MTH 26001 - Elementary Number Theory

Student ID: 20202026.

Student Name: Nguyen Minh Duc.

~~ASSIGN~~

ASSIGNMENT 2.

Sec 3.1.

Problem 4.

⊗ Since $p \geq 5$ is an odd prime, when dividing by 6, p takes the form of $6k+1$, $6k+3$ or $6k+5$ $(k \in \mathbb{Z})$.

⊗ However, $6k+3 = 3(3k+1)$ is divisible by 3, hence, not prime.

Thus, for $p \geq 5$ is a prime number, p takes one of the forms $6k+1$ or $6k+5$.

⊗ Case 1. $p = 6k+1$, $k \in \mathbb{Z}$.

$p^2+2 = (6k+1)^2+2 = 36k^2+12k+1+2 = 36k^2+12k+3 = 3(12k^2+4k+1)$

$\Rightarrow 3 \mid p^2+2 \Rightarrow p^2+2$ is composite. — (1)

⊗ Case 2: $p = 6k+5$, $k \in \mathbb{Z}$.

$p^2+2 = (6k+5)^2+2 = 36k^2+60k+25+2 = 36k^2+60k+27 = 3(12k^2+20k+9)$.

$\Rightarrow 3 \mid p^2+2 \Rightarrow p^2+2$ is composite. — (2).

⊗ From (1) and (2), if $p \geq 5$ is prime then p^2+2 is composite.

Problem 8. $p \geq q \geq 5$.

* let $\begin{cases} p = 6k_1 + r_p, \ k_1 \in \mathbb{Z}, 0 \leq r_p < 6 \\ q = 6k_2 + r_q, \ k_2 \in \mathbb{Z}, 0 \leq r_q < 6 \end{cases}$.

From the ~~pse~~ previous problem, we know that $r_p, r_q \in \{1, 5\}$

* $p^2 - q^2 = (p+q)(p-q) = (6k_1 + 6k_2 + r_p + r_q)(6k_1 - 6k_2 + r_p - r_q)$.

Consider 2 cases:

* Case 1. $r_p = r_q \Rightarrow \begin{cases} r_p + r_q \in \{2, 10\} \Rightarrow r_p + r_q = 2k_3 \ (\cancel{k_3 \in \mathbb{Z}}) \text{ is even.} \\ r_p - r_q = 0. \end{cases}$ $(k_3 \in \{1, 5\})$

Now, we obtain: $p^2 - q^2 = (6k_1 + 6k_2 + 2k_3)(6k_1 - 6k_2)$.

$= 2 \times 6 \times (3k_1 + 3k_2 + k_3)(k_1 - k_2)$.

Note that $k_3 \in \{1, 5\}$ is odd.

- If both k_1 and k_2 is even or odd, then $k_1 - k_2$ is even, i.e. $k_1 - k_2 = 2k'$, $k' \in \mathbb{Z}$.

$\Rightarrow p^2 - q^2 = 2 \times 6 \times 2(3k_1 + 3k_2 + k_3)k'$

$= 24k'(3k_1 + 3k_2 + k_3)$.

$\Rightarrow 24 \mid p^2 - q^2$. — (1)

- If one of k_1 or k_2 is even and the other is odd, then $k_1 + k_2$ is odd.

This implies $3k_1 + 3k_2$ is also odd, hence $3k_1 + 3k_2 + k_3$ is even ($\because k_3$ is odd).

$\Rightarrow 3k_1 + 3k_2 + k_3 = 2k'$, $k' \in \mathbb{Z}$.

Now, $p^2 - q^2 = 2 \times 6 \times 2 \times k'(k_1 - k_2)$.

$= 24k'(k_1 - k_2)$

$\Rightarrow 24 \mid p^2 - q^2$. — (2)

* Case 2. $r_p \neq r_q \Rightarrow \begin{cases} r_p + r_q = 6. \\ r_p - r_q \in \{-4, 4\} \Rightarrow r_p - r_q = \pm 4. \end{cases}$

Now, we obtain: $p^2 - q^2 = (6k_1 + 6k_2 + 6)(6k_1 - 6k_2 \pm 4)$.

$= 2 \times 6 \times (k_1 + k_2 + 1)(3k_1 - 3k_2 \pm 2)$.

- If both k_1 and k_2 is even or odd, $k_1 - k_2$ is even $\Rightarrow 3k_1 - 3k_2 \pm 2$ is also even
$\Rightarrow 3k_1 - 3k_2 \pm 2 = 2k'$, $k' \in \mathbb{Z}$.

Now, $p^2 - q^2 = 2 \times 6 \times 2 \times (k_1 + k_2 + 1)k'$

$= 24(k_1 + k_2 + 1)k'$

$\Rightarrow 24 \mid p^2 - q^2$. — (3)

- If one of k_1 and k_2 is even and the other is odd then $k_1 + k_2 + 1$ is even.

So $k_1 + k_2 + 1 = 2k'$, $k' \in \mathbb{Z}$.

Now, $p^2 - q^2 = 2 \times 6 \times 2 \times k'(3k_1 - 3k_2 \pm 2)$

$= 24k'(3k_1 - 3k_2 \pm 2)$

$\Rightarrow 24 \mid p^2 - q^2$ — (4).

* From (1), (2), (3) and (4), in any case, $24 \mid p^2 - q^2$ for $p \geq q \geq 5$ are primes.

Problem 13. $n > 1$

⊗ $n = 6k + r$, $k \in \mathbb{Z}$, $r \in \{0, 1, 2, 4, 5\}$

~~⊗ Case 1. r is even, i.e.~~

⊗ Case 1. r is even, i.e. $r \in \{0, 2, 4\}$.

Let $r = 2k'$, $k' \in \mathbb{Z}$.

Now, $n = 6k + 2k' = 2(3k + k')$

$\Rightarrow 2 \mid n \Rightarrow 2 \mid n^2 \Rightarrow 2 \mid n^2 + 2^n$ ($\because 2 \mid 2^n, n > 1$). — ①.

⊗. Case 2. r is odd, i.e $r \in \{1, 5\}$. $\Rightarrow n$ is also odd.

For $r = 5$, $n = 6k + 5 = 6k + 6 - 1 = 6(k+1) - 1$, $k \in \mathbb{Z}$.

Hence, n is of the form $6k - 1$ where $k \in \mathbb{Z}$.

Now, $r \in \{-1, 1\} \Rightarrow r = \pm 1$.

Substitute in $n^2 + 2^n$, we have:

$$n^2 + 2^n = (6k \pm 1)^2 + 2^n = 36k^2 \pm 12k + 1 + 2^{6k+1}.$$

Note that $x^n + y^n = (x + y)(x^{n-1} - x^{n-2}y + \ldots + (-1)^{n-1}y^{n-1})$ for n is odd.

Substitute $(x, y) = (1, 2)$, we obtain.

$$1 + 2^{6k+1} = 1^{6k+1} + 2^{6k+1} = (1+2)(1^{6k} - 1^{6k-1}.2 + \ldots + (-1)^{6k}.2^{6k}).$$

$$= 3u,$$

where $u = 1^{6k} - 1^{6k-1}.2 + \ldots + (-1)^{6k}.2^{6k} \Rightarrow u \in \mathbb{Z}$.

Now, we have: $n^2 + 2^n = 36k^2 \pm 12k + 3u$.

$= 3(12k^2 \pm 4k + u)$.

$\Rightarrow 3 \mid n^2 + 2^n$. — ②.

⊗. Note that $n > 1 \Rightarrow n^2 + 2^n > 1^2 + 2^1 \Rightarrow n^2 + 2^n > 3$ — ③.

From ①, ②, ③, $\Rightarrow n^2 + 2^n$ is composite for $n > 1$.

Sec 3.2

Problem 2. $\sqrt{200} \simeq 14.14$

⊗ Since $14 < \sqrt{200} < 15$, it is suffice to test prime less than 14, i.e. $p \in \{2, 3, 5, 7, 11, 13\}$.

~~100~~	$\boxed{101}$	~~102~~	$\boxed{103}$	~~104~~	~~105~~	~~106~~	$\boxed{107}$	~~108~~	$\boxed{109}$
~~110~~	~~111~~	~~112~~	$\boxed{113}$	~~114~~	~~115~~	~~116~~	~~117~~	~~118~~	~~119~~
~~120~~	~~121~~	~~122~~	~~123~~	~~124~~	~~125~~	~~126~~	$\boxed{127}$	~~128~~	~~129~~
~~130~~	$\boxed{131}$	~~132~~	~~133~~	~~134~~	~~135~~	~~136~~	$\boxed{137}$	~~138~~	$\boxed{139}$
~~140~~	~~141~~	~~142~~	~~143~~	~~144~~	~~145~~	~~146~~	~~147~~	~~148~~	$\boxed{149}$
~~150~~	$\boxed{151}$	~~152~~	~~153~~	~~154~~	~~155~~	~~156~~	$\boxed{157}$	~~158~~	~~159~~
~~160~~	~~161~~	~~162~~	$\boxed{163}$	~~164~~	~~165~~	~~166~~	$\boxed{167}$	~~168~~	~~169~~
~~170~~	~~171~~	~~172~~	$\boxed{173}$	~~174~~	~~175~~	~~176~~	~~177~~	~~178~~	$\boxed{179}$
~~180~~	$\boxed{181}$	~~182~~	~~183~~	~~184~~	~~185~~	~~186~~	~~187~~	~~188~~	189
~~190~~	$\boxed{191}$	~~192~~	$\boxed{193}$	~~194~~	~~195~~	~~196~~	$\boxed{197}$	~~198~~	$\boxed{199}$
~~200~~									

Problem 4.

(a) Assume that $\sqrt{p}$ is rational, i.e. $\sqrt{p} = \frac{r}{s}$, $r, s \in \mathbb{Z}$ and $\gcd(r,s) = 1$.

Now, square both sides: $p = \frac{r^2}{s^2} \Rightarrow ps^2 = r^2$

$\Rightarrow p \mid r^2 \Rightarrow p \mid r.$

Let $r = pk$, $k \in \mathbb{Z}$, now, $ps^2 = p^2k^2 \Rightarrow s^2 = pk^2$

$\Rightarrow p \mid s^2 \Rightarrow p \mid s.$

Since p is prime, $p > 1$. Thus, $\begin{cases} p \mid r \\ p \mid s \end{cases} \Rightarrow \gcd(r,s) \neq 1$, contradicts assumption $\gcd(r,s) = 1$.

Therefor, $\sqrt{p}$ is irrational for p is prime.

(b) Let $\sqrt[n]{a} = \frac{p}{q}$, $p, q \in \mathbb{Z}$ and $\gcd(p,q) = 1$.

$\Rightarrow a = \frac{p^n}{q^n} \Rightarrow aq^n = p^n \Rightarrow q^n \mid p^n \Rightarrow q \mid p$, but $\gcd(p,q) = 1$

$\Rightarrow q = 1.$

Thus, $\sqrt[n]{a} = \frac{p}{q} = p \in \mathbb{Z}$.

(c) Assume $\sqrt[n]{n}$ is rational.

From (b), $\sqrt[n]{n}$ is actually integer.

Let $x = \sqrt[n]{n} \Rightarrow x^n = n$, but $n < 2^n$

$\Rightarrow x^n < 2^n$

$\Rightarrow x < 2$

Since $n \geq 2$, $\sqrt[n]{n} \geq \sqrt[2]{2} > 1$. $\Big\} \Rightarrow 1 < x < 2$. But $x \in \mathbb{Z}$.

$\Rightarrow$ This is a contradiction.

Thus, $\sqrt[n]{n}$ is irrational.

Problem 5.

Since n is prime $\Leftrightarrow p \nmid n \ \forall p \leq \sqrt{n}$,

n is composite $\Leftrightarrow \exists p \leq \sqrt{n} : p \mid n$.

Now, $\sqrt{999} > \sqrt{936} = 31 \Rightarrow \sqrt{999} > 31$.

Hence, for any 3-digit composite, i.e. less than 999 will have a prime divisor less than ~~31~~ or equal to 31.

Problem 12.

(a) Base case: For $n = 5$, $P_n = 11 > 2(5) - 1 = 9$.

$\Rightarrow$ The statement is true for $n = 5$.

Induction: Assume that the statement is true for $n = k$,

That is $P_k > 2k - 1$.

$\Rightarrow P_k + 2 > 2k - 1 + 2 = 2(k+1) - 1$.

Since $P_k + 1$ is even, the next prime must be at least $P_k + 2$,

Thus, $P_{k+1} \geq P_k + 2 > 2(k+1) - 1$.

$\Rightarrow$ The statement also holds for $n = k+1$.

Thus, by induction hypothesis, $P_n > 2n - 1 \ \forall n \geq 5$.

(b) Note that $P_1 = 2$, $P_n = 2(P_2 P_3 \cdots P_n) + 1 \Rightarrow P_n$ is odd.

Using Division algorithm, $P_n = 4k + r$, $k \in \mathbb{Z}$, $0 \leq r < 4$.

Since P_n is odd, $r \in \{1, 3\}$.

If $r = 1$, then ~~P~~ $P_1 P_2 \cdots P_n + 1 = 4k + 1 \Rightarrow 2(P_2 P_3 \cdots P_n) = 4k \Rightarrow P_2 P_3 \cdots P_n = 2k$.

But it is impossible since P_i is odd for $i > 1$.

Thus, $r = 3$, i.e. $P_n = 4k + 3$, $\forall n$.

Let $P_n = s^2$, $s \in \mathbb{Z}$. $\Rightarrow s^2$ is odd $\Rightarrow s$ is also odd. Let $s = 2a + 1$, $a \in \mathbb{Z}$.

Now, $\underset{4k+3 =}{~~s^2=4k+3~~}\ s^2 = (2a+1)^2 = 4a^2 + 4a + 1 = 4(a^2 + a) + 1$.

Note that the left hand side is of form $4k+1$ while the right is of the form $4k+1$

~~Thus~~ $\Rightarrow$ This is contradiction, hence P_n cannot be perfect square $\forall n$.

(c) Let $S_n = \frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_n}$. Assume that S_n is an integer.

Now, we have:

$$p_1 p_2 \cdots p_n S_n = 2 p_2 \cdots p_n \left(\frac{1}{\cancel{p_1}2} + \frac{1}{p_2} + \cdots + \frac{1}{p_n} \right)$$

$$= \underbrace{p_2 p_3 \cdots p_n}_{\text{Odd}} + \underbrace{2 p_3 p_4 \cdots p_n + \cdots + 2 p_2 p_3 \cdots p_{n-1}}_{\text{Even}}.$$

$\Rightarrow p_1 p_2 \cdots p_n S_n$ is odd.

However, $p_1 = 2$, which implies $p_1 p_2 \cdots p_n S_n = 2(p_2 p_3 \cdots p_n S_n)$ is even.

This is contradiction, hence, S_n ~~can~~ is never an integer, $\forall n$.

Sec 3.3

Problem 12.

From the hint, we know that $p_{n+3}^2 < 4p_{n+2}^2 < 8 p_{n+1} p_{n+2}$.

Since $p_5 = 11 > 8$, we obtain:

$$p_{n+3}^2 < 8 p_{n+1} p_{n+2} < p_5 p_{n+1} p_{n+2}.$$

Thus, for $n \geq 5$, we have $p_n \geq p_5$, hence, the inequality holds:

$$p_{n+3}^2 < p_5 p_{n+1} p_{n+2} = p_n p_{n+1} p_{n+2}.$$

For $n = 4$, $p_{4+3}^2 = p_7^2 = 17^2 = 289 < 1001 = 7 \times 11 \times 13 = p_4 p_5 p_6$.

For $n = 3$, $p_{3+3}^2 = p_6^2 = 13^2 = 169 < 385 = 5 \times 7 \times 11 = p_3 p_4 p_5$.

Therefore, $p_{n+3}^2 < p_n p_{n+1} p_{n+3}$ $\forall n \geq 3$.

Problem 13.

⊗ Firstly, let's calculate products of numbers of form $6k+1$ and $6k+3$.

$(6k_1+1)(6k_2+1) = 36k_1k_2 + 6k_1 + 6k_2 + 1 = 6(6k_1k_2 + k_1 + k_2) + 1$

$(6k_1+1)(6k_2+3) = 36k_1k_2 + 18k_1 + 6k_2 + 3 = 6(6k_1k_2 + 3k_1 + k_2) + 3$

$(6k_1+3)(6k_2+3) = 36k_1k_2 + 18k_1 + 18k_2 + 9 = 6(6k_1k_2 + 3k_1 + 3k_2 + 1) + 3.$

Thus, Product of numbers in the form $6k+1$ and $6k+3$ will also be in the form of $6k+1$ and $6k+3$.

- Assume that there are only finite number of primes of form $6n+5$. Let those primes be $p_1, p_2, \cdots, p_k$.
- Consider $Q = 6p_1p_2\cdots p_k - 1 = 6(p_1p_2\cdots p_k - 1) + 5$.

  Let $Q = r_1 r_2 \dots r_s$ be prime factorization.

  Since Q is odd, $r_i \neq 2 \; \forall i \Rightarrow r_i$ can be of the form $6n+1, 6n+3$ or $6n+5$.
- We know that product of numbers of form $6n+1$ and $6n+3$ will also be of form $6n+1$ and $6n+3$. ~~Thus~~

  Thus, Q must contain at least 1 prime factor r_i of form $6n+5$.
- From the construction of Q,

$$Q - 6p_1p_2\cdots p_k = -1 \Rightarrow 1 = 6p_1p_2\cdots p_k - Q.$$

  Note that $r_i \mid 6p_1p_2\cdots p_k$ and $r_i \mid Q$.

  $\Rightarrow r_i \mid 6p_1p_2\cdots p_k - Q \Rightarrow r_i \mid 1$ ~~$\Rightarrow r_i$~~ But r_i is a prime.

  This is a contradiction, thus, there are infinitely many prime number of the form $6n+5$.

Problem 20.

- For $p \geq 5$, we know that $p = 6k+1$ or $p = 6k+5$.

$$\Rightarrow p^2+8 = 36k^2+12k+9 \text{ or } p^2+8 = 36k^2+60k+33.$$
$$= 3(12k^2+4k+3) \qquad\qquad = 3(12k^2+20k+11).$$

  In both cases, $3 \mid p^2+8$ and since $p^2+8 > 3$, p^2+8 is composite.

  Thus, if $p \geq 5$ is a prime number, p^2+8 cannot be prime.
- For $p = 3$, $p^2+8 = 3^2+8 = 17$ is a prime number.

  Consider $p^3+4 = 3^3+4 = 31$ also a prime number
- For $p = 2$, $p^2+8 = 2^2+8 = 12$ not a prime number $\Rightarrow$ Needn't proceed
- Thus, if ~~p is a~~ p and p^2+4 are both prime numbers then p^3+4 is also prime.