

gcd와 lcm의 유용한 성질

- 임의의 양의 정수  $a, b$ 에 대해  $\gcd(a, b) \cdot \text{lcm}(a, b) = ab$ .
- 임의의 양의 정수  $a, b$ 와  $\gcd(ma, mb) = m \gcd(a, b)$ 이고  $\text{lcm}(ma, mb) = m \text{lcm}(a, b)$
- $d \mid \gcd(a, b)$ 이면  $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{\gcd(a, b)}{d}$   
 특히  $d = \gcd(a, b)$ ,  $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ ;  $\frac{a}{d}$ 와  $\frac{b}{d}$ 는 서로소이다.
- $a \mid bc$ 이고  $\gcd(a, c) = 1$ 이면  $a \mid b$ 이 성립된다.
- $m = dm'$ ,  $n = dn'$ 이고  $\gcd(m', n') = 1$ 이면  $d = \gcd(m, n)$ .
- 만약  $d'$ 가  $m$ 와  $n$ 의 공약수이면  $d'$ 은  $\gcd(m, n)$ 을 나눌 수 있다.  
 이 성질은 특히  $\gcd(m, n)$ 이  $m$ 과  $n$ 의 최대공약수임을 말한다.
- 양의 정수  $a$ 와  $b, d$ 가 양의 정수일 때  $d \mid a$ ,  $d \mid b$ 이고 어떤  $d'$ 에서  $d' \mid a$  이고  $d' \mid b$ 이라 하면  $d' \mid d$ 이고  $d = \gcd(a, b)$ 이 성립된다.  
 이 성질은  $a$ 와  $b$ 의 공통인수가  $\gcd(a, b)$ 을 나눌 수 있다.
- $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ 이고  $n = p_1^{\beta_1} \cdots p_k^{\beta_k}$ 이고  $\alpha_i, \beta_i \geq 0$ ,  $i = 1, 2, 3, \dots, k$ 이면  
 $\gcd(m, n) = p_1^{\min(\alpha_1, \beta_1)} \cdots p_k^{\min(\alpha_k, \beta_k)}$ 이 성립한다.
- $a, b \in \mathbb{Z}$ 에 대하여  $d = \gcd(a, b)$ 라고 하면  
 어떤  $x, y \in \mathbb{Z}$  ;  $ax + by = d$   
 [증명]  
 $S = \{au + bv \mid u, v \in \mathbb{Z}, au + bv > 0\}$ 이라 놓으면  $S \neq \emptyset$ 이므로 최소원 법칙에 의하여  $S$ 에는 가장 작은 원소가 존재한다. 이것을  $e$ 라고 하자.  
 $e \in S$ 이므로 적당한 정수  $x, y$ 에 대하여  
 $e = ax + by$ 이다.  
 그러면  $e = d$ 만 보이면 되므로  
 $e > 0$ 이므로 나눗셈 알고리즘을 이용하면  
 $a = eq + r$ ,  $0 \leq r < e$ 을 만족시키는 정수  $q, r$ 이 존재한다.  
 $r = a - eq = a - q(ax + by) = a(1 - qx) + b(-qy)$ 이므로  
 만약  $r > 0$ 라면  $r \in S$ 이고,  $r < e$ 가 되어  $e$ 가  $S$ 의 가장 작은 원소라는 사실에 모순이 된다.  
 $r = 0$ , 즉,  $a = eq$ 로서  $e \mid a$ ,  
 같은 방법으로  $e \mid b$ 이므로  $e$ 는  $a$ 와  $b$ 의 공약수이다.  
 한편  $f$ 가  $a$ 와  $b$ 의 공약수이면  
 $f \mid (ax + by)$ 이므로  $f \mid e$ , 즉,  $f \leq e$ 이다.  
 따라서  $e = d$ 이다.

연습문제

1. 정수  $a$ 와  $b$ 를 자연수  $m$ 으로 나눈 나머지가 같으면,  $\gcd(a, m) = \gcd(b, m)$ 임을 보여라.
2. (1) 101, 10101, 1010101, ...들은 제곱수가 될 수 없음을 보여라.  
(2)  $n$ 이 제곱수인 동시에 세 제곱수이면  $n = 7k$  또는  $n = 7k + 1$ 꼴임을 보여라.  
(3)  $2 \nmid a$ ,  $3 \nmid a$ 이면,  $24 \mid (a^2 - 1)$ 임을 보여라.
3.  $a, m, \in N$ ,  $m \neq n$ 일 때,  $\gcd(a^{2^m} + 1, a^{2^n} + 1)$ 을 구하여라.
4. 모든 음 아닌 정수  $n$ 에 대하여  $13 \mid (4^{2n+1} + 3^{n+2})$ 임을 보여라.
5. 세 자리수  $n$ 이 11의 배수이고, 각 자리수의 제곱의 합이  $n/11$ 이라고 할 때, 이러한 자연수  $n$ 을 모두 구하여라. (IMO '60)
6.  $\frac{21n+4}{14n+3}$ 가 기약분수가 되는 자연수  $n$ 을 구하여라. (IMO '59)

IMO : International Mathematical Olympiad(국제 수학 올림피아드)

5번 원본

Determine all three-digit numbers  $N$  having the property that  $N$  is divisible by 11, and  $N/11$  is equal to the sum of the squares of the digits of  $N$ .

6번 원본

Prove that the fraction  $\frac{21n+4}{14n+3}$  is irreducible for every natural number  $n$ .

[연습문제 풀이]

1.  $a = q_1m + r$ ,  $b = q_2m + r$ ,  $0 \leq r < m$ 로 놓으면

$$\gcd(a, m) = \gcd(b, m)$$

$$d_1 = \gcd(a, m), d_2 = \gcd(b, m)$$

$$d_1 \mid a \text{와 } d_2 \mid m \text{에서}$$

$$d_1 \mid a - q_1m = r$$

$$d_2 \mid q_2m + r = b$$

$$d_1 \mid r \text{이고 } d_2 \mid b \text{이므로}$$

$$d_2 \mid d_1 \text{이 성립된다.}$$

$$d_1 = \gcd(a, m), d_2 = \gcd(b, m)$$

$$d_1 \mid m \text{와 } d_2 \mid b \text{에서}$$

$$d_1 \mid mq_2 + r = b$$

$$d_2 \mid b - q_2m = r$$

$$d_1 \mid b \text{이고 } d_2 \mid r \text{이므로}$$

$$d_1 \mid d_2 \text{이 성립된다.}$$

$$d_2 \mid d_1 = d_1 \mid d_2 \text{이 성립되므로 } \gcd(a, m) = \gcd(b, m)$$

2. (1) 홀수  $2k+1$ ,  $(2k+1)^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1$

위의 식에서  $k(k+1)$ 은 짝수와 홀수의 곱이므로 짝수일 수밖에 없다.

$$\text{즉, } (2k+1)^2 = 4k(k+1) + 1 \text{이므로}$$

$k=3$ , 홀수의 제곱은 12로 나눈 나머지가 1이 된다.

그런데 문제에서 101, 10101, 1010101, ...은 12로 나눈 나머지가 5인 수들이다.

즉, 홀수의 제곱 수 일 수 없으므로 짝수의 제곱수가 될 수 없다.

- (2)  $a = 7m + r$ ,  $0 \leq r < 7$ 로 놓고

$a^2$ 과  $a^3$ 을 7로 나눈 나머지를 각각  $r_1$ ,  $r_2$ 라 하면

$$r=0 \text{일 때, } a=7m, a^2=7^2m^2, a^3=7^3m^3 \text{이므로}$$

$$r_1=0, r_2=0$$

$$r=1 \text{일 때, } a=7m+1, a^2=(7m+1)^2=7^2m^2+14m+1=7m(m+2)+1,$$

$$a^3=(7m+1)^3=7^3m^3+3 \times 7^2m+3 \times 7m+1=7m(7^2m^2+24)+1$$

$$r_1=1, r_2=1$$

$$r=2 \text{일 때, } a=7m+2, a^2=(7m+2)^2=7^2m^2+28m+4=7m(7m+4)+4,$$

$$a^3=(7m+2)^3=7^3m^3+3 \times 7^2m^2+3 \times 7m \times 2^2+2^3=7^3m^3+3 \times 7^2m^2+12 \times 7m+8$$

$$a^3=(7m+2)^3=7^3m^3+3 \times 7^2m^2+12 \times 7m+8=7(7^2m^3+21m^2+12m+7)+1$$

$$r_1=4, r_2=1$$

위와 같은 과정을 하면 계산이 복잡해지므로 다음과 같이  $r=3, 4, 5, 6$ 을 하면

$$r=2 \text{일 때, } r_2=2^3=8 \text{이므로 7로 나눈 나머지는 1이 됨을 알 수 있다.}$$

$$r=3 \text{일 때, } r_1^2=9 \text{이므로 7로 나눈 나머지는 2, } r_2^3=27 \text{을 7로 나눈 나머지는 6이 됨}$$

을 알 수 있다.

$r = 4$ 일 때,  $r_1^2 = 16$ 이므로 7로 나눈 나머지는 2,  $r_2^3 = 64$ 이므로 7로 나눈 나머지는 1

$$r_1 = 2, r_2 = 1$$

$r = 5$ 일 때,  $r_1^2 = 25$ 이므로 7로 나눈 나머지는 4,  $r_2^3 = 125$ 이므로 7로 나눈 나머지는 6

$$r_1 = 4, r_2 = 6$$

$r = 6$ 일 때,  $r_1^2 = 36$ 이므로 7로 나눈 나머지는 1,  $r_2^3 = 216$ 이므로 7로 나눈 나머지는 6

$$r_1 = 1, r_2 = 6$$

따라서  $n$ 이 제곱수인 동시에 세 제곱수이면  $n = 7k$  또는  $n = 7k + 1$  꼴이다.

