Section 3.7

Problem 10: Prove that \( \sqrt{2} \) is irrational

Solution:
Note that if \( n^3 \) is even, then \( n \) is even, for otherwise, \( n \) would be odd, making \( n^3 \), the product of odd integers, odd.

Suppose \( \sqrt{2} \) is rational. Thus \( \sqrt{2} = a/b \), where \( a \) and \( b \) are integers and \( b \neq 0 \). Also assume that they don’t have any common factors. Cubing both sides we get,
\[ 2 = a^3/b^3 \] or \( a^3 = 2b^3 \). Which implies \( a^3 \) is even. Thus \( a \) is even, and so \( a^3 \) is divisible by 8. Thus, \( b^3 \) is divisible by 4, making \( b^3 \), and thus \( b \) even. Which implies \( a \) and \( b \) do have a common factor leading to a contradiction. Hence, \( \sqrt{2} \) is irrational.

Problem 13: Prove that \( \sqrt{2} \) is irrational, using the unique prime factorization theorem

Solution:
Suppose \( \sqrt{2} \) is rational. Thus \( \sqrt{2} = a/b \), where \( a \) and \( b \) are integers and \( b \neq 0 \). Also \( a^2 = 2b^2 \). Now consider the unique prime factorization of \( a^2 \). Since every prime factor of \( a \) occurs twice in the upf (unique prime factorization) of \( a^2 \), the upf of \( a^2 \) must contain an even number of 2’s. If 2—a, then this even number is positive, else zero. Similarly, upf of \( b^2 \) also has an even number of 2’s thus upf of \( 2b^2 \) has an odd number of 2’s, leading to a contradiction. Hence, \( \sqrt{2} \) is irrational.

Problem 22: Prove that there is a unique prime number of the form \( n^2 + 2n - 3 \), where \( n \) is a positive integer.

Solution:
It’s not difficult to see that \( n^2 + 2n - 3 = (n + 3)(n - 1) \). Now if this were to be a prime, then one of the two of \( n + 3 \) or \( n - 1 \) must be 1 and the other must be prime, else they will be the two factors. Since \( n > 0 \), \( n + 3 > 1 \). Thus only \( n - 1 = 1 \) is possible, which means \( n = 2 \) is the only case when
\( n^2 + 2n - 3 \) will be a prime. Indeed, \( n = 2 \) gives us \( n^2 + 2n - 3 = 5 \) which is a prime. For other values of \( n \), \( n^2 + 2n - 3 \) is composite. Hence there is a unique prime of the form \( n^2 + 2n - 3 \).

Section 3.8

**Problem 14:** Using Euclidean method, find the GCD of 3, 510 and 672

**Solution:**

\[
3510 = 672 \cdot 5 + 150 \\
672 = 150 \cdot 4 + 72 \\
150 = 72 \cdot 2 + 6 \\
72 = 6 \cdot 12
\]

Thus \( \gcd(3510, 672) = 6 \).

**Problem 24a:** Find \( \text{lcm}(12, 18) \)

**Solution:**

\[
\text{lcm}(12, 18) = \text{lcm}(2^2 \cdot 3^1, 2^1 \cdot 3^2)
\]

Thus \( \text{lcm}(12, 18) = 2^2 \cdot 3^2 = 36 \).

**Problem 24b:** Find \( \text{lcm}(12, 18) \)

**Solution:**

\[
\text{lcm}(2^1 \cdot 3^2 \cdot 5, 2^3 \cdot 3^1)
\]

Thus \( \text{lcm}(12, 18) = 2^3 \cdot 3^2 \cdot 5 = 360 \).

**Problem 24c:** Find \( \text{lcm}(3500, 1960) \)

**Solution:**

\[
\text{lcm}(3500, 1960) = \text{lcm}(2^2 \cdot 5^3 \cdot 7, 2^3 \cdot 5 \cdot 7^2)
\]

Thus \( \text{lcm}(12, 18) = 2^3 \cdot 5^3 \cdot 7^2 = 49,000 \).

**Problem 28:** Prove that for any two numbers \( a \) and \( b \), \( \gcd(a, b) \cdot \text{lcm}(a, b) = a \cdot b \)

**Solution:**

Claim: \( \gcd(a, b) \cdot \text{lcm}(a, b) \leq a \cdot b \)
Proof: Since \( \gcd(a, b)|a, \frac{a}{\gcd(a,b)} \) is an integer. Thus \( b \) divides \( \frac{ab}{\gcd(a,b)} \). Similarly, \( a \) divides \( \frac{ba}{\gcd(a,b)} \). Thus \( \frac{a}{\gcd(a,b)} \) is a common multiple of \( a \) and \( b \), implying \( \text{lcm}(a, b) \leq \frac{a}{\gcd(a,b)} \), or, \( \gcd(a, b) \cdot \text{lcm}(a, b) \leq a \cdot b \)

Claim: \( \gcd(a, b) \cdot \text{lcm}(a, b) \geq a \cdot b \)

Proof: By definition, \( a \nmid \text{lcm}(a, b) \). Thus \( \text{lcm}(a, b) = ak \), for some integer \( k \). Thus \( b \cdot \text{lcm}(a, b) = abk \) which implies \( b = \frac{ab}{\text{lcm}(a, b)} \cdot k \), which implies \( b \mid \frac{ab}{\text{lcm}(a, b)} \). Similarly \( a \mid \frac{ab}{\text{lcm}(a, b)} \). Thus \( \frac{ab}{\text{lcm}(a, b)} \) is a common divisor. Hence, \( \frac{ab}{\text{lcm}(a, b)} \leq \gcd(a, b) \) implying \( \gcd(a, b) \cdot \text{lcm}(a, b) \geq a \cdot b \)

By the two claims, \( \gcd(a, b) \cdot \text{lcm}(a, b) = a \cdot b \)

\[ \square \]

Section 4.2

Problem 2: Using mathematical Induction, show that any postage of denomination greater that \( 8c \) can get from stamps of \( 3c \) and \( 5c \)

Solution:
Base Case: \( 8c = 1 \) \( 3c \) stamp + \( 1 \) \( 5c \) stamp

Induction Hypothesis: Any postage of denomination \( k \) can be got from stamps of \( 3c \) and \( 5c \), when \( k \geq 8 \).

Claim: A stamp of denomination \( k + 1 \) can be got from \( 3c \) and \( 5c \) stamps.

Proof:
Suppose there is a \( 5c \) stamp used to make the \( k \) cents postage. Remove it and put 2 \( 3c \) stamps, we get a postage of \( k + 1 \) stamps.

If no \( 5c \) stamps were used, then atleast 3 \( 3c \) stamps must have been used to make the \( k \) cent amount as \( k \geq 8 \). Thus remove 3 \( 3c \) stamps and put in 2 \( 5c \) stamps to get \( k + 1c \) worth of postage.

hence proved

\[ \square \]

Problem 7: Use Mathematical Induction to show that \( 1 + 5 + 9 + \cdots + 4n - 3 = n(2n - 1) \)

Solution:
Base Case: \( n = 1 \).

\[ \text{LHS} = 1 \]
\[ RHS = 1(2 - 1) \]
\[ = 1 \]

**Induction Hypothesis:** Let \( 1+5+9+ \cdots + 4n - 3 = n(2n - 1) \) for all \( n \leq k \).

**Claim:** \( 1+5+9+ \cdots + 4(k + 1) - 3 = (k + 1)(2(k + 1) - 1) \)

**Proof:**

\[
LHS = 1 + 5 + 9 + \cdots + 4(k + 1) - 3
= 1 + 5 + 9 + \cdots + 4k - 3 + 4(k + 1) - 3
= k(2k - 1) + (4k + 1) \quad \text{By Induction Hypothesis}
= 2k^2 + 3k + 1
\]

\[
RHS = (k + 1)(2(k + 1) - 1)
= (k + 1)(2k + 1)
= 2k^2 + 3k + 1
\]

Hence Proved

\[ \blacksquare \]

**Problem 13:** Using Mathematical Induction, prove \( \sum_{i=1}^{n+1} i^2 = n2^{n+2} + 2 \) for all \( n \geq 0 \)

**Solution:**

**Base Case:** \( n=0 \).

\[
LHS = 1.2^1
= 2
\]

\[
RHS = 0 + 2
= 2
\]

**Induction Hypothesis:** \( \sum_{i=1}^{n+1} i^2 = n2^{n+2} + 2 \) for all \( n \leq k \)

**Claim:** \( \sum_{i=1}^{k+2} i^2 = (k + 1)2^{k+3} + 2 \)

**Proof:**

\[
LHS = \sum_{i=1}^{k+2} i^2
= \sum_{i=1}^{k+1} i^2 + (k + 2)2^{k+2}
\]
\[ = k \cdot 2^{k+2} + 2 + (k + 2)2^{k+2} \quad \text{By Induction Hypothesis} \]
\[ = 2^{k+2} (2k + 2) + 2 \]
\[ = (k + 1)2^{k+3} + 2 \]
\[ = \text{RHS} \]

Hence Proved.

Additional problem

**Problem:** Find the GCD of 34709 and 100313; also express the GCD as an integer combination of the two numbers

**Solution:**
Using Euclid’s algorithm,
100313 = 34709 \cdot 2 + 30895
34709 = 30895 \cdot 1 + 3814
30895 = 3814 \cdot 8 + 383
3814 = 383 \cdot 9 + 367
383 = 367 \cdot 1 + 16
367 = 16 \cdot 22 + 15
16 = 15 \cdot 1 + 1

Thus \( \gcd(100313, 34709) = 1 \)

Backtracking we get the following.

16 - 15 \cdot 1 = 1
16 - (367 - 16 \cdot 22) \cdot 1 = 1
16 \cdot 23 - 367 \cdot 1 = 1
(383 - 367) \cdot 23 - 367 \cdot 1 = 1
383 \cdot 23 - 367 \cdot 24 = 1
383 \cdot 23 - (3814 - 383 \cdot 9) \cdot 24 = 1
383 \cdot 239 - 3814 \cdot 24 = 1

Continuing thus we shall finally get, 100313 = 2175 + 34709 \cdot (-6286) = 1.

**A few Optional Problems**

**Problem 3.7.15:** Prove that \( \log_2 3 \) is irrational

**Solution:**
Suppose not. Then \( \log_2 3 = a/b \) for some integers \( a \) and \( b \). Thus \( 2^a = 3^b \).
Now the LHS has the prime factors 2 while the RHS has prime factors 3. Since \( b \neq 0 \), there is at least one 3 in the RHS, but none in the LHS. Thus there is a contradiction.

\[ \bullet \]

**Problem 3.7.18:** Suppose for any odd prime \( p \), there exists no solutions to the equation \( x^p + y^p = z^p \). Then show that for every integer which is not a power of 2, \( x^n + y^n = z^n \) has no solutions

**Solution:**

Since \( n \) is not a power of two, there exists an odd prime factor \( p \) of \( n \). Suppose \( n = pk \). Then \( x^n = (X^k)^p \). Thus if the equation \( x^n + y^n = z^n \) had solutions \( x_0, y_0, z_0 \) then \( x_0^k, y_0^k, z_0^k \) form the solutions to the equation \( x^p + y^p = z^p \), contradicting the premise of the problem. Hence proved

\[ \bullet \]

**Problem 3.8.23.a:** Prove: \( \text{gcd}(a, b) = \text{gcd}(b, a - b) \) for any two integers \( a \geq b > 0 \).

**Solution:**

Suppose \( d|a \) and \( d|b \). Then \( d|(a - b) \) Thus every common divisor of \( a \) and \( b \) is a common divisor of \( b, a - b \). Suppose \( d|b \) and \( d|a - b \) then \( d|b + (a - b) \) that is \( d|a \). Thus every common divisor of \( b \) and \( a - b \) is a common divisor of \( a \) and \( b \). In other words all common divisors are same, or more specifically the Greatest common divisors are same.

\[ \bullet \]

**Problem 4.2.8:** Using Mathematical Induction, prove: \( 1 + 2 + 2^2 + \ldots + 2^n = 2^{n+1} - 1 \) for all \( n \geq 0 \)

**Solution:**

**Base Case:** \( n=0 \).

\[
\begin{align*}
LHS &= 1 \\
RHS &= 2^1 - 1 \\
&= 1
\end{align*}
\]

**Induction Hypothesis:** \( 1 + 2 + 2^2 + \ldots + 2^n = 2^{n+1} - 1 \) for all \( n \leq k \)

**Claim:** \( 1 + 2 + 2^2 + \ldots + 2^{k+1} = 2^{k+2} - 1 \)

**Proof**

\[
\begin{align*}
LHS &= 1 + 2 + 2^2 + \ldots + 2^{k+1}
\end{align*}
\]
\[ \begin{align*}
= & \ 1 + 2 + 2^2 + \cdots + 2^k + 2^{k+1} \\
= & \ 2^{k+1} - 1 + 2^k + 1 \\
= & \ 2\cdot 2^{k+1} - 1 \\
= & \ 2^{k+2} - 1 \\
= & \ RHS
\end{align*} \]