GCD

(a) Calculate $\gcd(100, 50)$.

Solution: 50

(b) Calculate $\gcd(17, 31)$.

Solution: 1

(c) Find the multiplicative inverse of 6 modulo 7.

Solution: 6

(d) Does 49 have an multiplicative inverse modulo 7?

Solution: It does not. Intuitively, this is because $49x$ for any $x$ is going to be 0 mod 7, which means it can never be 1.

(e) Find the multiplicative inverse of 7 modulo 311.

Solution: 89

(f) Find the multiplicative inverse of 27 modulo 151.

Solution: 28

More Number Theory

(a) Prove that if $n^2 + 1$ is a perfect square, where $n$ is an integer, then $n$ is even.

Solution: Suppose $n^2 + 1$ is a perfect square. Then, by definition of perfect square, $n^2 + 1 = k^2$ for some $k \in \mathbb{N}$. Suppose for contradiction that $n$ is odd. Then, $n^2 + 1 = (2j + 1)^2 + 1 = 4j^2 + 4j + 1 + 1 = 4(j^2 + j) + 2$.

(b) Prove that if $n$ is a positive integer such that the sum of the divisors of $n$ is $n+1$, then $n$ is prime.

Solution: Note that $n \mid n$. If the sum of divisors of $n$ is $n+1$, then $n + 1 - n = 1$ must be the only other divisor. It follows, by definition of prime, that $n$ is prime.
Induction

(a) Prove that if you have two groups of numbers, \(a_1, \ldots, a_n\) and \(b_1, \ldots, b_n\), such that \(\forall (i \in [n]), a_i \leq b_i\), then it must be that:

\[
\sum_{i=1}^{n} a_i \leq \sum_{i=1}^{n} b_i
\]

Solution: We prove this by induction on \(n\):

Base Case \((n = 1)\). We know that:

\[
\sum_{i=1}^{1} a_i = \sum_{i=1}^{1} a_1 = a_1
\]

Because we’re given that \(a_1 \leq b_1\), we know that:

\[
\sum_{i=1}^{n} a_i = a_1 \leq b_1 = \sum_{i=1}^{n} b_i
\]

Induction Hypothesis. Assume for some \(k \in \mathbb{N}\) that \(\sum_{i=1}^{k} a_i \leq \sum_{i=1}^{k} b_i\) for all sequences \(a_1, \ldots, a_n\) and \(b_1, \ldots, b_n\) such that \(a_i \leq b_i\) for all \(i \in [n]\)

Induction Step. Let a sequence of numbers \(a_1, \ldots, a_{k+1}\) and \(b_1, \ldots, b_{k+1}\) be two sequences such that \(a_i \leq b_i\) for all \(i \in [n+1]\).

We can do the following work:

\[
\sum_{i=1}^{n+1} a_i \leq \sum_{i=1}^{n+1} b_i \quad [\text{Induction Hypothesis}]
\]

\[
a_{n+1} + \sum_{i=1}^{n} a_i \leq b_{n+1} + \sum_{i=1}^{n} b_i \quad [a_{n+1} \leq b_{n+1}]
\]

\[
\sum_{i=1}^{n+1} a_i \leq \sum_{i=1}^{n+1} b_i \quad [\text{Shifting elements into Sum}]
\]

Thus we have shown in true for the case of \(k + 1\) elements.

Therefore, we have shown the claim true by induction.

(b) For any \(n \in \mathbb{N}\), define \(S_n\) to be the sum of the squares of the first \(n\) positive integers, or

\[
S_n = \sum_{i=1}^{n} i^2
\]

For all \(n \in \mathbb{N}\), prove that \(S_n = \frac{1}{6}n(n + 1)(2n + 1)\).

Solution: Let \(P(n)\) be the statement \(“S_n = \frac{1}{6}n(n + 1)(2n + 1)”\) defined for all \(n \in \mathbb{N}\). We prove that \(P(n)\) is true for all \(n \in \mathbb{N}\) by induction on \(n\).
**Base Case.** When \( n = 0 \), we know the sum of the squares of the first \( n \) positive integers is the sum of no terms, so we have a sum of 0. Thus, \( S_0 = 0 \). Since \( \frac{1}{6}(0)(0 + 1)((2)(0) + 1) = 0 \), we know that \( P(0) \) is true.

**Induction Hypothesis.** Assume that \( P(k) \) is true for some \( k \in \mathbb{N} \).

**Induction Step.** Examining \( S_{k+1} \), we see that

\[
S_{k+1} = \sum_{i=1}^{k+1} i^2 = \sum_{i=1}^{k} i^2 + (k + 1)^2 = S_k + (k + 1)^2.
\]

By the induction hypothesis, we know that \( S_k = \frac{1}{6}k(k + 1)(2k + 1) \). Therefore, we can substitute and rewrite the expression as follows:

\[
S_{k+1} = S_k + (k + 1)^2 \\
= \frac{1}{6}k(k + 1)(2k + 1) + (k + 1)^2 \\
= (k + 1) \left( \frac{1}{6}k(2k + 1) + (k + 1) \right) \\
= \frac{1}{6}(k + 1) (k(2k + 1) + 6(k + 1)) \\
= \frac{1}{6}(k + 1) (2k^2 + 7k + 6) \\
= \frac{1}{6}(k + 1)(k + 2)(2k + 3) \\
= \frac{1}{6}(k + 1)((k + 1) + 1)(2(k + 1) + 1)
\]

Thus, we can conclude that \( P(k + 1) \) is true.

Therefore, because the base case and induction step hold, \( P(n) \) is true for all \( n \in \mathbb{N} \) by induction.

(c) Define the triangle numbers as \( \triangle_n = 1 + 2 + \cdots + n \), where \( n \in \mathbb{N} \). We showed in lecture that

\[
\triangle_n = \frac{n(n+1)}{2}.
\]

Prove the following equality for all \( n \in \mathbb{N} \):

\[
\sum_{i=0}^{n} i^3 = \triangle_n^2
\]

**Solution:**

First, note that \( \triangle_n = \sum_{i=0}^{n} i \). So, we are trying to prove \( \sum_{i=0}^{n} i^3 = \left( \sum_{i=0}^{n} i \right)^2 \).

Let \( P(n) \) be the statement:

\[
\sum_{i=0}^{n} i^3 = \left( \sum_{i=0}^{n} i \right)^2
\]

We prove that \( P(n) \) is true for all \( n \in \mathbb{N} \) by induction on \( n \).
Base Case.  $0^3 = 0^2$, so $P(0)$ holds.

Induction Hypothesis. Assume that $P(k)$ is true for some $k \in \mathbb{N}$.

Induction Step. We show $P(k+1)$:

\[
\sum_{i=0}^{k+1} i^3 = \sum_{i=1}^{k} i^3 + (k+1)^3
\]

[Take out a term]

\[
= \left( \sum_{i=0}^{k} i \right)^2 + (k+1)^3
\]

[Induction Hypothesis]

\[
= \left( \frac{k(k+1)}{2} \right)^2 + (k+1)^3
\]

[Substitution from part (a)]

\[
= (k + 1)^2 \left( \frac{k^2}{2^2} + (k + 1) \right)
\]

[Factor $(k + 1)^2$]

\[
= (k + 1)^2 \left( \frac{k^2 + 4k + 4}{4} \right)
\]

[Add via common denominator]

\[
= (k + 1)^2 \left( \frac{(k + 2)^2}{4} \right)
\]

[Factor numerator]

\[
= \left( \frac{(k + 1)(k + 2)}{2} \right)^2
\]

[Take out the square]

\[
= \left( \sum_{i=0}^{k+1} i \right)^2
\]

[Substitution from part (a)]

Therefore, $P(n)$ is true for all $n \in \mathbb{N}$ by induction.