Homework 1

Dakota Wicker
Abstract Algebra I

September 4, 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. $\square$

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. $\square$

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

1	6419	6157
23	6157	6026
2	262	131
1	131	131
	131	0

This shows that GCD(6419,6157) = 131. Calculating s_k and t_k I get

s_k	t_k
0	1
1	0
-1	1
24	-23
-49	47
73	-70

Giving the linear combination of $6157 \cdot 73 + 6419 \cdot -70 = 131$

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 6. Use the two-column method to find the integers s and t such that

$$101s + 7007t = 1.$$

Finding the GCD(7007,101) gives me

69	7007	101
2	101	38
1	38	25
1	25	13
1	13	12
12	12	1
	1	0

GCD(7007,101) = 1. Finding s_k and t_k I get

s_k	t_k
0	1
1	0
-69	1
139	-2
-208	3
347	-5
-555	8

Therefore $s = -555, t = 8$.

Problem 7. Use the result from the last problem to solve the congruence

$$101x \equiv 1 \pmod{7007}$$

$101 \cdot -555 \equiv 1 \pmod{7007}$. So, $x = 5$.

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

A modular multiplicative inverse of an integer a (mod m) is an integer x where $ax \equiv 1 \pmod{m}$. So, for this problem I need to find x where $7007 \cdot x \equiv 1 \pmod{101}$. Since 7007 (mod 101) is equivalent to 38 $(101 \cdot 69) \pmod{101}$, the problem is rewritten to be $38 \cdot x \equiv 1 \pmod{101}$. It now becomes easier to see that $38 \cdot 8 = 304 = (101 \cdot 3) + 1 \equiv 1 \bmod(101)$. Therefore, $7007^-1 \pmod{101} = 8$.

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

$$\begin{aligned}
12^1 &= 12 \pmod{37} \\
12^2 &= -4 \pmod{37} \\
12^4 &= (-4)^2 \pmod{37} = 16 \pmod{37} \\
12^8 &= 16^2 \pmod{37} = -3 \pmod{37} \\
12^{16} &= (-3)^2 \pmod{37} = 9 \pmod{37} \\
12^{32} &= 9^2 \pmod{37} = 7 \pmod{37} \\
12^{64} &= 7^2 \pmod{37} = 12 \pmod{37} \\
12^{128} &= 12^2 \pmod{37} = -4 \pmod{37}
\end{aligned}$$

Since $12^{189} = 12^{128} \cdot 12^{32} \cdot 12^{16} \cdot 12^8 \cdot 12^4 \cdot 12^1$ this means that $12^{189} \pmod{37} = -4 \cdot 7 \cdot 9 \cdot -3 \cdot 16 \cdot 12 = 1 \pmod{37}$

Problem 10. Write the complex number $\frac{1+2i}{(2-3i)(3+4i)}$ in the standard form $a + bi$

First, I factor the denominator.

$$\frac{1+2i}{18-i}$$

Then, I mutliply by the conjugate.

$$\frac{1+2i}{18-i} \cdot \frac{18+i}{18+i} = \frac{16+37i}{325}$$

Putting this in $a+bi$ form gives me the answer.

$$\frac{16}{325} + \frac{37i}{325}$$