FIRST MIDTERM
MATH 104C, UCSD, SPRING 18

You have 80 minutes.
There are 5 problems, and the total number of points is 60. 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>15</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>10</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>10</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>60</td>
<td></td>
</tr>
</tbody>
</table>
1. (15pts) (i) Give the definition of a primitive representation as a sum of two squares.

The representation \( n = a^2 + b^2 \) as a sum of two squares is primitive if \((a, b) = 1\).

(ii) Give the definition of an involution.

A function \( f: S \rightarrow S \) is an involution if it is its own inverse.

(iii) Give the definition of the norm of a Gaussian integer.

If \( \alpha = a + ib \) the norm of \( \alpha \) is

\[ \alpha \bar{\alpha} = a^2 + b^2. \]
2. (15pts) (i) If \(a, b, c\) and \(d\) are real numbers then show that
\[
(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2.
\]

If we expand the LHS we get
\[
(a^2 + b^2)(c^2 + d^2) = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2
\]
which is the same as the expansion of the RHS
\[
(ac + bd)^2 + (ad - bc)^2 = a^2c^2 + 2abcd + b^2d^2 + a^2d^2 - 2abcd + b^2c^2
\]
\[
= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2.
\]

(ii) If \(n\) has a primitive representation as a sum of two squares and \(p|n\) then show that \(-1\) is a quadratic residue of \(p\).

If \(a^2 + b^2 = n\) and \((a, b) = 1\) then \(a^2 + b^2 \equiv 0 \mod p\). If \(p|b\) then \(p|a\), a contradiction. Thus \(b\) is invertible modulo \(p\) and so \((ac)^2 = -1\) \mod \(p\), where \(c\) is the inverse of \(b\). Thus \(-1\) is a quadratic residue of \(p\).

(iii) If \(n\) is a sum of two squares and \(p \equiv 3 \mod 4\) then show that \(n = p^{2k}m\) where \(m\) is coprime to \(p\).

Suppose that \(n = a^2 + b^2\). Let \(d = (a, b)\). Then \(a = da_1\), \(b = db_1\) and \(d^2\) divides \(n\), so that \(n = d^2m\). As \(a_1^2 + b_1^2 = m\) is a primitive representation of \(m\) and \(-1\) is not a quadratic residue of \(p\), it follows that \(m\) is coprime to \(p\).
If \(d = p^k e\), where \(e\) is coprime to \(p\) then \(n = p^{2k}m\).
3. (10pts) If $a$ is not divisible by $m$ and $1 < \lambda < m$ then show that we can find $1 \leq x < \lambda$ and $1 \leq |y| \leq m/\lambda$ such that $ax \equiv y \mod m$.

We can either apply Brauer-Reynolds or prove the result directly. We prove the result directly.

We first prove that we can find $|x| < \lambda$ and $|y| \leq m/\lambda$ such that $ax \equiv y \mod m$, where $x$ and $y$ are not both zero.

Consider the possible values of $ax - y$ modulo $m$. There are $m$ different possible values. Suppose that $0 \leq x < \lambda$ and $0 \leq y \leq m/\lambda$. Let

$$
\mu = \begin{cases} 
\lfloor \lambda \rfloor + 1 & \text{if } \lambda \text{ is not an integer} \\
\lambda & \text{if } \lambda \text{ is an integer.}
\end{cases}
$$

Then $x$ can take on $\mu$ different values and $y$ can take on $\lfloor m/\lambda \rfloor + 1$ possible different values. As

$$
\mu + \lfloor m/\lambda \rfloor + 1 > m,
$$

it follows that there are two vectors $(x_i, y_i)$ such that

$$
av_1 - y_1 \equiv ax_2 - 2y_2 \mod m.
$$

The difference $(x = x_1 - x_2, y = y_1 - y_2)$ has the property that

$$
av \equiv y \mod m,
$$

where $x$ and $y$ are not both zero. But if one is zero then the other is zero and so neither is zero. Therefore we have $1 \leq |x| < \lambda$ and $1 \leq |y| \leq m/\lambda$. If $x < 0$ then replacing $(x, y)$ by $(-x, -y)$ gives the result.
4. (10pts) If $p$ is an odd prime, $1 \leq g \leq p$, $h = \lfloor p/g \rfloor$ and $r$ is a quadratic residue of $p$ then show that one of the numbers $1^2, 2^2, 3^3, \ldots, h^2$ is congruent to one of the numbers $r, 2^2r, \ldots, (g-1)^2r$, modulo $p$.

By assumption there is a number $a$ such that $a^2 \equiv r \mod p$. By 3 we can find $x$ and $y$ such that $ax \equiv y \mod p$, where $1 \leq x \leq g$ and $1 \leq |y| \leq p/g$. First note that if the integer $|y| \leq p/g$ then in fact $|y| \leq h$.

Then

$$y^2 = (-y)^2$$

$$\equiv a^2 x^2$$

$$\equiv r x^2 \mod p.$$ 

On the other hand $1 \leq x \leq g - 1$ and either $1 \leq y \leq h$ or $1 \leq -y \leq h$. 
5. (10pts) Show that every positive prime \( p > 2 \) of which \(-3\) is a quadratic residue can be represented in the form \( x^2 + 3y^2 \).

By assumption we may find \( a \) such that
\[
a^2 \equiv -3 \mod p.
\]
By 3 we may find \( x \) and \( y \) such that
\[
x \equiv ay \mod p,
\]
where \( 1 \leq |x| \leq \sqrt{p} \) and \( 1 \leq y < \sqrt{p} \). As \( p \) is prime, we must have\( 1 \leq |x| < \sqrt{p} \). Note that
\[
x^2 + 3y^2 \equiv 0 \mod p.
\]
Possibly replacing \( x \) by \(-x\) we have \( 1 \leq y < \sqrt{p} \). Thus
\[
x^2 + 3y^2 = Ap,
\]
where \( A = 1, 2 \) or \( 3 \). If \( A = 1 \) then we are done. If \( A = 2 \) then we have
\[
x^2 + 3y^2 = 2p.
\]
x and \( y \) must have the same parity. If \( x \) and \( y \) are both even then the LHS is divisible by 4, a contradiction. If \( x \) and \( y \) are both odd then the LHS is still divisible by 4, a contradiction. Thus the case \( A = 2 \) is not possible.
Suppose \( A = 3 \). Note that if \( p = 3 \) we may take \( x = 0 \) and \( y = 1 \). Thus we may assume that \( p > 3 \). We have
\[
x^2 + 3y^2 = 3p.
\]
It follows that \( x \) is divisible by 3. Suppose that \( x = 3z \). Then
\[
9z^2 + 3y^2 = 3p.
\]
Dividing both sides by 3 we get
\[
3z^2 + y^2 = p.
\]
Bonus Challenge Problems

6. (10pts) Derive an expression for $p_2(n)$.

See lecture 2.
7. (10pts) Show that every natural number is a sum of four squares.

See lecture 5.