x_3 &= \frac{1}{x_2 - a_2} = \frac{5+\sqrt{37}}{2} \\
a_3 = \lfloor x_3 \rfloor = 5,\ x_4 &= \frac{1}{x_3 - a_3} = \frac{5+\sqrt{37}}{6} = x_1.
\end{aligned}$$

So the continued fraction for $\frac{1+\sqrt{37}}{2}$ is $[3; \overline{1, 1, 5}]$.

Remark: 5 points for correct algorithm, 1 points for reading off the continued fraction expansion correctly.

(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 the continued fraction 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 to the Pell's equations will be (p_4, q_4) (1 mark). Computing we get that

$$\begin{aligned}
c_0 &= [7] = \frac{7}{1} \\
c_1 &= [7; 3] = \frac{22}{3} \\
c_2 &= \frac{p_3}{q_3} = \frac{1 \cdot 22 + 7}{1 \cdot 3 + 1} = \frac{29}{4} \\
c_3 &= \frac{p_3}{q_3} = \frac{1 \cdot 29 + 22}{1 \cdot 4 + 3} = \frac{51}{7} \\
c_4 &= \frac{p_4}{q_4} = \frac{3 \cdot 51 + 29}{3 \cdot 7 + 4} = \frac{182}{25}
\end{aligned}$$

So the fundamental solution is $(182, 25)$ (3 marks).

In the lectures we proved that if (x_1, y_1) is the fundamental solution 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, $k = 1, 2, \dots$ defined by

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

We also proved that if h is the period of the continued fraction then

$$x_k^2 - dy_k^2 = (-1)^{hk}.$$

so since h is odd the solutions to $x^2 - 53y^2 = -1$ are given by x_k, y_k defined by the formula

$$x_k + y_k\sqrt{53} = (182 + 25\sqrt{53})^k \qquad k \text{ is odd}$$

(3 marks). As we proved in the lectures all the solutions to both Pell's equations are generated by the fundamental solution in this way so only the numbers x_{2k+1}, y_{2k+1}, $k = 0, 1, \dots$ are solutions to the negative Pell equation. (2 marks).

4 Question:

(a) Given a positive integer n define the **order of** x (mod n). State Euler's Theorem. [bookwork]

(b) Find the last two digits of 3^{40845}. Explain your working. [similar to examples/coursework]

(c) Let m and n be positive integers. Prove that $\phi(m)\phi(n) \leq \phi(mn)$. [unseen]

(d) Find a primitive root (mod 17). Explain why the integer you gave has the desired properties. [similar to examples/coursework]

Solution:

(a) Let n be a positive integer. The *order* of x (mod n) is the smallest positive integer d such that $x^d \equiv 1 \pmod{n}$. (2 marks)

(Euler's Theorem) Let n be a positive integer, and x an integer such that $\gcd(x, n) = 1$. Then $x^{\phi(n)} \equiv 1 \pmod{n}$. (2 marks)

(b) We need to compute $3^{40845} (\mathrm{mod}\, 100)$ (1 mark). Since $\phi(100) = \phi(2^2) \cdot \phi(5^2) = (4 - 2)(25 - 5) = 40$ (2 marks) we get by Euler's theorem

$$3^{40} \equiv 1 (\mathrm{mod}\, 100).$$

Also $40845 = 40 \cdot 1021 + 5$ so

$$3^{40845} = (3^{40})^{1021} \cdot 3^5 \equiv 1 \cdot 3^5 (\mathrm{mod}\, 100)$$

Since $3^5 = 243$ we get that the last two digits of 3^{40845} are $4, 3$ (2 marks).

(c) In the lectures we proved (2 marks)

$$\phi(m) = m \prod_{p|m} \left(1 - \frac{1}{p}\right).$$

Observe that

$$\prod_{p|m} \left(1 - \frac{1}{p}\right) \prod_{p|n} \left(1 - \frac{1}{p}\right) = \prod_{p|mn} \left(1 - \frac{1}{p}\right) \prod_{p|\gcd(m,n)} \left(1 - \frac{1}{p}\right).$$

(2 marks) Since for each p, $1 - 1/p \leq 1$ it follows that

$$\prod_{p|m} \left(1 - \frac{1}{p}\right) \prod_{p|n} \left(1 - \frac{1}{p}\right) \leq \prod_{p|mn} \left(1 - \frac{1}{p}\right)$$

Hence

$$\phi(m)\phi(n) \leq \phi(mn).$$

(1 mark)

(d) Using the primitive root test, to determine if $a \pmod p$ is a primitive root we must check if $a^{(p-1)/d} \equiv 1 \pmod p$ for some (proper) divisor $d|p-1$ (2 marks for the explanation). We will check if 2 is a primitive root. Since $17 - 1 = 16$ has divisors $2, 4, 8$ we need to check $2^2, 2^4, 2^8$ modulo 17.

$$2^4 \equiv 16 \pmod{17}$$

so 2 is not a primitive root since $2^8 \equiv 1 \pmod{17}$. Next try 3,

$$3^4 = 81 \equiv -4(17)$$

So

$$3^8 \equiv 16(17).$$

Hence we can conclude by the primitive root test that 3 is a primitive root $\pmod{17}$ (3 marks for the calculation).

5 Question:

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

(b) Calculate the value of $\left(\frac{99}{101}\right)$. You should clearly state any rules you use for calculating the Legendre symbol. [similar to coursework]

(c) State and prove Euler's Criterion. [bookwork]

Solution:

(a) An integer a is a *quadratic non-residue* (mod p) if there does not exist an integer x with $x^2 \equiv a \pmod p$. (2 marks)

Let p be an odd prime. The *Legendre symbol* $\left(\frac{a}{p}\right)$ is defined by

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

(2 marks)

(Law of Quadratic Reciprocity) For any two distinct odd primes p and q,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} = \begin{cases} -1 & \text{if } p \equiv q \equiv 3 \pmod 4, \\ +1 & \text{otherwise.} \end{cases}$$

(2 marks).

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

$$\begin{aligned} \left(\frac{99}{101}\right) &= \left(\frac{3}{101}\right)^2 \cdot \left(\frac{11}{101}\right) && \text{Multiplicativity (R1)} \\ &= 1 \cdot \left(\frac{101}{11}\right) && \text{Quad. Recip. (R4)} \\ &= \left(\frac{2}{11}\right) && \text{Periodicity (R0)} \\ &= -1 && \text{Rule for 2 (R1)} \end{aligned}$$

(5 marks) in the last step we used that $11 \equiv 3(\text{mod} 8)$, so $\left(\frac{2}{11}\right) = -1$. (1 mark)

(c) (Euler's Criterion) Statement: Let a be an integer not divisible by p. Then

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p.$$

(2 marks)

Proof: Let g be a primitive root of p, and $a \equiv g^i \pmod p$ (2 marks). Consider $z = g^{(p-1)/2}$. We have $z^2 = g^{p-1} \equiv 1 \pmod p$, but z is not congruent to 1 (mod p) since g is a primitive root. Hence, that $g^{(p-1)/2} \equiv -1 \pmod p$ (2 marks).

Therefore, since $g^{p-1} \equiv 1 \pmod p$, we have modulo p:

$$a^{(p-1)/2} \equiv \begin{cases} 1 & \text{if } i \text{ is even,} \\ g^{(p-1)/2} & \text{if } i \text{ is odd.} \end{cases}$$

(2 marks) Since $\left(\frac{a}{p}\right) = (-1)^i$ the result follows.

6 Question:

(a) For each of the equations, determine whether there exists a solution x, y in positive integers. If there is a solution explain why. If no solution exists explain why not. Explicitly state any results from the lectures that you use. [similar to coursework/examples]

   (i) $x^2 + y^2 = 5850$;

   (ii) $x^2 + y^2 = 9450$.

(b) Use Hensel's Lemma to find all integer solutions to the equation [similar to coursework/examples]

$$x^2 \equiv 3 \pmod{11^2}.$$

Explain your working.

Solution:

(a) In the lectures we proved the following result:

The positive integer n is the sum of two squares of integers if and only if the squarefree part of n has no prime factors congruent to 3 (mod 4).

   (i) Factor $5850 = 50 \cdot 117 = 50 \cdot 13 \cdot 9 = 2^2 5^2 3^2 \cdot 13$ (1 mark). Hence it can be written as a sum of two squares since its square free part is $13 \equiv 1 \pmod 4$ (2 marks).

   (ii) Factor $9450 = 10 \cdot 945 = 10 \cdot 5 \cdot 189 = 2 \cdot 5^2 3^2 7 \cdot 3$ Since the square free part of 9450 is $2 \cdot 7 \cdot 3$ and $3 \equiv 3 \bmod 4$ the result above implies that 9450 cannot be written as a sum of two squares.

(b) First we check if 3 is a quadratic residue $\pmod{11}$

$$\left(\frac{3}{11}\right) = -\left(\frac{11}{3}\right) = -\left(\frac{2}{3}\right) = 1.$$

Since 3 is a quadratic residue and $11 \equiv 3 \pmod 4$ we know from the lectures that $3^{(11+1)/4}$ is a solution to

$$x^2 \equiv 3 \pmod{11}.$$

So $3^3 \equiv 5 \pmod{11}$. So all the solutions to the above equation are $x = 5, 6,$ (mod11) (2 marks). (**Remark**: Computing the solution by inspection is fine here)

We need to compute the lift of this solution to a solution $\pmod{11^2}$. Since $f'(x) = 2x$ we know that $f(x_0) \not\equiv 0 \pmod{11^2}$ (with $x_0 = 5, 6$) so we can apply Hensel's Lemma. The unique solution corresponding to $x_0 = 5$ is given by the formula

$$x_1 = x_0 - f(x_0)/f'(x_0)$$

where $1/f'(x_0)$ is the inverse of $f'(x_0) \pmod{11}$ (3 marks). Note $f'(x_0) \equiv 10 \pmod{11}$. By inspection $11 \cdot 1 - 1 \cdot 10 = 1$ so $1/f'(x_0) = -1$ (1 mark)

$$x_1 = 5 - (25 - 3) \cdot (-1) = 27$$

(1 mark) The other solution is $-27 \equiv 94 \pmod{11^2}$ (2 marks).