Homework 1

Dakota Wicker
Abstract Algebra I

September 3, 2019

Problem 1. Prove that if x is rational, and y is irrational, then $x + y$ is also irrational.

Proof. Suppose $x + y$ is rational, then $x + y$ can be written as

$$x + y = \frac{p}{q} \quad p, q \in \mathbb{Z}, \quad q \neq 0.$$

Since x is also rational, then x can be written as

$$x = \frac{a}{b} \quad a, b \in \mathbb{Z}, \quad b \neq 0.$$

Substituting, this can be rewritten as

$$\frac{a}{b} + y = \frac{p}{q}$$

With further algebraic manipulation, this is written as

$$y = \frac{p}{q} - \frac{a}{b} = \frac{pb - aq}{qb}$$

Since y can be written in terms of the quotient of two integers, then y must be rational. This is a contradiction with the initial assumption that y is irrational. Therefore $x + y$ is irrational. □

Problem 2. Use mathematical induction to prove that the following holds for all positive integers

$$\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}$$

Proof. Using the steps of induction I first show that this holds for $n = 1$

$$1^3 = \frac{n^2(n+1)^2}{4} = \frac{1(2)^2}{4} = 1$$

Following the steps of induction, I assume this is true for some $n = k, k \geq 1$. That is,

$$\sum_{i=1}^{k} i^3 = \frac{k^2(k+1)^2}{4}$$

Now I show this works for k+1. To do this, I will show that

$$\frac{(k+1)^2(k+2)^2}{4} = \frac{k^2(k+1)^2}{4} + (k+1)^3$$

We can show this by algebraic manipulation

$$\begin{aligned}
\frac{(k+1)^2(k+2)^2}{4} &= \frac{k^2(k+1)^2}{4} + (k+1)^3 \\
&= \frac{k^2(k+1)^2}{4} + (k^3 + 3k^2 + 3k + 1) \\
&= \frac{k^4 + 2k^3 + k^2}{4} + (k^3 + 3k^2 + 3k + 1) \\
&= \frac{k^4 + 2k^3 + k^2}{4} + \frac{4k^3 + 12k^2 + 12k + 4}{4} \\
&= \frac{k^4 + 6k^3 + 13k^2 + 12k + 4}{4} \\
&= \frac{(k+1)^2(k+2)^2}{4}
\end{aligned}$$

Therefore,

$$\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}$$

is true for all positive integers. □

Problem 3. Use induction to show that $2^{2n} - 1$ is divisible by 3 for all positive integers n.

Proof. Using the steps of induction I first show that this holds for $n = 1$. $2^2 - 1 = 3$ and 3 is divisible by 3. Next I assume that

$$2^{2k} - 1 = 3c$$

is true for some $n = k, k \geq 1$ and $c \in \mathbb{Z}$. Now I show this holds true for $n = k + 1$

$$\begin{aligned}
2^{2(k+1)} - 1 &= (2^{2k}2^2) - 1 \\
&= ((3c+1)2^2) - 1 \\
&= (12c + 4) - 1 \\
&= 12c + 3 \\
&= 3(4c + 1)
\end{aligned}$$

Since this relationship holds for k+1, this proves that $2^{2k} - 1$ is divisible by 3. □

Problem 4. Use two-column method to find the linear combination that produces the greatest common divisor of 6157 and 6419.

$$\begin{array}{c|cc|c} 1 & 2 & 4 & 3 \\ \hline \end{array}$$

Problem 5. Evaluate, *by hand* (hence, in the easiest way), the value of $25^4 \cdot 20^3 \pmod{23}$. Explain how you obtain the answer by showing the intermediate steps.

Since, $25 \equiv 2 \pmod{23}$ and $20 \equiv -3 \pmod{23}$, I can rewrite the problem as finding the value of

$$2^4 \cdot -3^3 \pmod{23}.$$

This is equivalent to

$$16 \cdot -27 \pmod{23}$$

and since $16 \equiv -7 \pmod{23}$ and $-27 \equiv -4 \pmod{23}$, it follows that

$$-7 \cdot -4 \pmod{23} = 28 \pmod{23} = 5$$

leaving 5 as the value of $25^4 \cdot 20^3 \pmod{23}$.

Problem 8. Evaluate $7007^-1 \pmod{101}$

A modular multiplicative inverse of an integer a (mod m) is an integer x where $ax \equiv 1 \pmod{m}$. 7007 has no multiplicative inverse (mod 101) because $7007 \equiv 0 \pmod{101}$.

Problem 9. Use repeated squaring to evaluate $12^189 \pmod{37}$.