Problem 1: (a) Use mathematical induction to show that

\[ \prod_{i=2}^{n} \left(1 - \frac{1}{i^2}\right) = \frac{n+1}{2n} \]

for every \( n \geq 2 \). Recall that \( \prod_{i=2}^{n} \left(1 - \frac{1}{i^2}\right) \) denotes the product \((1 - \frac{1}{4})(1 - \frac{1}{9}) \ldots (1 - \frac{1}{n^2})\).

(b) Let \( a_1, a_2, a_3, a_4, \ldots \) be the integer sequence defined recursively by \( a_1 = 1, a_2 = 8, \) and \( a_n = a_{n-1} + 2a_{n-2} \) for every \( n \geq 3 \). Use mathematical induction to show that

\[ a_n = 3 \cdot 2^{n-1} + 2(-1)^n \]

for every \( n \geq 1 \).

Solution: (a) Base case: \( n = 2 \). The product on the left hand side of the formula has only one factor, \( 1 - 1/4 \), and the right hand side is \( 3/4 \). Thus the right hand side and the left hand side are equal when \( n = 1 \).

Induction step: Suppose \( \prod_{i=2}^{n} \left(1 - \frac{1}{i^2}\right) = \frac{n+1}{2n} \) for some \( n \geq 2 \). We want to show that the same formula holds when we replace \( n \) by \( n + 1 \).

Multiply both sides by \( 1 - \frac{1}{(n+1)^2} \):

\[ \left(1 - \frac{1}{(n+1)^2}\right) \prod_{i=2}^{n} \left(1 - \frac{1}{i^2}\right) = \left(1 - \frac{1}{(n+1)^2}\right) \frac{n+1}{2n}. \]

The left hand side is \( \prod_{i=2}^{n+1} \left(1 - \frac{1}{i^2}\right) \), which is the quantity we are interested in. It remains to show that the right hand side is \( \frac{(n+1) + 1}{2(n+1)} \), i.e., \( \frac{n+2}{2(n+1)} \). Indeed,

\[ \left(1 - \frac{1}{(n+1)^2}\right) \frac{n+1}{2n} = \frac{(n+1)^2 - 1}{(n+1)^2} \cdot \frac{n+1}{2n} = \frac{n^2 + 2n + 1}{n+1} \cdot \frac{1}{2n} = \frac{n+2}{2(n+1)}, \]

as desired. This completes the induction step.

(b) Let \( b_n = 3 \cdot 2^{n-1} + 2(-1)^n \). Our goal is to show that \( a_n = b_n \) for every \( n \geq 1 \).

We will use strong induction on \( n \). Consider two base cases: \( n = 1 \) and \( n = 2 \). Using the formula for \( b_n \), we see that \( b_1 = 3 \cdot 2^{-1} + 2 \cdot (-1)^1 = 3 - 2 = 1 = a_1 \) and \( b_2 = 3 \cdot 2^1 + 2 \cdot (-1)^2 = 3 \cdot 2 + 2 = 8 = a_2 \).

For the induction step, assume that \( n \geq 3 \). The induction assumption is that \( a_m = b_m \) for every \( 1 \leq m \leq n - 1 \). We want to show that \( a_n = b_n \). Setting \( m = n - 2 \) and \( n - 1 \), we obtain \( a_{n-2} = b_{n-2} \) and \( a_{n-1} = b_{n-1} \). Thus \( a_n = a_{n-1} + 2a_{n-2} = b_{n-1} + 2b_{n-2} \). Using the formula for \( b_{n-2} \) and \( b_{n-1} \), we see that

\[
\begin{align*}
b_{n-1} + 2b_{n-2} &= 3 \cdot 2^{n-2} + 2 \cdot (-1)^{n-1} + 2(3 \cdot 2^{n-3} + 2 \cdot (-1)^{n-2}) \\
&= 2^{n-3}(3 \cdot 2 + 3 \cdot 2) + 2 \cdot (-1)^{n-1} \cdot 1 \\
&= 3 \cdot 2^{n-1} + 2 \cdot (-1)^n = b_n,
\end{align*}
\]

as desired.
Problem 2: (a) Find all integers \( x \) satisfying \( 84x \equiv 5 \pmod{49} \).
(b) Find all integers \( y \) satisfying \( 12y \equiv 4 \pmod{14} \).

Solution: (a) \( \gcd(84, 49) = 7 \) does not divide 5, so this congruence has no solutions.
(b) \( \gcd(12, 14) = 2 \) divides 4, so there will be solutions. As we showed in class, \( 12y \equiv 4 \pmod{14} \) is equivalent to \( 6y \equiv 2 \pmod{7} \). Since \( 6 \equiv -1 \pmod{7} \), this is the same as \( -y \equiv 2 \pmod{7} \) or equivalently, \( y \equiv -2 \pmod{7} \) or \( y \equiv 5 \pmod{7} \). In summary, \( y = 5 + 7n \), where \( n \) is an integer.

Problem 3: Consider the linear Diophantian equation \( 13x + 17y = 1000 \).
(a) Find the general solution \((x, y)\) to this equation, i.e., a formula describing all integer solutions.
(b) How many pairs of positive integers \((x, y)\) satisfy this equation?

Solution: (a) A particular solution to \( 13x + 17y = 4 \) is \((-1, 1)\). Multiplying by 250, we see that \((-250, 250)\) is a particular solution to \( 13x + 17y = 1000 \). A general solution to \( 13x + 17y = 1000 \) is thus
\[
x = -250 + 17t \quad \text{and} \quad y = 250 - 13t,
\]
where \( t \) runs over the integers.
(b) We want to choose \( t \) so that \( x > 0 \) and \( y > 0 \). That is, \( 17t > 250 \) and \( 13t < 250 \).
Thus there are five solutions \((x, y)\) with \( x, y \) positive integers, corresponding to \( t = 15, 16, 17, 18, 19 \).

I did not ask you to list the solutions on the exam, but I will list them here, so that you can see more clearly what is going on. Every time we increase \( t \) by 1, we add 17 to \( x \) and subtract 13 from \( y \).
\[
t = 15: \quad x = -250 + 17 \cdot 15 = 5, \quad \text{and} \quad y = 250 - 13 \cdot 15 = 55.
\]
\[
t = 16: \quad x = 22 \quad \text{and} \quad y = 42,
\]
\[
t = 17: \quad x = 39 \quad \text{and} \quad y = 29,
\]
\[
t = 18: \quad x = 56 \quad \text{and} \quad y = 16,
\]
\[
t = 19: \quad x = 73 \quad \text{and} \quad y = 3.
\]

Problem 4: Recall that \( n \) is called a perfect cube if \( n = x^3 \) for some positive integer \( x \).
For example, 1, 8, 27, 64 and 125 are perfect cubes, where as 4, 5, 12, 20 and 100 are not.
(a) Let \( n = p_1^{d_1} \cdots p_r^{d_r} \), where \( p_1, \ldots, p_r \) are distinct primes and \( d_1, \ldots, d_r \) are non-negative integers. Complete the following statement and prove it.
\[
n \text{ is a perfect cube if and only if } d_1, \ldots, d_r \text{ are } \ldots
\]
(b) Suppose \( n \) be a positive integer. Show that if \( n^2 \) is a perfect cube, then \( n \) is also a perfect cube.
(c) Suppose \( a, b \) and \( c \) are positive integers. Show that if \( ab, ac \) and \( bc \) are perfect cubes, then \( a, b \) and \( c \) are also perfect cubes.

Solution: (a) \( n \) is a perfect cube if and only if \( d_1, \ldots, d_r \) are all divisible by 3.
Proof: If \( n = x^3 \) is a perfect cube, write \( x = q_1^{e_1} \cdots q_s^{e_s} \), where \( q_1, \ldots, q_s \) are distinct primes and \( e_1, \ldots, e_s \geq 1 \). Then \( n = x^3 = q_1^{3e_1} \cdots q_s^{3e_s} \). By the Fundamental Theorem of
Arithmetic, the prime decomposition of $n$ is unique. Thus the non-zero exponents among $d_1, \ldots, d_r$ are $3e_1, \ldots, 3e_r$, and each of them is divisible by 3.

Conversely, suppose each of the exponents $d_1, \ldots, d_r$ is divisible by 3. Then $d_1 = 3e_1$, $\ldots, d_r = 3e_r$ for some non-negative integers $e_1, \ldots, e_r$. Then $x = p_1^{e_1} \cdots p_r^{e_r}$ is a positive integer, and $n = x^3$ is a perfect cube.

(b) Suppose $n^2 = p_1^{2d_1} \cdots p_r^{2d_r}$ is a perfect cube. Then by part (a), $2d_1, \ldots, 2d_r$ are all divisible by 3. In other words, $2d_i \equiv 0 \pmod{3}$ for $i = 1, \ldots, r$. Since $\gcd(2, 3) = 1$, this is only possible if each $d_i \equiv 0 \pmod{3}$. By part (a), we conclude that $n$ is a perfect cube.

(c) Write $a = p_1^{d_1} \cdots p_r^{d_r}$, $b = p_1^{e_1} \cdots p_r^{e_r}$ and $c = p_1^{f_1} \cdots p_r^{f_r}$. Since $p_1, \ldots, p_r$ are distinct primes and $d_1, \ldots, d_r, e_1, \ldots, e_r, f_1, \ldots, f_r \geq 0$. Since

\[ ab = p_1^{d_1+e_1} \cdots p_r^{d_r+e_r}, \]
\[ ac = p_1^{d_1+f_1} \cdots p_r^{d_r+f_r}, \]
\[ bc = p_1^{e_1+f_1} \cdots p_r^{e_r+f_r} \]

are perfect cubes, part (a) tells us that,

\[ d_i + e_i \equiv d_i + f_i \equiv e_i + f_i \equiv 0 \pmod{3} \]

for every $i = 1, \ldots, r$. Thus

\[ 2(d_i + e_i + f_i) \equiv (d_i + e_i) + (d_i + f_i) + (e_i + f_i) \equiv 0 \pmod{3}. \]

Since $2 \equiv -1 \pmod{3}$, we conclude that $d_i + e_i + f_i \equiv 0 \pmod{3}$ for each $i$. Now

\[ d_i = (d_i + e_i + f_i) - (e_i + f_i) \equiv 0 - 0 \equiv 0 \pmod{3}. \]

Similarly, $e_i \equiv 0 \pmod{3}$ and $f_i \equiv 0 \pmod{3}$ for each $i$. Using part (a), we conclude that $a, b$ and $c$ are perfect cubes.

**Problem 5:** Find all integers $x$ between 0 and 500 satisfying the following system of congruences

\[
\begin{align*}
x &\equiv 2 \pmod{3}, \\
x &\equiv 3 \pmod{5}, \\
x &\equiv 4 \pmod{7}.
\end{align*}
\]

**Solution:** Recall that by the Chinese Remainder Theorem,

\[ x \equiv a_1y_1N_1 + a_2y_2N_2 + a_3y_3N_3 \pmod{N} \]

where

\[
\begin{align*}
a_1 &= 2, \quad a_2 = 3, \quad a_3 = 4, \\
N &= 3 \cdot 5 \cdot 7 = 105, \\
N_1 &= 5 \cdot 7 = 35, \\
N_2 &= 3 \cdot 7 = 21, \\
N_3 &= 3 \cdot 5 = 15, \\
y_1 &\equiv (N_1)^{-1} \equiv (-1)^{-1} \equiv -1 \pmod{3}, \\
y_2 &\equiv (N_2)^{-1} \equiv 1^{-1} \equiv 1 \pmod{5}, \text{ and} \\
y_3 &\equiv (N_3)^{-1} \equiv 1 \pmod{7}.
\end{align*}
\]

Putting it all together,

\[ x \equiv 2 \cdot (-1) \cdot 35 + 3 \cdot 1 \cdot 21 + 4 \cdot 1 \cdot 15 \equiv -70 + 63 + 60 \equiv 53 \pmod{105}. \]
In other words, $x = 53 + 105t$.

The condition that $0 \leq x \leq 500$ is satisfied only when $t = 0, 1, 2, 3$ or $4$, so that $x = 53, 158, 263, 368$ or $473$.

**Problem 6:** How many integers $x$ between 1 and $n$ satisfy $x^2 \equiv 1 \pmod{n}$, if

(a) $n = 8$?
(b) $n = pq$, where $p$ and $q$ are distinct odd primes?
(c) $n = 8p$, where $p$ is an odd prime?

**Hint:** In parts (b) and (c) use the Chinese Remainder Theorem.

**Solution:**

(a) Clearly any $x$ satisfying $x^2 \equiv 1 \pmod{8}$ has to be odd. The only possibilities are $x = 1, 3, 5, 7 \pmod{8}$. We can square each of them easily and find that $x^2 \equiv 1 \pmod{8}$ for each of them. (Check!) Thus there are four solutions.

(b) By the Chinese Remainder Theorem (CRT), $x^2 \equiv 1 \pmod{pq}$ if and only if $x^2 \equiv 1 \pmod{p}$ and $x^2 \equiv 1 \pmod{q}$. As we showed in class, the first congruence has two solutions, $x \equiv \pm 1 \pmod{p}$. Similarly $x^2 \equiv 1 \pmod{q}$ is equivalent to $x \equiv \pm 1 \pmod{q}$. In summary, $x^2 \equiv 1 \pmod{pq}$ if and only if $x$ satisfies one of the following systems

$$\begin{align*}
x \equiv 1 & \pmod{p}, \\
x \equiv 1 & \pmod{q},
\end{align*}$$

or

$$\begin{align*}
x \equiv -1 & \pmod{p}, \\
x \equiv 1 & \pmod{q},
\end{align*}$$

or

$$\begin{align*}
x \equiv 1 & \pmod{p}, \\
x \equiv -1 & \pmod{q},
\end{align*}$$

or

$$\begin{align*}
x \equiv -1 & \pmod{p}, \\
x \equiv -1 & \pmod{q},
\end{align*}$$

Each of these system has a unique solution modulo $pq$. This solution is $x = 1$ for the first system and $x = -1$ for the second one; the other two are difficult to describe explicitly (but nevertheless we know that they exist by the CRT). Hence, $x^2 \equiv 1 \pmod{pq}$ has 4 distinct solutions modulo $n = pq$. In other words, there are 4 integers $x$ between 1 and $n$ such that $x^2 \equiv 1 \pmod{n}$.

(c) Same reasoning as in part (b), but with $q$ replaced by 8. Here $x^2 \equiv 1 \pmod{8p}$ is equivalent to $x^2 \equiv 1 \pmod{8}$

$$\begin{align*}
x^2 & \equiv 1 \pmod{8}, \\
x^2 & \equiv 1 \pmod{p}.
\end{align*}$$

The first congruence has 4 solutions, $1, 3, 5, 7 \pmod{8}$, the second has two solutions $x = \pm 1 \pmod{p}$. Once we know what $x$ is modulo 8 and modulo $p$, the CRT allows us to combine the into $4 \cdot 2 = 8$ different solutions modulo $n = 8p$. modulo $n = pq$. In other words, for $n = 8p$ there are 8 integers $x$ between 1 and $n$ such that $x^2 \equiv 1 \pmod{n}$. 