MAT2120 Number Theory
Problems I

Suhyun Park (20181634)

Department of Computer Science and Engineering, Sogang University

1. Show that $(a, c) = 1$, $(b, c) = 1$ if and only if $(ab, c) = 1$.

Proof. ($\Rightarrow$) Suppose $(ab, c) = d > 1$. Then

$$d \mid c, d \mid ab.$$

For all integers d_1, d_2 such that $d_1 \mid a$, $d_2 \mid b$ and $d = d_1 d_2$,

$$d_1 \mid c, d_2 \mid c \Rightarrow (a, c) = d_1, (b, c) = d_2.$$

Since $d_1 d_2 = d > 1$, $d_1 > 1$ or $d_2 > 1$. This is a contradiction; thus $(ab, c) = 1$ if $(a, c) = 1$, $(b, c) = 1$.

($\Leftarrow$) Suppose $(a, c) = d > 1$. Then $d \mid ab$, thus $(ab, c) = d > 1$, which contradicts. Similarly when if $(b, c) = d > 1$, $(ab, c) = d > 1$. Thus $(a, c) = 1$, $(b, c) = 1$ if $(ab, c) = 1$. $\square$

2. If $(a, b) = 1$, prove that $(a + b, a - b) = 1$ or 2.

Proof. Since $(a, b) = 1$, $(2a, 2b) = 2$.

Let $(a + b, a - b) = d$. Then

$$\begin{aligned} & d \mid (a+b), d \mid (a-b) \\ \Rightarrow & d \mid [(a+b) + (a-b)], d \mid [(a+b) - (a-b)] \\ \Rightarrow & d \mid 2a, d \mid 2b \end{aligned}$$

Thus $d = 1$ or 2, given the fact that $(2a, 2b) = 2$. $\square$

3. Let $(a, b) = 10$. Find all possible values of $\left(a^3, b^4\right)$.

Lemma 1. *If $(x, y) = 1$, $\left(x^a, y^b\right) = 1$ for nonnegative integers a and b.*

Proof. If the set of prime factors of x is $P = \{p_1, p_2, \cdots, p_n\}$, and that of y is $Q = \{q_1, q_2, \cdots, q_m\}$, i. e.

$$x = \prod_{k=1}^{n} p_k^{e_k}$$
$$y = \prod_{k=1}^{m} q_k^{e'_k}$$

for $e_i, e'_i \in \mathbb{Z}^+$, then clearly if and only if $P \cap Q = \emptyset$, then $(x, y) = 1$.

Since

$$x^a = \left[\prod_{k=1}^{n} p_k^{e_k}\right]^a = \prod_{k=1}^{n} p_k^{ae_k}$$
$$y^b = \left[\prod_{k=1}^{m} q_k^{e'_k}\right]^b = \prod_{k=1}^{m} q_k^{be'_k},$$

the set of prime factors of x^a is also P, and that of y^b is also Q. Since $P \cap Q = \emptyset$, $\left(x^a, y^b\right) = 1$. $\square$

Since $(a, b) = 10$, $10 \mid a$, $10 \mid b$. We let $a = 10a_0$ and $b = 10b_0$, hence $(a_0, b_0) = 1$. Then

$$\begin{aligned}\left(a^3, b^4\right) &= \left(10^3 a_0^3, 10^4 b_0^4\right) \\ &= 10^3 \left(a_0^3, 10 b_0^4\right)\end{aligned}$$

Suppose $\left(a_0^3, 10b_0^4\right) = k$, which $k \mid a_0^3$ and $k \mid 10b_0^4$. Note that $\left(a_0^3, b_0^4\right) = 1$ by Lemma and $k \mid a_0^3$, hence $k \nmid b_0^4$, thus $k \mid 10$.

Since a and b are nonnegative, possible values for k is 1, 2, 5, and 10. Thus, possible values of $\left(a^3, b^4\right) = 10^3 k$ is 10^3, $2 \cdot 10^3$, $5 \cdot 10^3$, and 10^4.

4. Show that $e = \sum_{n=0}^{\infty} \frac{1}{n!}$ is irrational. (Hint. Suppose $e = \frac{p}{q}$ with positive integers p and q. Show that $q!e$ and $q!\sum_{n=0}^{q} \frac{1}{n!}$ are both integers.)

Proof. Suppose that $e = \sum_{n=0}^{\infty} \frac{1}{n!}$ is rational. i. e., there exists positive integers p and q such that $e = \frac{p}{q}$.

Then $q!e = (q-1)!qe = (q-1)!p$ is an integer. Also,

$$\begin{aligned} q! \sum_{n=0}^{q} \frac{1}{n!} &= \sum_{n=0}^{q} \frac{q!}{n!} \\ &= \sum_{n=0}^{q} \prod_{k=n+1}^{q} k \end{aligned}$$

is an integer. Thus,

$$\begin{aligned} q!e - q! \sum_{n=0}^{q} \frac{1}{n!} &= q! \sum_{n=0}^{\infty} \frac{1}{n!} - q! \sum_{n=0}^{q} \frac{1}{n!} \\ &= q! \sum_{n=q+1}^{\infty} \frac{1}{n!} \end{aligned}$$

should be also an (positive) integer.

Since

$$\frac{q!}{n!} = \frac{1}{\prod_{k=q+1}^{n} k} \leq \frac{1}{(q+1)^{n-q}}$$

is strict for every $n \geq b+2$, we can conclude that

$$\begin{aligned} q! \sum_{n=q+1}^{\infty} \frac{1}{n!} &< \sum_{n=q+1}^{\infty} \frac{1}{(q+1)^{n-q}} \\ &= \sum_{k=1}^{\infty} \frac{1}{(q+1)^{k}} \\ &= \frac{1}{q}. \end{aligned}$$

Note that $q! \sum_{n=q+1}^{\infty} \frac{1}{n!}$ should be a positive integer, but it is impossible that a positive integer is less than $\frac{1}{q}$, given the fact that q is also a positive integer. Hence e is not rational, thus irrational.

5. Show that if k is an integer, then the integers $6k-1$, $6k+1$, $6k+2$, $6k+3$, and $6k+5$ are pairwise relatively prime.

Proof. If $(a,b)=d$, then $d \mid a$ and $d \mid b$; giving that $d \mid (a-b)$.

Hence for some integer k, if $a+k=b$ and $(a,k)=1$ and $(b,k)=1$, then $(a,b)=1$ because $(a,b) \mid (b-a) \Rightarrow (a,b) \mid k$, giving that (a,b) is a common divisor of a and k.

For $k=1$, $(6k+1,6k+2)=1$ and $(6k+2,6k+3)=1$.

For $k=2$, $(6k-1,6k+1)=1$, $(6k+1,6k+3)=1$, and $(6k+3,6k+5)=1$.

For $k=3$, $(6k-1,6k+2)=1$, and $(6k+2,6k+5)=1$.

For $k=4$, $(6k-1,6k+3)=1$, and $(6k+1,6k+5)=1$.

For $k=6$, $(6k-1,6k+5)=1$.

Hence the integers $6k-1$, $6k+1$, $6k+2$, $6k+3$, and $6k+5$ are pairwise relatively prime. □

6. Show that if a and p are positive integers such that a^p-1 is prime, then $a=2$ or $p=1$.

Proof. Note that

$$a^p-1=\sum_{r=0}^{p-1}\left(a^{r+1}-a^r\right)=(a-1)\sum_{r=0}^{p-1}a^r.$$

Thus $(a-1) \mid (a^p-1)$ and $\left(\sum_{r=0}^{p-1}a^r\right) \mid (a^p-1)$.

Suppose that a^p-1 is prime.

1. If $a<2$, then $a=1 \Rightarrow 1^p-1=0$ is not prime.
2. If $a>2$, then $a-1 \geq 2$.
   Since a^p-1 is prime, the only prime factor for a^p-1 has to be $a-1$, implying that $\sum_{r=0}^{p-1}a^r = 1 \Rightarrow p=1$.
3. If $p>1$, then $\sum_{r=0}^{p-1}a^r \geq \sum_{r=0}^{2-1}a^r = 1+a \geq 2$.
   Since a^p-1 is prime, the only prime factor for a^p-1 has to be $\sum_{r=0}^{p-1}a^r$, implying that $a-1 = 1 \Rightarrow a=2$.

Hence if a^p-1 is prime, then $a=2$ or $p=1$. □

7. Show that if $2^p - 1$ is prime, then p is prime.

Proof. Note that

$$2^p - 1 = \sum_{k=0}^{p-1} 2^k.$$

Suppose p is not prime, giving the fact that there exists some integers $p_1, p_2 \geq 2$ such that $p = p_1 p_2$. Then

$$\begin{aligned}
2^p - 1 &= \sum_{k=0}^{p-1} 2^k \\
&= \sum_{k=0\cdot p_1}^{1\cdot p_1 - 1} 2^k + \sum_{k=1\cdot p_1}^{2\cdot p_1 - 1} 2^k + \cdots + \sum_{k=(p_2-2)p_1}^{(p_2-1)p_1-1} 2^k + \sum_{k=(p_2-1)p_1}^{p_2 p_1 - 1} 2^k \\
&= (2^{p_1})^0 \sum_{k=0}^{p_1-1} 2^k + (2^{p_1})^1 \sum_{k=0}^{p_1-1} 2^k + \cdots + (2^{p_1})^{p_2-2} \sum_{k=0}^{p_1-1} 2^k + (2^{p_1})^{p_2-1} \sum_{k=0}^{p_1-1} 2^k \\
&= \left[\sum_{k=0}^{p_2-1} (2^{p_1})^k\right] \left[\sum_{k=0}^{p_1-1} 2^k\right]
\end{aligned}$$

which $2^p - 1$ is clearly not prime. Hence if $2^p - 1$ is prime, then p is also prime. □

8. Show that if a is a positive integer and $a^m + 1$ is an odd prime, then $m = 2^n$ for some nonnegative integer n.

Proof. Suppose that $a^m + 1$ is prime and $m \neq 2^n$ for any integer n. Then m can be expressed as $m = rs$, where $1 \leq r, s < m$, and s is odd.

Note that for any $l \in \mathbb{Z}^+$,

$$(x - y) \mid \left(x^l - y^l\right).$$

Put $x = a^r$ and $y = -1$. then

$$\begin{aligned}
&(a^r - 1) \mid [(a^r)^s - (-1)^s] \\
\Rightarrow &(a^r - 1) \mid (a^{rs} + 1) \\
\Rightarrow &(a^r - 1) \mid (a^m + 1).
\end{aligned}$$

Hence if $m \leq 2^n$, $a^m + 1$ is clearly not prime; thus if $a^m + 1$ is prime then $m = 2^n$ for some nonnegative integer n.

9. Show that if a and b are positive integers and if $a^3 \mid b^2$, then $a \mid b$.

Let

$$a = p_1^{a_1} p_2^{a_2} \times \cdots \times p_{n-1}^{a_{n-1}} p_n^{a_n}$$
$$b = p_1^{b_1} p_2^{b_2} \times \cdots \times p_{n-1}^{b_{n-1}} p_n^{b_n}.$$

where $a_i, b_i \in \mathbb{Z}^+ \cup \{0\}$ and p_i is prime for $1 \leq i \leq n$.

Then if $a^3 \mid b^2$, it is clear that

$$\left(p_1^{a_1} p_2^{a_2} \times \cdots \times p_{n-1}^{a_{n-1}} p_n^{a_n}\right)^3 \mid \left(p_1^{b_1} p_2^{b_2} \times \cdots \times p_{n-1}^{b_{n-1}} p_n^{b_n}\right)^2$$
$$\Rightarrow \left(p_1^{3a_1} p_2^{3a_2} \times \cdots \times p_{n-1}^{3a_{n-1}} p_n^{3a_n}\right) \mid \left(p_1^{2b_1} p_2^{2b_2} \times \cdots \times p_{n-1}^{2b_{n-1}} p_n^{2b_n}\right).$$

Since $p_1, p_2, \cdots, p_n$ are primes,

$$3a_i \leq 2b_i$$
$$\Rightarrow a_i \leq b_i \qquad \text{for all } 1 \leq i \leq n.$$

Hence

$$\left(p_1^{a_1} p_2^{a_2} \times \cdots \times p_{n-1}^{a_{n-1}} p_n^{a_n}\right) \mid \left(p_1^{b_1} p_2^{b_2} \times \cdots \times p_{n-1}^{b_{n-1}} p_n^{b_n}\right)$$
$$\Rightarrow a \mid b.$$

□

10. Find all integer solutions of the following system of Diophantine equations:

$$\begin{cases} x + y + z = 100 \\ x + 8y + 50z = 156 \end{cases}$$

Subtracting the first equation from the second equation, we get

$$7y + 49z = 56 \Rightarrow y + 7z = 8.$$

Then the arbitary solution for y and z is given by $y_0 = 1$, $x_0 = 1$, and the general solution exists as

$$\{y, z\} = \left\{ y_0 + \frac{7}{(1,7)}t,\, z_0 - \frac{1}{(1,7)}t \right\} = \{1+7t,\, 1-t\}$$

for any integer t.

Given the fact that $y+z = (1+7t)+(1-t) = 2+6t$,

$$x + (y+z) = 100 \Rightarrow x+2+6t = 100 \Rightarrow x+6t = 98.$$

Then the arbitary solution for x and t is given by $x_0 = 98$, $t_0 = 0$, and the general solution exists as

$$\{x, t\} = \left\{ x_0 + \frac{6}{(1,6)}u,\, t_0 + \frac{1}{(1,6)}u \right\} = \{98+6u,\, -u\}$$

for any integer u.

Thus the general solution for $\{x, y, z\}$ is

$$\begin{aligned}\{x, y, z\} &= \{98+6u, 1+7t,\, 1-t\}\\ &= \{98+6u, 1-7u,\, 1+u\}\end{aligned}$$

for any integer u.

11. What is the smallest positive rational number that can be expressed in the form of $\frac{x}{30} + \frac{y}{36}$ with integers x and y?

Note that $\frac{x}{30} + \frac{y}{36} = \frac{6x+5y}{180}$. Since $(6,5) = 1$, there exists integer solution to equation $6x+5y = 1$, given that $1 \mid 1$.

Therefore the smallest positive rational number that can be expressed in the form of $\frac{x}{30} + \frac{y}{36}$ is $\frac{1}{180}$.

12. Let $m_1, \cdots, m_k$ be positive integers and $a, b \in \mathbb{Z}$. Show that $a \equiv b \pmod{m_i}$ for each i if and only if $a \equiv b \pmod{[m_1, \cdots, m_k]}$.

Proof. By definition, if $a \equiv b \pmod{m}$, then $m \mid (a-b)$. Let $l = [m_1, \cdots, m_k]$.

($\Rightarrow$) If $a \equiv b \pmod{m_i}$ for all i, then $m_i \mid (a-b)$ for all i. Suppose $l \nmid (a-b)$. Then by the division algorithm, $(a-b) = lp+q$, where $p, q \in \mathbb{Z}$ and $1 \leq q < l$.

Suppose $a \equiv b \pmod{m_i}$ for each i. Then $m_i \mid (a-b) = (lp+q)$ for all i. Since $m_i \mid l$, $m_i \mid q$ for all i, which means that q is a common multiple of $m_1, m_2, \cdots, m_k$, but the fact that the LCM of $m_1, m_2, \cdots, m_k$ is l and $1 \leq q < l$ leads to contradiction. Thus if $a \equiv b \pmod{m_i}$ for each i, then $a \equiv b \pmod{[m_1, \cdots, m_k]}$.

($\Leftarrow$) If $a \equiv b \pmod{l}$, then $l \mid (a-b)$. Since $m_i \mid l$ for all i, $m_i \mid (a-b)$ for all i. Thus if $a \equiv b$ $\pmod{[m_1, \cdots, m_k]}$, then $a \equiv b \pmod{m_i}$ for each i.