1. Find the coefficient of \(x^7y^2\) in the expansion of \((2y - x)^9\).

**Solution.** From the binomial theorem, we find the coefficient to be

\[
(-1)^7 \cdot 4 \cdot \binom{9}{2} = -4 \cdot \frac{9 \cdot 8}{2} = -144.
\]

2. Find the smallest positive integer \(x\) such that

\[
x \equiv 2 \mod 3,
\]

\[
x \equiv 3 \mod 4,
\]

\[
x \equiv 4 \mod 5.
\]

**Solution.** From the first equation we write \(x = 3t + 2\), for a nonnegative integer \(t\). The second equation then gives \(x = -t + 2 = 3 \mod 4\), therefore \(t = 3 \mod 4\). We write \(t = 4s + 3\), which makes \(x = 12s + 11\). The third equation now gives \(x = 2s + 1 = 4 \mod 5\), so \(2s = 3 \mod 5\), therefore \(s = 4 \mod 5\). The smallest positive \(s\) is thus \(s = 4\) which gives \(x = 12 \cdot 4 + 11 = 59\).

3. Determine whether the following functions are injective, surjective or bijective (briefly explain). Indicate which are invertible.

(a) \(f : \mathbb{R} \to \mathbb{R}, f(x) = 3x + 1\)

(b) \(f : \mathbb{N} \to \mathbb{N}, f(x) = x^2\)

(c) \(f : [-\frac{\pi}{2}, \frac{\pi}{2}] \to [-1, 1], f(x) = \sin x\).

**Solution.** (a) \(f\) is bijective, therefore invertible. (b) \(f\) is injective but not surjective. (c) \(f\) is injective, therefore invertible.

4. Calculate \(17^{58} \mod 77\).

**Solution.** We use the Chinese Remainder Theorem, so we calculate first the residues modulo 7 and modulo 11. We have

\[
\text{mod 7 : } 17^{58} = 17^{6 \cdot 9 + 4} = (\text{Euler’s theorem}) 17^4 = 3^4 = 81 = 4.
\]

\[
\text{mod 11 : } 17^{58} = 17^{10 \cdot 5 + 8} = (\text{Euler’s theorem}) 17^8 = 6^8 = 36^4 = 3^4 = 81 = 4.
\]

By the Chinese Remainder Theorem, we have \(17^{58} = a \mod 77\), where \(a\) is the minimal positive integer satisfying

\[
a = 4 \mod 7 \text{ and } a = 4 \mod 11.
\]

Clearly \(a = 4\), so \(17^{58} = 4 \mod 77\).
5. Let \( a_n, n \geq 1, \) be the Fibonacci sequence, defined by
\[
a_1 = a_2 = 1, \quad a_n = a_{n-1} + a_{n-2}.
\]
Show by induction that
\[
\sum_{n=1}^{k} (-1)^n a_n = (-1)^k a_{k-1} - 1.
\]

**Solution.** The expression on the right makes sense when \( k \geq 2. \) We take \( k = 2 \) as the base case of the induction. The statement is in this case \(-a_1 + a_2 = a_1 - 1. \) Both sides of the equality are in this case zero, so the equality holds. We now assume the statement holds for \( k \) and show it for \( k + 1. \) We have
\[
\sum_{n=1}^{k+1} (-1)^n a_n = \left( \sum_{n=1}^{k} (-1)^n a_n \right) + (-1)^{k+1} a_{k+1}
\]
\[
= \left( (-1)^k a_{k-1} - 1 \right) + (-1)^{k+1} a_{k+1}
\]
\[
= (-1)^{k+1} (a_{k+1} - a_{k-1}) - 1
\]
\[
= (-1)^{k+1} a_k - 1,
\]
which is exactly the statement that was to be proved, for \( k + 1. \) In the equation above, the induction hypothesis (the statement for \( k \)) was used on the second line, and the Fibonacci defining equality \( a_{k+1} = a_k + a_{k-1} \) was used on the last line.

6. Prove or disprove the following statement: The product of two irrational numbers is always irrational.

**Solution.** The statement is false. \( \sqrt{2} \) is an irrational number, but \( \sqrt{2} \cdot \sqrt{2} = 2 \in \mathbb{Q}. \)

7. Negate the statement "For all positive real numbers \( y \) and \( z, \) there exists a real number \( x \) so that \( e^x \cdot y = z. \)"

**Solution.** The negation is: "There exist positive real numbers \( y \) and \( z \) so that for all real numbers \( x, \) \( e^x \cdot y \neq z. \)"

8. Prove that \( S(n, n - 1) = \binom{n}{2}. \)

**Solution.** \( S(n, n - 1) \) is the number of ways in which a set with \( n \) elements can be partitioned into \( n - 1 \) subsets. In this type of partition, it will necessarily be the case that \( n - 2 \) of the subsets have one element, and the remaining subset has two elements. What determines entirely the partition is therefore the choice of a two-element subset. There is no choice afterwards: each remaining element will give rise to a one-element subset. The number of ways to choose a two-element subset out of an \( n \)-element set is simply the binomial number \( \binom{n}{2} \).

9. Suppose you go to Whole Foods and buy 12 items, each with a similar weight. You want to distribute the items into three identical bags of similar weight to carry. So you decide to place 4 items in each bag. In how many different ways can you do this?
The number of surjections from a set with 12 elements to a set with 3 elements so that each of the 3 target values is assumed 4 times is the multinomial number \( \binom{12}{4,4,4} \). Since the three bags are identical, swapping two does not lead to a new distribution of the items. There are \( 3! = 6 \) ways to permute the bags. So the number of ways in which the items can be distributed into the three identical bags is

\[
\binom{12}{4,4,4} \cdot \frac{1}{6} = \frac{12!}{4!4!4!6} = 23100.
\]

10. If \( a, b \in \mathbb{Z} \), prove that \( a^2 - 4b \neq 2 \).

**Solution.** Assume by contradiction that the equality \( a^2 - 4b = 2 \) can be satisfied for integer \( a \) and \( b \). We then have \( a^2 = 4b + 2 = 2(2b + 1) \). It follows that 2 divides \( a \), so we can write \( a = 2k \) for an integer \( k \). We then have \( 4k^2 = 2(2b + 1) \), so \( 2k^2 = 2b + 1 \). The left side is even while the right side is odd; this equality cannot hold. By reductio ad absurdum the equality \( a^2 - 4b = 2 \) cannot be satisfied for integer \( a \) and \( b \).

11. Consider the set \( S = \{15x - 9y \mid x, y \in \mathbb{Z} \} \). Show that \( S = 3\mathbb{Z} \).

**Solution.** Recall that \( 3\mathbb{Z} = \{3z \mid z \in \mathbb{Z} \} \). We show first \( S \subset 3\mathbb{Z} \), then \( 3\mathbb{Z} \subset S \). Let \( a \in S \), then \( a = 15x - 9y \) for some integers \( x \) and \( y \). So \( a = 3(5x - 3y) = 3z \), where we set \( z = 5x - 3y \in \mathbb{Z} \). Therefore \( a \in 3\mathbb{Z} \), so \( S \subset 3\mathbb{Z} \).

Conversely, let \( b = 3z \in 3\mathbb{Z} \). We write \( b = (15 \cdot 2 - 9 \cdot 3)z = 15(2z) - 9(3z) = 15x - 9y \), where we set \( x = 2z \) and \( y = 3z \), both integers. Thus \( b \in S \), so we conclude \( 3\mathbb{Z} \subset S \) as well.

12. Suppose Bob wants to establish a secure communication channel with Alice using the RSA scheme. Bob’s encryption is \( E(M) = M^e \mod (n) \) and he chooses \( p = 3 \) and \( q = 7 \) and forms \( n = pq \) with \( e = 5 \).

(i) What should his decryption function be?

(ii) If \( M = 16 \), what is the encrypted message \( E(M) \)?

(iii) Verify directly that the decryption gives back \( M \).

**Solution.** (i) The decryption function is \( D(N) = N^d \), where \( d \) is chosen so \( de = 1 \mod \phi(n) \). We have \( \phi(n) = (p - 1)(q - 1) = 2 \cdot 6 = 12 \). Thus we need to find \( d \) so that \( 5d = 1 \mod 12 \). We conclude \( d = 5 \).

(ii) The encrypted message is \( 16^5 \mod 21 \). We calculate this by the Chinese Remainder Theorem: we have \( 16^5 = 1 \mod 3 \), and \( 16^5 = 2^5 = 32 = 4 \mod 7 \). The smallest \( a \) so that \( a = 1 \mod 3 \) and \( a = 4 \mod 7 \) is \( a = 4 \). We conclude that \( 16^5 = 4 \mod 21 \), so the encrypted message is \( E(16) = 4 \).

(iii) The decryption is \( 4^5 \mod 21 \) which should give us back \( M = 16 \). Indeed, \( 4^5 = 16 \cdot 64 = 16 \mod 21 \), since \( 64 = 3 \cdot 21 + 1 \).

13. In how many ways can \( n \) indistinguishable balls be put into \( r \) distinguishable boxes so that no box is empty?
Solution. Since each box is supposed to be nonempty, the first $r$ balls are each placed into a distinct box. The remaining $n - r$ balls are then placed with no constraints into the $r$ boxes. We are to count the number of such placements. For each placement of the $n - r$ balls, we label each of the balls by the number of the box it went into, obtaining a sequence of numbers $(a_1, \ldots, a_{n-r})$ with the property that

$$1 \leq a_1 \leq a_2 \leq \cdots \leq a_{n-r} \leq r.$$  

The number of such sequences is, as explained below in Problem 16, the binomial number

$$\binom{r + (n - r - 1)}{n-r} = \binom{n-1}{n-r} = \binom{n-1}{r-1}.$$  

It is easy to see this gives the right answer in particular cases such as when $n = r + 1$.

14. How many integers between 1 and 1000 are not divisible by any of 2, 3, 11, 13?

Solution. We calculate $2 \cdot 3 \cdot 11 \cdot 13 = 858$. The number of integers $a$ so that $1 \leq a \leq 858$, which are not divisible by 2, 3, 11, or 13 and therefore are exactly coprime to 858, is $\phi(858) = 240$. We are still to calculate the number of positive integers $a$, not divisible by 2, 3, 11, or 13, so that $1 \leq a \leq 1000$. This is the same as the number of integers $b$, not divisible by 2, 3, 11, or 13, so that $1 \leq b \leq 142$. The last count, which can be performed in a variety of ways, gives 40. We conclude that the number of integers between 1 and 1000 not divisible by any of 2, 3, 11, 13 is 280.

15. Find $3^{-1}$ in $\mathbb{Z}_{13}$, and $5^{-1}$ in $\mathbb{Z}_{27}$.

Solution. In $\mathbb{Z}_{13}$, we have $3 \cdot 9 = 27 = 1 \mod 13$, so $3^{-1} = 9$. In $\mathbb{Z}_{27}$, we have $5 \cdot 11 = 55 = 1 \mod 27$, so $5^{-1} = 11$.

16. Let $n$ be a positive integer. Find the number of triples $(a_1, a_2, a_3)$ so that

$$1 \leq a_1 \leq a_2 \leq a_3 \leq n.$$  

Solution. If we let $b_1 = a_1$, $b_2 = a_2 + 1$, $b_3 = a_3 + 2$ we have

$$1 \leq b_1 < b_2 < b_3 \leq n + 2.$$  

The number of triples $(b_1, b_2, b_3)$ is the number of ways of choosing three distinct elements out of the set of first $n + 2$ positive integers, in other words, it is the binomial number

$$\binom{n+2}{3} = \frac{n(n+1)(n+2)}{6}.$$  

The number of original triples $(a_1, a_2, a_3)$ equals the number of triples $(b_1, b_2, b_3)$ so it is also given by the binomial above.

17. Prove by induction that for any natural number $n$, $10^0 + 10^1 + \cdots + 10^n < 10^{n+1}$. 
Solution. For \( n = 0 \), we have \( 10^0 = 1 < 10^{0+1} = 10 \). We assume now that the inequality holds for \( n \) and we show it for \( n + 1 \). We have

\[
\sum_{k=0}^{n+1} 10^k = \left( \sum_{k=0}^{n} 10^k \right) + 10^{n+1} < 10^n + 10^{n+1} = 2 \cdot 10^n + 10^{n+1} = 10^{n+2}.
\]

We have thus obtained the statement for \( n + 1 \). Note that in the above equation, the first inequality uses the induction hypothesis (the statement for \( n \)), \( \sum_{k=0}^{n} 10^k < 10^{n+1} \).