Name:

- This is a closed-book, closed-notes exam. No electronic aids are allowed.

- Read each questions carefully. Proof questions should be written out with all the details. You may use results proven in class, but you should explicitly cite the results being used.

- Answer the questions in the spaces provided on the question sheets. If you need extra room, use the back sides of each page. If you need extra paper, make sure to write your name on it and attach it to this exam. Do not unstaple or detach pages from this exam.

<table>
<thead>
<tr>
<th>Section</th>
<th>Points</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>22</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>5 (bonus)</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Grand Total</td>
<td>50</td>
<td></td>
</tr>
</tbody>
</table>
1. Section 1

Answer the following questions and explain your solution.

Exercise 1.1. (5 points) Can there be infinitely many primes of the form \(a^2 - b^2\) for some \(a, b \in \mathbb{Z}\)?

Solution:

YES. In fact, \(a^2 - b^2 = (a + b)(a - b)\), and an integer of this form can be prime if, and only if, of the two factors is equal to 1. If \(a - b = 1\), then \(a = b + 1\) and \(a^2 - b^2 = 2b + 1\). There are infinitely many \(b \in \mathbb{Z}\) such that \(2b + 1\) is a prime (in fact, all primes except 2 are odd, and thus of the form \(2b + 1\) for some \(b \in \mathbb{Z}\).

Exercise 1.2. (5 points) Are there infinitely many primes \(p\) such that \(p + 2, p + 6, p + 8, p + 14\) are all prime?

(Hint: you can assume that \(p > 5\). Consider the consecutive numbers \(p, p + 1, p + 2, p + 3\) and \(p + 4\).)

Solution:

NO. We can assume that \(p > 5\). Let us consider the following consecutive numbers: \(p, p + 1, p + 2, p + 3\) and \(p + 4\). One of them will be divisible by 5. Here are the five cases:

- \(5|p\). This is not possible because \(p > 5\) is a prime.
- If \(5|p + 1\), then \(5|p + 6\) and thus \(p + 6\) is not a prime.
- If \(5|p + 2\), then \(p + 2\) is not a prime.
- If \(5|p + 3\), then \(5|p + 8\) and thus \(p + 8\) is not a prime.
- If \(5|p + 4\), then \(5|p + 14\) and thus \(p + 14\) is not a prime.

Summarizing, in no case the numbers \(p, p + 2, p + 6, p + 8, p + 14\) can be simultaneously prime.
Answer the following questions and explain your solution.

**Exercise 2.1.** (8 points) Show that there cannot exist two integers $a, b$ such that $(a, b) = 3$ and $a + b = 65$.
(Hint: $65 = 5 \times 13$ but $3 \nmid 65$.)

**Solution:**

Note that $65 = 5 \times 13$. If $(a, b) = 3$, then $3|a$ and $3|b$. This implies that $3|(a + b)$ because $a + b$ is an integral linear combination of $a$ and $b$. However $3 \nmid 65$, and thus such $a$ and $b$ cannot exist.
3. Section 3

Answer the following questions and explain your solution.

**Exercise 3.1.** (10 points) Let $a, b, c, d \in \mathbb{N}$. If $b \neq d$ and $(a, b) = (c, d) = 1$, prove that
\[
\frac{a}{b} + \frac{c}{d} \notin \mathbb{Z}.
\]

Hint: recall from the practice midterm that if $a, b$ and $c$ are integers such that $(a, b) = 1$ and $a|bc$, then $a|c$.

**Solution:**
Assume, for a contradiction, that $\frac{a}{b} + \frac{c}{d}$ is an integer. Then, by finding a common denominator, we must have $bd|ad + bc$. Let $e$ be an integer for which $ad + bc = bde$. Then $ad = b(de - c)$ so that $b|ad$. Since $(a, b) = 1$, we obtain that $b|d$ (using the hint). A similar argument using $d|bc$ and $(c, d) = 1$ yields $d|b$. Since $b$ and $d$ are positive integers, $d = b$, a contradiction.
4. Section 4

Determine whether the statements are true or false. If the statement is true, then give a short proof. If it is false, then give a counterexample.

Exercise 4.1. (4 points) If \( a \equiv b \pmod{m} \) and \( c \neq 0 \), then \( ac \equiv bc \pmod{mc} \).

Solution:

True. We have

\[
a \equiv b \pmod{m} \Leftrightarrow m \mid (a - b) \Rightarrow a - b = md
\]

for some \( d \in \mathbb{Z} \). Let us multiply the latter by \( c \) with \( c \neq 0 \). We get \( ca - cb = cmd \). Hence

\[
\Rightarrow cm \mid (ac - bc) \Rightarrow ac \equiv bc \pmod{mc}.
\]

Exercise 4.2. (4 points) If \( a \equiv b \pmod{m} \) and \( d = (a, b) \), then \( \frac{a}{d} \equiv \frac{b}{d} \pmod{m} \).

Solution:

False. Let \( a = 2 \), \( b = 8 \) and \( m = 6 \). Then

\[
2 \equiv 8 \pmod{6}
\]

since \( 6 \mid (2 - 8) \). However,

\[
1 \not\equiv 4 \pmod{6}
\]

since \( 6 \not\mid (1 - 4) \).
Exercise 4.3. (4 points) If $p$ is a prime and $p|a^3$, then $p|a$.

Solution:

We saw in class that if $p$ is a prime and $p|ab$, then $p|a$ or $p|b$. This is Euclid’s lemma. Apply this to $a = a$ and to $b = a^2$. Then $p|a$ and in this case we are done, or $p|a^2$. In this second case, apply the above result to $a = a$ and $b = a$. We get that $p|a$ and we really are done.

Exercise 4.4. (10 points) Prove that there are infinitely many primes in $\mathbb{N}$ (Euclid’s theorem).

Solution:

See lecture notes.

Exercise 4.5. (5 points - bonus) What is Dirichlet’s theorem of primes in arithmetic progressions? You can state it or explain it.

Solution:

See lecture notes.