1.1 나눗셈 알고리즘

정리 1.1.1 나눗셈 알고리즘(The division Algorithm)

a와 b는 $b>0$인 정수라 하자. 그러면 $a=bq+r,\ 0\le r<b$를 만족하는 유일한 $q,r\in\mathbb{Z}$가 존재한다.

주의 : a는 음수일 수 있다.

따름정리 1.1.1 나눗셈 알고리즘의 변형

a와 c는 $c\neq 0$인 정수라 하자. 그러면 $a=cq+r,\ 0\le r<|c|$를 만족하는 유일한 $q,r\in\mathbb{Z}$가 존재한다.

예제) 9=2*4+1

-5=2*(-2)-1 x

-5=2*(-3)+1 O

예제 | 1.1.2 모든 홀수는 어떤 정수 k에 대하여 $4k+1$ 또는 $4k+3$ 꼴임을 증명하라.

►풀이◄

n이 임의의 홀수라 하자. 그러면 $m\in\mathbb{Z}$이 존재하여 $n=2m+1$을 만족한다.

경우1 : m이 짝수인 경우 그러면, $k_1\in\mathbb{Z}$이 존재하여 $m=2k_1$이고 $n=2(2k_1)+1=4k_1+1$ 이다.

경우2 : m이 홀수일 경우 그러면 $k_2\in\mathbb{Z}$이 존재하여 $m=2k_2+1$이고 $n=2(2k_2+1)+1=4k_2+3$ 이다.

1.2 나뉘어 떨어짐

정의 1.2.1 약수와 배수

a와 b는 $b>0$인 정수라 하자. 적당한 $c\in\mathbb{Z}$가 존재하여 $a=bc$이면 b는 a를 나눈다(b divides a) 또는 b는 a의 약수(devisor) 또는 b는 a의 인수(factor) 또는 a는 b의 배수(multiple)라 한다. 이 경우에 기호 $b|a$로 쓰고 b가 a의 약수가 아닐 때 기호 $b\nmid a$ 로 쓴다.

▌보기 1.2.2 ▐ 모든 0 아닌 정수 b는 0의 약수다.

왜냐하면 $0 = b \cdot 0$이기 때문이다.

모든 정수 a에 대하여 $1 | a$이다.

왜냐하면 $a = 1 \cdot a$ 이기 때문이다. ■

주목 1.2.1 b가 a의 약수이면, 어떤 c에 대하여 $a = bc$. 따라서 $-a = b(-c)$ 그러므로 $b | (-a)$. 비슷하게 $-a$의 모든 약수는 역시 a의 약수임을 알 수 있다. 따라서 $\boldsymbol{a}$와 $\boldsymbol{-a}$는 같은 약수들을 갖는다.

주목 1.2.2 $a \neq 0$ 이고 $b | a$라 가정하자. 그러면 $\exists\, c \in \mathbb{Z}$ $s.t.$ $a = bc$. 그래서 $|a| = |b||c|$. 그러므로 $0 \leq |b| \leq |a|$이다. 이 부등식은 $-|a| \leq b \leq |a|$와 논리적으로 같다. 따라서

(i) 0이 아닌 정수 a의 모든 약수는 $|a|$보다 작거나 같다.

(ii) 0이 아닌 정수는 유한개의 약수만을 갖는다.

정수 12의 모든 약수는

1, -1, 2, -2, 3, -3, 4, -4, 6, -6, 12, -12

비슷하게, 30의 모든 약수는

1, -1, 2, -2, 3, -3, 5, -5, 6, -6, 10, -10, 15, -15, 30, -30

12와 30의 공약수(common divisor)는 12와 30을 모두 나누는 수, 즉, 다음에 열거된 목록에 나타나는 수다.

1, -1, 2, -2, 3, -3, 6, -6.

이 공약수들 중에서 가장 큰 수 6을 12와 30의 최대공약수(the greatest common divisor)라 한다. 이것은 다음의 정의의 한 보기다.

정의 1.2.2 최대공약수

a와 b는 둘다 0아닌 정수라 하자. a와 b의 최대공약수(gcd)는 a와 b를 모두 나누는 가장 큰 정수 d를 말한다. 다른 말로 하면, 정수 d가 a와 b의 최대공약수일 필요충분조건은 d가 다음의 조건을 만족하는 것이다.

(i) $d | a$ 이고 $d | b$;

(ii) $c | a$ 이고 $c | b$ 면, $c \leq d$.

이때, d를 보통 (a, b)로 표시한다.

a와 b가 둘 다 0이 아니면, 이 두 정수의 gcd는 존재하고 유일하다. 그 이유는 0 아닌 정수는 유한개의 약수만을 가지므로, 유한개의 공약수만이 존재한다는 것이다. 그러므로 꼭 하나의 가장 큰 공약수가 존재해야만 한다. 더욱이, a와 b의 최대공약수는 부등식

$$(a,b) \geq 1$$

을 만족한다. 왜냐면, 1은 a와 b의 공약수이기 때문이다.

▌보기 1.2.3▐ 위에서 보여지듯이, (12, 30)=6. 10과 21의 공약수는 1과 -1뿐이다. 그러므로 (10,21)=1. 최대공약수가, 10과 21과 같은, 1인 두 정수를 서로소(relatively prime)라 한다. ■

6=(12,30)임을 알았다. 약간의 계산을 통하여 6은 12와 30의 1차 결합 (linear combination)으로 표시됨을 알 수 있다. 예로써,

6=12(-2)+30(1) 이고 6=12(8)+30(-3)

이다. 여러분은 $6=12u+30v$인 다른 정수 u와 v를 구할 수 있다.

정리 1.2.3

a와 b는 둘 다 0아닌 정수고 d는 이 두수의 최대공약수라 하자. 그러면 $d=au+bv$를 만족하는 정수 $u,v \in \mathbb{Z}$ (꼭 하나 일 필요는 없음)가 존재한다.

위의 정리에서 $d=1$일 때만 역도 성립한다.

따름정리 1.2.3

a와 b둘 다 0이 아닌 정수고 d는 양의 정수라 하자.
$d=(a,b)$일 필요충분조건은 다음과 같다.
(i) $d|a$이고 $d|b$;
(ii) $c|a$이고 $c|b$면, $c|d$.

다음의 질문에 대한 답은 여러 가지 경우에 필요하게 될 것이다.$a|bc$면, 어떤 조건에서 $a|b$ 또는 $a|c$가 성립하는가? 이것은 확실히 언제나 성립하지는 않는다. 예로써,

$6 \mid 3\cdot 4$ 이지만 $6 \nmid 3$ 이고 $6 \nmid 4$

이다.

정리 1.2.4

$a|bc$ 이고 $(a,b)=1$이면, $a|c$.

►증명◄ $(a,b)=1$이므로, 정리 1.2.3에 의하여,

$1=au+bv$를 만족하는 정수 $u,v\in\mathbb{Z}$가 존재한다.

그러면 $acu+bcv=c$. 한편 $a|bc$ 이므로 $r\in\mathbb{Z}$가 존재하여 $bc=ar$를 만족한다. 그래서

$$c=acu+bcv=acu+(ar)v=a(cu+rv)$$

이고 $a|c$가 된다. ■

임의의 정수 b에 대하여, 우리는 b와 $-b$가 같은 약수들을 가짐을 안다. 결국에, a와 b의 공약수들은 a와 $-b$의 공약수들과 같다. 그러므로 최대공약수들은 같아야만 한다. 즉, $(a,b)=(a,-b)$ 비슷한 주장에 대하여,

$$(a,b)=(a,-b)=(-a,b)=(-a,-b)$$

임을 우리는 안다. 그래서 두 양의 정수의 gcd를 구하는 방법이 역시 임의의 두 정수의 gcd를 구하기 위하여 사용될 수 있다. 여기에 상당히 효과적인 방법이 있다.

정리 1.2.5 유클리드의 알고리즘(The Euclilidean Algorithm)*

a와 b는 $a\geq b$인 양의정수라하자. $b|a$면, $(a,b)=b$이다. $b\nmid a$면, 다음과 같이 반복하여 나눗셈 알고리즘을 적용한다.

$$\begin{aligned}
a &= bq_0+r_0 && 0<r_0<b\\
b &= r_0q_1+r_1 && 0\leq r_1<r_0\\
r_0 &= r_1q_2+r_2 && 0\leq r_2<r_1\\
r_1 &= r_2q_3+r_3 && 0\leq r_3<r_2\\
r_2 &= r_3q_4+r_4 && 0\leq r_4<r_3\\
&\vdots
\end{aligned}$$

이 과정은 나머지가 0이 될 때 끝난다. 이것은 유한번의 단계 후에 일어나야만 한다 즉, 어떤 정수 t에 대하여

$$r_{t-2}=r_{t-1}q_t+r_t \qquad 0<r_t<r_{t-1}$$

$$r_{t-1}=r_tq_{t+1}+0$$

그러면 $r_t=(a,b)$.

우리는 유클리드의 알고리즘을 사용하여 (324,148)을 구한다. a=324이고 b=148 이라하고, 나눗셈 알고리즘을 사용하여, 우리는 $q=2$와 $r_0=28$을 구한다.

(1) 324 =148·2+28
(2) 148 = 28·5+ 8
(3) 28 = 8·3 + 4
8 = 4·2 + 0

각 가로줄에 있는 나눗수는 다음 가로줄에서

나뉨수가 되고 각 가로줄에 있는 나머지는 음 가로줄에서 나눗수가 됨에 주목한다.

마지막 0아닌 나머지는 4다. 그러므로 (324,148)=4. 이제 우리는 324와 148의 1차 결합으로 4를 쓰기 위하여 위의 방정식들에서 반대대입(back-substitution)을 사용 한다.

4 = 28-8·3
4 = 28-(148-28·5)·3

[이것은 바로 방정식(3)이다.]

4 = 28-148·3+28·15
4 =28·16-148·3
4 =(324-148·2)16-148·3
4 = 324·16-148·32-148·3
4 =324·16+148(-35).

[방정식(2)가 수 8을 다시쓰기 위하여 사용되었다.]
[방정식 (3)이 수 28을 다시쓰기 위하여 사용되었다.]

보조정리 1.2.6
$a,b,q,r\in\mathbb{Z}$ 이고 $a=bq+r$이면, $(a,b)=(b,r)$이다.

예제 | 1.2.1 **4144와 7696의 최대공약수를 구하라.**

►풀이◄ 7696 = 4144·1 + 3552
4144 = 3552·1 + 592
3552 = 592·6 + 0
따라서 (4144, 7696) = 592 ■

예제 | 1.2.2 $a|b$이고 $b|c$면, $a|c$ 임을 증명하라.

►풀이◄ $a|b$이고 $b|c$이므로, $\exists\, l,m\in\mathbb{Z}\ s.t.\ b=al$ 이고 $c=bm$이다. 따라서 $c=(al)m=a(lm)$이고 $l,m\in\mathbb{Z}$이다. 그러므로 $a|c$이다. ■

1.2.6 ►증명◄ c가 a와 b의 공약수라 가정하자. 그러면 $s,t\in\mathbb{Z}$가 존재하여 $a=cs$ 이고 $b=ct$이다.
따라서

$$r=a-bq=cs-c(t)q=c(s-tq)$$

이다. 그러므로 $c|r$이고 c는 b와 r의 공약수이다.

역으로 e가 b와 r의 공약수라 가정하자. 그러면

$x, y \in \mathbb{Z}$가 존재하여 $b = ex$, $r = ey$라 쓸 수 있다.

따라서 $a = bq + r = (ex)q + ey = e(xq + y)$

이므로 $e|a$이다. 즉, e는 a와 b의 공약수이다.

이제 S를 a, b의 공약수 전체집합이라 하고 T를 b, r의 공약수 전체집합이라 하면 $S = T$가 된다. 따라서 S의 최대원 (a,b)와 T의 최대원 (b,r)은 같다. ■

1.3 소수와 유일 소인수분해

정의 1.3.1 소수

다음을 만족하는 정수 p를 소수(prime)라 한다. $p \neq 0, \pm 1$이고 p의 약수는 ± 1과 $\pm p$ 뿐이다.

보기 1.3.1 3, -5, 7, -11, 13과 -17은 소수다. 그러나 15는 소수가 아니다. 정수 4567은? ■

정수 p는 $-p$와 같은 약수를 갖기 때문에, 우리는 다음의 사실을 안다 :

$$p\text{가 소수다} \Leftrightarrow -p\text{가 소수다.}$$

p와 q가 둘 다 소수이고 $p|q$면, p는 $1, -1, q, -q$중의 하나이어야만 한다. 그러나 p는 소수이므로, $p \neq \pm 1$. 따라서

$$p\text{와 } q\text{가 소수이고 } p|q\text{ 면, } p = \pm q.$$

정리 1.3.2

p는 $p \neq 0, \pm 1$인 정수라 하자. 그러면 p가 소수일 필요충분조건은 $p|bc$이면, $p|b$ 또는 $p|c$이다.

증명 ($\Rightarrow$): p는 소수고 $p|bc$라 가정하고 p와 b의 gcd를 생각하자. 분명히 $(p,b) = 1$과 $(p,b) = \pm p$ (어느 쪽이든 양이다)뿐이다. $(p,b) = \pm p$면, $p|b$. $(p,b) = 1$면, 정리 1.2.4에 의하여, $p|c$. 따라서 어느 경우에나 $p|b$ 또는 $p|c$이다.

($\Leftarrow$): d가 p의 약수라 하자. 그러면 적당한 $t \in \mathbb{Z}$가 존재하여 $p = dt$이다. $p|dt$이면, $p|d$ 또는 $p|t$이다. $p|d$이

고 $d|p$이므로 $d=\pm p$이다. $p|t$이면 마찬가지로 $t=\pm p$이다. 이말은 $d=\pm 1$이므로 p는 소수이다. ■

따름정리 1.3.2

p는 소수이고 $p \mid a_1 a_2 \cdots a_n$이면, p는 a_i들 중의 하나의 약수다.

정리 1.3.3

0과 ± 1을 제외한 모든 정수 n은 소수들의 곱이다.

소수가 아닌 0과 ± 1이외의 정수를 합성수(composite number)라 한다. 비록 합성수 45가

45=3·3·5

45=(-3)·5·(-3)

45=5·3·3

45=(-5)·(-3)·3

과 같은 여러 가지 다른 소인수분해(prime factorization)를 가질지라도, 이 소인수분해들은 본질적으로 같다. 인수들의 순서와 -부호를 끼워 넣는 차이만 있을 뿐이다. 여러분은 45의 모든 소인수분해는 정확하게 세 개의 소인수(prime factor),

$q_1\, q_2\, q_3$를 가짐을 쉽사리 확신할 수 있다. 더욱이, q들을 다시 배열하고 새 이름을 붙임으로써, 여러분은 언제나 $3=\pm q_1$, $3=\pm q_2$와 $5=\pm q_3$를 가질 것이다. 이것은 다음의 결과의 한 보기다.

정리 1.3.4 기본 계산정리 (The Fundamental Theorem of Arithmetic)

0과 ± 1이외의 모든 정수 n은 소수들의 곱이다. 이 소인수분해는 다음의 의미에서 유일하다 :

$n=p_1 p_2 \cdots p_r$이고 $n=q_1 q_2 \cdots q_s$면,

$r=s$(즉, 인수들의 갯수는 같다)이고 q들을 다시 배열하고 새로 이름을 붙인 후에,

$$p_1=\pm q_1,\ p_2=\pm q_2,\ p_3=\pm q_3,\ \cdots,\ p_r=\pm q_r.$$

여기서 각 p_i와 q_i는 소수다.

이 생각을 양의 정수로 제한하면, 유일한 소인수분해에 대한 더 강한 변형이 있다.

따름정리 1.3.4

모든 정수 $n>1$은 꼭 하나의 방법으로

$$n = p_1 p_2 p_3 \cdots p_r$$

꼴로 쓸 수 있다. 여기서 p_i는 $p_1 \le p_2 \le p_3 \le \cdots \le p_r$인 양의 소수다.

예제 | 1.3.1 p는 0과 ± 1이외의 정수라 하자. p가 소수일 필요충분조건은 모든 $a \in \mathbb{Z}$에 대하여 $(a,p)=1$ 또는 $p|a$이다. 이를 증명하라.

풀이 ($\Rightarrow$) : p는 소수라 가정하고 각 $a \in \mathbb{Z}$에 대하여 $(a,p)=d>1$라 가정하자. 그러면 $d|a$이고 $d|p$. p는 소수이고 $d>1$이므로, $d=\pm p$. 그러므로 $p|a$이다.

($\Leftarrow$) : 필요조건이 성립한다고 가정하고 $d|p$라 하자. 그러면 적당한 $t \in \mathbb{Z}$가 존재하여 $p=dt$이다. 가정에 의하여 $(d,p)=(d,dt)=1$ 또는 $dt|d$이다. 그러므로 $d=\pm 1$ 또는 $t=\pm 1$이다. $t=\pm 1$이면 $p=dt$이므로

$p=\pm d$이다. 따라서 p의 약수는 ± 1 또는 $\pm p$뿐이다. 따라서 p는 소수이다. ■

예제 | 1.3.2 $3^s 5^t$의 모든 약수들을 열거하라. 여기서 $s,t \in \mathbb{Z}$이고 $s,t \ge 00$.

풀이 $1, 3, 3^2, \cdots, 3^s$;

$5, 3 \cdot 5, 3^2 \cdot 5, \cdots, 3^s \cdot 5$;

$5^2, 3 \cdot 5^2, 3^2 \cdot 5^2, \cdots, 3^s \cdot 5^2$;

$5^3, 3 \cdot 5^3, 3^2 \cdot 5^3, \cdots, 3^s \cdot 5^3$;

$\cdots \quad \cdots \quad \cdots \quad \cdots$

$5^t, 3 \cdot 5^t, 3^2 \cdot 5^t, \cdots, 3^s \cdot 5^t$. ■

예제 | 1.3.3 $c^2=ab$이고 $(a,b)=1$이면, a와 b는 완전제곱수(perfect square)이다. 이를 증명하라.

풀이 $c=p_1 p_2 \cdots p_r$이라 하자. 여기서 p_i는 $p_1 \le p_2 \le \cdots \le p_r$인 양의 소수이다. 그러면

$$ab = c^2 = p_1 p_1 p_2 p_2 \cdots p_r p_r \qquad (*)$$

이다. 따라서 $p_1|ab$이다. 즉, $p_1|a$ 또는 $p_1|b$이다. 여기서 $p_1|a$라 하자.

$(a,b)=1$ 이므로, $p_1 \nmid b$이다. 그러므로 $p_1^2 | a$이어야 한다. 따라서 $i \neq j$에 대하여 $p_i^2 | a$ 또는 $p_j^2 | b$임을 알 수 있다. 이제 (*)에서 $p_i^2 | a$ 또는 $p_j^2 | b$인 것들을 분류하여 다음과 같이 쓸 수 있다.

$$a = p_1 p_1 p_2 p_2 \cdots p_i p_i = (p_1 p_2 \cdots p_i)^2$$

이고

$$b = p_{i+1} p_{i+1} \cdots p_r p_r = (p_{i+1} \cdots p_r)^2.$$

따라서 a와 b는 완전제곱수이다. ■