MTH6128 Number Theory

Solutions to exam

---

1 (a) Define the terms **algebraic number** and **minimal polynomial**. State the **Chinese Remainder Theorem**. [bookwork]

(b) Give an example of an algebraic integer, which is not an integer. Explain why the number you gave has the desired properties. [similar to examples]

(c) Find all integer solutions to the system of congruences [similar to coursework/examples]

$$\begin{aligned} x &\equiv 1 \pmod{7} \\ x &\equiv 2 \pmod{30}. \end{aligned}$$

(d) Determine the minimal polynomial of $\frac{\sqrt{7}}{2} - \frac{9}{2}$. Explain why the polynomial you gave has the desired properties. [similar to coursework/examples]

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 $f(\alpha) = 0$. (2 marks)

(ii) Let α be an algebraic number. The minimal polynomial of α is the non-zero, monic polynomial $f(x)$ of smallest possible degree with rational coefficients such that $f(\alpha) = 0$. (2 marks)

(iii) **The Chinese Remainder Theorem** Let m and n be coprime natural numbers, and let a and b be arbitrary integers. Then there is a solution to the simultaneous congruences

$$\begin{aligned} x &\equiv a \pmod{m}, \\ x &\equiv b \pmod{n}. \end{aligned}$$

Moreover, the solution is unique modulo mn; that is, if x_1 and x_2 are two solutions, then $x_1 \equiv x_2 \pmod{mn}$. (2 marks)

(b) An example is $\sqrt{2}$, which is a root of the monic polynomial $f(x) = x^2 - 2$, which has integer coefficients (2 marks). Note $\sqrt{2}$ is irrational so it's not an integer (1 mark)

(c) Using the Euclidean algorithm we can find multiplicative inverses for 7 (mod 30) and 30 (mod 7) as follows

$$\begin{aligned} 30 &= 7 \cdot 4 + 2 \\ 7 &= 2 \cdot 3 + 1. \end{aligned}$$

So rewriting these equations we get that

$$\begin{aligned} 1 = &\quad 7 - 3 \cdot 2 \\ 1 = &\quad 7 - 3 \cdot (30 - 4 \cdot 7) = 7 \cdot 13 - 3 \cdot 30 \end{aligned}$$

so that

$$\begin{aligned} 7 \cdot 13 &\equiv 1 \bmod 30 \\ 30 \cdot (-3) &\equiv 1 \bmod 7 \end{aligned}$$

(2 marks for the calculation, full marks for guessing the solution with justification).

Hence,

$$x = 1(30)(-3) + 2(13)(7) = 92$$

is the unique solution (mod 210) (3 marks). We can write all solutions as

$$92 + 210n \qquad n \in \mathbb{Z}$$

or equivalently $[92]_{210}$ (1 mark).

(d) Let $\alpha = \frac{\sqrt{7}}{2} - \frac{9}{2}$. Consider

$$\begin{aligned} f(x) = &\quad \left(x - \left(\tfrac{\sqrt{7}}{2} - \tfrac{9}{2}\right)\right)\left(x - \left(\tfrac{-\sqrt{7}}{2} - \tfrac{9}{2}\right)\right) \\ = &\quad x^2 + 9x - 74/4. \end{aligned}$$

(2 marks) Clearly $f(\alpha) = 0$ and f is a monic polynomial (1 mark). We also know that α cannot be the root of a degree one polynomial with rational coefficients since it is irrational, so the degree of f is minimal (2 marks).

2 Question:

(a) Find the value of the continued fraction

$$[4; \overline{1,6}].$$

Your answer should be a number of the form $u + v\sqrt{d}$, where $u, v \in \mathbb{Q}$, $d \in \mathbb{N}$. [similar to coursework/examples]

(b) Let x be an irrational number and n be a positive integer. Let $c_n = p_n/q_n$ be the nth convergent of the continued fraction of x. [unseen]

(i) Prove that

$$\frac{1}{q_n q_{n+1}} = \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| = \left|x - \frac{p_{n+1}}{q_{n+1}}\right| + \left|x - \frac{p_n}{q_n}\right|.$$

State precisely all results from the lectures you use in the proof.

(ii) Prove that $\frac{1}{q_n q_{n+1}} < \frac{1}{2q_n^2} + \frac{1}{2q_{n+1}^2}$.

(iii) Use parts (i) and (ii) to prove

$$\left|x - \frac{p_n}{q_n}\right| < \frac{1}{2q_n^2} \qquad \textit{or} \qquad \left|x - \frac{p_{n+1}}{q_{n+1}}\right| < \frac{1}{2q_{n+1}^2}.$$

Solution:

(a) First we find

$$u = [\overline{1;6}] = 1 + \frac{1}{6 + \frac{1}{u}}.$$

This implies that

$$6u^2 - 6u - 1 = 0.$$

(2 marks) This equation has solutions

$$\frac{3 \pm \sqrt{15}}{6}$$

since $u > 0$ we know that we should take the + solution (1 mark).

We now find

$$[4; \overline{1,6}] = [4; u] = 4 + \frac{1}{u} = 4 + \frac{6}{3 + \sqrt{15}} = 1 + \sqrt{15}.$$

(2 marks)

(b) (i) In the lectures we proved that

$$c_{n+1} - c_n = \frac{(-1)^n}{q_n q_{n+1}}$$

so that

$$\left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| = \frac{1}{q_n q_{n+1}}.$$

(2 mark) Also we proved that the even indexed convergents are an increasing sequence which converges to x, the odd indexed convergents are a decreasing sequence which converges to x and each odd indexed convergent is greater than each even convergent. (1 mark)

So if n is even

$$|c_{n+1} - c_n| = c_{n+1} - c_n = c_{n+1} - x + x - c_n = |x - c_{n+1}| + |x - c_n|$$

(1 mark). Similarly, if n is odd

$$|c_{n+1} - c_n| = c_n - c_{n+1} = c_n - x + x - c_{n+1} = |x - c_{n+1}| + |x - c_n|$$

(1 mark). Combining everything we get

$$\frac{1}{q_n q_{n+1}} = \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| = \left|x - \frac{p_{n+1}}{q_{n+1}}\right| + \left|x - \frac{p_n}{q_n}\right|.$$

(ii) Since for any positive real numbers a, b with $a \neq b$, $(a-b)^2 > 0$ it follows that $2ab < a^2 + b^2$ so $ab < \frac{1}{2}(a^2 + b^2)$ (1 mark), note that $q_n \neq q_{n+1}$ since the sequence q_k strictly increases with k (1 mark)

(iii) For sake of contradiction suppose that

$$|x - \frac{p_n}{q_n}| \geq \frac{1}{2q_n^2} \qquad and \qquad |x - \frac{p_{n+1}}{q_{n+1}}| \geq \frac{1}{2q_{n+1}^2}$$

(1 mark) By (i) and (ii) this implies that

$$\frac{1}{q_n^2} + \frac{1}{2q_{n+1}^2} \leq |x - c_n| + |x - c_{n+1}| \leq \frac{1}{q_n q_{n+1}} < \frac{1}{2q_n^2} + \frac{1}{2q_{n+1}^2}$$

which is a contradiction. (2 marks)

3 Question:

(a) Given that

$$\sqrt{19} = [4; \overline{2, 1, 3, 1, 2, 8}],$$

find the fundamental solution to

$$x^2 - 19y^2 = \pm 1.$$

Use your answer to write down all positive integer solutions to the equation $x^2 - 19y^2 = 1$. Explain why you have found ALL solutions. [Similar to coursework/examples]

(b) Given that $25^2 \equiv -1 \pmod{313}$ use Hermite's algorithm to find integers x, y such that

$$x^2 + y^2 = 313.$$

[Similar to coursework/examples]

Solution:

(a) 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 6 the smallest solution will be (p_5, q_5). Computing we get that

$$\begin{aligned}
c_0 &= [4] = \frac{4}{1} \\
c_1 &= [4; 2] = \frac{9}{2} \\
c_2 &= \frac{p_2}{q_2} = \frac{1 \cdot 9 + 4}{1 \cdot 2 + 1} = \frac{13}{3} \\
c_3 &= \frac{p_3}{q_3} = \frac{3 \cdot 13 + 9}{3 \cdot 3 + 2} = \frac{48}{11} \\
c_4 &= \frac{p_4}{q_4} = \frac{1 \cdot 48 + 13}{1 \cdot 11 + 3} = \frac{61}{14} \\
c_5 &= \frac{p_4}{q_4} = \frac{2 \cdot 61 + 48}{2 \cdot 14 + 11} = \frac{170}{39}
\end{aligned}$$

So the fundamental solution is $(170, 39)$.

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

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

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 even

So the solutions to $x^2 - 19y^2 = 1$ are given by x_k, y_k defined by the formula

$$x_k + y_k\sqrt{19} = (170 + 39\sqrt{19})^k \qquad k = 1, 2, 3, 4, \ldots$$

We proved in the lectures that the fundamental solution generates all the solutions in this way.

Remark The computation of the fundamental solution is worth (3 marks). Writing down all the solutions to both equations $x^2 - 19y^2 = 1$ is worth (1 mark) and (2 marks) for explaining why each k corresponds to a solution. Explaining why these are all the solutions is worth (2 marks).

(b) We run Hermite's algorithm from the lectures. First run the Euclidean algorithm on 313 and 25

$$\begin{aligned} 313 &= 25 \cdot 12 + 13 \\ 25 &= 13 \cdot 1 + 12 \\ 13 &= 12 \cdot 1 + 1 \\ 12 &= 1 \cdot 12 + 0 \end{aligned}$$

so

$$\frac{25}{313} = [0; 12, 1, 1, 12]$$

Applying the algorithm we compute convergents until the denominator is larger than $\sqrt{313}$

$$\begin{aligned} c_0 &= \frac{0}{1} \\ c_1 &= \frac{1}{12} \\ c_2 &= \frac{1}{13} \\ c_3 &= \frac{2}{25} \end{aligned}$$

since $25 > \sqrt{313}$ we stop. The algorithm now outputs

$$x = q_2 = 13, y = (q_2 \cdot 25 - 313 \cdot p_2) = (13 \cdot 25 - 313 \cdot 1) = 12$$

so

$$x^2 + y^2 = 313.$$

Remark The computation of the continued fraction is worth (3 marks). Correctly using the algorithm is worth (1 mark) and the explanation is worth (2 marks). Guessing the answer is worth (0 marks). (Note there is a slightly more efficient algorithm not covered during the lectures, students get full marks for using it).

4 Question:

(a) Define **Euler's ϕ-function**. Define the term **primitive root** (*mod* p), where p is prime. [bookwork]

(b) Find a primitive root (*mod* 29). [similar to coursework/examples]

(c) Find the number of primitive roots (*mod* 29). [similar to coursework/examples]

Solution:

(a) We had the following definitions from the lectures.

(i)

Definition *Euler's totient function*, or *Euler's ϕ-function*, is the function ϕ defined on the positive integers by the rule that $\phi(n)$ is the number of elements $[x]_n$ in $\mathbb{Z}_n$ which satisfy $\gcd(x, n) = 1$. (2 marks)

(ii)

Definition Let p be a prime number. An integer x is said to be a *primitive root* mod p if x has order $p - 1$ (mod p). (2 marks)

(b) 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 $d|p-1$ (3 marks for the explanation). We will check if 3 is a primitive root. Since $29 - 1 = 28$ has divisors $2, 7$ we need to check 3^4 and 3^{14} modulo 7.

$$3^4 = 81 \equiv 23 \pmod{29}$$

so it remains to check 3^{14}. Also, using the above calculation

$$3^8 = (23)^2 \equiv 6^2 \equiv 7 \pmod{29}$$

Hence $3^{14} = 3^8 3^4 9 \equiv 7(-6)9 \equiv 28 \pmod{29}$. Hence 3 is a primitive root (mod 29) (3 marks for the calculation)

(c) There are $\phi(p-1)$ primitive roots $\pmod p$ (1 mark). So the answer is $\phi(28) = 28(6/7)(1/2) = 12$ (2 marks).

5 Question:

(a) Define the term **quadratic residue**. State **Euler's criterion.** [bookwork]

(b) Find all integers between 1 and 53 which are solutions to the following equations. If no solutions exist explain why. [similar to coursework/examples]

(i) $x^2 \equiv 39 \pmod{53}$

(ii) $x^2 \equiv -1 \pmod{53}$

(c) Prove there are infinitely many prime numbers congruent to $1 \pmod 4$. [proved in the lectures]

Solution:

(a) (i)

Definition An integer a is a *quadratic residue* (mod p) if there exists an integer x with $x^2 \equiv a$ (mod p)

(ii)

Euler's criterion Let a be an integer not divisible by p. Then

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

(b) (i) First we check whether 35 is a quadratic residue mod 53 by computing the Legendre symbol.

$$\begin{aligned}
\left(\frac{35}{53}\right) &= \left(\frac{7}{53}\right)\cdot\left(\frac{5}{53}\right) && \text{mult.}\\
&= \left(\frac{53}{5}\right)\left(\frac{53}{7}\right) && \text{Quad. Recip.}\\
&= \left(\frac{3}{5}\right)\left(\frac{4}{7}\right) && \text{Period.}\\
&= -1\cdot 1
\end{aligned}$$

(2 marks). We know that

$$\left(\frac{3}{5}\right) = -1$$

since only $1, 4$ are quadratic residues $\pmod 5$ (by direct computation) (1 mark). Also $\left(\frac{4}{7}\right) = \left(\frac{2}{7}\right)^2 = 1$. (1 marks) for the computation with explanations.

Since 35 is a quadratic non-residue $\pmod{53}$ there are no solutions (2 marks).

(ii) Since $53 \equiv 1 \pmod 4$ we know there will be two solutions (1 mark). To find the solutions we follow the procedure from the lectures. We first need to find a quadratic non-residue $\pmod{53}$, we could take 35, but let's find a number that is more suitable for computations. Notice

$$\left(\frac{2}{53}\right) = -1$$

since $53 \equiv -3 \pmod 8$ (1 mark). So that by Euler's criterion $b = 2^{(p-1)/4}$

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

(explanation not required).

So we have $b = 2^{52/4} = 2^{13}$ (1 mark) is a solution we now compute

$$2^8 = 256 \equiv -9 \pmod{53}$$

and $2^5 = 32 \equiv -21 \pmod{53}$

$$2^{13} = 2^8 2^5 \equiv (-9)(-21) \equiv 30 \pmod{53}$$

(2 marks)

The other solution is $-30 \equiv 23 \pmod{53}$ (1 mark). The answer is $x = 23, 30$.

(c) We argue by contradiction. Suppose that $p_1, \ldots, p_r$ were all the primes congruent to 1 (mod 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.

6 Question:

(a) State **Hensel's Lemma**. [Bookwork]

(b) Find all integer solutions to the following equation

$$x^2 - 5 \equiv 0 \pmod{19^2}.$$

[Similar to coursework/examples]

Solution:

(a) **Hensel's Lemma.** Let $f(X) \in \mathbb{Z}[X]$. Suppose there exists an integer x_0 such that $f(x_0) \equiv 0 \pmod{p^e}$ and $f'(x_0) \not\equiv 0 \pmod{p}$. Then there exists an integer t which is unique $\pmod{p}$ such that $x_0 + tp^e$ is a solution to $f(x) \equiv 0 \pmod{p^{e+1}}$.

(b) First we check if 5 is a quadratic residue $\pmod{19}$ (1 mark)

$$\left(\frac{5}{19}\right) = \left(\frac{19}{5}\right) = \left(\frac{4}{5}\right) = 1.$$

Since it is a quadratic residue and $19 \equiv 3 \pmod{4}$ we know from the lectures that $5^{(19+1)/4}$ is a solution to

$$x^2 \equiv 5 \pmod{19}.$$

So $5^2 \equiv 6 \pmod{19}$ so $5^5 \equiv -2 \cdot 5 \equiv 9 \pmod{19}$. So all the solutions to the above equation are $x = 9, 10,$ (mod19) (2 marks). We need to compute the lift of this solution to a solution $\pmod{19^2}$.

Since $f'(x) = 2x$ we know that $f(x_0) \not\equiv 0 \pmod{19^2}$ so we can apply Hensel's lemma. The unique solution corresponding to $x_0 = 9$ is given by the formula

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

where $1/f'(x_0)$ is the inverse of $f'(x_0) \pmod{19}$. By inspection $19 \cdot 1 - 18 \cdot 1 = 1$ so $1/f'(x_0) = -1$

$$x_1 = 9 - (81 - 5) \cdot (-1) = 9 + 76 = 85$$

(3 marks) The other solution is $-85 \pmod{19^2}$ (1 mark).