FINAL EXAMINATION
AUTUMN SESSION 2010

SCHOOL OF COMPUTING & MATHEMATICS

<table>
<thead>
<tr>
<th>Student Family Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Student Given Names:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Student Number:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Course:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Unit Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABSTRACT ALGEBRA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Unit Number:</th>
</tr>
</thead>
<tbody>
<tr>
<td>200193</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Time Allowed:</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 hours plus 10 minutes reading time</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number of Questions:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Six(6)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Total Number of Pages:</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Lecturers:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stephen Lack</td>
</tr>
</tbody>
</table>

INSTRUCTIONS
PLEASE READ CAREFULLY BEFORE PROCEEDING

1 Write your name and student number on the top of this examination paper and on ALL answer booklets.

2 THIS IS A CLOSED BOOK EXAMINATION.

3 Answer all questions in the answer booklets provided.

4 There are 100 marks available in this exam. The value of each question is indicated.

5 Non-programmable calculators may be used.

6 Full justification and/or working must be shown in order to obtain full marks for a question.

DO NOT TAKE THIS PAPER FROM THE EXAMINATION ROOM
Question 1. (3+2+2+2+3+2+4=20 marks)

a) Find the remainder when $13^{2010}$ is divided by 18.
b) Find $\gcd(2328, 7315)$.
c) Find all solutions of $14x \equiv 6 \pmod{18}$.
d) Find all solutions of $x^2 \equiv x \pmod{6}$.
e) Write out the multiplication table of $\mathbb{Z}_6$.
f) For integers $a$ and $b$, define what the statement $a \equiv b \pmod{18}$ means.
g) State carefully what the division algorithm (for integers) allows you to do.
h) Suppose that $a$, $b$, and $c$ are integers for which $a \mid bc$ and $\gcd(a, c) = 1$. Show that $a \mid b$.

Question 2. (2+2+3+4+4=15 marks)

a) Explain why $\mathbb{Z}_n$ is not a field if $n$ is composite.
b) If $z = a + bi$, for $a, b \in \mathbb{R}$, what is $1/z$?
c) Find all solutions of $z^3 = 1$ in $\mathbb{C}$.
d) Find all solutions of $z^3 - 3z^2 + 5z - 3 = 0$ in $\mathbb{C}$, given that $z = 1$ is a solution.
e) Let $p(z)$ be a polynomial with real coefficients for which $p(1 + i) = 0$. Show that $p(1 - i) = 0$.

Question 3. (4+2+3+2+2+2=15 marks)

a) Factorize $x^3 + x^2 + 1$ into irreducible polynomials in $\mathbb{Z}_3[x]$.
b) How many elements does $\mathbb{Z}_3[x]/\langle x^3 + x^2 + 1 \rangle$ have?
c) Find the inverse of $x + 1$ in $\mathbb{Z}_3[x]/\langle x^3 + x^2 + 1 \rangle$.
d) Is $\mathbb{Z}_3[x]/\langle x^3 + x^2 + 1 \rangle$ a field? Explain.
e) Is $\mathbb{R}[x]/\langle x^3 + x^2 + 1 \rangle$ a field? Explain.
f) Find the principal representative of $2x^4 + 3x^2 + 4x + 5$ in $\mathbb{Q}[x]/\langle x^3 + x^2 + 1 \rangle$. 

Page 2 of 5
Question 4. (4+5+5+4 = 18 marks)

a) (i) Write the following permutation as a product of disjoint cycles.

\[
\begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
3 & 4 & 6 & 8 & 2 & 7 & 1 & 5 & 9
\end{pmatrix}
\]

(ii) Simplify the permutation \((1 3 4 6)(2 4 6)(3 4 5)(5 1)\).

b) \(\mathbb{U}_n\) is the group of units of \(\mathbb{Z}_n\).
   (i) List the elements of \(\mathbb{U}_{14}\).
   (ii) Show that \(\mathbb{U}_{14}\) is isomorphic to \(\mathbb{Z}_6\).

c) The dihedral group \(D_4\) is the group of symmetries of the square.
   (i) Is \(D_4\) abelian? Justify your answer.
   (ii) Is \(D_4\) isomorphic to a subgroup of \(\mathbb{U}_{18}\)? Justify your answer.

d) This question is about a group \(G\) with the following incomplete Cayley table.

\[
\begin{array}{cccccc}
& u & v & w & x & y & z \\
u & u & & & & & \\
v & & x & & & & \\
w & & & y & u & & \\
x & & & & y & v & \\
y & & & & & & \\
z & & & & & & \\
\end{array}
\]

(i) Complete the table.
(ii) Name a group that is isomorphic to \(G\).
Question 5. (8+12 = 20 marks)

a) This part of the question is about groups of order 6.
   (i) Give an example of a group of order 6 with an element of order 6.
   (ii) Give an example of a group of order 6 which has no element of order 6. Explain clearly why your group cannot have an element of order 6.
   (iii) Explain why no group of order 6 can ever have an element of order 4.
   (iv) Does there exist a group of order 6 with exactly one element of order 6?

b) This part of the question is about the symmetric group $S_n$; it is the group of all permutations of \{1, 2, \ldots, n\}.
   (i) What is the order of $S_n$?
   (ii) There is a group homomorphism $f : S_n \to \mathbb{Z}_2$ defined by
        \[ f(\alpha) = \begin{cases} 
        0 & \text{if } \alpha \text{ is even} \\
        1 & \text{otherwise} 
        \end{cases} \]
        What would you have to do to check that $f$ is a homomorphism? (You are not being asked to actually check it, just to state what you would need to do.)
   (iii) Calculate $f(\alpha)$ in the case $\alpha = (1 \ 3 \ 5 \ 7)(1 \ 2 \ 3 \ 4 \ 5)(2 \ 3 \ 5)(3 \ 1 \ 4 \ 2 \ 7 \ 5)$.
   (iv) Show that the set $A_n$ of even permutations is a normal subgroup of $S_n$, using only facts given on this page.
   (v) What is the order of the quotient group $S_n/A_n$?
   (vi) For which values $n > 1$ is $S_n$ a cyclic group? Be sure to justify your answer fully.
Question 6. (2+1+2+2+5 = 12 marks)

In this question \( \varphi \) denotes the Euler totient (phi) function.

a) Explain carefully why \( \varphi(p) = p - 1 \) if \( p \) is prime

b) Calculate \( \varphi(253) \).

c) You are going to use the RSA cryptosystem with encryption key \( (253, e) \). What property does \( e \) have to satisfy?

d) Show that \( e = 147 \) satisfies this property

e) A message has been encoded using the encryption key \( (253, 147) \) for the RSA cryptosystem and the correspondence

\[
\begin{align*}
A & \rightarrow 10 & J & \rightarrow 19 & S & \rightarrow 28 \\
B & \rightarrow 11 & K & \rightarrow 20 & T & \rightarrow 29 \\
C & \rightarrow 12 & L & \rightarrow 21 & U & \rightarrow 30 \\
D & \rightarrow 13 & M & \rightarrow 22 & V & \rightarrow 31 \\
E & \rightarrow 14 & N & \rightarrow 23 & W & \rightarrow 32 \\
F & \rightarrow 15 & O & \rightarrow 24 & X & \rightarrow 33 \\
G & \rightarrow 16 & P & \rightarrow 25 & Y & \rightarrow 34 \\
H & \rightarrow 17 & Q & \rightarrow 26 & Z & \rightarrow 35 \\
I & \rightarrow 18 & R & \rightarrow 27 \\
\end{align*}
\]

The encoded message is 74-158-5-155-49. Decode it.