정수론 이론 및 문제풀이 목차

1. 서론

유한 귀납법의 기본원리

양의 정수들로 이루어진 집합 S가 다음 두 가지 성질을 만족한다고 하자.
(i) 정수 1은 S에 속한다.
(ii) 정수 k가 S에 속하면, $k+1$또한 S에 속한다.
그러면 S는 모든 양의 정수를 가진다.

2. 정수의 나눗셈정리

(1) $a, b(\neq 0)$가 정수이면 $a=qb+r,\ 0 \le r < |b|$을 만족하는 유일한 정수 q, r이 존재한다.

$a|b,\ a \nmid b$

$c \in \mathbb{Z}$가 존재하여 $b=ac$를 만족할 때 b는 $a(\neq 0) \in \mathbb{Z}$로 나누어진다고 표현하고 $a|b$로 쓴다.
b가 a로 나누어지지 않는 경우 $a \nmid b$로 쓴다.

(1) 정수 a, b, c에 대해 다음이 성립한다.
(i) $a|0,\ 1|a,\ a|a$
(ii) $a|1 \Leftrightarrow a=\pm 1$
(iii) $a|b,\ c|d \Rightarrow ac|bd$
(iv) $a|b,\ b|c \Rightarrow a|c$
(v) $a|b,\ b|a \Leftrightarrow a=\pm b$
(vi) $a|b,\ b \neq 0 \Rightarrow |a| \le |b|$
(vii) $a|b,\ a|c \Rightarrow \forall x, y \in \mathbb{Z},\ a|(bx+cy)$

최대공약수 $\gcd(a, b)$

a, b를 적어도 둘 중 하나는 0이 아닌 정수라 하자. a, b의 최대공약수는 $\gcd(a, b)$로 쓰고 다음을 만족하는 양의 정수 d이다.
(i) $d|a,\ d|b$
(ii) $c|a,\ c|b \Rightarrow c \mid d$

a, b를 적어도 둘 중 하나는 0이 아닌 정수라 하자.
(1) $\gcd(a, b)=ax+by$ 를 만족하는 x, y가 존재한다.
(2) 집합 $T=\{ax+by | x, y \text{는 정수}\}$는 정확히 정수 $d=\gcd(a, b)$의 배수로 이루어진 집합이다.

서로 소

둘 중 하나는 0이 아닌 정수 a, b에 대해
$\gcd(a, b)=1$인 경우 서로 소라 한다.

(1) a, b를 둘 중 하나는 0이 아닌 정수라 하자.
$\gcd(a, b)=1 \Leftrightarrow 1=ax+by$를 만족하는 x, y가 존재
(2) $\gcd(a, b)=d \Rightarrow \gcd(a/d, b/d)=1$
(3) $a|c,\ b|c,\ \gcd(a, b)=1 \Rightarrow ab|c$
(4) 유클리드 보조정리: $a|bc,\ \gcd(a, b)=1 \Rightarrow a|c$
(5) $a=qb+r \Rightarrow \gcd(a, b)=\gcd(b, r)$
(6) $k(\neq 0) \in \mathbb{Z}$에 대해 $\gcd(ka, kb)=|k| \gcd(a, b)$

최소공배수 $lcm(a, b)$

영이 아닌 두 정수 a, b의 최소공배수는 다음을 만족하는 양의 정수 m이며 $lcm(a, b)$로 표현된다.
(i) $a|m, b|m$
(ii) $a|c, b|c$ 이면 $c>0$일 때 $m|c$이다.

(1) 양의 정수 a, b에 대해 $\gcd(a, b) lcm(a, b)=ab$.
(2) $\forall a, b \in \mathbb{Z},\ lcm(a, b)=ab \Leftrightarrow \gcd(a, b)=1$
(3) $ax+by=c$이 해를 가진다 $\Leftrightarrow \gcd(a, b)|c$
특수해 x_0, y_0에 대하여 모든 해는 다음과 같다.

$$x=x_0+\left(\frac{b}{d}\right)t,\ y=y_0-\left(\frac{a}{d}\right)t,\ t \in \mathbb{Z}$$

3. 소수와 그 분포

소수, 합성수

만약 정수 p의 양의 약수가 1과 p뿐일 때, 1보다 큰 p를 소수라 하자. 1보다 큰 정수 중 소수가 아닌 정수를 합성수라 한다.

(1) p가 소수, $p|a_1a_2 \cdots a_n$ 이면 $1 \le k \le n$ 인 어떤 k에 대해 $p|a_k$ 이다.
(2) 만약 $p, q_1, q_2, \cdots, q_n$이 소수이고 $p|q_1q_2 \cdots q_n$이면 $1 \le k \le n$ 인 어떤 k 에 대해 $p=q_k$ 이다.
(3) (산술의 기본정리) 모든 1보다 큰 양의 정수 n은 인수가 나타나는 순서를 고려하지 않을 때, 소수들의 곱으로 유일하게 표현된다.
(4) 모든 양의 정수 $n>1$에 대하여

$$n=p_1^{k_1}p_2^{k_2} \cdots p_r^{k_r}$$

을 만족하는 양수 k_i와 소수 $p_i(p_1<p_2<\cdots<p_r)$가 존재한다.
(5) (유클리드) 무한히 많은 소수가 존재한다.
(6) (디리클레) a와 b 가 서로 소인 양의 정수이면, 다음 수열은 무한히 많은 소수를 포함한다.

$$a,\ a+b,\ a+2b,\ a+3b,\ \cdots$$

4. 합동이론

합동

n을 주어진 양의 정수라 하자. n이 차 $a-b$를 나누면 정수 a와 b를 법 (또는 모듈로) n에 대해 합동이라 말하며 기호로 표현하면 다음과 같다.

$$a \equiv b \pmod{n}$$

(1) 임의의 정수 a와 b 에 대해 $a \equiv b \pmod{n}$일 필요충분조건은 a와 b는 n으로 나누었을 때, 음이 아닌 같은 나머지를 가진다.

(1) $a \equiv b \pmod{n} \Leftrightarrow a$와 b는 n으로 나눈 나머지가 같다.

(2) $n>1$ 이 고정되고, a, b, c, d를 임의의 정수라 하면 다음 성질이 성립한다.

 (ⅰ) $a \equiv a \pmod{n}$

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

 (ⅲ) $a \equiv b \pmod{n}$, $b \equiv c \pmod{n}$

 $\Rightarrow a \equiv c \pmod{n}$

 (ⅳ) $a \equiv b \pmod{n}$, $c \equiv d \pmod{n}$

 $\Rightarrow a+c \equiv b+d \pmod{n}$, $ac \equiv bd \pmod{n}$

 (ⅴ) $a \equiv b \pmod{n}$

 $\Rightarrow \forall k \in \mathbb{N}$, $a^k \equiv b^k \pmod{n}$

(3) $ca \equiv cb \pmod{n}$

 $\Rightarrow a \equiv b \left(\bmod \dfrac{n}{d}\right)$, $d=\gcd(c, n)$

(4) $ca \equiv cb \pmod{n}$, $\gcd(c, n)=1 \Rightarrow a \equiv b \pmod{n}$

(5) $ca \equiv cb \pmod{p}$, $p \nmid c$(p:소수) $\Rightarrow a \equiv b \pmod{p}$

정수의 2진법과 10진법 표현

(1) $P(x)=\sum_{k=0}^{m} c_k x^k$를 정수계수 c_k를 가진 x의 다항 함수라 하자.

 $a \equiv b \pmod{n}$이면 $P(a) \equiv P(b) \pmod{n}$이다.

(2) a가 합동식 $P(a) \equiv 0 \pmod{n}$의 해이고 $a \equiv b \pmod{p}$이면 b 또한 해이다.

(3) $N=a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_1 10 + a_0$, $0 \le a_k \le 10$ 에 대하여 $S=a_0+a_1+\cdots+a_m$이라 하면 $9|N$일 필요충분조건은 $9|S$이다.

(4) $N=a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_1 10 + a_0$, $0 \le a_k \le 10$ 에 대하여 $T=a_0-a_1+a_2-\cdots+(-1)^m a_m$이라 하면 $11|N$일 필요충분조건은 $11|T$이다.

선형 합동식과 중국인의 나머지 정리

(1) $ax \equiv b \pmod{n}$의 해가 존재한다 $\Leftrightarrow \gcd(a, n)|b$

 $d|b$이면 법 n에 대해 d개의 서로 합동이 아닌 해를 가진다.

(2) $\gcd(a, n)=1$이면 선형 합동식 $ax \equiv b \pmod{n}$은 법 n에 대해 유일한 해를 가진다.

(3) (중국인의 나머지 정리) $n_1, n_2, \cdots, n_r$을 $i \ne j$에 대해 $\gcd(n_i, n_j)=1$인 양의 정수라 하자. 그러면 연립 선형 합동식

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_r \pmod{n_r} \end{aligned}$$

 은 법 $n_1 n_2 \cdots n_r$에 대해 유일한 공통 해를 가진다.

5. 페르마 정리

페르마의 작은 정리와 유사소수

(1) (페르마 정리) p가 소수, $p \nmid a \Rightarrow a^{p-1} \equiv 1 \pmod{p}$

(2) $\forall p$:소수, $\forall a \in \mathbb{Z}$, $a^p \equiv a \pmod{p}$

(3) (윌슨의 정리)p가 소수이면 $(p-1)! \equiv -1 \pmod{p}$

(4) p가 홀수인 소수라 하자.

 $x^2+1 \equiv 0 \pmod{p}$가 해를 가짐 $\Leftrightarrow p \equiv 1 \pmod{4}$

6. 수론 함수

수론함수(산술함수)

정의역이 양의 정수의 집합인 임의의 함수를 수론 함수 또는 산술 함수라 부른다.

$\tau(n)$, $\sigma(n)$

양의 정수 n에 대해 τ, σ를 다음과 같이 정의한다.

$\tau(n)$: n의 양의 약수의 개수

$\sigma(n)$: n의 양의 약수들의 합

(1) $n=p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$이 $n>1$의 소인수분해라 하자.

 (ⅰ) $\tau(n)=(k_1+1)(k_2+1)\cdots(k_r+1)$

 (ⅱ) $\sigma(n)=\dfrac{p_1^{k_1+1}-1}{p_1-1}\dfrac{p_2^{k_2+1}-1}{p_2-1}\cdots\dfrac{p_r^{k_r+1}-1}{p_r-1}$

승법적

수론 함수 f를 $\gcd(m, n)=1$일 때

$$f(mn)=f(m)f(n)$$

이면 승법적이라 말한다.

(1) 함수 τ와 σ는 승법 함수이다.

(2) $\gcd(m, n)=1$이면 mn의 양의 약수의 집합은 $d_1|m$, $d_2|n$이고 $\gcd(d_1, d_2)=1$인 모든 곱 $d_1 d_2$로 구성된다. 더군다나 이 곱은 모두 다르다.

(3) f가 승법 함수이고 $F(n)=\sum_{d|n} f(d)$라고 정의하면 F도 또한 승법 함수이다.

$\mu(n)$

양의 정수 n에 대해 μ를 다음과 같이 정의 한다.

$$\mu(n)=\begin{cases}1 & ,\ n=1\\ 0 & ,\ p^2|n,\ p\text{는 소수}\\ (-1)^r & ,\ n=p_1p_2\cdots p_r,\ p_i\text{는 서로 다른 소수}\end{cases}$$

(1) 함수 μ는 승법함수이다.

(2) 양의 정수 $n\geq 1$에 대해

$$\sum_{d|n}\mu(d)=\begin{cases}1, & n=1\\ 0, & n>1\end{cases}$$

(3) (뫼비우스 역공식)

F와 f를 $F(n)=\sum_{d|n}f(d)$인 수론함수라 하자.

그러면, $f(n)=\sum_{d|n}\mu(d)F(\frac{n}{d})=\sum_{d|n}\mu(\frac{n}{d})F(d)$.

(4) F: 승법함수, $F(n)=\sum_{d|n}f(d)\ \Rightarrow\ f$: 승법함수

$[x]$

임의의 실수 x에 대해 $[x]$를 x보다 작거나 같은 가장 큰 정수라 한다.

(1) n가 양의 정수, p가 소수이면 $n!$을 나누는 가장 큰 p의 거듭제곱의 지수는 $\sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right]$ 이다.

7. 오일러 정리

$\varphi(n)$

$n\geq 1$에 대해 $\varphi(n)$을 n과 서로 소이면서 n을 넘지 않는 양의 정수의 개수라 정의한다.

(1) p: 소수, $k>0\ \Rightarrow\ \varphi(p^k)=p^k-p^{k-1}=p^k\left(1-\frac{1}{p}\right)$

(2) $\forall\, a, b, c\in\mathbb{Z}$,
$\gcd(a, bc)=1\ \Leftrightarrow\ \gcd(a, b)=1,\ \gcd(a, c)=1$

(3) 함수 φ는 승법함수이다.

(4) 정수 $n>1$이 $n=p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$인 소인수 분해이면

$$\varphi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)$$

(5) $n>1$이고 $\gcd(a, n)=1$이라 하자.
$a_1, a_2, \cdots, a_{\varphi(n)}$이 n보다 작고 n과 서로 소인 양의 정수이면 $aa_1, aa_2, \cdots, aa_{\varphi(n)}$은 법 n에 대해 어떤 순서로 $a_1, a_2, \cdots, a_{\varphi(n)}$과 합동이다.

(6) (오일러) $n\geq 1,\ \gcd(a, n)=1\ \Rightarrow\ a^{\varphi(n)}\equiv 1 \pmod n$

(7) (가우스) 양의 정수 $n\geq 1$에 대해 $n=\sum_{d|n}\varphi(d)$.

8. 원시근과 지표

법 n에 대한 a의 위수

$n>1$ 그리고 $\gcd(a, n)=1$이라 하자. 법 n에 대한 a의 위수는 $a^k\equiv 1 \pmod n$인 가장 작은 양의 정수 k이다.

$\mathrm{ord}_n a^h=k$라 하면 다음이 성립한다.

(1) $a^k\equiv 1 \pmod n\ \Leftrightarrow\ k|h$; 특히, $k|\varphi(n)$

(2) $a^i\equiv a^j \pmod n\ \Leftrightarrow\ i\equiv j \pmod k$

(3) $a, a^2, \cdots, a^k$는 법 n에 대해 서로 합동이 아니다.

(4) $h>0\ \Rightarrow\ \mathrm{ord}_n a^h=\dfrac{k}{\gcd(h, k)}$

원시근

$\gcd(a, n)=1$이고 법 n에 대한 a 의 위수가 $\varphi(n)$이면 a를 정수 n의 원시근이라 한다.

(1) $\gcd(a, n)=1$이고 $a_1, a_2, \cdots, a_{\varphi(n)}$을 n과 서로 소인 n보다 작은 양의 정수라 하자. a가 n의 원시근이면, $a, a^2, \cdots, a^{\varphi(n)}$은 법 n에 대해 어떤 순서로 $a_1, a_2, \cdots, a_{\varphi(n)}$와 합동이다.

(2) n이 원시근을 가지면 정확히 $\varphi(\varphi(n))$개의 원시근이 존재한다.

(3) p를 소수라 하고 $d|p-1$이면 법 p에 대해 위수 d를 갖는 정확히 $\varphi(d)$개의 합동이 아닌 해가 존재한다.

(4) 정수 $n>1$에 대하여 다음은 동치이다.
 (ⅰ) n의 원시근이 존재한다.
 (ⅱ) $n=2, 4, p^k$ 또는 $2p^k$ (p는 홀수인 소수)

지표

r을 n의 원시근이라 놓자.
$\gcd(a, n)=1$이면 $a\equiv r^k \pmod n$인 가장 작은 양의 정수 k를 r에 대한 a의 지표라 부른다.

(1) n이 원시근 r을 가지고 $\mathrm{ind}\,a$를 r에 대한 a의 원시근이라 놓으면 다음 성질이 성립한다.
 (ⅰ) $\mathrm{ind}(ab)\equiv \mathrm{ind}\,a+\mathrm{ind}\,b \pmod{\varphi(n)}$
 (ⅱ) $\mathrm{ind}\,a^k\equiv k\,\mathrm{ind}\,a \pmod{\varphi(n)},\ k>0$
 (ⅲ) $\mathrm{ind}\,1\equiv 0 \pmod{\varphi(n)},\ \mathrm{ind}\,r\equiv 1 \pmod{\varphi(n)}$

(2) n이 원시근을 갖는 정수, $\gcd(a, n)=1$이라 하면 다음은 동치이다.
 (ⅰ) $x^k\equiv a \pmod n$의 해가 존재한다.
 (ⅱ) $a^{\frac{\varphi(n)}{d}}\equiv 1 \pmod n,\ d=\gcd(k, \varphi(n))$
 해가 존재하는 경우 정확히 d개의 해가 존재한다.

9. 이차상호법칙

이차 잉여류, 이차 비잉여류

p는 홀수인 소수, $\gcd(a,p)=1$이라 하자.
이차 합동식 $x^2 \equiv a \pmod{p}$가 해를 가지면 a를 p의 이차 잉여류, 갖지 않으면, a를 p의 이차 비잉여류라 한다.

(1) p는 홀수인 소수, $\gcd(a,p)=1$이라 하자.

(ⅰ) a가 p의 이차 잉여류 $\Leftrightarrow$ $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

(ⅱ) a가 p의 이차 비잉여류 $\Leftrightarrow$ $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$

르장드르 기호

p는 홀수인 소수, $\gcd(a,p)=1$이라 하자.
그러면 르장드르 기호 $\left(\dfrac{a}{p}\right)$는 다음과 같이 정의된다.

$$\left(\frac{a}{p}\right)=\begin{cases} 1, & a\text{는 } p\text{의 이차 잉여류} \\ -1, & a\text{는 } p\text{의 이차 비잉여류}\end{cases}$$

(1) p:홀수인 소수, $\gcd(a,p)=\gcd(b,p)=1$ $\gcd(a,p)=1$이면 다음이 성립한다.

(ⅰ) $a \equiv b \pmod{p} \Rightarrow (a/p)=(b/p)$

(ⅱ) $(a^2/p)=1$

(ⅲ) $(a/p)=a^{\frac{p-1}{2}} \pmod{p}$

(ⅳ) $(ab/p)=(a/p)=(b/p)$

(ⅴ) $(1/p)=1$, $(-1/p)=(-1)^{\frac{p-1}{2}}$

(2) p를 홀수인 소수라 하면 $\sum_{a=1}^{p-1}(a/p)=0$이다. 따라서 정확히 $\dfrac{p-1}{2}$개의 p의 이차잉여류와 $\dfrac{p-1}{2}$개의 p의 이차 비잉여류가 존재한다.

(3) p를 홀수인 소수라 하면 다음이 성립한다.

$$(2/p)=(-1)^{\frac{p^2-1}{8}}$$

(4) (이차상호법칙) p,q: 서로 다른 홀수인 소수이면

$$(p/q)(q/p)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Chapter 1 서론

1.1 수학적 귀납법

(정렬성의 원리) 공집합이 아니고 음이 아닌 정수들을 원소로 갖는 모든 집합 S는 최소 원소를 가지고 있다.

정리 1.1 (아르키메데스 원리) a와 b가 양의 정수이면, $na \geq b$를 만족하는 양의 정수 n이 존재한다.

『증명』

정리 1.2 (유한 귀납법의 기본원리) 양의 정수들로 이루어진 집합 S가 다음 두 가지 성질을 만족한다고 하자.
(a) 정수 1은 S에 속한다.
(b) 정수 k가 S에 속하면, 다음 정수 $k+1$또한 S에 속한다.
그러면 S는 모든 양의 정수를 가진다.

『증명』

정리 1.3 양의 정수들로 이루어진 집합 S가 다음 두 가지 성질을 만족한다고 하자.
(a) 정수 1은 S에 속한다.
(b) $1, 2, \cdots, k$가 S에 속하면, 다음 정수 $k+1$또한 S에 속한다.
그러면 S는 모든 양의 정수를 가진다.

『증명』

※ 다음은 모든 자연수 n에 대하여 성립하지 않지만 **정리 1.2**의 (b)를 만족한다.

$$1+3+5+\cdots+(2n-1)=n^2+3$$

유한 귀납법의 원리에서 (a)는 반드시 필요한 조건이다.

예제 1.1

다음과 같이 정의 되는 Lucas 수열을 a_n이라 하면 모든 자연수 n에 대하여 $a_n < (7/4)^n$이 성립함을 보여라.

$$a_1=1,\ a_2=3,\ a_n=a_{n-1}+a_{n-2},\ n \geq 3$$

『풀이』

Chapter 2 정수의 나눗셈 알고리즘

2.2 나눗셈 알고리즘

정리 2.1 (나눗셈 알고리즘) 주어진 정수 a, b에 대해 $b>0$, 다음을 만족하는 유일한 정수 q, r이 존재한다.

$$a = bq + r, \quad 0 \le r < b$$

a를 b로 나누는 연산에서 q를 몫(quotient), r은 나머지(remainder)라 부른다.

『증명』

따름정리 2.2 a, b가 정수이면 $(b \neq 0)$ 다음 식을 만족하는 유일한 정수 q, r이 존재한다.

$$a = bq + r, \quad 0 \le r < |b|$$

『증명』

예제 2.1

모든 1이상의 정수 a에 대해 $\dfrac{a(a^2+2)}{3}$이 정수임을 보여라.

『풀이』

2.3 최대공약수

정의 2.1 정수 c가 존재하여 $b=ac$를 만족할 때 b는 0이 아닌 정수 a로 나누어진다고 표현하고 $a|b$로 쓴다. b가 a로 나누어지지 않는 경우 $a\nmid b$로 쓴다.

정리 2.3 정수 a, b, c에 대해 다음이 성립한다.

(a) $a|0,\ 1|a,\ a|a$

(b) $a|1$ 이면 $a=\pm1$이다. 그 역도 성립한다.

(c) $a|b$ 이고 $c|d$ 이면 $ac|bd$ 이다.

(d) $a|b$ 이고 $b|c$ 이면 $a|c$ 이다.

(e) $a|b$ 이고 $b|a$ 이면 $a=\pm b$ 이다. 그 역도 성립한다.

(f) $a|b$ 이고 $b\neq0$ 이면 $|a|\leq|b|$ 이다.

(g) $a|b$ 이고 $a|c$ 이면 임의의 정수 x, y에 대해 $a|(bx+cy)$이다.

『증명』

(참, 거짓 판정문제) p가 소수일 때, $p!+1$을 나누는 소수는 p보다 크다. [2011]

『풀이』

정의 2.2 a, b를 적어도 둘 중 하나는 0이 아닌 정수라 하자. a, b의 **최대공약수**(greatest common divisor)는 $\gcd(a, b)$로 쓰고 다음을 만족하는 양의 정수 d이다.
(a) $d|a$, $d|b$
(b) $c|a$ 이고, $c|b$ 이면 $c \le d$

예제 2.2

$$\gcd(-12, 30)=6,\ \gcd(-5, 5)=5,\ \gcd(8, 17)=1,\ \gcd(-8, -36)=4$$

『풀이』

정리 2.4 적어도 하나는 0이 아닌 주어진 정수 a, b에 대해

$$\gcd(a, b)=ax+by$$

를 만족하는 x, y가 존재한다.

『증명』

정의 2.3 정수 a, b에 대해 $\gcd(a, b)=1$인 경우 **서로소(relatively prime)**라 한다.

정리 2.5 a, b를 둘 중 하나는 0이 아닌 정수라 하자. a, b가 서로 소이면 x, y가 존재하여 $1=ax+by$이다. 역도 성립한다.

『증명』

따름정리 2.6 $a|c$, $b|c$ 그리고 $\gcd(a, b)=1$이면 $ab|c$이다.

『증명』

정리 2.7 (유클리드 보조정리) $a|bc$이고 $\gcd(a, b)=1$이면 $a|c$이다.

『증명』

정리 2.8 a, b를 둘 중 하나는 0이 아닌 정수라 하자. 양의 정수 d에 대해 $d=\gcd(a, b)$와 아래 명제는 필요충분조건이다.

(a) $d|a$, $d|b$

(b) $c|a$, $c|b$ 이면 $c|d$이다.

『증명』

2.4 유클리드 알고리즘

보조정리 2.9 $a = bq + r$이면 $\gcd(a, b) = \gcd(b, r)$

『증명』

예제 2.3

$\gcd(56, 72)$를 구하고 56과 72의 일차결합으로 표현하여라.

『풀이』

<보기>에서 옳은 것을 모두 고른 것은? [2009]

<보기>

ㄱ. 정수 a, b가 서로소이기 위한 필요충분조건은 적당한 정수 s, t에 대하여 $as + bt = 1$이 성립하는 것이다.

ㄴ. 양의 정수 m과 n에 대하여 $2^m - 1$과 $2^n - 1$이 서로소이기 위한 필요충분조건은 m과 n이 서로소인 것이다.

ㄷ. 양의 정수가 25진법으로 표현될 때 3자리 수이기 위한 필요충분조건은 5진법으로 표현될 때 6자리 수 인 것이다.

① ㄱ ② ㄴ ③ ㄱ, ㄴ
④ ㄱ, ㄷ ⑤ ㄴ, ㄷ

『풀이』

2.5 디오판투스 방정식 $ax+by=c$

정리 2.10 선형 디오판투스 방정식 $ax+by=c$는 해를 가지는 것은 $d=\gcd(a,\ b)$일 때 $d|c$임과 동치이다. $x_0,\ y_0$가 이 방정식의 특수해라면 다른 모든 해들은 t가 임의의 정수일 때 다음과 같이 표현할 수 있다.

$$x=x_0+\left(\frac{b}{d}\right)t, \qquad y=y_0-\left(\frac{a}{d}\right)t$$

『증명』

예제 2.4

한 고객이 1.32달러에 열 두 개의 과일, 사과와 오렌지를 구입하였다. 사과가 오렌지 보다 3센트 더 비싸고 사과를 오렌지보다 더 많이 구매하였다면 각각 얼마나 구입하였는가? (1달러=100센트)

『풀이』

(참, 거짓 판정문제) 부정방정식 $7x+31y=2$의 정수해가 존재한다. [2010]

『풀이』

방정식 $2x+3y=55$를 만족하는 양의 정수해 (x, y)의 개수를 구하시오. [1992]

『풀이』

절댓값이 10이하인 두 정수 x, y가 $32x+14y=(32, 14)$를 만족시킬 때, $|x|+|y|$의 값을 구하시오. (단, (a, b)는 a와 b의 최대공약수이다.) [2009 모의평가]

『풀이』