Imperial College
London

MATH97037 MATH70042

BSc, MSci and MSc EXAMINATIONS (MATHEMATICS)
May-June 2022

This paper is also taken for the relevant examination for the
Associateship of the Royal College of Science

Algebraic Number Theory

Date: 07 June 2022

Time: 09:00 – 11:30 (BST)

Time Allowed: 2:30 hours

Upload Time Allowed: 30 minutes

This paper has 5 Questions.

Candidates should start their solutions to each question on a new sheet of paper.

Each sheet of paper should have your CID, Question Number and Page Number on the top.

Only use 1 side of the paper.

Allow margins for marking.

Any required additional material(s) will be provided.

Credit will be given for all questions attempted.

Each question carries equal weight.

SUBMIT YOUR ANSWERS AS ONE PDF TO THE RELEVANT DROPBOX ON BLACKBOARD WITH COMPLETED COVERSHEETS WITH YOUR CID NUMBER, QUESTION NUMBERS ANSWERED AND PAGE NUMBERS PER QUESTION.

You can use, without proof, any results from the course provided you state them correctly and clearly.

1. (a) Find every reduced integral quadratic form of discriminant -59. You need to justify your answer. (11 marks)

   (b) Compute the class group $Cl(\mathcal{O}_{-59})$. What is the relation with the reduced quadratic forms in part (a)? (3 marks)

   (c) For every element $a \in Cl(\mathcal{O}_{-59})$ find a non-zero ideal $\mathfrak{a} \lhd \mathcal{O}_{-59}$ whose class is a. Justify your answer. (6 marks)

   (Total: 20 marks)

2. Let d be a fundamental discriminant and let $0 \neq \alpha \in \mathcal{O}_d$ be an element. Let

   $$N(\alpha) = p_1 p_2 \cdots p_n$$

   be the prime factorisation of its norm.

   (a) Assume that the norm $N(\alpha)$ is square-free. Prove that

   $$(p_1, \alpha)(p_2, \alpha) \cdots (p_n, \alpha)$$

   is a prime factorisation of the ideal (α) in $\mathcal{O}_d$. (Hint: compute the norm of the ideals (p_i, α) first.) (8 marks)

   (b) Find a counterexample to the claim above when the norm is not square-free. Justify your answer. (2 marks)

   (c) Prove that (α) can aways be written as the product of at most n prime ideals. (4 marks)

   (d) Prove that the bound above is optimal, that is, for every positive integer n there is a d and an α as above such that (α) cannot be written as the product of at most $n-1$ prime ideals. (Hint: use that there are infinitely many primes $\equiv 1 \bmod 4$.) (6 marks)

   (Total: 20 marks)

3. Let x, y be integer solutions of the Diophantine equation:

$$x^2 + 7 = 2y^3.$$

Show that there are integers b, c such that either

$$2(x-7) = b(b^2 - 21c^2),\ 2(x+1) = c(3b^2 - 7c^2),$$

or

$$2(x+7) = b(b^2 - 21c^2),\ 2(-x+1) = c(3b^2 - 7c^2).$$

You may use that the class number of $\mathcal{O}_{-7}$ is 1 without proof. (20 marks)

(Total: 20 marks)

4. Let $d = -p_1 p_2 \cdots p_n$, where $p_1, p_2, \ldots, p_n$ are different positive prime numbers, and $p_1 = 2$. For every non-zero ideal $I \triangleleft \mathcal{O}_d$ let $[I]$ denote the class of I in $Cl(\mathcal{O}_d)$.

(a) Prove that for every $1 \leq i_1 < i_2 < \ldots < i_k \leq n$ we have:

$$[(p_{i_1}, \sqrt{d})][(p_{i_2}, \sqrt{d})] \cdots [(p_{i_k}, \sqrt{d})] = [(p_{i_1} p_{i_2} \cdots p_{i_k}, \sqrt{d})]$$

in $Cl(\mathcal{O}_d)$. (4 marks)

(b) Deduce that the subgroup generated by $[(p_1, \sqrt{d})], [(p_2, \sqrt{d})], \ldots, [(p_n, \sqrt{d})]$ in $Cl(\mathcal{O}_d)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{n-1}$. (Hint: show that the ideal $(p_1 p_2 \cdots p_k, \sqrt{d})$ is principal first.) (8 marks)

Let $\mathbb{Q}(\sqrt{d})$ denote the fraction field of $\mathcal{O}_d$ and let $N(\cdot)$ be its norm function. Let $\bar{\cdot}$ denote the unique automorphism of $\mathbb{Q}(\sqrt{d})$ such that $\overline{\sqrt{d}} = -\sqrt{d}$. Finally for every fractional ideal $I \subset \mathbb{Q}(\sqrt{d})$ let $\overline{I}$ denote the image of I with respect to the map $\bar{\cdot}$.

(c) Let $z \in \mathbb{Q}(\sqrt{d})$ have norm $N(z) = 1$. Prove that there exists an $a \in \mathbb{Q}(\sqrt{d})$ such that $z = a/\overline{a}$. (2 marks)

(d) Prove that any element of order at most 2 in $Cl(\mathcal{O}_d)$ can be represented by a non-zero ideal $I \triangleleft \mathcal{O}_d$ such that $I = \overline{I}$. (Hint: use part (c).) (6 marks)

(Total: 20 marks)

5. (a) Let p be an odd prime. Show that the sets:

$$S = \{\alpha^2 \mod p \mid 0 \leq \alpha < \frac{p}{2}\} \quad \text{and} \quad S' = \{-1 - \beta^2 \mod p \mid 0 \leq \beta < \frac{p}{2}\}$$

both have $\frac{p+1}{2}$ elements. (4 marks)

(b) Deduce that there are $\alpha, \beta \in \mathbb{Z}$ such that $\alpha^2 + \beta^2 + 1 \equiv 0 \mod p$ for every prime number p. (3 marks)

(c) For every prime number p let

$$\Lambda_p = \{a \in \mathbb{Z}^4 \mid a_1 \equiv \alpha a_3 + \beta a_4 \mod p, \quad a_2 \equiv \beta a_3 - \alpha a_4 \mod p\}.$$

Show that Λ_p is a discrete lattice of rank 4 with covolume $\mathrm{covol}(\Lambda) \leq p^2$. (3 marks)

(d) For every prime number p let $B_p = \{a \in \mathbf{R}^4 \mid \|a\| < \sqrt{2p}\}$. Apply Minkowski's first theorem to B_p and Λ_p to deduce that p is a sum of four squares of integers. (You need to check that the conditions of the theorem apply.) (7 marks)

(e) Use the identity:

$$\begin{aligned}(a_1^2 + a_2^2 + a_3^2 + a_4^2) \cdot (b_1^2 + b_2^2 + b_3^2 + b_4^2) = \quad & (a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4)^2 \\ & + (a_1b_2 + a_2b_1 + a_3b_4 - a_4b_3)^2 \\ & + (a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2)^2 \\ & + (a_1b_4 + a_2b_3 - a_3b_2 + a_4b_1)^2\end{aligned}$$

to conclude that every positive integer is a sum of four squares of integers. (3 marks)

(Total: 20 marks)

Module:	MATH96028/MATH97037/MATH97145
Setter:	Pál
Checker:	Helm
Editor:	Pál
External:	Lotay
Date:	April 27, 2022
Version:	Draft version for checking

BSc, MSci and MSc EXAMINATIONS (MATHEMATICS)

May – June 2022

MATH96028/MATH97037/MATH97145 Algebraic Number Theory Solutions

The following information must be completed:

Is the paper suitable for resitting students from previous years:

Category A marks: available for basic, routine material (excluding any mastery question) (40 percent = 32/80 for 4 questions):
1(a),(b),(c) 8 marks; 2(a),(b),(c) 8 marks; 3 8 marks; 4(a),(b) 8 marks.

Category B marks: Further 25 percent of marks (20/ 80 for 4 questions) for demonstration of a sound knowledge of a good part of the material and the solution of straightforward problems and examples with reasonable accuracy (excluding mastery question):
1(a),(b) 5 marks; 2(a),(c) 5 marks; 3 5 marks; 4(b),(c) 5 marks.

Category C marks: the next 15 percent of the marks (= 12/80 for 4 questions) for parts of questions at the high 2:1 or 1st class level (excluding mastery question):
1(a),(c) 3 marks; 2(a),(d) 3 marks; 3 3 marks; 4(b),(c) 3 marks.

Category D marks: Most challenging 20 percent (16/80 marks for 4 questions) of the paper (excluding mastery question):
1(c) 4 marks; 2(d) 4 marks; 3 4 marks; 4(d) 4 marks.

Signatures are required for the final version:

Setter's signature	Checker's signature	Editor's signature
.....	.....	.....

Temporary front page

BSc, MSc and MSci EXAMINATIONS (MATHEMATICS)

May – June 2022

This paper is also taken for the relevant examination for the Associateship of the Royal College of Science.

Algebraic Number Theory Solutions

Date: ??

Time: ??

Time Allowed: 2 Hours for MATH96 paper; 2.5 Hours for MATH97 papers

This paper has *4 Questions (MATH96 version); 5 Questions (MATH97 versions)*.

Candidates should start their solutions to each question in a new main answer book.

Supplementary books may only be used after the relevant main book(s) are full.

Statistical tables will not be provided.

- DO NOT OPEN THIS PAPER UNTIL THE INVIGILATOR TELLS YOU TO.
- Affix one of the labels provided to each answer book that you use, but DO NOT USE THE LABEL WITH YOUR NAME ON IT.
- Credit will be given for all questions attempted.
- Each question carries equal weight.
- Calculators may not be used.

1. (a) We know that every reduced form of discriminant -59 is of the form $aX^2+bXY+cY^2 = [a,b,c]$ for some $a,b,c \in \mathbb{Z}$ such that $-59 = b^2 - 4ac$, $|b| \leq a \leq c$, moreover $b \geq 0$ if any of the two equalities occurs, and finally $a \leq \sqrt{\frac{59}{3}} < 5$. So $1 \leq a \leq 4$ and b must be odd. Now we compute:

   $a = 1$ In this case $b = 1$ and $c = 60/4 = 15$, hence we find the form $[1,1,15]$.

   $a = 2$ In this case $b = \pm 1$. We get the equation $-8c = -60$ which has no integral solution. No forms in this case.

   $a = 3$ In this case either $b = \pm 1$ or $b = 3$. In the first case we find the forms $[3, \pm 1, 5]$. In the second case we get the equation $-12c = -68$ which has no integral solution.

   $a = 4$ In this case we have $b = \pm 1$ or $b = \pm 3$. These lead to the equations $-16c = -60$ and $-16c = -68$, respectively, which have no integral solutions. No forms in this case.

   So the reduced forms are $[1,1,15], [3,-1,5]$ and $[3,1,5]$. **A,B,C** (11 marks)

   (b) By a fundamental theorem the class number of $\mathcal{O}_{-59}$, which is the order of $Cl(\mathcal{O}_{-59})$, is equal to the cardinality of reduced forms of discriminant -59. Therefore the order of $\mathcal{O}_{-59}$ is 3. Since this order is a prime number, the class group is isomorphic to the cyclic group $\mathbb{Z}/3\mathbb{Z}$. **A,B** (3 marks)

   (c) Since every non-trivial element of $Cl(\mathcal{O}_{-59})$ generates this group, it will be enough to produce a non-principal ideal $\mathfrak{a}$, as the classes will be given by $\mathfrak{a}, \mathfrak{a}^2$ and $\mathfrak{a}^3$. Now

$$(3, \frac{1+\sqrt{-59}}{2}) \cdot \overline{(3, \frac{1+\sqrt{-59}}{2})} = (9, 3(\frac{1+\sqrt{-59}}{2}), 3(\frac{1-\sqrt{-59}}{2}), 15) = (3),$$

   since the gcd of $9, 15$ is 3, so 3 is in the RHS, on the other hand in the middle all generators are divisible by 3. So $(3, \frac{1+\sqrt{-59}}{2})$ has norm 3. The Diophantine equation $x^2 + 59y^2 = 12$ has no solutions, so there are no elements of norm 3, and hence $(3, \frac{1+\sqrt{-59}}{2})$ is not principal. So $\mathfrak{a} = (3, \frac{1+\sqrt{-59}}{2})$ works. **C,D** (6 marks)

(Total: 20 marks)

2. (a) Note that

$$(p_i, \alpha)\overline{(p_i, \alpha)} = (p_i, \alpha)(p_i, \overline{\alpha}) = (p_i^2, N(\alpha), p_i \cdot \alpha) = (p_i, p_i \cdot \alpha) = (p_i),$$

since the gcd of p_i^2 and $N(\alpha)$ is p_i, as $N(\alpha)$ is square-free. Since the norm of the ideal (p_i, α) is prime, it is a prime ideal by results from the course. So it will be enough to show that

$$(\alpha) = (p_1, \alpha)(p_2, \alpha) \cdots (p_n, \alpha).$$

By the multiplicativity of the norm the RHS has norm $p_1 p_2 \cdots p_n = N(\alpha)$, so it will be sufficient to show that $\alpha \in \mathrm{RHS}$. It contains $\alpha \cdot (\prod_{i=1}^n p_i)/p_j$ for each j. Since the gcd of the $(\prod_{i=1}^n p_i)/p_j$ is 1, the claim follows. **A,B,C** (8 marks)

(b) Let $d = -4$; in this case $\mathcal{O}_d = \mathbb{Z}[\sqrt{-1}]$. Then $2 \in \mathbb{Z}[\sqrt{-1}]$ is a prime, and $N(2) = 4 = 2 \cdot 2$. However $(2, 2)(2, 2) = (2)(2) = (4) \neq (2)$. **A** (2 marks)

(c) By the unique factorisation of ideals in Dedekind domains there is a factorisation:

$$(\alpha) = \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_m$$

where $\mathfrak{p}_i$ are non-zero prime ideals. Taking norms we get:

$$|N(\alpha)| = N((\alpha)) = N(\mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_m) = N(\mathfrak{p}_1) N(\mathfrak{p}_2) \cdots N(\mathfrak{p}_m)$$

using the multiplicativity of the norm. Since $N(\mathfrak{p}_1) > 1$ fo each i, the RHS has at least m prime factors. Therefore $m \leq n$ by the fundamental theorem of arithmetic. **A,B** (4 marks)

(d) Let $d = -4$. By a result from the course there are infinitely many primes $\equiv 1 \mod 4$. Let $p_1, p_2, \ldots, p_n$ be pair-wise different positive primes $\equiv 1 \mod 4$. Since each p_i splits in $\mathbb{Z}[\sqrt{-1}]$, there is an $\alpha_i \in \mathbb{Z}[\sqrt{-1}]$ such that $N(\alpha_i) = p_i$. Then $\alpha = \alpha_1 \alpha_2 \cdots \alpha_m$ has norm $p_1 p_2 \cdots p_n$ by the multiplicativity of the norm. Therefore (α) has a prime factorisation consisting of the products of n prime ideals by part (a). Since the prime factorisation is unique up to reordering, there could be no factorisation with at most $n - 1$ prime factors. **C,D** (6 marks)

(Total: 20 marks)

3. As $-7 \equiv 1 \mod 4$, we have $\mathcal{O}_{-7} = \mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$. Since the Diophantine equation $a^2 + 7b^2 = 4$ has no non-trivial solutions, we have $\mathcal{O}_{-7}^* = \{\pm 1\}$. Moreover $\mathcal{O}_{-7}$ has class number one, so it is a UFD. We have the factorisation $2 = (\frac{1+\sqrt{-7}}{2}) \cdot (\frac{1-\sqrt{-7}}{2})$ in $\mathcal{O}_{-7}$. Since $\frac{1+\sqrt{-7}}{2} + \frac{1-\sqrt{-7}}{2} = 1$, we get that these elements are relatively prime, and hence the factorisation above is into prime elements.

First note that $2 \not| x$. Otherwise $7 \equiv x^2 + 7 \equiv 2y^3 \equiv 0 \mod 2$, which is a contradiction. Therefore we have the factorisations $x \pm \sqrt{-7} = 2 \cdot \frac{x \pm \sqrt{-7}}{2}$ in $\mathcal{O}_{-7}$. Also note that $7 \not| y$. Otherwise $7|x^2$, so $7|x$, and hence $7 \equiv x^2 + 7 \equiv 2y^3 \equiv 0 \mod 49$, which is a contradiction. The greatest common divisor of $x + \sqrt{-7}$ and $x - \sqrt{-7}$ must divide both their difference, which is $2\sqrt{-7}$, and their product $2y^2$, which is not divisible by 7, hence we get their greatest common divisor divides 2. Therefore $\frac{x+\sqrt{-7}}{2}$ and $\frac{x-\sqrt{-7}}{2}$ are relatively prime. **A,B,C,D** (10 marks)

In particular the prime factorisation of these elements are of the form:

$$\frac{x + \sqrt{-7}}{2} = \pm \alpha^a p_1^{a_1} p_2^{a_2} \cdots, \ \frac{x - \sqrt{-7}}{2} = \pm \overline{\alpha}^a \overline{p}_1^{a_1} \overline{p}_2^{a_2} \cdots,$$

where $\alpha = \frac{1 \pm \sqrt{-7}}{2}$, and the primes p_i are pair-wise different from each other, their conjugates, or from $\alpha, \overline{\alpha}$. Since

$$\alpha\overline{\alpha} \cdot \frac{x + \sqrt{-7}}{2} \cdot \frac{x - \sqrt{-7}}{2} = 2 \cdot \frac{x + \sqrt{-7}}{2} \cdot \frac{x - \sqrt{-7}}{2} = y^3,$$

we get that $3|a_i$ for each i and $a \equiv 2 \mod 3$. Since ± 1 are cubes, we get that $\alpha \cdot \frac{x+\sqrt{-7}}{2}$ is a cube in $\mathcal{O}_{-7}$.

When $\alpha = \frac{1+\sqrt{-7}}{2}, \frac{1-\sqrt{-7}}{2}$ this leads to the equations:

$$2(x-7) = b(b^2 - 21c^2), \ 2(x+1) = c(3b^2 - 7c^2), \ b \equiv c \mod 2,$$

$$2(x+7) = b(b^2 - 21c^2), \ 2(-x+1) = c(3b^2 - 7c^2), \ b \equiv c \mod 2,$$

respectively. **A,B,C,D** (10 marks)

(Total: 20 marks)

4. (a) It will be enough to show that

$$(p_{i_1}p_{i_2}\cdots p_{i_{k-1}},\sqrt{d})\cdot(p_{i_k},\sqrt{d})=(p_{i_1}p_{i_2}\cdots p_{i_k},\sqrt{d}),$$

since then the claim follows by induction on k and taking the class. We compute:

$$(p_{i_1}p_{i_2}\cdots p_{i_{k-1}},\sqrt{d})(p_{i_k},\sqrt{d})=(p_{i_1}p_{i_2}\cdots p_{i_k},p_{i_1}p_{i_2}\cdots p_{i_{k-1}}\sqrt{d},p_{i_k}\sqrt{d},d)=(p_{i_1}p_{i_2}\cdots p_{i_k},\sqrt{d}),$$

where we used in the second equation that the gcd of $p_{i_1}p_{i_2}\cdots p_{i_{k-1}}$ and p_{i_k} is 1, and $p_{i_1}p_{i_2}\cdots p_{i_k}$ divides d. **A** (4 marks)

(b) Since $(p_i,\sqrt{d})^2=(p_i)$, the ideal $(p_i,\sqrt{d})$ has norm p_i and its class has order at most 2. Therefore the group generated by these classes is 2-torsion. By part (a) they satisfy the relation:

$$[(p_1,\sqrt{d})][(p_2,\sqrt{d})]\cdots[(p_n,\sqrt{d})]=[(p_1p_2\cdots p_n,\sqrt{d})]=[(d,\sqrt{d})]=[(\sqrt{d})]=0,$$

so it remains to show that they do not satisfy any other. By part (a) this is equivalent to showing that $I=(p_{i_1}p_{i_2}\cdots p_{i_{k-1}},\sqrt{d})$ is not principal for any $k<n$. The norm of I is $p_{i_1}p_{i_2}\cdots p_{i_{k-1}}$ by the multiplicativity of the norm, so it will be enough to see that there are no elements with such norms in $\mathcal{O}_d$, that is, the equation $x^2+|d|y^2=p_{i_1}p_{i_2}\cdots p_{i_{k-1}}$ has no integer solutions. Otherwise we get $y=0$ as $p_{i_1}p_{i_2}\cdots p_{i_{k-1}}<|d|$, but $p_{i_1}p_{i_2}\cdots p_{i_{k-1}}$ is square-free. **A,B,C** (8 marks)

(c) Write $a=x+y\sqrt{d}$ and $z=z_1+z_2\sqrt{d}$, then $x+y\sqrt{d}=(z_1+z_2\sqrt{d})(x-y\sqrt{d})$ which gives a homogeneous system of two linear equations in x and y with zero determinant. **B,C** (2 marks)

(d) Since $J\cdot\overline{J}$ is principal for every ideal J, if the class of J has order at most 2 in $Cl(\mathcal{O}_d)$ then $J=x\overline{J}$ for some $0\neq x\in\mathbb{Q}(\sqrt{d})$. Write $x=\alpha/\beta$ where $\alpha,\beta\in\mathcal{O}_d$. Then $\alpha J=\beta J$. Taking norms and using the fact that $N(I)=N(\overline{I})$ we obtain $N(x)=\pm1$. The negative sign is not possible because $d<0$. By part (c) we can write $x=a/\overline{a}$ where $a\in\mathbb{Q}(\sqrt{d})$. Let $I=aJ$. This is a fractional ideal of $\mathbb{Q}(\sqrt{d})$ such that $I=\overline{I}$. Multiplying by a large enough positive integer get an ideal with the same property still in the same class. **C,D** (6 marks)

(Total: 20 marks)

5. (a) If $0 \leq \alpha, \alpha' < \frac{n}{2}$ with $\alpha^2 \equiv \alpha'^2 \mod p$, then $(\alpha+\alpha')(\alpha-\alpha') \equiv 0 \mod p$, and $\alpha+\alpha' \not\equiv 0 \mod p$ since $\alpha+\alpha' < p$, which implies that $\alpha - \alpha' \equiv 0 \mod p$, and hence $\alpha = \alpha'$. So S has $\frac{p+1}{2}$ elements. Similarly, if $0 \leq \beta, \beta' < \frac{p}{2}$ such that $-1-\beta^2 \equiv -1-\beta'^2$, then $\beta = \beta'$, so S' also has $\frac{p+1}{2}$ elements. (4 marks)

(b) If $p = 2$, take $\alpha = 1, \beta = 0$. When p is odd $S \cap S'$ cannot be empty by the pigeonhole principle, so we can find α and β such that $\alpha^2 \equiv -1 - \beta^2 \mod p$. (3 marks)

(c) Since Λ_p is a subgroup of $\mathbb{Z}^4$, it is a discrete lattice. The set $\{0, \ldots, p-1\}^2 \times \{(0,0)\}$ surjects onto $\mathbb{Z}^4/\Lambda_p$ under the projection, so Λ_p has finite index in $\mathbb{Z}^4$, and hence has rank 4. Moreover $\mathrm{covol}(\Lambda_p) = \#(\mathbb{Z}^4/\Lambda_p) \leq p^2$. (3 marks)

(d) Clearly B_p is a convex, symmetric open subset such that

$$\mathrm{vol}(B_p) = \frac{\pi^2}{2}(\sqrt{2p})^4 = 2\pi^2 p^2 > 16p^2 \geq 2^4 \mathrm{covol}(\Lambda_p).$$

Therefore by part (c) Minkowski's first theorem applies, so there is an $a \in \Lambda_p$ such that $0 < \|a\|^2 < 2p$. Now $\|a\|^2 = a_1^2 + a_2^2 + a_3^2 + a_4^2$ implies $\|a\|^2 \equiv (\alpha a_3 + \beta a_4)^2 + (\beta a_3 - \alpha a_4)^2 + a_3^2 + a_4^2 \equiv 0 \mod p$, and hence $a_1^2 + a_2^2 + a_3^2 + a_4^2$ is a multiple of p. Since $0 < \|a\|^2 < 2p$ this multiple must be 1. (7 marks)

(e) By the identity the product of sums of four squares of integers is the sum of four squares of integers. The claim now follows from the fundamental theorem of arithmetic and part (d), by induction on the number of prime factors. (3 marks)

(Total: 20 marks)

If your module is taught across multiple year levels, you might have received this form for each level of the module. You are only required to fill this out once for each question.			
Please record below, some brief but non-trivial comments for students about how well (or otherwise) the questions were answered. For example, you may wish to comment on common errors and misconceptions, or areas where students have done well. These comments should note any errors in and corrections to the paper. These comments will be made available to students via the MathsCentral Blackboard site and should not contain any information which identifies individual candidates. Any comments which should be kept confidential should be included as confidential comments for the Exam Board and Externals. If you would like to add formulas, please include a separate pdf file with your email.			
ExamModuleCode	**QuestionNumber**	**Comments for Students**	
	1	This was a fairly routine problem on reduction theory and class groups that most of the students did well. The exposition of solutions was sometimes poor.	
	2	This problem, which is on the length of prime factorisations, had parts which required a short proof which was not very different from the arguments which we used in concrete examples in class. Some students found the step to more abstraction a bit challenging, but this has to do with having difficulties writing down formal mathematics, then difficulties with the material itself. Still, many of the cohort did well.	
	3	This problem turned out to be more challenging then I anticipated. It was a slight twist on one of the most central arguments in the proof, namely, the separation of powers trick. The equation was different from usual Mordell equations by a single factor of 2 in front of y^3. Otherwise the equation was simple; the relevant quadratic ring is UFD, but the equation has a nontrivial solution (3^2+7=2*2^3), so there were no simple paths (like congruences) to rule out solutions. The actual solution is a very small modification of the proof of the original argument, as the two factors of the LHS are not relatively prime, their common divisor is 2. However many students already failed at the setup, and did not notice this or made some other whopping errors. Perhaps I should have gave more hints by cutting up the problem to smaller parts. Nevertheless this problem should be well within the reach of anyone who understands the proof of the separating powers trick and the general approach to these equations, and I consider the course a success if a student can solve such an equation on their own.	

	4	This exercise is what is known as genus theory. The first half of the problem was quite easy, mostly an exercise in writing an argument down. The second part was more interesting, a converse to the first part. Luckily there were several students who did both parts well; in fact there were students who came up with the very nice idea of using the theory of reduced quadratic forms to prove the harder part, which is very different from the proof in the solutions.		
	5	This problem is a routine application of the geometry of numbers to the four squares theorem, cut up to bite sizes. The majority of parts only required elementary number theory. Most students did well.		