Number Theory - Some Problems & Solutions

Sudev Naduvath

Problem 1. For all integers $n > 1$, show that the numbers $n^4 + 4$ and $8^n + 1$ are composite.

Sol: consider the integer $n^4 + 4$, where $n > 1$. Then,

$$\begin{aligned} n^4 + 4 &= (n^2)^2 + 2^2 \\ &= (n^2+2)^-(2n)^2 && (as\ a^2+b^2 = (a+b)^2 - 2ab) \\ &= (n^2+2-2n)(n^2+2+2n) && (as\ a^2-b^2 = (a+b)(a-b) \end{aligned}$$

That is, $n^4 + 4$ is a product of two integers and hence is not a prime.

From the factorization, we have $a^3 + 1 = (a+1)(a^2 - a + 1)$. Therefore, by a=2n we have

$$\begin{aligned} 8^n + 1 &= (2^3)^n + 1 \\ &= (2^n)^3 + 1 \\ &= (2^n+1)(2^{2n} - 2^n + 1). \end{aligned}$$

Since $2n > 1$ for any $n \in \mathbb{N} \cup \{0\}$ and $2^n + 1 = 8^n + 1 \iff n = 0$, we have $2^n + 1$ is a proper divisor of $8^n + 1$ for any $n \in \mathbb{N}$. Thus, $8^n + 1$ is composite. $\square$

Problem 2. Prove or disprove: The sum of squares of two odd integers cannot be a perfect square.

Sol: Assume to the contrary that the sum of the squares of two odd integers can be the square of an integer. Suppose that $x, y, z \in \mathbb{Z}$ such that $x^2 + y^2 = z^2$, and x and y are odd. Since x and y are odd, both x^2 and y^2 are odd and hence $x^2 + y^2$ must be even.

Let $x = 2m + 1$ and $y = 2n + 1$. Hence,

$$\begin{aligned} x^2 + y^2 &= (2m+1)^2 + (2n+1)^2 \\ &= 4m^2 + 4m + 1 + 4n^2 + 4n + 1 \end{aligned}$$

$$
\begin{aligned}
&= 4(m^2+n^2)+4(m+n)+2 \\
&= 2[2(m^2+n^2)+2(m+n)+1]
\end{aligned}
$$

Since $2(m^2+n^2)+2(m+n)+1$ is odd, which is a contradiction to the fact that x^2+y^2 is even. Hence, the sum of the squares of two odd integers cannot be the square of an integer. □

Problem 3. Prove or disprove: The product of four consecutive integers is 1 less than a perfect square.

Sol: Let the numbers be $n, n+1, n+2, n+3$. Therefore,

$$n(n+1)(n+2)(n+3) = n^4+6n^3+11n^2+6n. \tag{1}$$

If this last expression is a perfect square, it must be the square of something of the form n^2+an+b for some a and b. Squaring n^2+an+b, we get

$$(n^2+an+b)^2 = n^4+2an^3+(a^2+2b)n^2+(2ab)n+b^2. \tag{2}$$

Comparing Equations (1) and (2) and equating the coefficients of the RHS of these equations, we get $2a = 6, a2+2b = 11, 2ab = 6, b^2 = 1$.

Solving these equations, we get $a = 3, b = 1$. Therefore, we have

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

as required. □

Problem 4. Prove or disprove: There is an infinite number of primes.

Sol: Assume there are a finite number, say $p_i, 1 \leq i \leq n$, of primes and let p_n the largest of those primes. Consider the number that is the product of these, plus one: $N = p_1 p_2 \ldots p_n + 1$. By construction, N is not divisible by any of the p_i. Hence it is either prime itself, or divisible by another prime greater than p_n , contradicting the assumption that p_n is the largest prime. Hence, there are infinite number of primes. □

Problem 5. A certain numbers of sixes and nines are added to give a sum of 126. If the numbers of sixes and nines are interchanged, the new sum is 114. How many of each were there originally?

Sol: Let the number of sixes be x and number of nines be y. Then, we get the equations $6x+9y = 126$ and $9x+6y = 114$. Solving for x and y, (use Diophantine Equations method to solve these equations. The solution is left to the learner. □

Problem 6. Divide 100 into two summands such that one is divisible by 7 and the other is divisible by 11.

Sol: Let $100 = m + n$, where $7 \mid m$ and $11 \mid n$. Then, $m = 7x$ and $n = 11y$ for some integers x and y and hence we have $7x + 11y = 100$, which a Diophantine equation. Rest of the solution is left to the learner. □

Problem 7. A small clothing manufacturer produces two styles of sweaters: cardigan and pullover. She sells cardigans for \$31 each and pullovers for \$28 each. If her total revenue from a day's production is \$1460, how many of each type might she manufacture in a day?

Sol: Let x denotes the number of cardigans and y denotes the number of pullovers manufactured. Then, we have $31x + 28y = 1460$, which is a Diophantine equation. Rest of the solution is left to the learner. □

Problem 8. Obtain three consecutive integers such that each integer having a square factor.

Sol: Let $x, x+1, x+2$ be the three required consecutive integers with square factors. Therefore, $2^2 \mid x, 3^2 \mid x+1$ and $5^2 \mid x+2$ (note that we are not taking $4^2 \mid x+2$ since if so, obviously $2^2 \mid x+2$, which is not possible).

Since $4 \mid x$, we have $x \equiv 0 (\text{mod } 4)$. Since $9 \mid x+1$, we have $x \equiv -1 (\text{mod } 9)$ or equivalently $x \equiv 8 (\text{mod } 9)$. In a similar way, we have $25 \mid x+2$ and hence we have $x \equiv -2 (\text{mod } 25)$ or equivalently, we have $x \equiv 23 (\text{mod } 25)$.

Hence, we get a system of simultaneous linear congruences

$$\begin{aligned} x &\equiv 0 (\text{mod } 4) \\ x &\equiv 8 (\text{mod } 9) \\ x &\equiv 23 (\text{mod } 25) \end{aligned}$$

We can use the Chinese remainder Theorem to find the solution of the above system of linear congruences and the rest of the solution is left to the learner. □

Problem 9. Obtain three consecutive integers such that the first of which is divisible by a square, the second of which is divisible by a cube and the third is divisible by a fourth power.

Sol: Here, we want to find the integer x such that $5^2 \mid x, 3^3 \mid x+1$ and $2^4 \mid x+2$. Then,

(i) $5^2 \mid x \implies x \equiv 0 \ (\text{mod } 25)$.

(ii) $3^3 \mid x+1 \implies x \equiv -1 \ (\text{mod } 27) \implies x \equiv 26 \ (\text{mod } 27)$.

(iii $2^4 \mid x+2 \implies x \equiv -2 \ (\text{mod } 16) \implies x \equiv 14 \ (\text{mod } 16)$.

Hence, we get a system of simultaneous linear congruences

$$\begin{aligned} x &\equiv 0 (\text{mod } 25) \\ x &\equiv 26 (\text{mod } 27) \\ x &\equiv 14 (\text{mod } 16) \end{aligned}$$

We can use the Chinese remainder Theorem to find the solution of the above system of linear congruences and the rest of the solution is left to the learner. □

Problem 10. What is the remainder when the sum $1^5 + 2^5 + 3^5 + \ldots + 99^5 + 100^5$ is divided by 4?

Sol: Note that

$$\begin{aligned} 1^5 &\equiv 1 \pmod 4 \\ 2^5 &\equiv 0 \pmod 4 \\ 3^5 &\equiv 3 \pmod 4 \\ 4^5 &\equiv 0 \pmod 4 \end{aligned}$$

Therefore, $1^5 + 2^5 + 3^5 + 4^5 \equiv 1 + 3 \pmod 4 = 0 \pmod 4$.
Similarly,

$$\begin{aligned} 5^5 &\equiv 1 \pmod 4 \\ 6^5 &\equiv 0 \pmod 4 \\ 7^5 &\equiv 3 \pmod 4 \\ 8^5 &\equiv 0 \pmod 4 \end{aligned}$$

Hence, $5^5 + 6^5 + 7^5 + 8^5 \equiv 1 + 3 \pmod 4 = 0 \pmod 4$.
The pattern follows throughout and hence 0 is the remainder when $1^5 + 2^5 + 3^5 + \ldots + 99^5 + 100^5$ is divided by 4. □

Problem 11. For any integer a, show that $a^2 - a + 7$ ends in one of the digits $3, 7$ or 9.

Sol:

Problem 12. If p is an odd prime, the use Fermat's theorem to prove that

(i) $1^{p-1} + 2^{p-1} + 3^{p-1} + \ldots + (p-1)^{p-1} \equiv \ 1 \pmod p$.

(ii) $1^p + 2^p + 3^p + \ldots + (p-1)^p \equiv \ 0 \pmod p$.

Sol: (i) Since p is an odd prime, $p \not| a$ if $a < p$. Therefore, by Fermat's Theorem, $a^{p-1} \equiv 1 \pmod{p}$. Therefore, we have

$$\begin{array}{rcl} 1^{p-1} & \equiv & 1 \pmod{p} \\ 2^{p-1} & \equiv & 1 \pmod{p} \\ 3^{p-1} & \equiv & 1 \pmod{p} \\ \vdots & \vdots & \vdots \\ (p-1)1^{p-1} & \equiv & 1 \pmod{p} \end{array}$$

Now adding all the above congruences, we have

$$\begin{aligned} 1^{p-1} + 2^{p-1} + 3^{p-1} + \ldots + (p-1)^{p-1} &\equiv (p-1) \pmod{p} \\ &\equiv -1 \pmod{p}. \end{aligned}$$

(ii) By Fermat's Theorem, for any integer a $a^p \equiv a \pmod{p}$. Therefore, we have

$$\begin{array}{rcl} 1^{p} & \equiv & 1 \pmod{p} \\ 2^{p} & \equiv & 2 \pmod{p} \\ 3^{p} & \equiv & 3 \pmod{p} \\ \vdots & \vdots & \vdots \\ (p-1)1^{p} & \equiv & (p-1) \pmod{p} \end{array}$$

Now adding all the above congruences, we have

$$\begin{aligned} 1^p + 2^p + 3^p + \ldots + (p)^p &\equiv (1 + 2 + \ldots + (p-1)) \pmod{p} \\ &\equiv \frac{(p-1)p}{2} \pmod{p} \end{aligned}$$

Since p is an odd prime, $p-1$ is even and hence $\frac{p-1}{2}$ is an integer. Hence, we have $\frac{p-1}{2} \equiv 0 \pmod{p}$. Therefore, from the above two congruences, we have

$$1^p + 2^p + 3^p + \ldots + (p)^p \equiv 0 \pmod{p}.$$

$\square$

Problem 13. Assuming that a and b are integers not divisible by the prime p, establish the following:

(i) If $a^p \equiv b^p \pmod{p}$, then $a \equiv b \pmod{p}$.

(ii) If $a^p \equiv b^p \pmod{p}$, then $a^p \equiv b^p \pmod{p^2}$.

Sol: (i) We have $a^p \equiv a(\text{mod } p)$, by Fermat's Theorem. Then, by symmetry, we have $a \equiv a^p(\text{mod } p)$. Also, given that $a^p \equiv b^p(\text{mod } p)$. Then, by transitivity, we have Also, given that $a \equiv b^p(\text{mod } p)$. Again by Fermat's Theorem, we have $b^p \equiv b(\text{mod } p)$, Therefore, by transitivity we have $a \equiv b(\text{mod } p)$.

(ii) Given that $a^p \equiv b^p(\text{mod } p)$. Therefore, by (i), we have $p \mid a - b$ or equivalently, $a = b + pk$, for some positive integer k. Then, we have

$$\begin{aligned}
a^p - b^p &= (b+pk)^p - b^p \\
&= \left[b^p + \binom{n}{1} b^{p-1}pk + \binom{n}{2} b^{p-2}(pk)^2 + \ldots + \binom{n}{n}(pk)^n\right] - b^p \\
&= \binom{p}{1} b^{p-1}pk + \binom{p}{2} b^{p-2}(pk)^2 + \ldots + \binom{p}{p}(pk)^n \\
&= p.b^{p-1}pk + \frac{p(p-1}{2} b^{p-2}(pk)^2 + \ldots + (pk)^n
\end{aligned}$$

Note that every term in the above expression contains p^2 or higher powers of p and hence $p^2 \mid a^p - b^p$ or equivalently, $a^p \equiv b^p(\text{mod } p^2)$. $\square$