EXAMINATION PAPER

Examination Session: May/June	**Year:** 2022	**Exam Code:** MATH41620-WE01

Title: Number Theory V

Time:	3 hours	
Additional Material provided:		
Materials Permitted:		
Calculators Permitted:	Yes	Models Permitted: Casio FX83 series or FX85 series.

Instructions to Candidates:	Answer all questions. Section A is worth 20%, Section B is worth 60%, and Section C is worth 20%. Within Sections A and B, all questions carry equal marks. Students must use the mathematics specific answer book.

Revision:	

ED01/2022

SECTION A

Q1 Let K be a number field and write $R = \mathcal{O}_K$ for its ring of integers.

(a) Let I be a non-zero proper ideal in R. Show that $I \cap \mathbb{Z}$ is a non-zero proper ideal of $\mathbb{Z}$.

(b) Show that there exist infinitely many prime ideals in R. (Here you can use without proof the fact that there exist infinitely many primes in $\mathbb{Z}$).

Q2 (a) Find the fundamental unit of $\mathbb{Q}(\sqrt{10})$.

(b) Find two distinct solutions $(x, y) \in \mathbb{N} \times \mathbb{N}$, $x, y > 1$, to the equation

$$x^2 - 10y^2 = 1.$$

SECTION B

Q3 Let p be an odd prime and set $\zeta := e^{\frac{2\pi i}{p}} \in \mathbb{C}$. We set $K := \mathbb{Q}(\zeta)$.

(a) Show that the minimal polynomial of ζ over $\mathbb{Q}$ is $\Phi(x) = x^{p-1}+x^{p-2}+\ldots+x+1$.

(b) Show that $p = u(1-\zeta)^{p-1}$ for some $u \in \mathcal{O}_K^\times$.

(c) Show that $1-\zeta$ is an irreducible element in $\mathcal{O}_K$.

(d) Is there a field extension F of K with $[F : K]$ finite, such that the element $1-\zeta$ is not an irreducible element as an element in $\mathcal{O}_F$? Justify your answer.

Q4 (a) Let p and q be two distinct odd primes. Given that there exists at least one solution, find how many solutions there are to the equation

$$a^2 + 2b^2 = p^7 q^9,$$

with a and b in $\mathbb{Z}$. Here you may use without proof the fact that the ring $\mathbb{Z}[\sqrt{-2}]$ is a U.F.D.

(b) Let $K = \mathbb{Q}(\sqrt{-29})$ and write $R = \mathcal{O}_K$ for its ring of integers. Show that there exist non-principal ideals of norm 33 in R. Find one of them by giving generators for it.

Q5 (a) Let $K = \mathbb{Q}(\theta)$, where $\theta^3 - \theta - 3 = 0$. Compute the discriminant of $\mathbb{Z}[\theta]$.

(b) Let $K = \mathbb{Q}(\sqrt{7})$ and $R = \mathcal{O}_K = \mathbb{Z}[\sqrt{7}]$. Find a generating basis and compute the discriminant of the ideal

$$I = (2 + \sqrt{7})_R.$$

Q6 Let $K = \mathbb{Q}(\sqrt{-91})$ and $R := \mathcal{O}_{-91} = \mathbb{Z}[\frac{1+\sqrt{-91}}{2}]$.

(a) Find the class number of K. You may use the Minkowski bound, given by $B_K = \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}\sqrt{|\Delta_K|}$.

(b) Let $\alpha = x + \sqrt{-91} \in R$. Find three prime ideals P_1, P_2, P_3 of R such that any prime ideal of R that divides both (α) and $(\overline{\alpha})$ must be one of the three prime ideals P_1, P_2 or P_3.

(c) Find all the solutions $(x, y) \in \mathbb{Z}^2$ (if any) to the equation

$$x^2 + 91 = y^3.$$

(Hint: Use the previous parts.)

SECTION C

Q7 Let p be a prime integer. In the following we obey the convention that for a p-adic expansion $\sum_{n=m}^{\infty} a_n p^n \in \mathbb{Q}_p$ with $m \in \mathbb{Z}$, we select $a_n \in \{0, 1 \ldots, p-1\}$.

(a) Let $x = \sum_{i=m}^{\infty} x_i p^i \in \mathbb{Q}_p$ for some $m \in \mathbb{Z}$ and define $[x] := \sum_{i \geq 0} x_i p^i$ and $\langle x \rangle := \sum_{i<0} x_i p^i$.

(i) Show that $\langle x \rangle \in \mathbb{Z}[1/p]$. Show further that $0 \leq \langle x \rangle < 1$, when embedding $\mathbb{Z}[1/p]$ into the real numbers in the natural way.

(ii) We define the map $\tau : \mathbb{Q}_p \to \mathbb{C}^\times$, by $\tau(x) := \exp(2\pi i \langle x \rangle)$. Show that τ is a group homomorphism.

(iii) Define $\mu_{p^\infty} := \bigcup_{k \geq 1} \mu_{p^k}$ where for a $k \in \mathbb{N}$ we set

$$\mu_{p^k} := \{\zeta \in \mathbb{C}^\times \ : \ \zeta^{p^k} = 1\}.$$

Show that there exists a group isomorphism

$$\mathbb{Q}_p / \mathbb{Z}_p \cong \mu_{p^\infty}.$$

(b) (i) Let p and q be two distinct prime numbers. Show that there exists an $a \in \mathbb{Z}$ such that $\sqrt{a} \in \mathbb{Q}_p$ but $\sqrt{a} \notin \mathbb{Q}_q$.

(ii) With notation as above, show that there is no field isomorphism $\varphi : \mathbb{Q}_p \to \mathbb{Q}_q$.