You have three hours.

There are 9 problems, and the total number of points is 130. Show all your work. *Please make your work as clear and easy to follow as possible.*

Name:______________________________

Signature:__________________________

Student ID #:______________________

<table>
<thead>
<tr>
<th>Problem</th>
<th>Points</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>30</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>130</td>
<td></td>
</tr>
</tbody>
</table>
1. (30pts) Give the definition of
   (i) norm of an element of $\mathbb{Z}[\sqrt{d}]$.

   If $\alpha = a + b\sqrt{d}$ then
   \[ N(\alpha) = a^2 - b^2d. \]

   (ii) $p$-adic absolute value.

   \[ |m| = \frac{1}{p^e} \]
   where $p^e$ is the largest power of $p$ dividing $m$.

   (iii) algebraic number of degree $n$.

   $\alpha \in \mathbb{C}$ is algebraic of degree $n$ if there is a polynomial
   $m(x) \in \mathbb{Q}[x]$ of degree $n$ such that $m(\alpha) = 0$ and no lower degree
   polynomial with the same property.
(iv) \emph{Farey sequence} $\mathcal{F}_n$.

The sequence of all rational numbers with denominator no bigger than $n$.

(v) \emph{best approximation}.

$p/q$ is called a best approximation of $x$ if

$$|q'x - p'| \leq |qx - p|$$

for some $q' \leq q$ implies that $q = q'$.

(vi) \emph{quadratic irrational}.

a real number of degree two.
2. (15pts) (i) Show that the set of numbers represented as the sum of two squares is closed under multiplication.

If \( \alpha = a + bi \) and \( \beta = c + di \) then
\[
(a^2 + b^2)(c^2 + d^2) = N(\alpha)N(\beta)
\]
\[
= N(\alpha\beta)
\]
\[
= N(ac - bd + (bc + ad)i)
\]
\[
= (ac - bd)^2 + (bc + ad)^2.
\]

(ii) Show that every prime \( \rho \in \mathbb{Z}[i] \) divides some rational prime.

Let
\[
\rho \bar{\rho} = N(\rho)
\]
\[
= n \in \mathbb{N}.
\]

Thus \( \rho \) divides \( n \). Let
\[
n = p_1p_2\ldots p_k
\]
be the prime factorisation of \( n \).

As \( \rho \) is a prime it must divide one of the factors of \( n \). Thus \( \rho \) divides a prime.
(iii) Show that $(1 + i)|(a + bi)$ if and only if $a \equiv b \mod 2$.

Suppose that $(1 + i)|(a + bi)$. If we take the norm of both sides then we get

$$2 = N(1 + i)$$
$$|N(a + bi)| = a^2 + b^2.$$

As $2$ divides $a^2 + b^2$, $a$ and $b$ must have the same parity.

Now suppose that $a$ and $b$ have the same parity. If $a$ and $b$ are even, so that $a = 2k$ and $b = 2l$ then $1 + i$ divides $a + bi = 2(k + li)$ as $1 + i$ divides $2 = (1 + i)(1 - i)$. If $a$ and $b$ are both odd then consider

$$\alpha = (a + bi)$$
$$= (a - 1) + (b - 1)i + (1 + i)$$
$$= \beta + (1 + i).$$

As the components of $\beta$ are even, it follows that $1 + i$ divides $\beta$ and so $1 + i$ divides $\alpha$. 
3. (15pts) Show that the general integral solution of the equation
\[ x^2 + y^2 = z^2 \]
is of the form
\[ x = c(a^2 - b^2) \quad y = 2abc \quad \text{and} \quad z = c(a^2 + b^2), \]
where \(2c \in \mathbb{Z}\).

Consider lines through \((-1,0)\). These have the form
\[ y = m(x + 1). \]
If we substitute this into the equation of the circle \(x^2 + y^2 = 1\) we get
\[ x^2 + m^2(x + 1)^2 = 1 \quad \text{so that} \quad (m^2 + 1)x^2 + 2m^2x + (m^2 - 1) = 0. \]
One solution is \(x = -1\) and so it follows that the other is
\[ x = \frac{1 - m^2}{1 + m^2} \quad \text{so that} \quad y = \frac{2m}{1 + m^2}. \]
As \(m\) ranges over the rational numbers, this gives all rational solutions of the equation \(x^2 + y^2 = 1\), since if \(m\) is rational then \(x\) and \(y\) are rational and if \(x\) and \(y\) are rational then so is the slope.
If \(m = a/b\) then
\[ x = \frac{a^2 - b^2}{a^2 + b^2} \quad \text{and} \quad y = \frac{2ab}{a^2 + b^2}. \]
\(x/z\) and \(y/z\) are solutions of \(u^2 + v^2 = 1\) if and only if \(x, y\) and \(z\) are solutions of \(x^2 + y^2 = z^2\). Multiplying through by \(c(a^2 + b^2)\) to clear denominators we get the solution
\[ x = c(a^2 - b^2) \quad y = 2abc \quad \text{and} \quad z = c(a^2 + b^2), \]
Note that \(c\) need not be an integer, since the original \(x\) and \(y\) need not be in their lowest terms. However as \(z + x\) and \(z - x\) are integers, it follows that \(2c \in \mathbb{Z}\).
4. (10pts) Show that if \( p \) is an odd prime and \( a \) is coprime to \( p \) then the equation
\[
x^2 = a
\]
has two solutions in the \( p \)-adic integers if and only if \( a \) is a quadratic residue of \( p \).

If
\[
\alpha = a_0 + a_1 p + a_2 p^2 + \ldots
\]
is a solution of \( x^2 = a \) then certainly \( a_0^2 \equiv a \mod p \) so that \( a \) is a quadratic residue modulo \( p \).

Now suppose that \( a \) is a quadratic residue modulo \( p \). Pick \( a_0 \) so that \( a_0^2 \equiv a \mod p \). We will construct a sequence of integers in the range 0 to \( p - 1 \) so that
\[
\alpha_n = a_0 + a_1 p + \cdots + a_n p^n
\]
is a solution modulo \( p^{n+1} \) by induction on \( n \). Let \( f(x) = x^2 - a \). Then \( f'(x) = 2x \). Having chosen \( a_0, a_1, \ldots, a_n, a_{n+1} = a_n + tp^{n+1} \). We have to choose \( t \) such that
\[
f(\alpha_n + tp^{n+1}) \equiv f(\alpha_n) + 2tp^{n+1} \equiv 0 \mod p^{n+2}.
\]
Since \( f(\alpha_n) \) is divisible by \( p^{n+1} \) we can always find integers \( 0 \leq tp - 1 \) satisfying this equation. This defines \( a_{n+1} \).

Taking the limit gives a \( p \)-adic integer. We get two different solutions, one for each choice of \( a_0 \).
5. (10pts) Find the general solution of the equation
\[ x^2 - 2y^2 = 1. \]

We just have to find the fundamental solution. One way to find this is to compute the continued fraction expansion of \( \sqrt{2} \). \( \sqrt{2} = 1 + \sqrt{2} - 1. \)

\[
\sqrt{2} = 1 + \sqrt{2} - 1 = 2 + \sqrt{2} - 1.
\]

Thus

\[ \sqrt{2} = [1; 2]. \]

The convergents are

\[
\begin{array}{cc}
1 & 3 \\
1 & 2 \\
\end{array}
\]

and indeed

\[ 3^2 - 2^2 \cdot 2 = 1. \]

Thus the fundamental solution is

\[ \delta = 3 + 2\sqrt{2}. \]

One can also find this solution by trial and error.
It follows that the general solution is

\[ \pm(3 + 2\sqrt{2})^n, \]

where \( n \) is an integer.
6. (10pts) If \( \delta \) is the fundamental solution of the equation

\[ x^2 - dy^2 = 1 \]

then show that every solution has the form \( \pm \delta^n \).

Let \( \alpha \) be a non-trivial solution of

\[ x^2 - dy^2 = 1. \]

Note that

\[ \alpha \quad \bar{\alpha} \quad -\bar{\alpha} \quad \text{and} \quad -\alpha \]

are also solutions. Replacing \( \alpha \) by one of these four solutions, we may assume that the coefficients of \( \alpha \) are positive and it suffices to find a natural number \( n \) such that

\[ \alpha = \delta^n. \]

Note that \( \delta \leq \alpha \) by minimality of \( \delta \). Let \( n \) be the largest natural number such that

\[ \delta^n \leq \alpha < \delta^{n+1}. \]

Let

\[ \beta = \frac{\alpha}{\delta^n}. \]

By assumption

\[ 1 \leq \beta < \delta. \]

We have

\[ N(\beta) = N(\alpha)N(\delta^{-n}) = 1. \]

Thus \( \beta \) is also a solution of

\[ x^2 - dy^2 = 1. \]

It follows that \( \beta = 1 \) by minimality of \( \delta \). But then

\[ \alpha = \delta^n. \]
7. (20pts) (i) If $|pq - rs| = 1$ then $p/q$ and $r/s$ are adjacent in $\mathcal{F}_n$, for

$$\max(q, s) \leq n < q + s$$

and they are separated by the single element $(p + r)/(q + s)$ in $\mathcal{F}_{q+s}$.

We may assume that $p/q < r/s$ so that $qr - ps = 1$. Let

$$f: [0, \infty] \longrightarrow \left[\frac{p}{q}, \frac{r}{s}\right]$$

given by

$$f(t) = \frac{p + tr}{q + ts}.$$

Then $f$ is a monotonic increasing function, so that $f$ is a bijection. It is clear that $f$ induces a bijection between the rational points of both intervals. Let $t = u/v$. Then

$$f\left(\frac{u}{v}\right) = \frac{pv + ur}{qv + us}.$$

As

$$q(vp + ur) - p(vq + us) = u(qr - ps) = u$$

$$s(vp + ur) - r(vq + us) = v(ps - qr) = -v,$$

it follows that $vp + ur$ is coprime to $vq + us$, thus $f(u/v)$ is expressed in its lowest terms.

It is then clear that the rational number between $p/q$ and $r/s$ with the smallest denominator is given by $u = v = 1$. 

(ii) If $p/q$ and $r/s$ are adjacent in $F_n$ for some $n$ then $|ps - qr| = 1$.

We prove this by induction on $n$. If $n = 1$ then $q = s = 1$ and $p$ and $r = p \pm 1$ are adjacent integers. The result is clear in this case.

If we go from $n$ to $n + 1$ we just need to check the result for the integers we just added. If $p/q$ and $r/s$ are adjacent in $F_n$ then we can only add

$$\frac{p + r}{q + s}$$

between them in $F_n$. We have

$$|(p + r)q - (q + s)p| = 1$$

and

$$|r(q + s) - s(p + r)| = 1,$$

and this completes the induction.
8. (10pts) *Find all of the best approximations of \( \frac{339}{62} \).

We have

\[ \xi = \frac{339}{62} = 5 + \frac{29}{62}. \]

Thus \( a_0 = 5 \) and

\[ \xi_1 = \frac{62}{29} = 2 + \frac{4}{29}. \]

Thus \( a_2 = 2 \) and

\[ \xi_2 = \frac{29}{4} = 7 + \frac{1}{4}. \]

Thus \( a_2 = 7 \) and \( a_3 = 4 \). It follows that

\[ \frac{339}{62} = [5; 2, 7, 4]. \]

The convergents are:

\[ \frac{5}{1}, \frac{11}{2}, \frac{82}{15} \]

and \( \frac{339}{62} \)

and these are the best approximations.
9. (10pts) Show that if $\xi$ and $\eta$ have the same initial partial quotients $a_0, a_1, a_2, \ldots, a_n$ and $\xi < \theta < \eta$ then $\theta$ has the same initial partial quotients.

As $\xi < \theta < \eta$, it follows that

$$a_0 = \lfloor \xi \rfloor \leq \lfloor \theta \rfloor \leq \lfloor \eta \rfloor = a_0.$$ 

Thus

$$a_0 = \lfloor \theta \rfloor.$$

Moreover, it then follows that

$$\{ \xi \} < \{ \theta \} < \{ \eta \}.$$ 

Taking reciprocals

$$\eta_1 < \theta_1 < \xi_1.$$ 

As the partial quotients of $\eta_1$ and $\xi_1$ are $a_1, a_2, \ldots, a_n$, we are done by induction on $n$. 
Bonus Challenge Problems

10. (10pts) Describe all solutions of $x^2 - dy^2 = 4$.

See Proposition 12.5.
11. (10pts) Show that if \( \xi \) is irrational then there are infinitely many rational numbers \( p/q \) such that

\[
\left| \xi - \frac{p}{q} \right| < \frac{1}{\sqrt{5q^2}}.
\]

See the proof of Theorem 15.5.
12. (10pts) Show that $\xi$ is a quadratic irrational if and only if its continued fraction is eventually periodic.

See the proof of Theorem 19.1.
13. (10pts) Prove Legendre’s theorem.
    See the proof of Theorem 7.1.