Math 104A - Fall 2014 - Midterm I

Name: __________________________________________

Student ID: _________________________________

Instructions:

Please print your name, student ID.

During the test, you may not use books, calculators or telephones.

Read each question carefully, and show all your work. Answers with no explanation will receive no credit, even if they are correct.

There are 5 questions which are worth 10 points each. You have 50 minutes to complete the test.

<table>
<thead>
<tr>
<th>Question</th>
<th>Score</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>10</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>10</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>10</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>10</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>10</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td><strong>50</strong></td>
</tr>
</tbody>
</table>
Problem 1. [10 points.]

Find the values of \( m \in \mathbb{Z} \) for which the linear equation

\[ 4188x + 1011y = m \]

has integer solutions \((x, y)\). For the values of \( m \) you found, write down all solutions of the equation.

Solution: We first run the Euclidean algorithm. We have

\[
\begin{align*}
4188 &= 4 \cdot 1011 + 144 \\
1011 &= 7 \cdot 144 + 3 \\
144 &= 3 \cdot 48 + 0.
\end{align*}
\]

The last non-zero remainder is \( 3 = \gcd(4188, 1011) \).

The equation \( 4188x + 1011y = m \) has solutions if and only if \( 3|m \).

We next solve the equation. We begin by finding solutions to \( 4188x_0 + 1011y_0 = 3 \). This is obtained from the Euclidean algorithm. We have

\[
3 = 1011 - 7 \cdot 144 = 1011 - 7 \cdot (4188 - 4 \cdot 1011) = 29 \cdot 1011 - 7 \cdot 4188.
\]

Thus a particular solution is

\[
x_0 = -7, \quad y_0 = 29.
\]

A particular solution of \( 4188x + 1011y = m \) is

\[
x_1 = -7 \cdot \frac{m}{3}, \quad y_1 = 29 \cdot \frac{m}{3}.
\]

All other solutions are of the form

\[
x = x_1 + \frac{1011}{3} t, \quad y = y_1 - \frac{4188}{3} t \quad \Rightarrow \quad x = -\frac{7m}{3} + 337t, \quad y = \frac{29m}{3} - 1396t, \quad t \in \mathbb{Z}.
\]
Problem 2. [10 points.]

Consider the ring \( R = \mathbb{Z}[\sqrt{-29}] = \{a + b\sqrt{-29} : a, b \in \mathbb{Z}\} \).

(i) Prove that \( 5 \in R \) is irreducible.
(ii) Show that \( 5 \in R \) is not prime.
(iii) Conclude that \( R \) is not a unique factorization domain.

Solution:

(i) Assume that \( 5 \) is reducible, so that \( 5 = \alpha \cdot \beta \) where \( \alpha, \beta \) are not units. Taking norms we obtain
\[
25 = N(5) = N(\alpha) \cdot N(\beta).
\]
This shows that \( N(\alpha) = N(\beta) = 5 \) or else either \( N(\alpha) = 1 \) or \( N(\beta) = 1 \). If \( \alpha = a + b\sqrt{-29} \)
then
\[
N(\alpha) = 5 \implies a^2 + 29b^2 = 5 \implies b^2 \leq \frac{5}{29} \implies b = 0 \implies a^2 = 5
\]
which cannot happen. Thus either \( N(\alpha) = 1 \) or \( N(\beta) = 1 \). In the first case, it follows with the above notation
\[
a^2 + 29b^2 = 1 \implies b = 0 \implies a = \pm 1 \implies \alpha = \pm 1
\]
which is a unit, which is not allowed. The case \( N(\beta) = 1 \) implies \( \beta \) is a unit, also not allowed. These contradictions show that our assumption is wrong, hence \( 5 \) is irreducible.

(ii) Note that
\[
(1 + \sqrt{-29})(1 - \sqrt{-29}) = 30
\]
is divisible by 5. If 5 were a prime, then by definition, we’d have
\[
5|1 + \sqrt{-29} \text{ or } 5|1 - \sqrt{-29}.
\]
Both these statements are impossible. For instance, in the first case, we could write
\[
5(a + b\sqrt{-29}) = 1 + \sqrt{-29}
\]
for some integers \( a, b \). We find \( 5a = 1 \implies a = \frac{1}{5} \) which is not an integer. This contradiction shows that 5 is not a prime.

(iii) In a UFD, all irreducible elements are prime. However this is not the case for \( R \) by (i) and (ii), hence \( R \) is not a UFD.
Problem 3. [10 points.]

Let $A$ be any positive integer, and let $B$ be an integer obtained from $A$ by permuting its digits. Show that

$$9 \mid A \iff 9 \mid B.$$ 

(i) Prove that 9 divides $10^k - 1$ for all $k \geq 0$.

(ii) Use (i) to show that 9 divides $A$ if and only if 9 divides the sum of digits of $A$.

(iii) Use (ii) to conclude the proof.

Solution:

(i) We have

$$10^k - 1 = 10 \ldots 0 - 1 = 99 \ldots 9 = 9 \cdot 11 \ldots 1.$$ 

(ii) Write $a_0, a_1, \ldots, a_n$ for the digits of $A$ in this order. Let $s(A)$ be the sum of digits of $A$. Then

$$A - s(A) = (10^n a_0 + 10^{n-1} a_{n-1} + \ldots + a_n) - (a_0 + a_1 + \ldots + a_n)$$

$$= a_0 (10^n - 1) + a_1 (10^{n-1} - 1) + \ldots + a_1 (10 - 1) + a_0 (1 - 1).$$

By (i), we know that $9 \mid 10^k - 1$ for all $k$, hence 9 divides each of the terms of the above expression. Thus

$$9 \mid A - s(A).$$

This implies

$$9 \mid A \iff 9 \mid s(A).$$

(iii) Since the digits of $B$ are obtained from those of $A$ by permutation, it follows that $s(A) = s(B)$. Thus by applying (ii) twice we have

$$9 \mid A \iff 9 \mid s(A) \iff 9 \mid s(B) \iff 9 \mid B.$$
Problem 4. [10 points.]

Let $a, b, c, n$ be positive integers, such that $c < 2^n$. Show that if

$$a^n | cb^n \text{ then } a | b.$$ 

Solution: If $a = 1$ there is nothing to prove.

Assume $a > 1$, and consider the prime factorization of $a$. We show that if $p$ is any prime appearing in the prime factorization of $a$ with exponent equal to $e$, then it appears in the prime factorization of $b$ as well with exponent at least equal to $e$. This shows that $a | b$. (Indeed, $b/a$ is product of primes appearing with non-negative exponents, hence it is an integer, hence $a | b$.)

Assume that $p$ appears in $b$ with exponent $e' < e$, possibly equal to 0. Then,

$$p^e | a \implies p^{ne} | a^n \implies p^{ne} | b^n c.$$ 

But $p$ appears in the factorization of $b^n$ with exponent $ne'$, hence it must appear in the factorization of $c$ with exponent at least

$$ne - ne' = n(e - e') \geq n.$$ 

Thus

$$p^n | c \implies p^n \leq c.$$ 

But $p \geq 2$ being prime hence $c \geq 2^n$ contradicting our hypothesis. Therefore, our assumption $e' < e$ is false, hence $e' \geq e$, as claimed above.
Extra credit. [10 points.]

Let \( a, b, c \) be integers such that \((a,b) = (b,c) = (c,a) = 1\). Show that \( N = 2abc - bc - ac - ab \) cannot be written in the form

\[ N = bcx + acy + abz \]

for integers \( x, y, z \geq 0 \).

*Hint: This is an extension of the homework problem about integers representable as \( ax + by \) with \( x, y \geq 0 \).*

**Solution:** Assume

\[
2abc - bc - ac - ab = bcx + acy + abz \implies bc(x + 1) + ac(y + 1) + ab(z + 1) = 2abc
\]

\[
\implies bc(x + 1) < 2abc \implies x + 1 < 2a.
\]

On the other hand

\[
bc(x + 1) + a[ac(y + 1) + ab(z + 1)] = 2abc \implies a|bc(x + 1) \implies a|x + 1.
\]

This uses \( (a,bc) = 1 \) which is a consequence of \( (a,b) = 1 \) and \( (a,c) = 1 \). (Indeed, \( a,b \) have no common factors, \( a,c \) have no common factors, hence \( a \) and \( bc \) have no common factors as well.) Since \( 1 \leq x + 1 < 2a \), we must have \( x + 1 = a \implies x = a - 1 \). Similarly, \( y = b - 1 \), \( z = c - 1 \). Substituting into the equation we find

\[
2abc - bc - ac - ab = bc(a - 1) + ac(b - 1) + ab(c - 1) = 3abc - bc - ac - ab \implies abc = 0
\]

which is a contradiction.