Number Theory: HW1

Aamod Varma

August 25, 2025

Problem 1

(a). Given $a, b, c \in \mathbb{Z}$ and $c \neq 0$, we need to show that $a|b$ if and only if $ac|bc$.
First we show that $a|b$ implies $ac|bc$. If $a|b$ then there exists some $x \in \mathbb{Z}$ such that $ax = b$. Now multiply c on both sides to get $acx = bc$. This means that there is some $x \in \mathbb{Z}$ for which ac multiplied by x is bc. In other words by definition we have $ac|bc$.
Now we show that $ac|bc$ implies that $a|b$. If $ac|bc$, by definition we have some $x \in \mathbb{Z}$ such that $acx = bc$. Now, because $c \neq 0$ we can divide c from both sides to get $ax = b$. Again by definition this means that b is a multiple of a or that $a|b$.
(b). Consider $a = 3$ and $b = 5$. If $c = 0$ we have $ac = 0$ and $bc = 0$. Now $0|0$ is true because for any choice of $x \in \mathbb{Z}$ we have $0x = 0$. So we have $ac|bc$. However, we can easily see that $3|5$ is not true. So this counterexample shows that the statement if and only if doesn't hold if $c = 0$

Problem 2

We have a, m, n are positive integers with $a > 1$. We need to show that $a^m - 1|a^n - 1$ if and only if $m|n$.
First we show that if $m|n$ then $a^m - 1|a^n - 1$. If $m|n$ then we have for some $x \in \mathbb{Z}$ that $mx = n$ which means that $a^{mx} - 1 = a^n - 1$. We can write the left hand side as $(a^m)^x - 1 = (a^m - 1)(a^{m(x-1)} + a^{m(x-2)} + \cdots + 1) = (a^m - 1)(k)$ where $k = (a^{m(x-1)} + a^{m(x-2)} + \cdots + 1)$. This give us,

$$(a^m - 1)k = a^n - 1$$

Or that $a^m - 1|a^n - 1$
Now, we show that $a^m - 1|a^n - 1$ implies that $m|n$. If $a^m - 1|a^n - 1$ then that means $\exists x \in \mathbb{Z}$ such that $(a^m - 1)x = a^n - 1$. Now as $n > m$ (we know this because x is a positive integer, which means that $a^n > a^m$ which means that $n > m$) we can take $n = qm + r$ for some $q, r \in \mathbb{N}$ where $r < m$. Now we can write,

$$\begin{aligned} a^n - 1 &= a^{qm}a^r - 1 \\ &= a^{qm}a^r - a^r + a^r - 1 \\ &= (a^{qm} - 1)a^r + (a^r - 1) \end{aligned}$$

Now we know that $a^m - 1|a^n - 1$ by assupmtion and we also know from the above proof that $a^m - 1|a^{qm} - 1$ as $m|qm$. Hence, this also must mean that $a^m - 1|a^r - 1$. However, by construction we have $r < m$ based on how we constructed n as $n = qm + r$. This meanss that $a^m - r > a^r - 1$. A larger mumber divides a smaller number only when the smaller number is zero. SO we have $a^r - 1 = 0$. Or that $r = 0$. This gives us, $n = qm + r = qm + 0 = qm$ which implies that $m|n$.

Problem 3

Give $n \in \mathbb{Z}$,

(a). To show that $3|n^3 - n$.
First we rewrite $n^3 - n = n(n^2 - 1) = n(n+1)(n-1)$
We have three cases,
Case 1: $n = 3q + 0$ for some $q \in Z$
Here $n = 3q$ so we have

$$n(n+1)(n-1) = 3q(3q+1)(3q-1) = 3(k)$$

where $k = q(3q+1)(3q-1)$. Hence we have $3|n^3 - n$
Case 2: $n = 3q + 1$ for some $q \in Z$
Here $n = 3q + 1$ so we have

$$n^3 - n = n(n+1)(n-1) = (3q+1)(3q+2)(3q) = 3k$$

where $k = (3q+1)(3q+2)q$ so we have $3|n^3 - n$
Case 3: $n = 3q + 2$ for some $q \in Z$
Here $n = 3q + 2$ so we have

$$n^3 - n = n(n+1)(n-1) = (3q+2)(3q+3)(3q+1) = 3(3q+2)(q+1)(3q+1) = 3k$$

where $k = (3q+2)(q+1)(3q+1)$ which means that $3|n^3 - n$
So, in all three cases we have $3|n^3 - n$
(b). Similar to above we have 5 cases as any number can only leave reminaders $0, 1, 2, 3, 4$ when divided by 5. We can also expand

$$n^5 - n = n(n^4 - 1) = n(n^2+1)(n+1)(n-1)$$

Now the five cases are,
Case 1: $n = 5q + 0$
Here $n = 5q$ so

$$n^5 - n = n(n^2+1)(n+1)(n-1) = 5q(5q^2+1)(5q+1)(5q-1) = 5k$$

where $k = q(5q^2+1)(5q+1)(5q-1)$ which gives us $5|n^5 - n$
Case 2: $n = 5q + 1$
Here $n = 5q + 1$ so

$$n^5 - n = n(n^2+1)(n+1)(n-1) = (5q+1)((5q+1)^2+1)(5q+2)(5q) = 5k$$

where $k = (5q+1)((5q+1)^2+1)(5q+2)q$ which gives us $5|n^5 - n$
Case 3: $n = 5q + 2$
Here $n = 5q + 2$ so

$$\begin{aligned} n^5 - n = n(n^2+1)(n+1)(n-1) &= (5q+2)((5q+2)^2+1)(5q+3)(5q+1) \\ &= (5q+2)(25q^2+4+20q+1)(5q+3)(5q+1) \\ &= (5q+2)5(5q^2+1+4q)(5q+3)(5q+1) \\ &= 5k \end{aligned}$$

where $k = (5q+2)(5q^2+1+4q)(5q+3)(5q+1)$ so we have $5|n^5 - n$
Case 4: $n = 5q + 3$

Here $n = 5q + 3$ so

$$\begin{aligned}
n^5 - n = n(n^2+1)(n+1)(n-1) &= (5q+3)((5q+3)^2+1)(5q+4)(5q+2) \\
&= (5q+3)(25q^2+9+30q+1)(5q+4)(5q+2) \\
&= (5q+3)(25q^2+10+30q)(5q+4)(5q+2) \\
&= 5(5q+3)(5^2+2+6)(5q+4)(5q+2) \\
&= 5k
\end{aligned}$$

where $k = (5q+3)(5^2+2+6)(5q+4)(5q+2)$ which gives us $5|n^5 - n$
Case 5: $n = 5q + 4$
Here $n = 5q + 4$ so

$$\begin{aligned}
n^5 - n = n(n^2+1)(n+1)(n-1) &= (5q+4)((5q+4)^2+1)(5q+5)(5q+3) \\
&= 5(5q+4)((5q+4)^2+1)(q+1)(5q+3) \\
&= 5k
\end{aligned}$$

where $k = (5q+4)((5q+4)^2+1)(q+1)(5q+3)$ which means that $5|n^5 - n$
So in all three cases we have $5|n^5 - n$
In all cases we have $5|n^5 - n$
(c). We need to either prove or disprove that $4|n^4 - n$. We will disprove the statement by giving a counter example. Consider $n = 3$. Here we have $n^4 - n = 81 - 3 = 77$. We see that $77 = 4 \times 19 + 1$ which means that $4 \not| 77$ and hence disproves the statement.

Problem 4

We have a, n are positive integers with $a > 1$. We need to show that $a^n + 1$ is prime then a is even and n is a power of 2.
Let us assume the contrary that a is odd or n is not a power of 2.
Case 1 we have n is odd. This means that a^n is odd (as odd times odd is always odd). If a^n is odd then $a^n + 1$ is even and not equal to 2(as $a > 1$ we have $a^n + 1 > 2$). And we know that 2 is the only even prime number. This means that $a^n + 1$ is composite which breaks our assumption that it is prime. Hence, n cannot be odd.
Case 2 we have n not a power of 2. If a is odd we already showed that $a^n + 1$ is composite regardless of n a power of 2 or not. Now if a is even we have $a = 2x$ for some odd x. Now we have $(2x)^n + 1$ where n is not a power of 2. We have $2^n(2m + 1)^n + 1$. We can expand this as,

$$2^n((2m)^n + n(2m)^{n-1} + n\frac{n-1}{2}(2m)^{n-2} + \cdots + n(2m) + 1) + 1$$

Problem 5

Given that $n^2 + 1$ is prime. We know from above that n has to be even as if its odd the number would be composite. Now assume to the contrary that $n^2 + 1$ is not expressibel int he form $4k + 1$ with integer k. This means that it's expressible as either $4k, 4k + 2, 4k + 3$.

If $n^2+1=4k$ or$4k+2$ then n^2+1 is even making it composite and not prime. If $n^2+1=4k+3$ then $n^2=4k+2=2(2k+1)$. However we know that n^2 is a perfect square and perfect squares cannot have an odd number of factors of 2 (it must have an even exponent for every prime factor). Hence this must mean that n^2 cannot be of the form $4k+2$ or that n^2+1 cannot be $4k+3$. So, in all three cases we show that n^2+1 cannot be prime and of that form. So our assumption must be wrong and $n^2+1=4k+1$

Problem 6

(a). We have $GCD(a,b)=1$. We need to show that $a|c, b|c$ implies that $ab|c$.
If $GCD(a,b)=1$ we have some $m,n\in\mathbb{Z}$ such that $am+bn=1$. If $a|c, b|c$ then we have some $x,y\in\mathbb{Z}$ such that $ax=c$ and $by=c$.
We have,

$$\begin{aligned} am+bn &= 1 \\ cam+cbn &= c \\ byam+axbn &= c \qquad \text{as } c=ax=by \\ ab(ym+xn) &= c \\ ab(z) &= c \end{aligned}$$

which by definition mean that $ab|c$
(b). Consider if $a=5$ and $b=10$, so we have $(a,b)=5$. We see that if $c=20$ we have, $a=5|20$ and $b=10|20$. However we see that $ab=50 \not| 20$.
(c). We have $a_1,\ldots,a_n\in\mathbb{Z}$ which are pairwise relatively prime numbers. We need to show that if $a_j|c$ then $a_1\ldots a_n|c$.
First we prove a primliminary result that given relatively prime numbers $a_1,\ldots,a_n$, the gcd of the product of a subset of these numbers is relatively prime with numbers outside the subset. In other words we show that,

$$gcd(a_1\ldots a_i, a_k)=1 \text{ if } k>i$$

We will do this by induction. For the base case we have $i=1$ for which this is trivially true by construction (as all the numbers are pairwise relatively prime). Now consider the case for some arbitrary m. So we have,

$$gcd(a_1\ldots a_m, a_{m+1})=1$$

We need to show this is true for $m+1$. Now let $a_1\ldots a_m=x, a_{m+1}=y, a_k=z$ where $k>m+1$
So we have,

$$\begin{aligned} xm_1+zn_1 &= 1 \text{ for some } m_1,n_1\in\mathbb{Z} \\ ym_2+zn_2 &= 1 \text{ for some } m_2,n_2\in\mathbb{Z} \end{aligned}$$

Now multiplying these two together we have,

$$xym_1m_2+z(xm_1n_2+zn_1n_2+yn_1m_2)=1$$

$$xym_3 + z(n_3) = 1 \text{ where } m_3 = m_1m_2, n_3 = xm_1n_2 + zn_1n_2 + yn_1m_2$$

This by definition means that $gcd(xy, z) = 1$. Or expending it gives us,

$$gcd(a_1 \dots a_m a_{m+1}, a_{m+2}) = 1$$

Which is the case for $n = m + 1$

Now we prove the initial statement inductively. Consider $i = 1$ for which the statement is trivially true. Now consider the statement is true for some arbitrary i so we have $a_1 \dots a_i | c$ given $a_1 | c, \dots, a_i | c$. Now, consider a_{i+1}. Let $a_1 \dots a_i = a'$ so we have $gcd(a', a_{i+1}) = 1$ based on the proof above. Similarly we have $a' | c$ and $a_{i+1} | c$ by assumption. So based on the proof in (a) this means that $a' a_{i+1} | c$ or that $a_1 \dots a_{i+1} | c$ which is the case for $i + 1$. Hence we compute the inductive step and show that it must be true for any i.

Problem 7

We have $a, b \in \mathbb{Z}$. We need to show that $(a, b) = 1$ if and only if $(a + b, ab) = 1$. First we show the if condition. So we have,

$$(a + b, ab) = 1$$

which means that,

$$(a + b)m + abn = 1 \text{ for some } m, n \in \mathbb{Z}$$

Now we have,

$$\begin{aligned} am + bm + abn &= 1 \\ a(m + bn) + bm &= 1 \\ ax + by &= 1 \end{aligned}$$

By definition this means that $(a, b) = 1$

Now we show the only if condition.

Let's assume the contrary that $(a + b, ab) = x > 1$ so we have,

$$x | a + b \text{ and } x | ab$$

If $x | ab$ let p be a prime dividing x then it must mean either $p | a$ or $p | b$ as p can't divide a and b as $gcd(a, b) = 1$. So assume without loss of generality that $p | a$. Now we know that $x | a + b$ which means $p | a + b$. But if $p | a + b$ and $p | a$, then that must mean p also divides their difference or that $p | (a + b) - a$ or $p | b$. However, then we get that $p | a$ and $p | b$ or that a and b are not coprime as $p \neq 1$ which is a contradiction as we know that $gcd(a, b) = 1$. Hence, our assumption must be wrong and it must be true that $(a + b, ab) = 1$.

Problem 8

We need to compute $gcd(441, 1155)$ using the euclidean algorithm,

$$\begin{aligned}
1155 &= 441 \times 2 + 273 \\
441 &= 273 \times 1 + 168 \\
273 &= 168 \times 1 + 105 \\
168 &= 105 \times 1 + 63 \\
105 &= 63 \times 1 + 42 \\
63 &= 42 \times 1 + 21 \\
42 &= 21 \times 2 + 0
\end{aligned}$$

This gives us the GCD as 21
To find the linear combination we go backwards to get,

$$\begin{aligned}
1 \times 105 &= 63 + (63 - 21) = 2 \times 63 - 21 \\
2 \times 168 &= 2 \times 105 + (105 + 21) = 3 \times 105 + 21 \\
3 \times 273 &= 3 \times 168 + (2 \times 168 - 21) = 5 \times 168 - 21 \\
5 \times 441 &= 5 \times 273 + (3 \times 273 + 21) = 8 \times 273 + 21 \\
8 \times 1155 &= 16 \times 441 + (5 \times 441 - 21) = 21 \times 441 - 21
\end{aligned}$$

This gives us,

$$21 \times 441 - 8 \times 1155 = 21$$

Problem 9

We need to find two rations with denominators 11 and 13 whose sum is $\frac{7}{143}$. Consider the rationals to be $\frac{p}{11}$ and $\frac{q}{13}$ so we have,

$$\begin{aligned}
\frac{p}{11} + \frac{q}{13} &= \frac{7}{143} \\
\frac{13p + 11q}{143} &= \frac{7}{143} \\
13p + 11q &= 7
\end{aligned}$$

We know that 13 and 11 have gcd of 1 so there exists m, n such that $13m+11n = 1$.

$$\begin{aligned}
13 &= 11 \times 1 + 2 \\
11 &= 2 \times 5 + 1 \\
5 \times 13 &= 5 \times 11 + (11 - 1) \\
6 \times 11 - 5 \times 13 = 1
\end{aligned}$$

Multiplying this by 7 we get,

$$11 \times 42 + 13 \times -35 = 7$$

Hence we get $p = -35$ and $q = 42$ to get,

$$\frac{-35}{11} + \frac{42}{13} = \frac{7}{143}$$