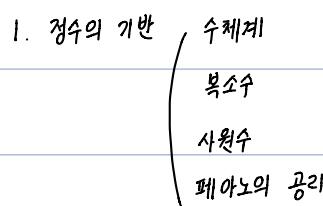


I 수체계와 소인수분해

1. 정수의 기반
2. 수의 표현
3. 약수·배수
4. 유clidean 알고리즘과 부정방정식
5. 소수
6. 소인수분해



Thm 1.2) 정수의 경계성 (Well-ordering Principle)

어떤 성질 P 를 만족하면서 주어진 a 보다 큰 모든 정수의 집합 $S \neq \emptyset$ 에는 최소의 정수가 존재한다.

Thm 1.4) 유한 귀납법의 원리

N 의 부분집합 S 가 조건

$$(i) 1 \in S \quad (ii) k \in S \Rightarrow k+1 \in S$$

을 만족할 때, $S = N$ 이다.

(P) (정수의 경계성을 이용한 증명) **귀류법**

$S \neq N$ 이면 $N-S$ 는 공집합이 아님으로 최소원 n 을 가진다.

$1 \in S$ 이므로 $1 < n$ 이고 여기서 $0 < n-1 < n$ 이다.

$n = \min(N-S)$ 이므로 $n-1 \in N-S$ 이고 따라서 $n-1 \in S$ 이다.

이제 조건 (ii)에 의하여 $n \in S$ 이고 이는 $n \in N-S$ 라는 사실에 모순.

2223 $N-S = \emptyset$, 즉 $S = N$ 이다.

Thm 1.5) 제 2 유한 계법법의 원리

N 의 부분집합 S 가 조건

$$(i) 1 \in S \quad (ii) \{1, 2, \dots, k\} \subset S \Rightarrow k+1 \in S \text{ 를 만족할 때, } S = N$$

• 나눗셈 알고리즘

Thm 1.6) 정수 a 와 정수 b 에 대하여 $a = bq + r$, $0 \leq r < |b|$ 을 만족하는 정수 q, r 이 유일하게 존재.

q : 몫 (quotient), r : 나머지 (remainder)

2. 수의 표현

• 정수의 여러가지 표현

Thm) 진법에 대한 기본정리

$b \in \mathbb{Z}$, $b \geq 2$ 일 때, 임의의 자연수 a 에 대하여

$$a = r_m b^m + r_{m-1} b^{m-1} + \dots + r_1 b^1 + r_0$$

을 만족하는 정수 m, r_0, r_1, \dots, r_m 이 존재.

(단, $m \geq 0$, $r_m > 0$, $0 \leq r_i < b$, $0 \leq i \leq m$)

Proof (1) $a = r_m b^m + r_{m-1} b^{m-1} + \dots + r_1 b^1 + r_0$

$\xrightarrow{\text{bx } q + r \text{ 의 form.}}$

$$= b(r_m b^{m-1} + r_{m-1} b^{m-2} + \dots + r_1) + r_0$$

이므로 r_0 은 a 를 b 로 나눈 나머지이다.

(2) $r_m b^{m-1} + r_{m-1} b^{m-2} + \dots + r_1 = b(r_m b^{m-2} + r_{m-1} b^{m-3} + \dots + r_0) + r_1$

이므로 r_1 은 a 를 b 로 나눈 몫을 b 로 나눈 것의 나머지이다.

(3) 비슷하게 r_2, \dots, r_m 을 각각 구할 수 있다.

표시법 $a = (r_m r_{m-1} \dots r_0)_b$ 라 쓴다.

이것을 정수 a 의 b 진법 표현이라 한다.

$$\begin{array}{r} b \mid a \\ 2 \mid 14 - 0 \rightarrow r_0 \\ 2 \mid 2 - 0 \rightarrow r_1 \\ \hline 1 \rightarrow r_2 \end{array}$$

• 실수의 소수 표현

→ 10 진수로 변환하는 방법을 원박히게 읽힌다.

→ 10진수에서 2진수 / 8진수 / 16진수로 각각 변환한다.

10진수	일상생활에서 사용(0~9)	10진수를 변환...	정수의 변환 - 해당 진법으로 나누어준 후에 나머지 부분만을 역으로 취한다. 소수의 변환 - 해당 진법으로 곱한 결과의 정수 부분을 취하여 소수부분이 0이 되거나 반복수가 나올 때까지 진행
2진수	0,1 (2비트)		
8진수	0,1,2,3,4,5,6,7 (8비트)		8진수 1자리는 2진수 3자리(421)에 대응
16진수	0~9, A~F (16비트)		16진수 1자리는 2진수 4자리(8421)에 대응
	10~15는 A~F로 표현		

※ 10진수로의 변환

2, 8, 16진수에서 → 10진수로 변환할 경우

진수의 전개식 사용하여 자리값을 곱하여 계산 (모든 수의 0제곱은 1: 약속)

▶ 2진수를 10진수로

$$(예제) 101101.101_{(2)} \rightarrow 45.625$$

$$1 \times 32 + 0 \times 16 + 1 \times 8 + 1 \times 4 + 0 \times 2 + 1 \times 1 + 1 \times 0.5 + 0 \times 0.25 + 1 \times 0.125$$

▶ 8진수를 10진수로

$$(예제) 132.5_{(8)} \rightarrow 90.625_{(10)}$$

$$1 \times 8^2 + 3 \times 8 + 2 \times 1 + 5 \times 0.125 \\ (= \frac{1}{8})$$

▶ 16진수를 10진수로

$$(예제) 1AD.5_{(16)} \rightarrow 429.3125_{(10)}$$

$$1 \times 256 + A(10) \times 16 + D(13) \times 1 + 5 \times \frac{1}{16} (= 0.0625)$$

※ 10진수로의 변환

① 정수부분 - 해당 진법으로 나누어 끊이 진수보다 작아질 때까지 진행하며 나머지를 역으로 취한다.

② 소수부분 - 해당 진법으로 곱한 결과의 정수부분을 취하여 소수부분이 0이 되거나 반복수가 나올 때까지 진행한다.

▶ 29. 895₍₁₀₎ 를 2진수로 변환

정수부분 소수부분

$$\begin{array}{r}
 2 | 29 \\
 2 | 14 \cdots 1 \\
 2 | 7 \cdots 0 \\
 2 | 3 \cdots 1 \\
 \hline
 1 \cdots 1
 \end{array}
 \quad
 \begin{array}{r}
 0.895 \\
 \times 2 \\
 \hline
 1.790 \\
 \times 2 \\
 \hline
 1.0
 \end{array}
 \quad
 \begin{array}{r}
 0.450 \\
 \times 2 \\
 \hline
 0.900 \\
 \times 2 \\
 \hline
 0.0
 \end{array}
 \quad
 \begin{array}{r}
 0.50 \\
 \times 2 \\
 \hline
 1.0
 \end{array}$$

0. 111

$$\therefore 29.895_{(10)} = 11101.111$$

▶ 129.895₍₁₀₎ 를 10진수로 변환

정수부분 소수부분

$$\begin{array}{r}
 8 | 129 \\
 8 | 16 \cdots 1 \\
 \hline
 2 \cdots 0
 \end{array}
 \quad
 \begin{array}{r}
 0.895 \\
 \times 8 \\
 \hline
 1.000
 \end{array}$$

0. 1

0을 때까지

201

$$\therefore 129.895_{(10)} = (201.1)_8$$

▶ 408.8125₍₁₀₎ 를 16진수로

$$\begin{array}{r}
 16 | 408 \\
 16 | 25 \cdots 8 \\
 \hline
 1 \cdots 9
 \end{array}
 \quad
 \begin{array}{r}
 0.8125 \\
 \times 16 \\
 \hline
 13 \ 000
 \end{array}$$

198

0. D

$$\therefore 408.8125_{(10)} = (198.D)_{16}$$

3. 약수 배수

* 정수의 정렬성

* 수학적 귀납법

Def) $a|b$ (a 는 b 를 나누다) $\Leftrightarrow b=aq, q \in \mathbb{Z}$ $a \in S (\neq \emptyset), S$ 의 최소원 존재.

(1) $p(n)$: 참

a : b 의 약수 (divisor) 또는 인수 (factor)

* 유한귀납법의 원리

(2) $p(n)$: 참 $\Rightarrow p(n+1)$: 참

b : a 의 배수 (multiple)

(1) $| \in S$ (2) $k \in S \Rightarrow k \cdot h \in S$ 이면 $S = N$

Thm) 정수 a, b 의 정수배의 합, 즉 $ax+by, (x, y \in \mathbb{Z})$ 꼴의 표현을 a, b 의 일차결합이라 한다.

Thm) (1) $a|0, 1|a, a|a, \forall a \in \mathbb{Z}$

(2) $a|1 \Rightarrow a = \pm 1$

(3) $a|b$ and $c|d \Rightarrow ac|bd$

(4) $a|b$ and $b|c \Rightarrow a|c$

* (5) $a|b$ and $b|a \Rightarrow a = \pm b$

(6) $a|b$ and $b \neq 0 \Rightarrow |a| \leq |b|$

(7) $a|b$ and $a|c \Rightarrow a|bx+cy, \forall x, y \in \mathbb{Z}$

Def) $a \in \mathbb{Z}, a\mathbb{Z} = \{ax \mid x \in \mathbb{Z}\}$: a 의 배수의 집합

Thm) $a, b \in \mathbb{Z}$

(1) $a\mathbb{Z} \supseteq b\mathbb{Z} \Leftrightarrow a|b$ [예] $2|4$ 일 때 $2\mathbb{Z} \supseteq 4\mathbb{Z}$

(2) $a\mathbb{Z} = b\mathbb{Z} \Leftrightarrow b = \pm a$

• 공약수와 공배수

Def) $a, b, x \in \mathbb{Z}$ 에 대하여, $x|a$ 이고 $x|b$ 일 때 x 를 a 와 b 의 공약수라 한다.

$a, b \in \mathbb{Z}, (a, b) \neq (0, 0)$ 공약수 중 최대의 수를 a, b 의 최대공약수(greatest common division) 라 하고 $\gcd(a, b)$ 로 표시

* $\gcd(a, b) = 1$ 일 때, a 와 b 를 서로 소(relatively prime)

Thm) a, b 의 공약수는 a, b 의 일차결합의 약수.

$k|a, k|b \Rightarrow k|ax+by \Rightarrow a=km, b=kn \quad \forall m, n \in \mathbb{Z}$

$$ax+by = kmx+kn$$

$$= k(mx+ny)$$

$$\therefore k|ax+by$$

Rmk) $\gcd(a, b) = \gcd(\pm a, \pm b)$

Thm 3.4) \gcd 은 일차결합

$(a, b) \neq (0, 0)$ 인 정수 a, b 에 대하여 $\gcd(a, b) = ax+by$ 를 만족하는 정수 x, y 가 존재한다.

(예) $\gcd(8, 20) = 4 = 8 \times 3 + 20 \times (-1)$

Thm) $p > 0, \gcd(pa, pb) = p \gcd(a, b)$

$$(예) \ gcd(80, 200) = 10 \ gcd(8, 20) = 10 \cdot 4 = 40$$

$$gcd(12, 30) = 2 \ gcd(6, 15) = 2 \cdot 3 \ gcd(2, 5) = 6$$

Thm 3.6) $(a, b) \neq (0, 0)$ 인 경우 a, b 에 대하여 $gcd(a, b) = 1$ 일 필요충분 조건은 어떤 정수 x, y 가 있어서 $ax + by = 1$ 일 것이다.

$$\text{Coroll}) \ gcd(a, b) = g \Rightarrow gcd\left(\frac{a}{g}, \frac{b}{g}\right) = 1$$

$$\therefore ax + by = g \Rightarrow \frac{1}{g}(ax + by) = 1 \Leftrightarrow \left(\frac{a}{g}\right)x + \left(\frac{b}{g}\right)y = 1$$

$$\text{Coroll}) \ a|k, b|k \ \& \ gcd(a, b) = 1 \Rightarrow ab|k$$

$$\text{Coroll}) \ a|bk \ \& \ gcd(a, b) = 1 \Rightarrow a|k$$

$$\therefore ax + by = 1 \Rightarrow akx + bky = k, \ a|ak \ \& \ a|bky \Rightarrow a|k$$

$$\text{Thm}) \ gcd(a, b) = 1, \ \forall m \in \mathbb{Z}, \ gcd(am, b) = gcd(m, b)$$

여러 정수의 최대공약수

Def) (1) $a_1, a_2, \dots, a_n \in \mathbb{Z}$ ($n \geq 2$), e : a_1, \dots, a_n 의 공약수

$$\Leftrightarrow e|a_i, \ i=1, 2, \dots, n$$

(2) d : a_1, \dots, a_n 의 최대공약수

$$\Leftrightarrow \begin{array}{l} \textcircled{1} \ d \geq 0 \\ \textcircled{2} \ d|a_i \ (i=1, 2, \dots, n) \end{array}$$

$$\textcircled{3} \ e|a_i \ (i=1, 2, \dots, n) \Rightarrow e|d$$

Thm 3.12) 짝수도 핵심은 0이 아닌 a_1, a_2, \dots, a_n 에 대하여

$$gcd(a_1, a_2, \dots, a_n) = gcd(gcd(a_1, a_2), a_3, \dots, a_n)$$

$$(예) \ gcd(12, 18, 21) = gcd(gcd(12, 18), 21) = gcd(6, 21) = 3$$

Def) (1) $a_1, a_2, \dots, a_n \in \mathbb{Z}$ ($n \geq 2$) : 서로소 (mutually prime)

$$\Leftrightarrow gcd(a_1, a_2, \dots, a_n) = 1$$

(2) $a_1, a_2, \dots, a_n \in \mathbb{Z}$ ($n \geq 2$) : 서로 소 (pairwise relatively prime)

$$\Leftrightarrow \gcd(a_i, a_j) = 1 \quad (1 \leq i \neq j \leq n)$$

Note) 서로다른 서로소 \Rightarrow 서로소, 서로소 $\not\Rightarrow$ 서로다른 서로소

Def) $a, b, n \in \mathbb{Z}$ 에 대하여, $a|b$ 이고 $b|c$ 일 때, c 를 a 와 b 의 공배수라 한다.

$a, b \in \mathbb{Z}$ ($a \neq 0 \neq b$) 양의 공배수 중 최소의 수를 a, b 의 최소공배수 (least common multiple) 이라고 하고 $\text{lcm}(a, b)$ 로 표시한다.

Thm 3.11) $a, b \in N$. $ab = \gcd(a, b) \cdot \text{lcm}(a, b)$

Corol) $a, b \in N$. $\text{lcm}(a, b) = ab \Leftrightarrow \gcd(a, b) = 1$

• 여러 정수의 최소공배수

Thm 3.13) 0이 아닌 정수 a_1, a_2, \dots, a_m 에 대하여

$$\text{lcm}(a_1, a_2, \dots, a_n) = \text{lcm}(\text{lcm}(a_1, a_2), a_3) = \text{lcm}(30, 20) = 60$$

Thm) $\gcd(a, b) = 1 \Rightarrow \forall m \in \mathbb{Z}, \gcd(am, b) = \gcd(m, b)$

4. 유clidean 알고리즘과 부정방정식

• 유clidean 알고리즘

Lemma 4.1) $a, b, q, r \in \mathbb{Z}$ and $a = bq + r \Rightarrow \gcd(a, b) = \gcd(b, r)$

p 46에 Lemma 3.3 안에서 책대로 증명 X

보조 3.3 안쓰고 다른 방법으로 하기 위해 몇몇 정리 → 정리 #1#2

Thm #1) $a_1 + a_2 + \dots + a_n = b_1 + b_2 + \dots + b_k$ 일 때 하나의 항을 제외하고 모든 항이 q의 배수이면 그 하나의 항 또한 q의 배수이다.

Thm #2) $\gcd(a, b) = d$ 일 때 $\gcd(a, a-b) = d$ 이다.

Thm 4.3) 유clidean 알고리즘

만약 a 와 b ($\neq 0$) 가 양의 정수이고

$$a = b q_1 + r_1, \quad 0 < r_1 < b \quad \Rightarrow \quad \gcd(a, b) = \gcd(b, r_1)$$

$$b = r_1 q_2 + r_2, \quad 0 < r_2 < r_1 \quad \Rightarrow \quad \gcd(b, r_1) = \gcd(r_1, r_2)$$

$$r_1 = r_2 q_3 + r_3, \quad 0 < r_3 < r_2 \quad \Rightarrow \quad \gcd(r_1, r_2) = \gcd(r_2, r_3)$$

$$\vdots \quad \vdots$$

$$r_{n-2} = r_{n-1} q_n + r_n, \quad 0 < r_n < r_{n-1} \quad \Rightarrow \quad \gcd(r_{n-2}, r_{n-1}) = \gcd(r_{n-1}, r_n)$$

$$r_{n-1} = r_n q_{n+1} + 0 \quad \Rightarrow \quad \gcd(r_{n-1}, r_n) = \gcd(r_n, 0)$$

$$\Rightarrow \gcd(a, b) = r_n \quad = r_n \quad \text{* } 0 \notin 모든 수의 약수}$$

• $\gcd(a, b)$ 을 $ax+by$ 를 형태로

Thm 3.4) $\gcd(a, b) = d$ 일 때 $ax+by = d$ 인 정수 x, y 가 반드시 존재한다.

Thm) $p > 0, \gcd(pa, pb) = p \gcd(a, b)$

(예) $\gcd(299, 247)$ 을 유clidean 알고리즘을 이용하여 구하라.

$$(sol) \quad 299 = 247 \times 1 + 52$$

$$\Rightarrow 247 = 52 \times 4 + 39$$

$$\Rightarrow 52 = 39 \times 1 + 13$$

$$\Rightarrow 39 = 13 \times 3 + 0 \\ = r_7$$

(예) $\gcd(299, 247) = 13$ 일 때, $299x + 247y = 13$ 일 때 x, y 를 찾으라.

$$(sol) \quad \gcd(299, 247) = 13$$

$$= 52 - 39 \cdot 1$$

$$= 52 - (247 - 52 \cdot 4)$$

$$= 52 \cdot 5 - 247$$

$$= 5(299 - 247) - 247$$

$$= 299.5 + 249 \cdot (-6)$$

$$\text{249으로 } x=5, y=-6$$

• 부정방정식 $ax+by=c$: (이지수 계수) > (방정식 개수)

• 부정방정식, 디오판투스 방정식 : 해가 정수로서 결정되는 정수계수 방정식

Thm) a, b, c 가 임의의 정수이고, $\gcd(a, b) = d$ 일 때,

(1) 일차부정방정식 $ax+by=c$ 가 해를 가질 필요충분조건은 $d|c$ 이다.

(2) (1)의 경우에 x_0, y_0 을 이 부정방정식의 하나의 해(특수해) 라 할 때 이 방정식의 해는 $\begin{cases} x = x_0 + \frac{b}{d}k \\ y = y_0 - \frac{a}{d}k \end{cases} \quad (k \in \mathbb{Z})$

(Ex 4.7) 부정방정식 $89x + 29y = 624 \quad (x \geq 0, y \geq 0)$ 을 풀어라.

(sol) ① $\gcd(89, 29)$ 구하기. $\gcd(89, 29) = 3 \Rightarrow \gcd(89, 29) | 624$ 이므로 해가 존재.

$$89 = 29 \times 3 + 6$$

$$29 = 6 \times 4 + 5$$

$$6 = 5 \times 1 + 1$$

② $89x + 29y = 3$ 을 만족하는 x, y 구하기.

$$3 = 29 - 6 \times 4$$

$$= 29 - 4(89 - 29 \times 3)$$

$$= 89 \times (-4) + 29 \times 13 \rightarrow x = -4, y = 13$$

$$624 \div 3 = 208$$

③ $89x + 29y = 624$ 를 만족하는 특수해 $\begin{cases} x_0 = (-4) \times 208 = -832 \\ y_0 = 13 \times 208 = 2704 \end{cases}$

$$+\frac{29}{3}$$

$$\therefore x = -832 + 29m \geq 0 \quad \text{을 만족하는 } m = 93 \Rightarrow x = 5, y = 7$$

$$y = 2704 - 29m \geq 0$$

$$-\frac{832}{3}$$

Coroll) $\gcd(a, b) = 1$ 인 정수 a, b 에 대하여 (x_0, y_0) 가 부정방정식 $ax+by=c$ 의 특수해라고 할 때,

일반해는 $(x, y) = (x_0 + bk, y_0 - ak) \quad (k \in \mathbb{Z})$

정수 x, y, z 에 관한 다음 방정식의 일반해를 구하시오.

$$3x + 4y + 5z = 2$$

(P6) $\gcd(3, 4) = 1$ 이므로 임의의 정수 t 에 대하여 $3x + 4y = 2 - 5z$ 는 해를 갖는다.

$$3(-1) + 4 \cdot 1 = 1 \text{ 이므로 } x_0 = 5t - 2, y_0 = 2 - 5t \text{ 는 } 3x + 4y = 2 - 5z \text{의 특수해}$$

$$\begin{aligned} 4 &= 3 \times 1 + 1 \quad \Rightarrow \quad 1 = 4 - 3 \\ 1 &= 1 \times 1 + 0 \quad = 4 + 3 \times (-1) \end{aligned} \quad \left. \begin{array}{l} x_0 = (-1) \times (2 - 5t) = 5t - 2 \\ y_0 = 2 - 5t \end{array} \right\}$$

$\gcd(4, 3) = 1$

따라서 일반해는 $x = 5t - 2 + 4s, y = 2 - 5t - 3s, z = t \quad (s, t \in \mathbb{Z})$ 이다.

정답) $x = 5t - 2 + 4s, y = 2 - 5t - 3s, z = t, (s, t \in \mathbb{Z})$

5. 소수 (Prime)

- 소수 : 1과 자기 자신만을 양의 약수로 가지는 자연수

- 합성수 : 소수가 아닌 2 이상의 자연수

자기 자신보다 작은 두 자연수의 곱으로 표현되는 수

- 자연수 a 의 약수 중 소수를 a 의 소인수라고 한다.

Thm 5.1) 1이 아닌 모든 자연수 n 은 소인수를 갖는다. ($n \geq 2$)

(P6) 수학적 귀납법 이용

- 소수의 판정 (제곱근 판정법)

Thm) 합성수 n 은 $1 < p \leq \sqrt{n}$ 인 소수인 약수 p 를 갖는다.

* 소수의 판정 (제곱근 판정법)

\sqrt{n} 이하의 소인수를 가지지 않는 자연수 n 은 소수

Rmk) 에라토스네스의 체

에라토스네스의 체라고 하는 방법으로 50 이하 소수를 모두 찾을 수 있다.

$\cancel{150} = 1, 0, 1, \dots$ 이하의 소수는 2, 3, 5, 7이다. 따라서 50 이하의 합성수는 2, 3, 5, 7 이 아닌 2, 3, 5, 7의 배수이다.

아래 표에서 2 이외의 2의 배수, 3 이외의 3의 배수, 5 이외의 5의 배수, 7 이외의 7의 배수를 차례로 지워나가면 50 이하의 모든 소수가 남는다

2	3	4	5	6	7	8	9	10	→ 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

• 소수 존재의 무한성과 크기

Thm 5.2) 소수는 무한히 많다. → 유한개라 가정하여 증명

Thm 5.3) n 번째 소수를 p_n 이라 하면, $p_n \leq 2^{2^n-1}$ 이다.

* 특별한 꼴의 소수

• $an+b$ 꼴의 소수

각 자연수는 $4n, 4n+1, 4n+2, 4n+3$ 중 하나의 꼴을 하고 있고, 이 중 소수가 가질 수 있는 꼴은 $4n+1, 4n+3$ 중 하나.

Thm 5.4) $4n+3$ 꼴의 소수는 무수히 많다. → 유한개라 가정하여 증명

* $an+b$ 꼴의 수가 소수이기 위해서는 $\gcd(a, b) = 1$ 이어야 한다.

Thm 5.5) (리만레)

서로 소인 자연수 a, b 에 대하여, $4a+b$ 꼴의 소수는 무수히 많다.

* 2^n-1 꼴의 소수: 메르센 소수

Def) $M_n = 2^n - 1$ ($n \geq 1$) 꼴의 소수를 메르센 수라 하고, 특히 M_n 이 소수일 때 이 소수를 메르센 소수라 한다.

Coroll 5.6) $n \geq k$ 인 자연수 k, n 에 대하여 $k|n \Rightarrow (2^k - 1)|(2^n - 1)$

$$\frac{||}{M_k} \quad \frac{||}{M_n}$$

Thm 5.7) 메르센 수 $M_n = 2^n - 1$ 이 소수이면, n 도 소수이다. * 역은 성립하지 않음.

* $2^m + 1$ 꼴의 소수

Thm) $2^m + 1$ 이 소수이면 m 은 2의 거듭제곱이다.

Def) $F_n = 2^{2^n} + 1$, ($n \geq 0$) 꼴의 수를 페르마 수라 하고. 특히 F_n 이 소수일 때 이 소수를 페르마 소수라 한다.

* $n = 0, 1, 2, 3, 4$ 일 때는 F_n 이 소수이다. But $F_5 = 2^{32} + 1$: 소수 아님.

Thm) F_n 이 n 번째 페르마 수이다. 이 때, $n \geq 1$ 일 때 $F_n = F_{n-1}^2 - 2F_{n-1} + 2$

* 모든 페르마 소수는 다음 정화식으로도 구할 수 있다.

$$F_n = F_0 F_1 \cdots F_{n-1} + 2 \quad (n \geq 1)$$

Thm 5.9) (골드바흐) 자연수 m, n 에 대하여 $m+n \Rightarrow \gcd(F_m, F_n) = 1$

* 소수의 분포

< 소수에 대한 추측 >

(3.5) (5.7) (II.13)

① 쌍둥이 소수 (자가 2인 한쌍의 소수) 추측: p 와 $p+2$ 가 모두 소수인 p 는 무수히 많다.

② 골드바흐의 추측: 임의의 양의 짝수는 (소수) + (소수) 또는 (소수 + 1) 꼴로 표현된다.

③ $n^2 + 1$ 추측: 양의 정수 n 에 대하여 $n^2 + 1$ 형태의 소수는 무수히 많다.

Thm) 임의의 양의 정수 n 에 대하여 적어도 n 개의 연속된 합성수가 존재한다.

* 소인수 분해에서 같은 소인수의 품을 거듭제곱으로 나타내면 그 이상의 임의의 자연수 n 의 소인수분해는 다음과 같은 유일한 표준형으로 나타낼 수 있다.

$$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} \quad (p_1 < p_2 < \cdots < p_r \text{은 소수}, e_1, e_2, \dots, e_r \text{은 자연수})$$

* 소인수분해의 응용

소수 p 와 양의 정수 n 에 대해 $p^r | n$, $p^{r+1} \nmid n$ 일 때, p^r 을 n 의 p 성분이라 한다.

(예) 12의 2 성분은 2^2 이고, 5 성분은 $5^0 = 1$ 이다.

* 양의 정수 n 의 p 성분 p^r 의 차수 r 를 $\varepsilon_p(n)$ 으로 나타낸다.

(예) $360 = 2^3 \times 3^2 \times 5$ 이므로 $\varepsilon_2(360) = 3$, $\varepsilon_3(360) = 2$, $\varepsilon_5(360) = 1$ 이다.

Thm 6.5) m, n 이 양의 정수일 때, 임의의 소수 p 에 대하여 $\varepsilon_p(mn) = \varepsilon_p(m) + \varepsilon_p(n)$

Thm 6.7) 소수 p 와 양의 정수 n 에 대하여 $\varepsilon_p(n!) = \left[\frac{n}{p} \right] + \left[\frac{n}{p^2} \right] + \left[\frac{n}{p^3} \right] + \dots$

Def) $4, 9, 16, 25, \dots$ 과 같이 2이상의 정수의 제곱인 수를 완전제곱수 또는 간단히 제곱수라고 한다.

* 양의 정수 n 이 완전제곱수일 필요충분조건은 임의의 소수 p 에 대하여 $\varepsilon_p(n)$ 이 짝수인 것이다.

* 약수 배수 다시 보기

< 확장된 표준형 소인수분해 >

Thm 6.10) 양의 정수 a, b 의 확장된 표준형 소인수분해가 각각

$$a = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} \quad (e_1, e_2, \dots, e_r \geq 0)$$

$$b = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r} \quad (f_1, f_2, \dots, f_r \geq 0)$$

$$\text{일 때, } \gcd(a, b) = p_1^{\min\{e_1, f_1\}} p_2^{\min\{e_2, f_2\}} \cdots p_r^{\min\{e_r, f_r\}}$$

$$\text{lcm}(a, b) = p_1^{\max\{e_1, f_1\}} p_2^{\max\{e_2, f_2\}} \cdots p_r^{\max\{e_r, f_r\}}$$

$$(\text{Rmk}) \quad \gcd(192, 405) = \gcd(2^3 \cdot 3^2 \cdot 5^0, 2^0 \cdot 3^2 \cdot 5^1) = 2^0 \cdot 3^2 \cdot 5^0$$

$$\text{lcm}(192, 405) = 2^3 \cdot 3^2 \cdot 5^1$$

Corol 6.11) $\gcd(m, n) = 1$ 인 자연수 m, n 의 약수 전체의 집합을 각각 $\{x_1, x_2, \dots, x_r\}, \{y_1, y_2, \dots, y_s\}$ 라고 하면,

mn 의 약수 전체는 다음 행렬의 성분 전체이다.

$$\begin{bmatrix} x_1y_1 & x_1y_2 & \cdots & x_1y_s \\ x_2y_1 & x_2y_2 & \cdots & x_2y_s \\ \vdots & \vdots & \ddots & \vdots \\ x_ny_1 & x_ny_2 & \cdots & x_ny_s \end{bmatrix}$$

더욱이 이 행렬의 성분은 모두 서로 다르다.

* 약수의 개수와 약수의 합

Def) 자연수 전체의 집합을 정의역으로 하고 실수 전체의 집합을 공역으로 하는 함수를 정수론적 함수라고 한다.

* 약수 개수

Def) 자연수 n 의 양의 약수의 개수를 $\tau(n)$ 으로 나타낸다.

(예) $\tau(6) = 4$

Def) 정수론적 함수 f 가 조건 $\gcd(m, n) = 1 \Rightarrow f(mn) = f(m)f(n)$ 을 만족할 때, f 는 승법적이라 한다.

Thm 6.12) 함수 τ 는 승법적이다.

Thm) $n > 1$ 이고 자연수 n 의 표준형 인수분해가 $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ 일 때,

$$\tau(n) = (e_1 + 1)(e_2 + 1) \cdots (e_r + 1)$$

* 약수의 합

Def) 자연수 n 의 양의 약수의 합을 $\sigma(n)$ 으로 나타낸다.

(예) $\sigma(6) = 12$

Thm) 함수 σ 는 승법적이다.

Thm) $n > 1$ 이고 자연수 n 의 표준형 인수분해가 $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ 일 때.

$$\tau(n) = \frac{p_1^{e_1+1}-1}{p_1-1} \cdot \frac{p_2^{e_2+1}-1}{p_2-1} \cdots \frac{p_r^{e_r+1}-1}{p_r-1}$$

(Ex) $\tau(10000) = \tau(2^6 5^6) = \tau(2^6) \tau(5^6) = \frac{2^7-1}{2-1} \cdot \frac{5^7-1}{5-1} = 2480437$

* 완전수

Def) 어떤 자연수가 자기 자신 이외의 양의 약수의 합과 같을 때. 그 수를 완전수라 함.

(예) 6

* 자연수 n 에 대하여, n 이외의 양의 약수의 합은 $\tau(n)-n$ 이므로 n 이 완전수일 필요충분조건은 $\tau(n) = 2n$ 이다.

p95

(예) (1) $496 = 2^4 \cdot 31$

$$\tau(496) = \tau(2^4 \cdot 31) = \frac{2^5-1}{2-1} \cdot \frac{31^2-1}{31-1} = 31 \cdot 32 = 2^5 \cdot 31 = 2 \times 496$$

$$\tau(496) = \tau(2^4 \cdot 31)$$

$$= (4+1)(1+1) = 10 = \tau(2^4) \cdot \tau(31)$$

\therefore 증명

Thm 6.16) 짝수 n 이 완전수일 필요충분조건은 어떤 정수 $r \geq 2$ 이 존재하여

" $n = 2^{r-1}(2^r - 1)$, $2^r - 1$ 은 소수 " 일 것이다.

II 합동식과 원시근

1. 합동식 (임용)*

2. 일차합동식

3. 페르마의 정리

4. 오일러의 정리

5. 원시근과 이산로그

6. 원시근의 존재

1. 합동식

* 합동의 뜻과 기본 성질

Def) 고정된 자연수 n 과 정수 a, b 에 대하여 a, b 를 n 으로 나눈 나머지가 같으면 a 와 b 는 $\pmod n$ 에 관하여 합동이라 하고 $a \equiv b \pmod n$

(예) $2 \equiv 7 \pmod 5$

Lemma) 고정된 자연수 n 에 대하여 $a \equiv b \pmod n$ 일 필요충분 조건은 $n | (a-b)$ 이다.

Thm 1.1) 고정된 양의 정수 n 과 정수 a, b 에 대하여 $a \equiv b \pmod n$ 일 필요충분 조건은 $a = b + kn$ 을 만족하는 정수 k 가 존재하는 것이다.

Lemma) n 이 양의 정수일 때 다음이 성립한다.

① (reflexivity) $a \equiv a \pmod n$

② (symmetry) $a \equiv b \pmod n \Rightarrow b \equiv a \pmod n$

③ (transitivity) $a \equiv b \pmod n, b \equiv c \pmod n \Rightarrow a \equiv c \pmod n$

Thm 1.3) $a \equiv b \pmod n, c \equiv d \pmod n$ 일 때,

(1) $a \pm c \equiv b \pm d \pmod n$ (2) $ac \equiv bd \pmod n$

(예) $13 \equiv 3 \pmod 5$ 이고 $2 \equiv 7 \pmod 5$ 이므로

$$\rightarrow 13+2 = 15 \equiv 3+7 = 10 \pmod 5 \quad \rightarrow 13 \cdot 2 = 26 \equiv 3 \cdot 7 = 21 \pmod 5$$

Lemma) $a \equiv b \pmod n$ 일 때, 다음이 성립한다. (す, c 는 임의의 정수)

(1) $a \pm c \equiv b \pm c \pmod n$ (2) $ac \equiv bc \pmod n$

(3) $a^k \equiv b^k \pmod n$ (す, k 는 임의의 정수)

(예) $19 \equiv 3 \pmod 8 \Rightarrow 19+7 = 26 \equiv 3+7 = 10 \pmod 8$

$$3^2 = 19 \cdot 2 \equiv 3 \cdot 2 = 6 \pmod 8$$

(예) $14 = 7 \cdot 2 \equiv 4 \cdot 2 = 8 \pmod 6 \Rightarrow 7 \equiv 4 \pmod 6$

(예) $6 \equiv 1 \pmod 5 \Rightarrow 6^3 = 216 \equiv 1^3 \pmod 5$

Thm 7.4) 정수계수다항식 $f(x)$ 에 대하여,

$$a \equiv b \pmod{n} \Rightarrow f(a) \equiv f(b) \pmod{n}$$

Thm 7.5) n 에 관한 소거율

$$\gcd(c, n) = 1 \text{ 일 때}, \quad ac \equiv bc \pmod{n} \Rightarrow a \equiv b \pmod{n}$$

Corol 7.7) $ac \equiv bc \pmod{n} \Rightarrow a \equiv b \pmod{\frac{n}{\gcd(c, n)}}$

Thm 7.8) $a \equiv b \pmod{n}$ 일 때, $\gcd(a, n) = \gcd(b, n)$ 이다.

Thm 7.10) 자연수 N 의 십진법의 전개식이 $N = a_n 10^n + \dots + a_2 10^2 + a_1 10^1 + a_0$ 라고 하자.

(1) $9 | N \Leftrightarrow 9 | (a_n + \dots + a_2 + a_1 + a_0)$

* $3 | N \Leftrightarrow 3 | (a_n + \dots + a_2 + a_1 + a_0)$

(2) $11 | N \Leftrightarrow 11 | (-1)^n a_n + \dots + a_2 - a_1 + a_0$

(3) N 을 1000 진법으로 나타내어

$$N = B_m 1000^m + \dots + B_2 1000^2 + B_1 1000^1 + B_0 \text{ 와 같이 쓰자.}$$

$$k=7, 11, 13 \text{ 일 때}, \quad k | N \Leftrightarrow k | (-1)^m B_m + \dots + B_2 - B_1 + B_0$$

* 완전 임여계

Def) n 이 양의 정수라 하자. 정수 a 와 r 에 대해 $a \equiv r \pmod{n}$ 이면 r 은 n 에서 a 의 임여류 한다.

$a \equiv r \pmod{n}$ 에 관한 등치류를 n 에 관한 임여류라고 하고 $r \in \mathbb{Z}$ 에 의하여 얻어지는 임여류를 E_r 로 나타내면

$$E_r = \{r + nk \mid k \in \mathbb{Z}\} = \{ \dots, r-2n, r-n, r, r+n, \dots \}$$

(예) 정수 집합은 양의 정수 n 을 범위로 n 개의 임여류로 분할된다.

$n=3$ 일 때의 임여류는 다음과 같다.

$$E_0 = \{ \dots, -9, -6, -3, 0, 3, 6, 9, \dots \} = 3k$$

$$E_1 = \{ \dots, -2, 1, 4, 7, \dots \} = 3k+1$$

$$E_2 = \{ \dots, -1, 2, 5, 8, \dots \} = 3k+2$$

Thm) 범 n 에 관한 합동관계에 대하여 다음이 성립

$$(1) a \equiv r \pmod{n} \Leftrightarrow E_a = E_r$$

(2) \mathbb{Z} 는 모든 임여류의 합집합이다.

$$(3) i \neq j \text{ 일 때, } E_i \cap E_j = \emptyset$$

Def) 범 n 에 관한 n 개의 임여류 $E_0, E_1, E_2, \dots, E_{n-1}$ 각각에서 하나씩의 원소를 택하여 만든 집합

$$\{a_0, a_1, a_2, \dots, a_{n-1}\}, \quad (a_k \in E_k, \quad k = 0, 1, 2, \dots, n-1)$$