학부 대수학을 위한 정수론

네냐플(Nenyaffle)

2018. 03. 31

유의사항

작성자 : 네냐플(Nenyaffle)

1. 이 책은 학부수준의 대수학 과목(선형대수, 현대대수, 체론 등)을 공부하기 위해 필요하다고 생각하는 정수론 내용을 소개하는 책입니다. 제가 학부수준의 선형대수, 현대대수, 체론을 공부할 때 알고 있었다면 더 편하게 공부했을거라고 생각하는 정수론 내용입니다. 그래서 내용이 부족하다고 느낄수도 있고 반대로 너무 과하다고 느낄수도 있습니다.

2. 오류나 오타가 없는지 미리 검토했지만 혹시 발견된다면 댓글이나 쪽지, 이메일로 제보해주시면 감사하겠습니다. 제 이메일 주소는 mindo1103@naver.com입니다.

목차

작성자 : 네냐플(Nenyaffle)

1. 기초 정수론

1.1 나눗셈 정리

작성자 : 네냐플(Nenyaffle)

이 책에서는 자연수 전체의 집합을 $\mathbb{N}$, 정수 전체의 집합을 $\mathbb{Z}$, 유리수 전체의 집합을 $\mathbb{Q}$, 실수 전체의 집합을 $\mathbb{R}$, 복소수 전체의 집합을 $\mathbb{C}$ 라고 쓰겠습니다.

1장에서 다루는 내용중엔 초등학교나 중학교에서 배운것도 많을겁니다. 차이점이라면 그때 배운것보다 더 엄밀하게 배우는 것 뿐입니다.

먼저 다음 정리는 증명없이 받아들이도록 하겠습니다. 정렬원리는 공집합이 아닌 자연수 집합의 부분집합은 가장 작은 원소가 존재한다는 정리인데 조금만 생각해보면 당연하다고 느낄수 있습니다.

Theorem 1.1.1 정렬원리(Well-Ordering Principle)
집합 S 가 공집합이 아니고 $\mathbb{N}$의 부분집합이면 S 는 가장 작은 원소를 갖는다.

$\mathbb{N}$은 1을 가장 작은 원소로 가지고 있으므로 공집합이 아닌 $\mathbb{N}$의 부분집합 S 는 1보다 크거나 같은 원소만 포함하고 있어야 하고 자연수는 크기 순서대로 놓을수 있으므로 S 는 가장 작은 원소를 갖는다고 생각하면 됩니다.

당연해보이는 사실이 정리가 된 이유는 자연수를 수학적으로 구성할 때 정렬원리를 공리로 채택하지 않아서 그렇습니다. 자연수를 구성할때는 보통 다음에 소개할 수학적 귀납법을 공리로 채택하고 수학적 귀납법을 가지고 정렬원리를 증명합니다.

그런데 수학적 귀납법을 가지고 정렬원리를 증명하는 과정은 비직관적이라서 자연수를 수학적으로 엄밀하게 구성하는 과정을 소개하는 책이 아니면 정렬원리를 증명없이 받아들이고 수학적 귀납법을 정렬원리를 가지고 증명하는 편입니다. 이 책에서도 그렇게 하겠습니다.

Theorem 1.1.2 수학적 귀납법(Mathematical Induction)
자연수 n에 따라 참, 거짓이 달라지는 명제를 $p(n)$이라고 하고 집합 S 를

$$S=\{n\in\mathbb{N} : p(n)\text{은 참이다.}\}$$

라고 하자. 이때 집합 S 가 다음 두 조건을 만족하면 $S=\mathbb{N}$ 이다.

(a). $1\in S$ 이다.
(b). 모든 자연수 n에 대하여 $n\in S$ 이면 $n+1\in S$ 이다.

(증명)
집합 T 를 $T=\{n\in\mathbb{N} : p(n)\text{은 거짓이다.}\}$ 라고 하자. 그리고 결론을 부정해서 $S\neq\mathbb{N}$ 이라고 가정하자. 그러면 T 는 공집합이 아니고 자연수 집합의 부분집합이므로 정렬원리에 의하면 가장 작은 원소를 갖는다. 그것을 a라고 하면 $a\notin S$ 이다.

(a)에 의하면 $a \neq 1$ 이다. 따라서 $a \geq 2$ 이므로 $a-1$ 은 자연수이고 a가 T 의 가장 작은 원소이므로 $a-1 \in S$ 를 만족한다. 그러므로 (b)에 의해 $a = (a-1)+1 \in S$ 를 만족하는데 이것은 모순이다. 따라서 $S = \mathbb{N}$ 이다. ■

같은 방법으로 강한 귀납법이라고 부르는 다음 정리도 증명할수 있습니다.

Theorem 1.1.3 강한 귀납법(Strong Induction)
자연수 n에 따라 참, 거짓이 달라지는 명제를 $p(n)$이라고 하고 집합 S 를

$$S = \{n \in \mathbb{N} : p(n)\text{은 참이다.}\}$$

라고 하자. 이때 집합 S 가 다음 두 조건을 만족하면 $S = \mathbb{N}$ 이다.

(a). $1 \in S$ 이다.
(b). 모든 자연수 n에 대하여 $1,2,...,n \in S$ 이면 $n+1 \in S$ 이다.

(증명)
집합 T 를 $T = \{n \in \mathbb{N} : p(n)\text{은 거짓이다.}\}$ 라고 하자. 그리고 결론을 부정해서 $S \neq \mathbb{N}$ 이라고 가정하자. 그러면 T 는 공집합이 아니고 자연수 집합의 부분집합이므로 정렬원리에 의하면 가장 작은 원소를 갖는다. 그것을 a라고 하면 $a \notin S$ 이다.

(a)에 의하면 $a \neq 1$ 이다. 따라서 $a \geq 2$ 이므로 $a-1$ 은 자연수이고 a가 T 의 가장 작은 원소이므로 $1,2,...,a-1 \in S$ 를 만족한다. 그러므로 (b)에 의해 $a = (a-1)+1 \in S$ 를 만족하는데 이것은 모순이다. 따라서 $S = \mathbb{N}$ 이다. ■

강한 귀납법은 n번째 단계만 참이라고 가정하면 증명하기 힘들 때 유용하게 쓰입니다.
수학적 귀납법과 강한 귀납법을 사용하는 문제를 하나씩 보여드리겠습니다.

Problem 1.1.1 자연수 n과 $0 \leq k \leq n$ 을 만족하는 정수 k에 대하여
이항계수(Binomial Coefficient)를 다음과 같이 정의한다.

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

$a, b \in \mathbb{C}$ 가 임의로 주어져있다고 하자. 그러면 모든 자연수 n에 대하여

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

가 성립함을 증명하시오. 이것을 **이항정리(Binomial Theorem)**라고 부른다.

(증명)
집합 S 를 $S = \left\{ n \in \mathbb{N} : (a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \right\}$ 라고 하자.

그러면 $(a+b)^1 = \sum_{k=0}^{1} \binom{1}{k} a^k b^{1-k} = \binom{1}{0} b + \binom{1}{1} a = a+b$ 가 성립함은 명백하므로

$1 \in S$ 이다. 이제 임의의 자연수 n을 하나 택하고 $n \in S$ 라고 가정하자.

$(a+b)^n = \sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k}$ 이므로 다음 등식을 얻는다.

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)(a+b)^n \\
&= (a+b)\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k} \\
&= \sum_{k=0}^{n}\binom{n}{k}a^{k+1}b^{n-k} + \sum_{k=0}^{n}\binom{n}{k}a^k b^{n+1-k} \\
&= \sum_{k=1}^{n+1}\binom{n}{k-1}a^k b^{n+1-k} + \sum_{k=0}^{n}\binom{n}{k}a^k b^{n+1-k} \\
&= a^{n+1} + b^{n+1} + \sum_{k=1}^{n}\left(\binom{n}{k-1} + \binom{n}{k}\right)a^k b^{n+1-k} \\
&= a^{n+1} + b^{n+1} + \sum_{k=1}^{n}\left(\frac{n!}{(k-1)!(n+1-k)!} + \frac{n!}{k!(n-k)!}\right)a^k b^{n+1-k} \\
&= a^{n+1} + b^{n+1} + \sum_{k=1}^{n}\frac{(n+1)!}{k!(n+1-k)!}a^k b^{n+1-k} \\
&= \sum_{k=0}^{n+1}\binom{n+1}{k}a^k b^{n+1-k}
\end{aligned}$$

따라서 $n+1 \in S$ 이므로 수학적 귀납법에 의하면 $S = \mathbb{N}$ 이다.

즉, 모든 자연수 n에 대하여 $(a+b)^n = \sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k}$ 가 성립한다. ■

Problem 1.1.2 양항수열 $\{a_n\}$은 모든 자연수 n에 대하여 다음을 만족한다.

$$\sum_{k=1}^{n} a_k^3 = \left(\sum_{k=1}^{n} a_k\right)^2 \tag{1}$$

그러면 모든 자연수 n에 대하여 $a_n = n$ 임을 증명하시오.

(증명)

집합 S 를 $S = \{n \in \mathbb{N} : a_n = n\}$ 라고 하자. (1)에 $n = 1$ 을 대입하면

$a_1^3 = a_1^2$ 인데 $a_1 > 0$ 이므로 $a_1 = 1$ 이다. 따라서 $1 \in S$ 이다.

이제 임의의 자연수 n을 하나 택하고 $1, 2, ..., n \in S$ 라고 가정하자.

그러면 $a_1 = 1, a_2 = 2, \ ..., a_n = n$ 이므로 (1)에 의하면 다음 등식을 얻는다.

$$\begin{aligned}
\sum_{k=1}^{n+1} a_k^3 &= a_{n+1}^3 + \sum_{k=1}^{n} a_k^3 \\
&= a_{n+1}^3 + \left(\sum_{k=1}^{n} a_k\right)^2
\end{aligned} \tag{2}$$

$$\begin{aligned}\left(\sum_{k=1}^{n+1}a_k\right)^2 &= \left(a_{n+1}+\sum_{k=1}^{n}a_k\right)^2 \\ &= a_{n+1}^2+2a_{n+1}\sum_{k=1}^{n}a_k+\left(\sum_{k=1}^{n}a_k\right)^2 \\ &= a_{n+1}^2+2a_{n+1}\sum_{k=1}^{n}k+\left(\sum_{k=1}^{n}a_k\right)^2 \\ &= a_{n+1}^2+n(n+1)a_{n+1}+\left(\sum_{k=1}^{n}a_k\right)^2\end{aligned} \tag{3}$$

(1)에서 $\sum_{k=1}^{n+1}a_k^3=\left(\sum_{k=1}^{n+1}a_k\right)^2$ 이므로 (2), (3)에서 $a_{n+1}^3=a_{n+1}^2+n(n+1)a_{n+1}$ 이고 $a_{n+1}>0$ 이므로 방정식을 풀면 $a_{n+1}=n+1$ 을 얻는다.

따라서 $n+1\in S$ 이므로 강한 귀납법에 의하면 $S=\mathbb{N}$ 이다.
즉, 모든 자연수 n에 대하여 $a_n=n$ 이다. ■

기초 해석학에서는 아르키메데스 원리를 실수의 완비성을 이용해서 증명합니다.
그런데 정수론에서는 완비성 개념을 다루지 않기 때문에 자연수 범위일땐 아르키메데스 정리를 다음과 같이 정렬원리를 이용해서 증명합니다.

Theorem 1.1.4 아르키메데스 원리(Archimedean Property)
임의의 자연수 a,b 에 대하여 $na\geq b$ 를 만족하는 자연수 n이 존재한다.

(증명)
임의의 자연수 a,b 를 택하자. 그리고 결론을 부정해서 모든 자연수 n에 대하여 $na<b$ 가 성립한다고 가정하자. 그러면 $b-na$ 는 자연수이다.

집합 S 를 $S=\{b-na\in\mathbb{N}:n\in\mathbb{N}\}$ 라고 하자. 그러면 S 는 공집합이 아니고 자연수 집합의 부분집합이므로 정렬원리에 의하면 가장 작은 원소를 갖고 그 원소는 적당한 자연수 m에 대하여 $b-ma$ 라고 표현이 가능하다. 그리고 다음을 얻는다.

$$b-(m+1)a=(b-ma)-a<b-ma \tag{4}$$

$m+1$ 은 자연수이므로 $b-(m+1)a\in S$ 인데 (4)에 의하면 이것은 $b-ma$ 가 S 의 가장 작은 원소라는 것에 모순이다. 따라서 $na\geq b$ 를 만족하는 자연수 n이 존재한다. ■

이제 1.1절에서 가장 중요한 나눗셈 정리를 소개하려고 합니다. 사실 이것은 초등학생때 나눗셈의 검산식이라는 이름으로 배운 것을 수학적으로 엄밀하게 표현한것에 불과합니다.

15를 4로 나누면 몫이 3이고 나머지가 3입니다. 초등학생때 이 나눗셈이 잘 되었는지 검산하기 위해 검산식 $15=4\times3+3$ 으로 확인하라고 가르쳐줍니다.

여기서 소개하는 나눗셈 정리는 간단합니다. 15를 4로 나눈 것을 예로 들면
15를 $4\times3+3$ 이렇게 몫 3과 나머지 3을 이용해서 나타낼수 있다는 정리입니다.
물론 나머지는 나누는 수의 절댓값보다 작아야 합니다.

절댓값이 나오는 이유는 나머지는 양수여야 하고 나눗셈에서는 음수로 나누는것도 정의하기 때문인데 15를 -4로 나누면 몫은 -3이고 나머지는 3, 그리고 $3<|-4|=4$ 입니다.

나눗셈 정리를 증명하려면 다음 2개의 보조정리가 필요합니다.

Lemma 1.1.1 $A=\mathbb{N}\cup\{0\}$일 때 집합 S 가 공집합이 아니고 A의 부분집합이면 S 는 가장 작은 원소를 갖는다.

(증명)
공집합이 아닌 A의 임의의 부분집합 S 를 하나 택하자. 그러면 $0\in S$ 또는 $0\notin S$ 이다.

$0\in S$ 이면 S 는 A의 부분집합이고 A의 가장 작은 원소가 0이므로 0은 S 의 가장 작은 원소이다. $0\notin S$ 이면 S 는 공집합이 아닌 $\mathbb{N}$의 부분집합이므로 정렬원리에 의하면 S 는 가장 작은 원소를 갖는다. 따라서 어느 경우든 S 는 가장 작은 원소를 갖는다. ■

다음 보조정리는 지금 다루는 대상이 정수이기 때문에 의미가 있습니다. 실수는 0이 아니면 곱셈에 대한 역원이 존재하기 때문에 다음 보조정리에 있는 성질은 양변에 곱셈에 대한 역원을 곱하는 행위로 간단하게 보일수 있지만 정수는 곱셈에 대한 역원이 존재하는 원소가 $-1,1$ 2개밖에 없어서 다음 보조정리를 그렇게 증명할수 없습니다.

Lemma 1.1.2 임의의 $a,b,c\in\mathbb{Z}$ 에 대하여 다음이 성립한다.
(a). $ab=0$ 이면 $a=0$ 또는 $b=0$ 이다.
(b). $a\neq0$ 이고 $ab=ac$ 이면 $b=c$ 이다.
(c). $a\neq0$ 이고 $ab<ac$ 이면 $a>0$ 일 때 $b<c$ 이고 $a<0$ 일 때 $b>c$ 이다.

(증명)
(a). 대우명제를 증명하자. 즉, $a\neq0$ 이고 $b\neq0$ 이면 $ab\neq0$ 임을 보이자.
a,b가 모두 0이 아니면 $|a|,|b|$는 자연수이므로 $|ab|=|a||b|\geq1$ 이다.
따라서 $ab\neq0$ 이다. $ab=0$ 이면 $0=|ab|\geq1$ 이므로 모순이다.

그러므로 $ab=0$ 이면 $a=0$ 또는 $b=0$ 이다. ■

(b). 조건에 의하면 $a(b-c)=0$ 이고 $a\neq0$ 이므로 (a)에 의하면 $b=c$ 이다. ■

(c). case1) $a>0$
결론을 부정해서 $b\geq c$ 라고 가정하자. 그러면 $a>0$ 이므로 $ab\geq ac$ 인데
이것은 조건에 모순이다. 따라서 $b<c$ 이다.

case2) $a < 0$

결론을 부정해서 $b \leq c$ 라고 가정하자. 그러면 $a < 0$ 이므로 $ab \geq ac$ 인데 이것은 조건에 모순이다. 따라서 $b > c$ 이다. ■

이제 나눗셈 정리를 증명하겠습니다. 나눗셈 정리를 수학적으로 표현하면 다음과 같습니다.

Theorem 1.1.5 나눗셈 정리(Division Algorithm)

정수 a와 $b \neq 0$ 을 만족하는 정수 b가 임의로 주어져있다고 하자.

그러면 다음 등식을 만족하는 두 정수 q, r이 유일하게 존재한다.

$$a = bq + r \ (0 \leq r < |b|) \tag{5}$$

이때 (5)에서 q를 a를 b로 나눈 **몫(Quotient)**이라고 정의하고 r을 a를 b로 나눈 **나머지(Remainder)**라고 정의한다.

(증명)

정수 a와 $b \neq 0$ 을 만족하는 정수 b를 임의로 택하자.

case1) b는 자연수

이 경우 $|b| = b$ 이다. 집합 S 를 다음과 같이 정의하자.

$$S = \{a - nb \in \mathbb{Z} : n\text{은 } a - nb \geq 0\text{을 만족하는 정수}\}$$

이때 S 가 $\mathbb{N} \cup \{0\}$의 부분집합임은 명백하다.

한편 b는 자연수이고 $a + |a| \geq 0$ 이므로 다음 부등식이 성립한다.

$$a - (-|a|)b = a + |a|b \geq a + |a| \geq 0$$

따라서 $a - nb \geq 0$ 을 만족하는 정수 n은 $n = -|a|$로 존재하므로 S 는 공집합이 아니다. 그러므로 Lemma 1.1.1에 의하면 S 는 가장 작은 원소를 갖는다. S 의 가장 작은 원소를 r이라고 하면 적당한 정수 q가 존재해서 $r = a - bq$ 를 만족하고 $r \geq 0$ 이다.

이제 $r < b$ 임을 보이자. 결론을 부정해서 $r \geq b$ 라고 가정하면

$$r - b = (a - qb) - b = a - (q+1)b \geq 0$$

이므로 $a - (q+1)b \in S$ 인데 $a - (q+1)b = r - b < r$ 이므로 이것은 r이 S 의 가장 작은 원소라는 것에 모순이다. 따라서 $r < b$ 이다.

$a = bq + r \ (0 \leq r < |b|)$ 를 만족하는 정수 q, r의 존재성이 증명되었다.

이제 유일성을 증명하자.

정수 q_1, q_2 와 $0 \leq r_1 < b, 0 \leq r_2 < b$ 를 만족하는 정수 r_1, r_2 에 대하여 $a = bq_1 + r_1 = bq_2 + r_2$ 를 만족한다고 하자. 그러면 $bq_1 + r_1 = bq_2 + r_2$ 에서 $r_2 - r_1 = b(q_1 - q_2)$ 이고 이때 $-b < r_2 - r_1 < b$ 이다.

b는 자연수이므로 Lemma 1.1.2에 의하면 $-1 < q_1 - q_2 < 1$ 을 얻는다.

$q_1 - q_2$ 는 정수이므로 위 부등식을 만족하면 $q_1 = q_2$ 이고 따라서 $r_1 = r_2$ 이다.
그러므로 $a = bq + r\ (0 \le r < |b|)$ 를 만족하는 정수 q, r은 유일하게 존재한다.

case2) b가 음의 정수
이 경우 $|b| = -b$ 이고 $-b$는 자연수이므로 case1)에 의하면
$a = -bq' + r\ (0 \le r < -b)$ 를 만족하는 정수 q', r은 유일하게 존재한다.

$q = -q'$ 라고 하면 q는 정수이고 $a = bq + r\ (0 \le r < -b)$ 이므로
$a = bq + r\ (0 \le r < |b|)$ 를 만족하는 정수 q, r의 존재성이 증명되었다.

이제 유일성을 증명하자. 정수 q_1, q_2 와 $0 \le r_1 < -b, 0 \le r_2 < -b$ 를 만족하는 정수 r_1, r_2 에 대하여 $a = bq_1 + r_1 = bq_2 + r_2$ 를 만족한다고 하자.

그러면 $bq_1 + r_1 = bq_2 + r_2$ 에서 $r_2 - r_1 = b(q_1 - q_2)$ 이고 b는 음의 정수이므로
$b < r_2 - r_1 < -b$ 이다. 따라서 Lemma 1.1.2에 의하면 $-1 < q_1 - q_2 < 1$ 을 얻는다.

$q_1 - q_2$ 는 정수이므로 위 부등식을 만족하면 $q_1 = q_2$ 이고 따라서 $r_1 = r_2$ 이다.
그러므로 $a = bq + r\ (0 \le r < |b|)$ 를 만족하는 정수 q, r은 유일하게 존재한다. ■

나눗셈 정리를 이용하면 모든 정수를 분류할수 있습니다.
사실 다음 따름정리는 나눗셈 정리를 기호로 나타낸것에 불과합니다.

Corollary 1.1.1 $a, b \in \mathbb{Z}$ 가 임의로 주어졌을 때 집합 $a\mathbb{Z} + b$ 를 다음과 같이 정의하자.

$$a\mathbb{Z} + b = \{an + b : n \in \mathbb{Z}\}$$

그러면 $m \neq 0$ 인 모든 정수 m에 대하여 다음이 성립한다.

(a). $\mathbb{Z} = \bigcup_{r=0}^{|m|-1} (m\mathbb{Z} + r) = m\mathbb{Z} \cup (m\mathbb{Z} + 1) \cup \cdots \cup (m\mathbb{Z} + |m| - 1)$ 이다.

(b). $0 \le r_1 < |m|, 0 \le r_2 < |m|$ 을 만족하는 임의의 정수 r_1, r_2 에 대하여
$r_1 \neq r_2$ 이면 $(m\mathbb{Z} + r_1) \cap (m\mathbb{Z} + r_2) = \varnothing$ 이다.

(증명)
(a). $\bigcup_{r=0}^{|m|-1} (m\mathbb{Z} + r) \subset \mathbb{Z}$ 는 명백하므로 $\mathbb{Z} \subset \bigcup_{r=0}^{|m|-1} (m\mathbb{Z} + r)$ 를 증명하면 충분하다.
임의의 $n \in \mathbb{Z}$ 을 택하자. 그러면 나눗셈 정리에 의해 $n = mq + r\ (0 \le r < |m|)$ 을 만족하는 정수 q, r이 존재하고 $mq + r \in m\mathbb{Z} + r$ 이므로 $n \in \bigcup_{r=0}^{|m|-1} (m\mathbb{Z} + r)$ 이다.

따라서 $\mathbb{Z} \subset \bigcup_{r=0}^{|m|-1} (m\mathbb{Z} + r)$ 이므로 $\mathbb{Z} = \bigcup_{r=0}^{|m|-1} (m\mathbb{Z} + r)$ 를 얻는다. ■

(b). 결론을 부정해서 $0 \le r_1 < |m|,\ 0 \le r_2 < |m|$ 과 $r_1 \neq r_2$ 를 만족하는 적당한 r_1, r_2 가 존재해서 $(m\mathbb{Z}+r_1)\cap(m\mathbb{Z}+r_2) \neq \varnothing$ 이라고 가정하자.

$x \in (m\mathbb{Z}+r_1)\cap(m\mathbb{Z}+r_2)$ 를 임의로 하나 택하면 적당한 정수 q_1, q_2가 존재해서 $x = mq_1 + r_1 = mq_2 + r_2$ 를 만족하는데 이것은 x를 m으로 나누었을 때 몫이 q_1, q_2 이고 나머지가 r_1, r_2 임을 의미한다.

나눗셈 정리에 의하면 $q_1 = q_2,\ r_1 = r_2$ 인데 이것은 모순이므로 (b)가 증명된다. ■

Corollary 1.1.1은 모든 정수가 $m \neq 0$ 인 임의의 정수 m에 대하여

$$mk, mk+1, mk+2, \ ..., mk+(|m|-1)\ (k \in \mathbb{Z})$$

위 $|m|$개중 하나의 형태로만 표현된다는 것을 의미합니다. 이것은 어떤 명제가 모든 정수에 대하여 참이라는 것을 증명할 때 유용하게 쓰입니다.

다음에 소개할 따름정리도 대학입학 전에 한번쯤은 생각해봤을 내용입니다.

16을 5로 나누면 몫은 3이고 나머지는 1이므로 $16 = 5\times 3 + 1$ 인데 여기서 5×3 은 3으로 나누어 떨어지므로 16을 3으로 나눈 나머지는 16의 나머지 1을 3으로 나눈 나머지 1과 같습니다. 이것을 수학적으로 일반화하려고 합니다.

일반화하기 전에 기호를 하나 소개하겠습니다. 집합 $A \subset \mathbb{C}$ 에 대하여 A의 원소를 계수와 상수항으로 갖는 모든 1변수 다항식의 집합을 앞으로 $A[x]$라고 쓰겠습니다. 예를 들면 $\mathbb{Z}[x]$는 계수와 상수항이 정수인 모든 1변수 다항식의 집합입니다.

Corollary 1.1.2 $a \in \mathbb{Z}$ 와 $b \neq 0$ 인 $b \in \mathbb{Z}$, 그리고 $f(x) \in \mathbb{Z}[x]$가 임의로 주어져있다고 하자. 이때 적당한 정수 q, r 이 존재해서 $a = bq + r$ 를 만족하면 $f(a)$를 b로 나눈 나머지는 $f(r)$을 b로 나눈 나머지와 같다.

(증명)

$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ 라고 하자. 이때 n은 음이 아닌 정수이고 $a_0, a_1, ..., a_n \in \mathbb{Z}$ 이다.

이항정리에 의하면 m이 자연수일 때 적당한 정수 k에 대하여 다음을 만족한다.

$$\begin{aligned} a^m &= (bq+r)^m \\ &= \sum_{i=0}^{m} \binom{m}{i} (bq)^i r^{m-i} \\ &= r^m + \binom{m}{1}(bq)^1 r^{m-1} + \cdots + \binom{m}{m}(bq)^m \\ &= bk + r^m \end{aligned}$$

그러므로 $f(a)$는 적당한 정수 k'에 대하여 $f(a) = bk' + f(r)$ 형태로 표현된다.

$f(r)$을 b로 나눈 나머지를 r_1 이라고 하자. 그러면 $0 \le r_1 < |b|$ 이고 나눗셈 정리에 의해 적당한 정수 q가 존재해서 $f(r)= bq + r_1$ 을 만족한다.

따라서 $f(a)= b(k'+q)+r_1$ 이고 $0 \le r_1 < |b|$ 이므로 나눗셈 정리에 의하면 $f(a)$를 b로 나눈 나머지는 r_1 이고 이것은 $f(r)$을 b로 나눈 나머지와 같다. ■

Corollary 1.1.3 a는 정수이고 b는 0이 아닌 정수일 때 a를 b로 나눈 나머지를 $R_b(a)$ 라고 정의하자. 그러면 모든 $a, b \in \mathbb{Z}$ 와 $c \neq 0$ 인 모든 $c \in \mathbb{Z}$ 에 대하여 다음 등식이 성립한다.

(a). $R_c\big(R_c(a)\big)= R_c(a)$
(b). $R_c(a+b)= R_c\big(R_c(a)+ R_c(b)\big)$
(c). $R_c(a-b)= R_c\big(R_c(a)- R_c(b)\big)$
(d). $R_c(ab)= R_c\big(R_c(a)R_c(b)\big)$

(증명)
Corollary 1.1.2에서 다항식을 $f(x)= x$ 로 택하면 a를 b로 나눈 나머지는 r을 b로 나눈 나머지와 같다는 결론을 얻을수 있다. (6)

(a). 나눗셈 정리에 의하면 적당한 정수 q가 존재해서 다음을 만족한다.

$$a = cq + R_c(a) \ \big(0 \le R_c(a) < |b|\big)$$

따라서 (6)에 의하면 $R_c\big(R_c(a)\big)= R_c(a)$ 가 성립한다. ■

(b) 나눗셈 정리에 의하면 적당한 정수 q_1, q_2 가 존재해서 다음을 만족한다.

$$a = cq_1 + R_c(a) \ \big(0 \le R_c(a) < |c|\big)$$
$$b = cq_2 + R_c(b) \ \big(0 \le R_c(b) < |c|\big)$$

따라서 $a+b = c\big(q_1+q_2\big)+ R_c(a)+ R_c(b)$ 이므로 (6)에 의하면
$R_c(a+b)= R_c\big(R_c(a)+ R_c(b)\big)$ 가 성립한다. ■

(c) 나눗셈 정리에 의하면 적당한 정수 q_1, q_2 가 존재해서 다음을 만족한다.

$$a = cq_1 + R_c(a) \ \big(0 \le R_c(a) < |c|\big)$$
$$b = cq_2 + R_c(b) \ \big(0 \le R_c(b) < |c|\big)$$

따라서 $a-b = c\big(q_1-q_2\big)+ R_c(a)- R_c(b)$ 이므로 (6)에 의하면
$R_c(a-b)= R_c\big(R_c(a)- R_c(b)\big)$ 가 성립한다. ■

(d) 나눗셈 정리에 의하면 적당한 정수 q_1, q_2 가 존재해서 다음을 만족한다.

$$a = cq_1 + R_c(a) \ \big(0 \le R_c(a) < |c|\big)$$
$$b = cq_2 + R_c(b) \ \big(0 \le R_c(b) < |c|\big)$$

따라서 다음 등식을 얻는다.

$$\begin{aligned} ab &= \big(cq_1 + R_c(a)\big)\big(cq_2 + R_c(b)\big) \\ &= c^2 q_1 q_2 + cq_1 R_c(b) + cq_2 R_c(a) + R_c(a)R_c(b) \\ &= c\big(cq_1 q_2 + q_1 R_c(b) + q_2 R_c(a)\big) + R_c(a)R_c(b) \end{aligned}$$

그러므로 (6)에 의하면 $R_c(ab) = R_c\big(R_c(a)R_c(b)\big)$ 가 성립한다. ■

Problem 1.1.3 모든 완전제곱수는 4로 나눈 나머지가 0 또는 1임을 보이고 이것을 이용해서 모든 자리의 숫자가 1이고 자리수가 2 이상인 모든 자연수는 완전제곱수가 될수 없음을 증명하시오.

(증명)

임의의 정수 n에 대하여 n^2을 4로 나눈 나머지가 0 또는 1임을 보이자. (7)

Corollary 1.1.2에 의하면 n^2에 $n = 0, 1, 2, 3$ 만 대입해서 확인하면 충분하다.

$n = 0$ 이면 $n^2 = 0$ 이므로 4로 나눈 나머지는 0

$n = 1$ 이면 $n^2 = 1$ 이므로 4로 나눈 나머지는 1

$n = 2$ 이면 $n^2 = 4$ 이므로 4로 나눈 나머지는 0

$n = 3$ 이면 $n^2 = 9$ 이므로 4로 나눈 나머지는 1

따라서 n^2을 4로 나눈 나머지는 0 또는 1이다. 이제 결론을 부정해서 $m \geq 2$ 인 적당한 자연수 m에 대하여 모든 자리의 숫자가 1인 m자리 자연수 $111\cdots111$ 가 완전제곱수라고 가정하자.

case1) $m = 2$

11은 4로 나누면 나머지가 3이므로 (6)에 의하면 완전제곱수가 될수 없다.

case2) $m \geq 3$

$$\begin{aligned} 111\cdots111 &= 10^{m-1} + 10^{m-2} + \cdots + 10^2 + 10 + 1 \\ &= 10^2 \times \big(10^{m-3} + \cdots + 10 + 1\big) + 8 + 3 \\ &= 4 \times 25 \times \big(10^{m-3} + \cdots + 10 + 1\big) + 4 \times 2 + 3 \\ &= 4 \times \big(25 \times \big(10^{m-3} + \cdots + 10 + 1\big) + 2\big) + 3 \end{aligned}$$

이므로 $111\cdots111$ 을 4로 나누면 나머지가 3이다. 따라서 (7)에 의하면 완전제곱수가 될수 없다. 어느 경우든 모순이 발생하므로 주어진 자연수는 완전제곱수가 될수 없다. ■

Problem 1.1.4 방정식 $x^2 - 3y^2 = 11$ 을 만족하는 정수 x, y 는 존재하지 않는다는 것을 증명하시오.

(증명)

먼저 모든 완전제곱수는 3으로 나눈 나머지가 0 또는 1임을 보이자. (8)

이것도 Problem 1.1.3에서 이야기한대로 $0, 1, 2$ 에서만 확인하면 충분하다.

$0^2 = 0$ 을 3으로 나눈 나머지는 0
$1^2 = 1$ 을 3으로 나눈 나머지는 1
$2^2 = 4$ 를 3으로 나눈 나머지는 1

따라서 모든 완전제곱수는 3으로 나눈 나머지가 0 또는 1이다.

이제 결론을 부정해서 적당한 정수 x, y 가 존재해서 $x^2 - 3y^2 = 11$ 을 만족한다고 가정하자. 그러면 $x^2 = 3y^2 + 11$ 이므로 x^2을 3으로 나눈 나머지는 11을 3으로 나눈 나머지 2와 같은데 이것은 (8)에 모순이다.

그러므로 $x^2 - 3y^2 = 11$ 을 만족하는 정수 x, y 는 존재하지 않는다. ■

1.2 약수와 배수

작성자 : 네냐플(Nenyaffle)

1.2절에서는 최대공약수와 최소공배수를 정의하고 그들의 성질을 소개하는게 목표입니다.

1.2절의 내용도 대부분 대학 입학 전에 이미 배운 내용입니다. 수학적으로 엄밀하게 다시 정의하고 설명하는 것 뿐입니다.

Definition 1.2.1 약수(Divisor), 배수(Multiple)
$a \neq 0$ 인 정수 a와 정수 b가 임의로 주어져있다고 하자. 이때 적당한 정수 c가 존재해서 $b = ac$ 를 만족하면 a는 b의 **약수(Divisor)**, b는 a의 **배수(Multiple)**라고 정의한다.

그리고 적당한 정수 c가 존재해서 $b = ac$ 를 만족하는 것을 기호로 $a \mid b$ 라고 나타내고 $a \mid b$ 를 'a는 b를 나눈다' 또는 'b는 a에 의해 나누어진다' 라고 표현한다.

$b = ac$ 를 만족하는 정수 c가 존재하지 않으면 기호로 $a \nmid b$ 라고 나타내고 $a \nmid b$ 를 'a는 b를 나누지 않는다' 또는 'b는 a에 의해 나누어지지 않는다' 라고 표현한다.

$12 = 3 \times 4$ 이므로 3과 4는 12의 약수입니다. 그리고 12는 3과 4의 배수입니다.
그리고 $12 = 2 \times 6$ 이기도 하므로 $2, 6$은 12의 약수이고 12는 $2, 6$의 배수입니다.
기호로는 $3 \mid 12,\ 4 \mid 12,\ 2 \mid 12, 6 \mid 12$ 라고 나타내고 이때 $2, 3, 4, 6$은 12를 나눈다고 표현합니다. 마찬가지로 12는 $2, 3, 4, 6$에 의해 나누어진다고 표현합니다.

$7 = 2k$ 를 만족하는 정수 k는 존재하지 않으므로 $2 \nmid 7$ 입니다.
그러므로 2는 7을 나누지 않고 2는 7의 약수가 아닙니다.

$a \in \mathbb{Z}$ 가 $2 \mid a$ 를 만족하면 a를 **짝수(Even Number)**라고 부르고 $2 \nmid a$ 이면 a를 **홀수(Odd Number)**라고 부릅니다. a가 홀수일 필요충분조건은 a를 2로 나눈 나머지가 1인 것임을 쉽게 알수 있습니다.

나눗셈 정리에 의하면 a가 b의 약수가 될 필요충분조건은 b를 a로 나눈 나머지가 0인 것을 쉽게 알수 있습니다. 초등학교 수학에서는 이런 경우 b는 a로 나누어 떨어진다고 표현하는데 대학수학에서는 a는 b를 나눈다고 표현합니다. 앞으로 나눈다는 표현을 사용하겠습니다.

Theorem 1.2.1 임의의 $a, b, c, d \in \mathbb{Z}$ 에 대하여 다음이 성립한다.
(a). $a \neq 0$ 이면 $a \mid 0,\ 1 \mid a,\ a \mid a$ 이다.
(b). $a \neq 0, c \neq 0$ 일 때 $a \mid b$ 이고 $c \mid d$ 이면 $ac \mid bd$ 이다.
(c). $a \neq 0, c \neq 0$ 일 때 $a \mid b$ 이고 $b \mid c$ 이면 $a \mid c$ 이다.
(d). $a \neq 0$ 일 때 $a \mid b$ 이고 $a \mid c$ 이면 임의의 $x, y \in \mathbb{Z}$ 에 대해 $a \mid bx + cy$ 이다.
(e). $a \neq 0, b \neq 0$ 일 때 $a \mid b$ 이면 $|a| \leq |b|$ 이다.
(f). $a \neq 0, b \neq 0$ 일 때 $a \mid b$ 이고 $b \mid a$ 일 필요충분조건은 $|a| = |b|$ 이다.
(g). $a \neq 0$ 일 때 $a \mid 1$ 일 필요충분조건은 $a = \pm 1$ 이다.

(증명)
(a). $a \neq 0$ 이면 $0 = a \times 0,\ a = a \times 1$ 이므로 정의에 의하면 명백하다. ■

(b). 조건에 의하면 적당한 정수 k_1, k_2 가 존재해서 $b = ak_1,\ d = ck_2$ 를 만족하고
따라서 $bd = ack_1k_2$ 이므로 $ac \mid bd$ 이다. ■

(c). 조건에 의하면 적당한 정수 k_1, k_2 가 존재해서 $b = ak_1,\ c = bk_2$ 를 만족하고
따라서 $c = ak_1k_2$ 이므로 $a \mid c$ 이다. ■

(d). 조건에 의하면 적당한 정수 k_1, k_2 가 존재해서 $b = ak_1,\ c = ak_2$ 를 만족하므로
임의의 $x, y \in \mathbb{Z}$ 에 대해 $bx + cy = a\left(k_1x + k_2y\right)$ 이다. 따라서 $a \mid bx + cy$ 이다. ■

(e). 조건에 의하면 적당한 정수 k가 존재해서 $b = ak$ 를 만족하고 $a \neq 0,\ b \neq 0$ 이므로
$k \neq 0$ 이다. 따라서 $|k|$는 자연수이므로 $|b| = |k||a| \geq |a|$ 이다. ■

(f). $(\Longrightarrow)$ (e)에 의하면 $|a| \leq |b|$와 $|b| \leq |a|$를 동시에 만족하므로 $|a| = |b|$ 이다.

$(\Longleftarrow)$ 조건에 의하면 $a = \pm b$ 인데 $a = b$ 이면 (a)에 의해 참이고 $a = -b$ 이면
$a = b \times (-1),\ b = a \times (-1)$ 이므로 참이다. ■

(g). (f)에 의하면 $a \mid 1$ 일 필요충분조건은 $|a| = 1$ 이고 이것은 $a = \pm 1$ 과 동치이다. ■

Theorem 1.1.2의 (d)는 수학적 귀납법을 이용하면 다음과 같이 확장시킬수 있는데
$k = 1, 2, \ldots, n$ 일 때 모든 k에 대하여 $a \mid b_k$ 이면 모든 $x_1, x_2, \ldots, x_n \in \mathbb{Z}$ 에 대하여
$a \mid b_1x_1 + b_2x_2 + \cdots + b_nx_n$ 가 성립합니다.

Problem 1.2.1 모든 $n \in \mathbb{Z}$ 에 대하여 $4 \nmid n^2 + 2$ 임을 증명하시오.

(증명)
결론을 부정해서 적당한 정수 n에 대하여 $4 \mid n^2 + 2$ 라고 가정하자.
그러면 적당한 정수 m이 존재해서 $n^2 + 2 = 4m$ 을 만족한다.

$n^2 = 4(m-1) + 2$ 이므로 이 경우 n^2을 4로 나눈 나머지는 2인데 Problem 1.1.3에
의하면 완전제곱수를 4로 나눈 나머지는 0 또는 1이므로 이것은 모순이다.

그러므로 모든 $n \in \mathbb{Z}$ 에 대하여 $4 \nmid n^2 + 2$ 이다. ■

Problem 1.2.2 임의의 $n \in \mathbb{Z}$ 에 대하여 $5 \mid n + m^3$ 을 만족하는 $m \in \mathbb{Z}$ 이 존재함을
증명하시오.

(증명)
먼저 세제곱수를 5로 나눈 나머지를 분류하자. Corollary 1.1.2에 의하면 $0, 1, 2, 3, 4$ 의 세제곱만 관찰하면 충분하고 각각의 세제곱은 $0, 1, 8, 27, 64$ 이므로 각각을 5로 나눈 나머지는 $0, 1, 3, 2, 4$ 이다.

따라서 임의의 $k \in \{0,1,2,3,4\}$ 에 대하여 m^3을 5로 나눈 나머지가 k가 되도록 하는 $m \in \mathbb{Z}$ 이 항상 존재한다는 것을 알수 있다. 이 사실을 이용하자.

n을 5로 나눈 나머지를 r이라고 하자. 그러면 적당한 정수 q가 존재해서 $n = 5q + r$ 이고 $r \in \{0,1,2,3,4\}$ 이다. 따라서 $5 - r \in \{0,1,2,3,4\}$ 이다.

이제 m^3을 5로 나눈 나머지가 $5 - r$ 이 되도록 하는 정수 m을 택하자.
그러면 적당한 정수 q'이 존재해서 $m^3 = 5q' + (5 - r)$ 이고 따라서
$n + m^3 = 5(q + q')$ 을 만족한다. 그러므로 $5 \mid n + m^3$ 이다. ■

Problem 1.2.3 임의의 $a \in \mathbb{Z}$ 에 대하여 $a, a+2, a+4$ 셋중 적어도 하나는 3의 배수임을 증명하시오.

(증명)
Corollary 1.1.1에 의하면 임의의 $a \in \mathbb{Z}$ 는 $n \in \mathbb{Z}$ 에 대하여 $a = 3n,\ 3n+1,\ 3n+2$ 셋중 하나로 표현 가능하다.

$a = 3n$ 이면 $3 \mid a$
$a = 3n+1$ 이면 $a + 2 = 3(n+1)$ 이므로 $3 \mid a+2$
$a = 3n+2$ 이면 $a + 4 = 3(n+2)$ 이므로 $3 \mid a+4$

따라서 셋중 적어도 하나는 3의 배수이다. ■

Problem 1.2.4 a가 홀수이면 $4 \mid a^2 + 7$ 임을 증명하시오.

(증명)
임의의 홀수 a는 $n \in \mathbb{Z}$ 에 대하여 $a = 2n + 1$ 로 표현 가능하고 이때
$a^2 + 7 = 4n^2 + 4n + 8 = 4(n^2 + n + 2)$ 이므로 $4 \mid a^2 + 7$ 가 성립한다. ■

$a, b \in \mathbb{Z}$ 가 임의로 주어져있을 때 $c \neq 0$ 인 적당한 $c \in \mathbb{Z}$ 가 존재해서 $c \mid a,\ c \mid b$ 를 만족하면 c를 a, b의 **공약수(Common Divisor)**라고 정의합니다. 단어 그대로 c가 a의 약수이면서 b의 약수이므로 공통된 약수라는 뜻입니다.

마찬가지로 a, b가 모두 0이 아닌 정수일 때 적당한 $c \in \mathbb{Z}$ 가 존재해서 $a \mid c,\ b \mid c$ 를 만족하면 c를 a, b의 **공배수(Common Multiple)**라고 정의합니다. 이것도 단어 그대로 c가 a의 배수이면서 b의 배수이므로 공통된 배수라는 뜻입니다.

공약수와 공배수의 범위를 자연수로 한정시켜보면 $1 \mid a, 1 \mid b$ 이므로 공약수는 항상 존재하고 1이 가장 작은 양의 공약수입니다. 그리고 $ab \neq 0$ 일 때 $a \mid ab, b \mid ab$ 이므로 공배수도 항상 존재합니다.

따라서 다음 두 집합은 공집합이 아닌 자연수 집합의 부분집합입니다.

$$S = \{c \in \mathbb{N} : c \mid a, c \mid b\}$$
$$T = \{c \in \mathbb{N} : a \mid c, b \mid c\}$$

$ab \neq 0$ 일 때 정렬원리에 의하면 T 는 가장 작은 원소를 갖습니다.
따라서 T 의 가장 작은 원소를 **최소공배수(Least Common Multiple)**라고 정의합니다.

그런데 $a = b = 0$ 일 경우 $S = \mathbb{N}$ 이므로 S 는 가장 큰 원소가 존재하지 않습니다.
따라서 S 의 가장 큰 원소를 논하기 위해서는 a, b 둘중 적어도 하나가 0이 아니어야 합니다.

$a \neq 0$ 이라고 가정해도 일반성을 잃지 않습니다. 그리고 이 경우 자연수 c에 대하여 $c \mid a$ 이면 Theorem 1.2.1에 의해 $|c| \leq |a|$ 가 성립합니다.

따라서 $S \subset \{c \in \mathbb{N} : |c| \leq |a|\}$ 이고 $|c| \leq |a|$ 를 만족하는 자연수 c의 개수는 유한하므로 S 는 공집합이 아닌 유한집합입니다. 그러므로 가장 큰 원소가 존재하고 S 의 가장 큰 원소를 **최대공약수(Greatest Common Divisor)**라고 정의합니다.

Definition 1.2.2 최대공약수(Greatest Common Divisor)
적어도 하나는 0이 아닌 정수 a, b가 임의로 주어져있다고 하자. 이때 자연수 d가 다음 두 조건을 만족하면 d를 a, b의 **최대공약수(Greatest Common Divisor)**라고 정의하고 기호로는 $d = \gcd(a,b)$ 라고 나타낸다.

(a). $d \mid a$ 이고 $d \mid b$ 이다.
(b). 모든 자연수 c에 대하여 $c \mid a$ 이고 $c \mid b$ 이면 $c \leq d$ 이다.

Definition 1.2.3 최소공배수(Least Common Multiple)
0이 아닌 정수 a, b가 임의로 주어져있다고 하자. 이때 자연수 m이 다음 두 조건을 만족하면 m를 a, b의 **최소공배수(Least Common Multiple)**라고 정의하고 기호로는 $m = \mathrm{lcm}(a,b)$ 라고 나타낸다.

(a). $a \mid m$ 이고 $b \mid m$ 이다.
(b). 모든 자연수 c에 대하여 $a \mid c$ 이고 $b \mid c$ 이면 $m \leq c$ 이다.

실제 수학에서는 최대공약수를 압도적으로 많이 사용합니다. 수학책을 보면 최소공배수는 최대공약수에 비하면 마주치는 경우가 거의 없을겁니다.

적어도 하나는 0이 아닌 정수 a, b가 $\gcd(a,b) = 1$ 을 만족하면 두 정수 a, b는 **서로소(Relatively Prime)**라고 부릅니다.

다음 정리는 기초 정수론에서 굉장히 중요한 정리입니다.

Theorem 1.2.2 베주의 항등식(Bezout's Identity)
적어도 하나는 0이 아닌 정수 a, b가 임의로 주어져있다고 하자. 그러면 $d = \gcd(a,b)$ 라고 할 때 $ax + by = d$ 를 만족하는 정수 x, y 가 존재한다.

(증명)
집합 S 를 다음과 같이 정의하자.

$$S = \{ax + by \in \mathbb{Z} : x,y\text{는 } ax + by > 0\text{을 만족하는 정수}\}$$

만약 $a \neq 0$ 이면 $a > 0$ 일땐 $a = a \times 1 + b \times 0 > 0$ 으로 표현 가능하므로 $a \in S$ 이고 $a < 0$ 일땐 $-a = a \times (-1) + b \times 0 > 0$ 이므로 $-a \in S$ 이다. 따라서 S 는 공집합이 아니다. $b \neq 0$ 일때도 같은 방법으로 S 는 공집합이 아님을 보일수 있다.

그러므로 S 는 공집합이 아니고 자연수 집합의 부분집합이므로 정렬원리에 의하면 가장 작은 원소를 갖는다. 그것을 d라고 하면 $d > 0$ 이고 적당한 정수 x, y 가 존재해서 $ax + by = d$ 를 만족한다. 이제 $d = \gcd(a,b)$ 임을 보이자.

나눗셈 정리에 의하면 $a = dq + r \ (0 \leq r < d)$ 를 만족하는 정수 q, r 이 존재하고 따라서 다음 등식을 얻는다.

$$\begin{aligned} r &= a - dq \\ &= a - q(ax + by) \\ &= a(1 - qx) + b(-qy) \end{aligned}$$

만약 $r > 0$ 이면 S 의 정의에 의해 $r \in S$ 인데 $r < d$ 이므로 이것은 d가 S 의 가장 작은 원소라는 것에 모순이다. 따라서 $r = 0$ 이고 $a = dq$ 이므로 $d \mid a$ 를 얻는다.

동일한 방법으로 $d \mid b$ 도 얻을수 있다. 이제 자연수 c가 $c \mid a$, $c \mid b$ 를 만족한다고 하자. 그러면 Theorem 1.2.1에 의해 $c \mid ax + by = d$ 이고 c, d는 자연수이므로 $c \leq d$ 이다.

따라서 최대공약수의 정의에 의하면 $d = \gcd(a,b)$ 이다. ■

Corollary 1.2.1 임의의 $a, b \in \mathbb{Z}$ 에 대하여 $a\mathbb{Z} + b\mathbb{Z}$ 를 다음과 같이 정의하자.

$$a\mathbb{Z} + b\mathbb{Z} = \{ax + by \in \mathbb{Z} : x, y \in \mathbb{Z}\}$$

이때 적어도 하나는 0이 아닌 $a, b \in \mathbb{Z}$ 에 대하여 $d = \gcd(a,b)$ 라고 하면 $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ 가 성립한다. 특히 $d = 1$ 이면 $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$ 이다.

(증명)
$(\subset)$ 임의의 $z \in a\mathbb{Z} + b\mathbb{Z}$ 를 택하자. 그러면 적당한 $x, y \in \mathbb{Z}$ 가 존재해서 $z = ax + by$ 이고 $d \mid a$, $d \mid b$ 이므로 $d \mid ax + by = z$ 이다. 따라서 적당한 $m \in \mathbb{Z}$ 이 존재해서 $z = dm$ 이므로 $z \in d\mathbb{Z}$ 이다.

$(\supset)$ 임의의 $z\in d\mathbb{Z}$ 를 택하자. 그러면 적당한 $m\in\mathbb{Z}$ 에 대하여 $z=dm$ 이고 Theorem 1.2.2에 의하면 적당한 $x,y\in\mathbb{Z}$ 가 존재해서 $d=ax+by$ 를 만족하므로 $z=dm=a(mx)+b(my)\in a\mathbb{Z}+b\mathbb{Z}$ 이다.

그러므로 $a\mathbb{Z}+b\mathbb{Z}=d\mathbb{Z}$ 가 성립한다. ■

다음 정리는 적어도 하나는 0이 아닌 두 정수 a,b가 서로소일 필요충분조건을 제시해주는 정리인데 이것도 기초 정수론에서 자주 쓰입니다.

Theorem 1.2.3 적어도 하나는 0이 아닌 $a,b\in\mathbb{Z}$ 에 대하여 a,b가 서로소일 필요충분조건은 $ax+by=1$ 을 만족하는 $x,y\in\mathbb{Z}$ 가 존재하는 것이다.

(증명)
$(\Rightarrow)$ Theorem 1.2.2에 의하면 명백하다.

$(\Leftarrow)$ $d=\gcd(a,b)$ 라고 하자. 그러면 $d\mid a,\ d\mid b$ 이므로 $d\mid ax+by=1$ 이고 d는 자연수이므로 $d=1$ 이다. 따라서 a,b는 서로소이다. ■

Corollary 1.2.2 적어도 하나는 0이 아닌 $a,b\in\mathbb{Z}$ 에 대하여 $d=\gcd(a,b)$ 라고 하면 다음이 성립한다.

(a). $\gcd\left(\frac{a}{d},\frac{b}{d}\right)=1$ 이다.
(b). $ab\neq 0$ 이고 $d=1$ 일 때 임의의 $c\in\mathbb{Z}$ 에 대하여 $a\mid c$ 이고 $b\mid c$ 이면 $ab\mid c$ 이다.
(c). $a\neq 0$ 이고 $d=1$ 일 때 임의의 $c\in\mathbb{Z}$ 에 대하여 $a\mid bc$ 이면 $a\mid c$ 이다.

(증명)
(a). 조건에 의하면 적당한 $x,y\in\mathbb{Z}$ 가 존재해서 $ax+by=d$ 를 만족한다.
따라서 $\left(\frac{a}{d}\right)x+\left(\frac{b}{d}\right)y=1$ 이므로 Theorem 1.2.3에 의하면 $\gcd\left(\frac{a}{d},\frac{b}{d}\right)=1$ 이다. ■

(b). $d=1$ 이므로 Theorem 1.2.3에 의하면 적당한 $x,y\in\mathbb{Z}$ 가 존재해서 $ax+by=1$ 을 만족한다. 그러므로 $c=acx+bcy$ 이고 조건에 의하면 적당한 정수 r,s 가 존재해서 $c=ar=bs$ 를 만족한다.

따라서 $c=absx+abry=ab(sx+ry)$ 이므로 $ab\mid c$ 이다. ■

(c). $d=1$ 이므로 Theorem 1.2.3에 의하면 적당한 $x,y\in\mathbb{Z}$ 가 존재해서 $ax+by=1$ 을 만족한다. 그러므로 $c=acx+bcy$ 이고 조건에 의하면 적당한 정수 k가 존재해서 $bc=ak$ 를 만족하므로 $c=acx+aky=a(cx+ky)$ 에서 $a\mid c$ 를 얻는다. ■

Problem 1.2.5 적어도 하나는 0이 아닌 $a, b \in \mathbb{Z}$ 와 자연수 d가 주어져있을 때 $d = \gcd(a,b)$ 일 필요충분조건은 다음 두 조건을 만족하는 것임을 증명하시오.

(a). $d \mid a$ 이고 $d \mid b$ 이다.
(b). 모든 자연수 c에 대하여 $c \mid a$ 이고 $c \mid b$ 이면 $c \mid d$ 이다.

(증명)
$(\Longrightarrow)$ 최대공약수의 정의에 의하면 (a)를 만족함은 명백하다. 임의의 자연수 c에 대하여 $c \mid a$, $c \mid b$ 라고 하면 적당한 $x, y \in \mathbb{Z}$ 가 존재해서 $ax + by = d$ 를 만족하므로 $c \mid ax + by = d$ 이다. 따라서 (b)도 만족한다.

$(\Longleftarrow)$ c, d는 자연수이므로 (b)를 만족하면 $c \leq d$ 이다. 그리고 (a)도 만족하므로 최대공약수의 정의에 의하면 $d = \gcd(a,b)$ 이다. ■

Problem 1.2.5에 의하면 공약수는 최대공약수의 약수라는 사실을 알수 있습니다.

최대공약수와 최소공배수는 다음과 같은 관계를 가지고 있습니다.
이것도 대학 입학 전에 몇 번 봤을겁니다.

Theorem 1.2.4 임의의 자연수 a, b에 대하여 다음 등식이 성립한다.

$$ab = \gcd(a,b)\mathrm{lcm}(a,b)$$

(증명)
$d = \gcd(a,b)$ 라고 하자. 그러면 적당한 정수 r, s 에 대하여 $a = dr$, $b = ds$ 이다.
$m = \dfrac{ab}{d}$ 라고 하자. 그러면 m은 자연수이고 $m = as = br$ 을 만족한다.
따라서 $a \mid m$, $b \mid m$ 을 만족한다.

임의의 자연수 c에 대하여 $a \mid c$, $b \mid c$ 라고 하자. 그러면 적당한 정수 u, v 에 대하여 $c = au = bv$ 를 만족하고 적당한 정수 x, y 에 대하여 $ax + by = d$ 도 만족하므로 다음 등식을 얻는다.

$$\frac{c}{m} = \frac{cd}{ab} = \frac{c(ax+by)}{ab} = \left(\frac{c}{b}\right)x + \left(\frac{c}{a}\right)y = vx + uy$$

따라서 $\dfrac{c}{m}$은 정수이므로 $m \mid c$ 이고 m, c는 자연수이므로 $m \leq c$ 이다. 그러므로 최소공배수의 정의에 의하면 $m = \mathrm{lcm}(a,b)$ 이다. 따라서 다음 등식을 얻는다.

$$ab = \gcd(a,b)\mathrm{lcm}(a,b)$$

■

Corollary 1.2.3 임의의 자연수 a, b에 대하여 a, b가 서로소일 필요충분조건은 $\mathrm{lcm}(a,b) = ab$ 인 것이다.

(증명)
Theorem 1.2.4에 의하면 명백하다. ■

Problem 1.2.6 0이 아닌 $a,b\in\mathbb{Z}$ 와 자연수 m이 주어져있을 때 $m=\mathrm{lcm}(a,b)$ 일 필요충분조건은 다음 두 조건을 만족하는 것임을 증명하시오.

(a). $a\mid m$ 이고 $b\mid m$ 이다.
(b). 모든 자연수 c에 대하여 $a\mid c$ 이고 $b\mid c$ 이면 $m\mid c$ 이다.

(증명)
$(\Rightarrow)$ 최소공배수의 정의에 의하면 (a)를 만족함은 명백하다.
이제 임의의 자연수 c에 대하여 $a\mid c,\ b\mid c$ 라고 하자. 그러면 $m\le c$ 이다.

나눗셈 정리에 의하면 m이 자연수이므로 $c=mq+r\ (0\le r<m)$ 을 만족하는 정수 q,r 이 존재한다. $r=0$ 임을 보이자.

만약 $r\neq 0$ 이면 $r=c-mq$ 이므로 조건과 가정에 의하면 $a\mid r,\ b\mid r$ 을 얻고 r은 자연수이므로 최소공배수의 정의에 의하면 $m\le r$ 인데 이것은 모순이다.
따라서 $r=0$ 이고 그러므로 $m\mid c$ 이다.

$(\Leftarrow)$ c,m는 자연수이므로 (b)를 만족하면 $m\le c$ 이다. 그리고 (a)도 만족하므로 최소공배수의 정의에 의하면 $m=\mathrm{lcm}(a,b)$ 이다. ■

Problem 1.2.6에 의하면 공배수는 최소공배수의 배수라는 사실을 알수 있습니다.

3개 이상의 정수에 대해서도 최대공약수와 최소공배수를 정의할수 있습니다.

Definition 1.2.4 최대공약수(Greatest Common Divisor) (일반적인 경우)
$n\ge 2$ 일 때 적어도 하나는 0이 아닌 정수 $a_1,a_2,\ldots,a_n$ 가 임의로 주어져있다고 하자. 이때 자연수 d가 다음 두 조건을 만족하면 d를 $a_1,a_2,\ldots,a_n$ 의 **최대공약수(Greatest Common Divisor)**라고 정의하고 기호로는 $d=\gcd(a_1,a_2,\ldots,a_n)$ 라고 나타낸다.

(a). $k=1,2,\ldots,n$ 일 때 모든 k에 대하여 $d\mid a_k$ 이다.
(b). $k=1,2,\ldots,n$ 일 때 모든 k와 모든 자연수 c에 대하여 $c\mid a_k$ 이면 $c\le d$ 이다.

Definition 1.2.5 최소공배수(Least Common Multiple) (일반적인 경우)
$n\ge 2$ 일 때 0이 아닌 정수 $a_1,a_2,\ldots,a_n$ 가 임의로 주어져있다고 하자. 이때 자연수 m이 다음 두 조건을 만족하면 m를 $a_1,a_2,\ldots,a_n$ 의 **최소공배수(Least Common Multiple)**라고 정의하고 기호로는 $m=\mathrm{lcm}(a_1,a_2,\ldots,a_n)$ 라고 나타낸다.

(a). $k=1,2,\ldots,n$ 일 때 모든 k에 대하여 $a_k\mid m$ 이다.
(b). $k=1,2,\ldots,n$ 일 때 모든 k와 모든 자연수 c에 대하여 $a_k\mid c$ 이면 $m\le c$ 이다.

일반적인 경우에서도 최대공약수가 1이면 n개의 정수는 서로소라고 부릅니다. 그런데 수학에서 3개 이상의 정수에 대한 최대공약수와 최소공배수의 정의는 잘 사용하지 않습니다.

예를 들어 3개의 정수 $6, 10, 15$ 가 주어져있을 때 대학 입학 전에 배운 지식에 의하면 $\gcd(6,10,15)=1$ 입니다. 그런데 $\gcd(6,10)=2, \gcd(10,15)=5, \gcd(6,15)=3$ 이므로 모든 2쌍의 정수가 서로소가 아니어도 3쌍의 정수는 서로소일수도 있습니다.

기초 정수론에서는 서로소가 되는 경우를 중요하게 취급하기 때문에 위처럼 3쌍의 정수는 서로소인데 모든 2쌍의 정수는 서로소가 아니면 다루기가 불편합니다. 그래서 3개 이상의 정수를 다룰 때 서로소 조건이 필요하면 보통 다음과 같이 설정합니다.

$$0\text{이 아닌 정수 } a_1, a_2, \ldots, a_n \text{ 에 대하여 } i \neq j \text{ 이면 } \gcd(a_i, a_j)=1 \tag{9}$$

(9)를 만족하면 $\gcd(a_1, a_2, \ldots, a_n)=1$ 을 만족한다는 것은 쉽게 알수 있습니다.

베주의 항등식도 다음과 같이 일반화시킬수 있는데 마주칠 일은 거의 없을테니 연습문제 하나 푸는 느낌으로 읽어보면 충분하다고 생각합니다.

Theorem 1.2.5 베주의 항등식(Bezout's Identity) (일반적인 경우)

$n \geq 2$ 일 때 적어도 하나는 0이 아닌 정수 $a_1, a_2, \ldots, a_n$ 가 임의로 주어져있다고 하자. 그러면 $d=\gcd(a_1, a_2, \ldots, a_n)$ 라고 할 때 다음 등식을 만족하는 정수 $x_1, x_2, \ldots, x_n$ 가 존재한다.

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = d$$

(증명)

집합 S 를 다음과 같이 정의하자.

$$S=\left\{\sum_{k=1}^{n} a_kx_k \in \mathbb{Z} : x_1, x_2, \ldots, x_n \text{은 } \sum_{k=1}^{n} a_kx_k > 0 \text{을 만족하는 정수}\right\}$$

만약 $a_1 \neq 0$ 이면 $a_1 > 0$ 일땐 $a_1 = a_1 \times 1 + a_2 \times 0 + \ldots + a_n \times 0 > 0$ 이므로 $a_1 \in S$ 이고 $a_1 < 0$ 일땐 $-a_1 = a_1 \times (-1) + a_2 \times 0 + \ldots + a_n \times 0 > 0$ 이므로 $-a_1 \in S$ 이다. 따라서 S 는 공집합이 아니다.

$a_2, a_3, \ldots, a_n$ 이 0이 아닐때도 같은 방법으로 S 는 공집합이 아님을 보일수 있다.

S 는 공집합이 아니고 자연수 집합의 부분집합이므로 정렬원리에 의하면 가장 작은 원소를 갖는다. 그것을 d라고 하면 $d > 0$ 이고 적당한 정수 $x_1, x_2, \ldots, x_n$ 가 존재해서 $a_1x_1 + a_2x_2 + \cdots + a_nx_n = d$ 를 만족한다. 이제 $d=\gcd(a_1, a_2, \ldots, a_n)$ 임을 보이자.

나눗셈 정리에 의하면 $a_1 = dq_1 + r_1 \ (0 \leq r_1 < d)$ 를 만족하는 정수 q_1, r_1 이 존재하고 따라서 다음 등식을 얻는다.

$$\begin{aligned} r_1 &= a_1 - dq_1 \\ &= a_1 - q_1(a_1x_1 + a_2x_2 + \cdots + a_nx_n) \\ &= a_1(1 - q_1x_1) + a_2(-q_1x_2) + a_3(-q_1x_3) + \cdots + a_n(-q_1x_n) \end{aligned}$$

만약 $r>0$ 이면 S 의 정의에 의해 $r\in S$ 인데 $r<d$ 이므로 이것은 d가 S 의 가장 작은 원소라는 것에 모순이다. 따라서 $r=0$ 이고 $a_1=dq_1$ 이므로 $d\mid a_1$ 를 얻는다.

동일한 방법으로 $k=2,3,...,n$ 일 때 $d\mid a_k$ 도 얻을수 있다. 이제 $k=1,2,...,n$ 일 때 자연수 c가 모든 k에 대하여 $c\mid a_k$ 를 만족한다고 하자. 그러면 (9)에 의해 $c\mid a_1x_1+a_2x_2+\cdots+a_nx_n=d$ 이고 c,d는 자연수이므로 $c\le d$ 이다.

따라서 최대공약수의 정의에 의하면 $d=\gcd(a_1,a_2,...,a_n)$ 이다. ■

Theorem 1.2.4는 3개 이상의 자연수가 주어져있을땐 성립하지 않을수도 있습니다.
$\gcd(6,10,15)=1,\ \mathrm{lcm}(6,10,15)=30$ 인데 $6\times10\times15=900$ 이므로
$6\times10\times15\neq\gcd(6,10,15)\mathrm{lcm}(6,10,15)$ 입니다.

이제 문제를 몇 개 풀어보고 1.2절을 마치겠습니다.

Problem 1.2.7 적어도 하나는 0이 아닌 임의의 $a,b\in\mathbb{Z}$ 에 대하여 다음 등식이 성립함을 증명하시오.

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

(증명)
$k\in\mathbb{Z}$ 와 $-k\in\mathbb{Z}$ 가 서로 동치라는 사실에 의하면 $a\neq0$ 일 때 $a,b\in\mathbb{Z}$ 에 대하여 다음이 성립한다는 것을 쉽게 알수 있다. $\Leftrightarrow$ 는 서로 동치라는 것을 의미한다.

$$a\mid b\Leftrightarrow a\mid(-b)\Leftrightarrow(-a)\mid b\Leftrightarrow(-a)\mid(-b) \tag{10}$$

따라서 $d=\gcd(a,b)$ 라고 하면 (11)과 Problem 1.2.5에 의해 $d=\gcd(-a,b)=\gcd(a,-b)=\gcd(-a,-b)$ 가 성립한다는 것을 쉽게 알수 있다. 그러므로 $\gcd(a,b)=\gcd(-a,b)=\gcd(a,-b)=\gcd(-a,-b)$ 이다. ■

Problem 1.2.8 0이 아닌 모든 정수 a에 대하여 다음이 성립함을 증명하시오.

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

(증명)
(10)에 의하면 $a\neq0$ 일 때 $a\mid|a|$ 임을 쉽게 알수 있다.
따라서 자연수 c에 대하여 $c\mid a$ 이면 $a\mid|a|$ 이므로 $c\mid|a|$ 가 성립한다.

이 사실과 Problem 1.2.5를 이용하면 $\gcd(a,0)=\gcd(a,a)=|a|$ 이것은 쉽게 증명할수 있다. 그리고 $d=\gcd(a,1)$ 라고 하면 d는 자연수이고 $d\mid1$ 이므로 $d=1$ 이다. ■

Problem 1.2.9 임의의 자연수 n과 정수 a에 대하여 $\gcd(a,a+n)$은 n을 나눈다는 것을 증명하시오. 따라서 $\gcd(a,a+1)=1$ 이다.

(증명)
$d=\gcd(a,a+n)$ 라고 하자. 그러면 $d\mid a,\ d\mid a+n$ 이므로
$d\mid (a+n)-a=n$ 이다. 따라서 d는 n을 나눈다.

특히 $n=1$ 이면 $d\mid 1$ 에서 $d=1$ 이므로 $\gcd(a,a+1)=1$ 이다. ■

Problem 1.2.10 $n\geq 2$ 일 때 정수 $a_1,a_2,\ldots a_n$ 이 주어져 있고 이들중 $a_1,a_2,\ldots,a_{n-1}$ 은 적어도 하나가 0이 아니다. 그러면 다음 등식이 성립함을 증명하시오.

$$\gcd(a_1,a_2,\ldots,a_{n-1},a_n)=\gcd(\gcd(a_1,a_2,\ldots,a_{n-1}),a_n)$$

(증명)
$d=\gcd(a_1,a_2,\ldots,a_{n-1},a_n),\ e=\gcd(a_1,a_2,\ldots,a_{n-1})$ 라고 하고
$d=\gcd(e,a_n)$ 임을 보이자.

$e=\gcd(a_1,a_2,\ldots,a_{n-1})$ 이므로 적당한 $x_1,x_2,\ldots,x_{n-1}\in\mathbb{Z}$ 가 존재해서
$a_1x_1+a_2x_2+\cdots+a_{n-1}x_{n-1}=e$ 를 만족한다. 그리고 $k=1,2,\ldots,n$ 일 때 모든
k에 대하여 $d\mid a_k$ 이므로 $d\mid a_1x_1+a_2x_2+\cdots a_{n-1}x_{n-1}=e$ 를 만족한다.

즉, $d\mid e,\ d\mid a_n$ 을 만족한다. 이제 임의의 자연수 c에 대하여 $c\mid e,\ c\mid a_n$ 라고 가정하자.
그러면 $e\mid a_1,\ e\mid a_2,\ \ldots,e\mid a_{n-1}$ 이므로 $c\mid a_1,\ c\mid a_2,\ \ldots,c\mid a_{n-1}$ 이고 $c\mid a_n$
인데 $d=\gcd(a_1,a_2,\ldots,a_{n-1},a_n)$ 이므로 최대공약수의 정의에 의하면 $c\leq d$ 이다.

따라서 $d=\gcd(e,a_n)$ 이다. ■

Problem 1.2.11 임의의 $a\in\mathbb{Z}$ 에 대하여 다음이 성립함을 증명하시오.
(a). $\gcd(2a+1,9a+4)=1$ 이다.
(b). $\gcd(5a+2,7a+3)=1$ 이다.
(c). a가 홀수이면 $\gcd(3a,3a+2)=1$ 이다.

(증명)
(a). 임의의 $a\in\mathbb{Z}$ 에 대하여 $9(2a+1)-2(9a+4)=1$ 이므로
Theorem 1.2.3에 의하면 $\gcd(2a+1,9a+4)=1$ 이다. ■

(b). 임의의 $a\in\mathbb{Z}$ 에 대하여 $5(7a+3)-7(5a+2)=1$ 이고
적어도 하나는 0이 아닌 정수 m,n 에 대하여 $\gcd(m,n)=\gcd(n,m)$ 이 성립함은
명백하므로 Theorem 1.2.3에 의하면 $\gcd(5a+2,7a+3)=1$ 이다. ■

(c). $d=\gcd(3a,3a+2)$ 라고 하자. 그러면 $d\mid 3a,\ d\mid 3a+2$ 이므로
$d\mid (3a+2)-3a=2$ 에서 $d=1,2$ 인데 a가 홀수이면 $3a,3a+2$ 는 모두
홀수이므로 $d\neq 2$ 이다. 따라서 $d=1$ 이므로 $\gcd(3a,3a+2)=1$ 이다. ■

Problem 1.2.12 자연수 a와 $m > n$ 을 만족하는 자연수 m, n이 임의로 주어져 있다. 그러면 $a^{2^n}+1 \mid a^{2^m}-1$ 임을 증명하시오.

(증명)

$m > n$ 이면 $m-n$ 은 자연수이므로 2^{m-n} 은 짝수이고 $2^m = 2^{m-n} \times 2^n$ 이다.

따라서 $d = 2^{m-n-1}$ 라고 하면 $2^m = 2^n \times (2d)$ 이고 자연수 p에 대하여 성립하는 다음 인수분해 공식

$$x^p - 1 = (x-1)\left(x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1\right)$$

을 이용하면 a, m, n이 자연수이므로 적당한 $k \in \mathbb{Z}$ 가 존재해서

$$\begin{aligned} a^{2^m} - 1 &= \left(a^{2^n}\right)^{2d} - 1 \\ &= \left(\left(a^{2^n}\right)^d - 1\right)\left(\left(a^{2^n}\right)^d + 1\right) \\ &= \left(a^{2^n} - 1\right)k \ (k \in \mathbb{Z}) \end{aligned}$$

라고 표현 가능하다. 그러므로 $a^{2^n}+1 \mid a^{2^m}-1$ 가 성립한다. ■

Problem 1.2.13 자연수 a와 $m \neq n$ 을 만족하는 자연수 m, n이 임의로 주어져 있다. 그러면 다음 등식이 성립함을 증명하시오.

$$\gcd\left(a^{2^m}+1, a^{2^n}+1\right) = \begin{cases} 1 & (a\text{는 짝수}) \\ 2 & (a\text{는 홀수}) \end{cases} \tag{11}$$

(증명)

최대공약수는 정수의 순서를 바꿔도 변하지 않으므로 $m > n$ 이라고 가정해도 일반성을 잃지 않는다. 그리고 $m > n$ 이면 Problem 1.2.12에서 $a^{2^n}+1 \mid a^{2^m}-1$ 이므로 적당한 $k \in \mathbb{Z}$ 가 존재해서 $a^{2^m}-1 = k\left(a^{2^n}+1\right)$ 을 만족한다.

따라서 $a^{2^m}+1 = k\left(a^{2^n}+1\right)+2$ 이므로 $d = \gcd\left(a^{2^m}+1, a^{2^n}+1\right)$ 라고 하면 $d \mid a^{2^m}+1,\ d \mid a^{2^n}+1$ 이므로 $d \mid \left(a^{2^m}+1\right) - k\left(a^{2^n}+1\right) = 2$ 이다.
그러므로 $d = 1, 2$ 를 얻는다.

case1) a는 짝수

이 경우 $a^{2^m}+1,\ a^{2^n}+1$ 은 모두 홀수이므로 $d \neq 2$ 이다. 따라서 $d = 1$ 이다.

case2) a는 홀수

이 경우 $a^{2^m}+1,\ a^{2^n}+1$ 은 모두 짝수이므로 $d = 2$ 가 되어야 한다.

정리하면 (11)을 얻을수 있다. ■

Problem 1.2.14 모든 자연수 n에 대하여 $\gcd(1+n!, 1+(n+1)!)=1$ 임을 증명하시오.

(증명)
모든 자연수 n에 대하여 $1+(n+1)! = (n+1)(1+n!)-n$ 가 성립한다.
따라서 $d=\gcd(1+n!, 1+(n+1)!)$ 라고 하면 $d \mid 1+n!$, $d \mid 1+(n+1)!$ 이므로
$d \mid (n+1)(1+n!)-(1+(n+1)!)=n$ 을 얻는다.

$n \mid n!$ 은 명백하므로 $d \mid n$ 이면 $d \mid n!$ 이고 따라서 $d \mid (1+n!)-n! = 1$ 이다.
그러므로 $d=1$ 을 얻는다. ■

Problem 1.2.15 임의의 정수 a, b, c, d 에 대하여 다음을 증명하시오.
각각의 문제에서 기호 $\mid$ 와 최대공약수는 잘 정의된다고 가정한다.

(a). $\gcd(a,b)=\gcd(a,c)=1$ 일 필요충분조건은 $\gcd(a,bc)=1$ 이다.
(b). $\gcd(a,b)=1$ 이고 $c \mid a$ 이면 $\gcd(b,c)=1$ 이다.
(c). $\gcd(a,b)=1$ 이면 $\gcd(ac,b)=\gcd(c,b)$ 이다.
(d). $\gcd(a,b)=1$ 이고 $c \mid a+b$ 이면 $\gcd(a,c)=\gcd(b,c)=1$ 이다.

(증명)
(a). $(\Longrightarrow)$ 조건에 의하면 적당한 정수 x, y, u, v 가 존재해서 다음을 만족한다.

$$ax+by=1$$
$$au+cv=1$$

따라서 $1=(ax+by)(au+cv)=a(axu+cxv+byu)+bc(yv)$ 이므로
Theorem 1.2.3에 의하면 $\gcd(a,bc)=1$ 이다.

$(\Longleftarrow)$ $d=\gcd(a,b)$ 라고 하자. 그러면 $d \mid a$, $d \mid b$ 이므로 $d \mid a$, $d \mid bc$ 이고
$\gcd(a,bc)=1$ 이므로 적당한 정수 x, y 가 존재해서 $ax+bcy=1$ 을 만족한다.

따라서 $d \mid ax+bcy=1$ 이므로 $d=1$ 이다. 즉, $\gcd(a,b)=1$ 을 얻는다.
같은 방법으로 $\gcd(a,c)=1$ 도 얻을수 있다. 따라서 $\gcd(a,b)=\gcd(a,c)=1$ 이다.
■

(b). 조건에 의하면 적당한 정수 x, y, u 가 존재해서 다음을 만족한다.

$$ax+by=1$$
$$a=cu$$

따라서 $by+c(xu)=1$ 이므로 Theorem 1.2.3에 의하면 $\gcd(b,c)=1$ 이다. ■

(c). 조건에 의하면 적당한 정수 x, y 가 존재해서 $ax+by=1$ 을 만족한다.
$d=\gcd(ac,b)$ 라고 하자. 그러면 $d \mid b$ 이므로 $d \mid bc$ 이고 $d \mid ac$ 이므로
$d \mid acx+bcy=c(ax+by)=c$ 가 성립한다. 따라서 $d \mid b$, $d \mid c$ 이다.

이제 임의의 자연수 k에 대하여 $k \mid b,\ k \mid c$ 라고 하자. 그러면 $k \mid ac$ 이고
따라서 $k \mid ac,\ k \mid b$ 인데 $d = \gcd(ac,b)$ 이므로 $k \le d$ 이다.

그러므로 최대공약수의 정의에 의하면 $d = \gcd(b,c)$ 이다.
즉, $\gcd(ac,b) = \gcd(c,b)$ 가 성립한다. ■

(d). 조건에 의하면 적당한 정수 x, y, u 가 존재해서 다음을 만족한다.

$$ax + by = 1$$
$$a + b = ck$$

$a = ck - b$ 이면 $1 = ax + by = b(y - x) + ckx$ 이므로 $\gcd(b,c) = 1$ 이고
$b = ck - a$ 이면 $1 = ax + by = a(x - y) + cky$ 이므로 $\gcd(a,c) = 1$ 이다. ■

Problem 1.2.16 $a \neq 0$ 일 때 정수 a, b, c 에 대하여 $a \mid bc$ 이면
$a \mid \gcd(a,b)\gcd(a,c)$ 임을 증명하시오.

(증명)
조건에 의하면 적당한 정수 x, y, u, v 가 존재해서 다음을 만족한다.

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

따라서 $\gcd(a,b)\gcd(a,c) = (ax + by)(au + cv) = a(axu + cxv + byu) + bc(yv)$
이고 $a \mid a$, 그리고 조건에 의하면 $a \mid bc$ 이므로 다음을 얻는다.

$$a \mid a(axu + cxv + byu) - bc(yv) = \gcd(a,b)\gcd(a,c)$$

■

Problem 1.2.17 두 정수 a, b 가 $\gcd(a,b) = 1$ 을 만족할 때 다음을 증명하시오. a, b 는 $\gcd(a,b) = 1$ 과 다음 문제에 주어진 모든 최대공약수가 잘 정의되는 정수라고 가정한다.

(a). $\gcd(a + b, a - b) = 1$ 또는 2이다.
(b). 임의의 자연수 m, n에 대하여 $\gcd(a^m, b^n) = 1$ 이다.
(c). $\gcd(a + b, a^2 + b^2) = 1$ 또는 2이다.
(d). $\gcd(a + b, ab) = 1$ 이다.

(증명)
조건에 의하면 적당한 정수 x, y 가 존재해서 $ax + by = 1$ 을 만족한다.

(a). $d = \gcd(a + b, a - b)$ 라고 하자. 그러면 $d \mid a + b,\ d \mid a - b$ 이므로
$d \mid (a + b) + (a - b) = 2a,\ d \mid (a + b) - (a - b) = 2b$ 를 얻는다.
따라서 $d \mid 2ax + 2by = 2(ax + by) = 2$ 이므로 $d = 1, 2$ 이다.

실제로 두 값을 모두 가질수 있다. $a = 1, b = 2$ 이면 $\gcd(a + b, a - b) = 1$ 이고
$a = 1, b = 3$ 이면 $\gcd(a + b, a - b) = 2$ 이다. ■

(b). 이항정리에 의하면 다음 등식을 얻는다.

$$\begin{aligned} 1 &= (ax+by)^{m+n} \\ &= \sum_{k=0}^{m+n}\binom{m+n}{k}(ax)^k(bx)^{m+n-k} \\ &= \sum_{k=0}^{m}\binom{m+n}{k}(ax)^k(bx)^{m+n-k} + \sum_{k=m+1}^{m+n}\binom{m+n}{k}(ax)^k(bx)^{m+n-k} \end{aligned}$$

그리고 다음 등식도 성립한다.

$$\begin{aligned} &\sum_{k=0}^{m}\binom{m+n}{k}(ax)^k(bx)^{m+n-k} \\ &= b^n\sum_{k=0}^{m}\binom{m+n}{k}(ax)^k b^{m-k}x^{m+n-k} \end{aligned} \tag{12}$$

$$\begin{aligned} &\sum_{k=m+1}^{m+m}\binom{m+n}{k}(ax)^k(bx)^{m+n-k} \\ &= a^m\sum_{k=m+1}^{m+n}\binom{m+n}{k}a^{k-m}x^k(bx)^{m+n-k} \end{aligned} \tag{13}$$

따라서 (12), (13)에 의하면 적당한 정수 u, v 에 대하여 $a^m u + b^n v = 1$ 을 만족하므로 $\gcd(a^m, b^n) = 1$ 을 얻는다. ■

(c). $d = \gcd(a+b, a^2+b^2)$ 라고 하자. 그러면 $d \mid a+b$, $d \mid a^2+b^2$ 이므로 다음을 얻을수 있다.

$$\begin{aligned} d \mid (a+b)(a-b) + (a^2+b^2) &= 2a^2 \\ d \mid (a^2+b^2) - (a+b)(a-b) &= 2b^2 \end{aligned}$$

그리고 (b)에 의하면 $\gcd(a^2, b^2) = 1$ 이므로 적당한 정수 u, v 가 존재해서 $a^2u + b^2v = 1$ 을 만족한다. 따라서 $d \mid 2(a^2u + b^2v) = 2$ 이므로 $d = 1, 2$ 이다.

실제로 두 값을 모두 가질수 있다. $a = b = 1$ 이면 $\gcd(a+b, a^2+b^2) = 2$ 이고 $a = 1, b = 2$ 이면 $\gcd(a+b, a^2+b^2) = 1$ 이다. ■

(d). $d = \gcd(a+b, ab)$ 라고 하자. 그러면 $d \mid a+b$, $d \mid ab$ 이므로 다음을 얻을수 있다.

$$\begin{aligned} d \mid a(a+b) - ab &= a^2 \\ d \mid b(a+b) - ab &= b^2 \end{aligned}$$

그리고 (b)에 의하면 $\gcd(a^2, b^2) = 1$ 이므로 Problem 1.2.5에 의하면 $d \mid 1$ 이다. 따라서 $d = 1$ 을 얻는다. ■

Problem 1.2.18 적어도 하나는 0이 아닌 $a, b \in \mathbb{Z}$ 에 대하여 $d = \gcd(a, b)$ 라고 하자. 그러면 $k \neq 0$ 인 모든 $k \in \mathbb{Z}$ 에 대하여 $\gcd(ka, kb) = |k|d$ 임을 증명하시오.

(증명)
$d \mid a,\ d \mid b$ 이므로 $|k|d \mid ka,\ |k|d \mid kb$ 는 명백하다. 이제 임의의 자연수 c에 대하여 $c \mid |k|a,\ c \mid |k|b$ 라고 가정하자. 그러면 $|k|a \mid ka,\ |k|b \mid kb$ 이므로 $c \mid ka,\ c \mid kb$ 를 얻는다.

한편 $d = \gcd(a,b)$ 이므로 적당한 정수 x, y 가 존재해서 $ax + by = d$ 를 만족하고 따라서 $kax + kby = kd$ 를 만족한다. 그러므로 $c \mid kax + kby = kd$ 이다.

$k \neq 0$ 이면 $\dfrac{|k|}{k} = \begin{cases} -1 & (k < 0) \\ 1 & (k > 0) \end{cases}$ 이므로 $\dfrac{|k|}{k}$는 정수이다.

따라서 $c \mid kd \times \dfrac{|k|}{k} = |k|d$ 이므로 Problem 1.2.5에 의하면 $\gcd(ka, kb) = |k|d$ 가 성립한다. ■

Problem 1.2.19 적어도 하나는 0이 아닌 $a, b \in \mathbb{Z}$ 가 임의로 주어져있다고 하자. 자연수 d가 $d \mid a,\ d \mid b$ 를 만족할 때 $d = \gcd(a,b)$ 일 필요충분조건은 $\gcd\left(\dfrac{a}{d}, \dfrac{b}{d}\right) = 1$ 임을 증명하시오.

(증명)
$(\Longrightarrow)$ Corollary 1.2.2에 의하면 명백하다.

$(\Longleftarrow)$ d는 a, b 의 양의 공약수이므로 2번째 조건을 만족한다는 것만 보이면 충분하다. 임의의 자연수 c에 대하여 $c \mid a,\ c \mid b$ 라고 하자.

조건에 의하면 적당한 정수 x, y 가 존재해서 $\left(\dfrac{a}{d}\right)x + \left(\dfrac{b}{d}\right)y = 1$ 을 만족한다.

따라서 $ax + by = d$ 이므로 $c \mid ax + by = d$ 이고 Problem 1.2.5에 의하면 $d = \gcd(a,b)$ 이다. ■

Problem 1.2.20 0이 아닌 임의의 $a, b \in \mathbb{Z}$ 에 대하여 다음은 동치임을 증명하시오.

(a). $a \mid b$
(b). $\gcd(a,b) = |a|$
(c). $\mathrm{lcm}(a,b) = |b|$

(증명)
$(a) \Longrightarrow (b)$
조건에 의하면 적당한 $c \in \mathbb{Z}$ 가 존재해서 $b = ac$ 를 만족하고 $a \neq 0$ 이므로 Problem 1.2.18에 의하면 $\gcd(a,b) = \gcd(a,ac) = |a|\gcd(1,c) = |a|$ 이다.

$(b) \Rightarrow (c)$
$a \mid b$ 이므로 $a \mid |b|$ 이고 $b \mid |b|$ 는 명백하다. 이제 임의의 자연수 c에 대하여 $a \mid c,\ b \mid c$ 라고 하자. 그러면 c는 자연수이고 $b \mid c$ 이므로 $|b| \leq |c| = c$ 이다. 따라서 최소공배수의 정의에 의하면 $\mathrm{lcm}(a,b) = |b|$ 이다.

$(c) \Rightarrow (a)$
조건에 의하면 $a \mid |b|$ 이고 $|b| \mid b$ 는 명백하므로 $a \mid b$ 이다. ■

Problem 1.2.21 적어도 하나는 0이 아닌 $a, b \in \mathbb{Z}$ 가 임의로 주어져있다고 하자. 그러면 $d = \gcd(a,b)$ 라고 할 때 모든 자연수 n에 대하여 $\gcd(a^n, b^n) = d^n$ 임을 증명하시오.

(증명)
조건에 의하면 $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ 이다. 따라서 Problem 1.2.17에 의하면
$\gcd\left(\frac{a^n}{d^n}, \frac{b^n}{d^n}\right) = 1$ 이고 $d \mid a,\ d \mid b$ 이므로 $d^n \mid a^n,\ d^n \mid b^n$ 은 명백하다.
그러므로 Problem 1.2.19에 의하면 $\gcd(a^n, b^n) = d^n$ 이다. ■

Problem 1.2.22 0이 아닌 $a, b \in \mathbb{Z}$ 가 임의로 주어져있다고 하자.
그러면 모든 자연수 n에 대하여 $a^n \mid b^n$ 일 필요충분조건은 $a \mid b$ 임을 증명하시오.

(증명)
$(\Rightarrow)$ Problem 1.2.20에 의하면 $\gcd(a^n, b^n) = |a|^n$ 이고 Problem 1.2.21에 의하면 $\gcd(a^n, b^n) = (\gcd(a,b))^n$ 이므로 $(\gcd(a,b))^n = |a|^n$ 인데 $\gcd(a,b)$와 $|a|$는 자연수이므로 $\gcd(a,b) = |a|$를 얻는다. 그러므로 Problem 1.2.20에 의하면 $a \mid b$ 이다.

$(\Leftarrow)$ $a \mid b$ 이면 $a^n \mid b^n$ 이 성립하는 것은 명백하다. ■

Problem 1.2.23 양의 약수가 1과 자기 자신만 존재하는 자연수 p를 **소수(Prime Number)** 라고 정의한다. 소수의 정의에 의하면 짝수인 소수는 2가 유일하다.

한편 n이 홀수일 때 성립하는 다음 항등식에 의하면

$$a^n + b^n = (a+b)\left(a^{n-1} - a^{n-2}b + \cdots - ab^{n-2} + b^{n-1}\right)$$

a, b가 자연수이고 p가 홀수인 소수일 때 $\frac{a^p + b^p}{a+b}$ 는 자연수임을 쉽게 알수 있다.

$\gcd(a,b) = 1$ 을 만족하는 임의의 자연수 a, b 와 홀수인 소수 p에 대하여
$\gcd\left(a+b, \frac{a^p + b^p}{a+b}\right) = 1$ 또는 p 임을 증명하시오.

(증명)

p는 홀수인 소수이므로 이항정리에 의하면 다음 등식을 얻는다.

$$\begin{aligned} a^p + b^p &= ((a+b)-b)^p + b^p \\ &= \sum_{k=0}^{p} \binom{p}{k} (a+b)^k (-b)^{p-k} + b^p \\ &= \sum_{k=1}^{p} \binom{p}{k} (a+b)^k (-b)^{p-k} \end{aligned}$$

따라서 $\dfrac{a^p+b^p}{a+b} = pb^{p-1} + \sum_{k=2}^{p} \binom{p}{k} (a+b)^k (-b)^{p-k}$ 를 얻는다. (14)

마찬가지로 이항정리에 의하면 다음 등식을 얻는다.

$$\begin{aligned} a^p + b^p &= a^p + ((a+b)-a)^p \\ &= a^p + \sum_{k=0}^{p} \binom{p}{k} (a+b)^k (-a)^{p-k} \\ &= \sum_{k=1}^{p} \binom{p}{k} (a+b)^k (-a)^{p-k} \end{aligned}$$

따라서 $\dfrac{a^p+b^p}{a+b} = pa^{p-1} + \sum_{k=2}^{p} \binom{p}{k} (a+b)^k (-a)^{p-k}$ 를 얻는다. (15)

이제 $d = \gcd\left(a+b, \dfrac{a^p+b^p}{a+b}\right)$ 라고 하자. 그러면 $d \mid a+b$, $d \mid \dfrac{a^p+b^p}{a+b}$ 이므로 (14), (15)에 의하면 $d \mid pa^{p-1}$, $d \mid pb^{p-1}$ 을 얻는다.

$\gcd(a,b)=1$ 이므로 $\gcd(a^{p-1}, b^{p-1})=1$ 이고 따라서 적당한 정수 x, y 가 존재해서 $a^{p-1}x + b^{p-1}y = 1$ 을 만족한다. 그러므로 $d \mid p(a^{p-1}x + b^{p-1}y) = p$ 이고 p는 소수이므로 $d = 1, p$ 이다. ■

1.3 유클리드 호제법

작성자 : 네냐플(Nenyaffle)

유클리드 호제법은 2개의 정수의 최대공약수를 구하는 알고리즘입니다. 최대공약수를 구하는 알고리즘을 따로 공부할 필요가 있는지 궁금해할수 있는데 수가 커지면 초등학생때 배운 방법으로 최대공약수를 구하기 힘들어서 그런것도 있지만 수학에서 중요한 알고리즘입니다.

초등학생때 $\gcd(6,15)$ 를 구하기 위해 다음과 같이 씁니다.

$$3\,\big|\,\underline{6\ 15}$$
$$\quad\ 2\ \ 5$$

$2,5$는 공약수가 1이므로 $\gcd(6,15)=3$ 이라고 하는게 초등학생때 배운 방법입니다.
그런데 수가 커지면 이 방법으로 최대공약수를 구하기 쉽지 않습니다.
$\gcd(1769,2378)$ 이 값을 초등학생때 배운 방법으로 구하려면 쉽지 않을겁니다.

$\gcd(1769,2378)$ 이 값은 유클리드 호제법을 사용하면 쉽게 구할수 있습니다.
실제로 최대공약수를 손계산으로 빠르게 구하는 일반적인 방법이 유클리드 호제법입니다.

유클리드 호제법을 소개하기 위해 먼저 다음 보조정리를 증명하겠습니다.

Lemma 1.3.1 $\gcd(a,b),\gcd(b,r)$ 두 값이 잘 정의되도록 하는 $a,b,q,r\in\mathbb{Z}$ 에 대하여 $a=bq+r$ 이라고 하자. 그러면 $\gcd(a,b)=\gcd(b,r)$ 이다.

(증명)
$d=\gcd(a,b)$ 라고 하자. 그러면 $d\mid a$, $d\mid b$ 이고 $a=bq+r$ 이므로 $d\mid a-bq=r$ 을 얻는다. 따라서 $d\mid b$, $d\mid r$ 가 성립한다.

이제 임의의 자연수 c에 대하여 $c\mid b$, $c\mid r$ 가 성립한다고 하자. 그러면 $c\mid bq+r=a$ 를 얻고 따라서 $c\mid a$, $c\mid b$ 이므로 최대공약수의 정의에 의하면 $c\le d$ 가 성립한다.

그러므로 최대공약수의 정의에 의하면 $d=\gcd(b,r)$ 이다.
즉, $\gcd(a,b)=\gcd(b,r)$ 가 성립한다. ■

적어도 하나는 0이 아닌 $a,b\in\mathbb{Z}$ 가 주어져있을 때 1.2절 Problem 1.2.7에 의하면
$\gcd(a,b)=\gcd(-a,b)=\gcd(a,-b)=\gcd(-a,-b)$ 가 성립합니다.

그리고 $\gcd(a,b)=\gcd(b,a)$ 는 명백하고 Problem 1.2.8에 의하면 $a\neq 0$ 일 때
$\gcd(a,0)=\gcd(a,a)=|a|$ 입니다.

따라서 2개의 정수 a,b 의 최대공약수를 구하는 알고리즘을 만들때는 위 관찰에 의해
a,b가 $a>b>0$ 을 만족한다고 가정하고 만들어도 충분합니다.

그러므로 $a>b>0$ 이라고 가정하겠습니다.

유클리드 호제법은 다음 알고리즘입니다.

1단계 : a를 b로 나눈 몫을 q_1, 나머지를 r_1 이라고 하자.
그러면 $a = bq_1 + r_1 \ (0 \le r_1 < b)$ 이다.

2단계 : $r_1 = 0$ 이면 Lemma 1.3.1에 의해 $\gcd(a,b) = \gcd(b,0) = b$ 이다.
$r_1 > 0$ 이면 b를 r_1으로 나눈 몫을 q_2, 나머지를 r_2 라고 하자.
그러면 $b = r_1q_2 + r_2 \ (0 \le r_2 < r_1)$ 이다.

3단계 : $r_2 = 0$ 이면 Lemma 1.3.1에 의해 $\gcd(a,b) = \gcd(b,r_1) = \gcd(r_1,0) = r_1$
이다. $r_2 > 0$ 이면 r_1을 r_2로 나눈 몫을 q_3, 나머지를 r_3 이라고 하자.
그러면 $r_1 = r_2q_3 + r_3 \ (0 \le r_3 < r_2)$ 이다.

4단계 : $r_3 = 0$ 이면 Lemma 1.3.1에 의해 $\gcd(a,b) = \cdots = \gcd(r_2,0) = r_2$ 이다.
$r_3 > 0$ 이면 r_2를 r_3으로 나눈 몫을 q_4, 나머지를 r_4 라고 하자.
그러면 $r_2 = r_3q_4 + r_4 \ (0 \le r_4 < r_3)$ 이다.

$\cdots$

이렇게 나머지가 0이 나올때까지 나누는 작업을 계속 반복하는겁니다.
나머지가 0이 나오면 Lemma 1.3.1을 이용해서 $\gcd(a,b)$를 구할수 있습니다.

나머지가 0이 되는 상황은 반드시 나타납니다. 그 이유는 다음과 같습니다.

편의상 $r_0 = b$ 라고 하면 알고리즘에서 등장한 수열 $\{r_n\}$은 모든 항이 음이 아닌
정수이고 $0 \le \cdots < r_3 < r_2 < r_1 < r_0 = b$ 를 만족합니다. 즉, $\{r_n\}$은 순감소하는
수열이고 $\{r_n\} \subset \{0,1,2,...,b\}$ 입니다.

모든 항이 음이 아닌 정수로 이루어진 순감소하는 수열 $\{r_n\}$이 $\{r_n\} \subset \{0,1,2,...,b\}$ 를
만족하면 $r_n = 0$ 을 만족하는 음이 아닌 정수 n은 존재합니다.

Lemma 1.1.1에 의하면 $r_n = 0$ 을 만족하는 가장 작은 음이 아닌 정수는 존재하고
그것을 m이라고 하면 알고리즘을 $m+1$ 단계까지 수행해서 $\gcd(a,b)$를 구할수
있습니다.

이것을 정리하면 다음과 같습니다.

Theorem 1.3.1 유클리드 호제법(Euclidean Algorithm)

a, b는 $a > b > 0$ 을 만족하는 정수이고 $r_0 = b$ 라고 하자. 이때 r_{n-1}을 r_n으로 나눈 나머지가 0이 나올때까지 다음 과정을 수행했다고 하자.

$$\begin{aligned} a &= bq_1 + r_1 \ (0 < r_1 < b) \\ b &= r_1 q_2 + r_2 \ (0 < r_2 < r_1) \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n \ (0 < r_n < r_{n-1}) \\ r_{n-1} &= q_{n+1} r_n + 0 \end{aligned}$$

그러면 $\gcd(a,b) = r_n$ 이다.

Problem 1.3.1 유클리드 호제법을 사용해서 다음 값을 구하시오.

(a). $\gcd(1769, 2378)$

(b). $\gcd(14965, 51611)$

(c). $\gcd(345465, 6455)$

(풀이)

(a). 유클리드 호제법을 사용하면 다음을 얻는다.

$$\begin{aligned} 2378 &= 1769 \times 1 + 609 \\ 1769 &= 609 \times 2 + 551 \\ 609 &= 551 \times 1 + 58 \\ 551 &= 58 \times 9 + 29 \\ 58 &= 29 \times 2 + 0 \end{aligned}$$

따라서 $\gcd(1769, 2378) = 29$ 이다. ■

(b). 유클리드 호제법을 사용하면 다음을 얻는다.

$$\begin{aligned} 51611 &= 14965 \times 3 + 6716 \\ 14965 &= 6716 \times 2 + 1533 \\ 6716 &= 1533 \times 4 + 584 \\ 1533 &= 584 \times 2 + 365 \\ 584 &= 365 \times 1 + 219 \\ 365 &= 219 \times 1 + 146 \\ 219 &= 146 \times 1 + 73 \\ 146 &= 73 \times 2 + 0 \end{aligned}$$

따라서 $\gcd(14965, 51611) = 73$ 이다. ■

(c). 유클리드 호제법을 사용하면 다음을 얻는다.

$$\begin{aligned} 345465 &= 6455 \times 53 + 3350 \\ 6455 &= 3350 \times 1 + 3105 \\ 3350 &= 3105 \times 1 + 245 \\ 3105 &= 245 \times 12 + 165 \\ 245 &= 165 \times 1 + 80 \\ 165 &= 80 \times 2 + 5 \\ 80 &= 5 \times 16 + 0 \end{aligned}$$

따라서 $\gcd(345465, 6455) = 5$ 이다. ■

유클리드 호제법을 이용해서 3개의 정수의 최대공약수도 구할수 있는데 Problem 1.2.10에 의해 유도되는 $\gcd(a,b,c,)=\gcd(\gcd(a,b),c)$ 이 등식을 이용하면 됩니다.
이때는 유클리드 호제법을 2번 사용하게 됩니다.

Problem 1.3.2 유클리드 호제법을 사용해서 $\gcd(198,288,512)$의 값을 구하시오.

(풀이)
먼저 $\gcd(198,288)$의 값을 구하자. 유클리드 호제법에 의하면

$$288=198\times1+90$$
$$198=90\times2+18$$
$$90=18\times5+0$$

이므로 $\gcd(198,288)=18$ 이다. 따라서 $\gcd(18,512)$의 값을 구하면 된다.
이것도 유클리드 호제법에 의하면

$$512=18\times28+8$$
$$18=8\times2+2$$
$$8=2\times4+0$$

이므로 $\gcd(18,512)=2$ 이다. 따라서 $\gcd(198,288,512)=2$ 이다. ■

1.2절에서 $d=\gcd(a,b)$ 이면 $ax+by=d$ 를 만족하는 정수 x,y 가 존재한다는 것을 배웠는데 유클리드 호제법을 이용하면 방정식 $ax+by=d$ 을 만족하는 정수 x,y 를 쉽게 구할수 있습니다. 나머지가 0이 아닌 시점부터 반대로 되돌아가면 됩니다.

$\gcd(1769,2378)$의 값을 구하기 위해 사용한 유클리드 호제법은 다음과 같습니다.

$$2378=1769\times1+609$$
$$1769=609\times2+551$$
$$609=551\times1+58$$
$$551=58\times9+29$$
$$58=29\times2+0$$

여기서 나머지가 0이 아닌 시점부터 반대로 되돌아가겠습니다.

1단계 : $551=58\times9+29$ 에서 $29=551-58\times9$ 이다.

2단계 : $609=551\times1+58$ 에서 $58=609-551\times1$ 이므로 다음을 얻는다.

$$\begin{aligned}29&=551-58\times9\\&=551-(609-551\times1)\times9\\&=551\times10-609\times9\end{aligned}$$

3단계 : $1769=609\times2+551$ 에서 $551=1769-609\times2$ 이므로 다음을 얻는다.

$$\begin{aligned}29&=551\times10-609\times9\\&=(1769-609\times2)\times10-609\times9\\&=1769\times10-609\times29\end{aligned}$$

4단계 : $2378=1769\times1+609$ 에서 $609=2378-1769\times1$ 이므로
다음을 얻는다.

$$\begin{aligned} 29 &= 1769\times 10 - 609\times 29 \\ &= 1769\times 10 - (2378 - 1769\times 1)\times 29 \\ &= 1769\times 39 - 2378\times 29 \end{aligned}$$

따라서 방정식 $1769x + 2378y = 29$ 의 하나의 정수해는 $x = 39,\ y = -29$ 입니다. 물론 방정식 $1769x + 2378y = 29$ 의 정수해가 $x = 39,\ y = -29$ 이것만 있는건 아닙니다. $x = 121,\ y = -90$ 이것도 해가 됩니다. (16)

실제로 방정식 $1769x + 2378y = 29$ 을 만족하는 정수 x, y 의 개수는 무한합니다. 임의의 $n \in \mathbb{Z}$ 에 대하여 $x = 39 + 82n,\ y = -29 - 61n$ 가 방정식을 만족하는 정수해입니다.

이런식으로 정수해만 고려하는 부정방정식을 **디오판토스 방정식(Diophantine Equation)** 이라고 부릅니다. 지금은 1차식만 생각했는데 디오판토스 방정식은 1차식만 이야기하는건 아닙니다. $x^2 + y^2 = 9$ 이 방정식도 정수해만 고려하면 디오판토스 방정식이 됩니다.

그런데 디오판토스 방정식은 일반적으로 해를 구하기가 어렵습니다. 심지어 해의 존재성을 판단하는것도 어렵습니다. 400년만에 풀린 **페르마의 마지막 정리(Fermat's Last Theorem)**는 $n \geq 3$ 일 때 방정식 $x^n + y^n = z^n$ 을 만족하는 0이 아닌 정수 x, y, z 가 존재하지 않는다는 정리인데 이것도 디오판토스 방정식입니다.

1.3절에서는 $ax + by = c$ 이런 형태의 디오판토스 방정식만 다루려고 합니다. 다음 문제만 풀고 $ax + by = c$ 이 방정식의 정수해에 대해 이야기하겠습니다.

Problem 1.3.3 다음 방정식의 정수해를 하나만 구하시오.

(a). $14965x + 51611y = 73$

(b). $345465x + 6455y = 10$

(c). $198x + 288y + 512z = 2$

(풀이)

(a). $\gcd(14965, 51611) = 73$ 을 얻기 위해 사용한 알고리즘은 다음과 같다.

$$\begin{aligned} 51611 &= 14965\times 3 + 6716 \\ 14965 &= 6716\times 2 + 1533 \\ 6716 &= 1533\times 4 + 584 \\ 1533 &= 584\times 2 + 365 \\ 584 &= 365\times 1 + 219 \\ 365 &= 219\times 1 + 146 \\ 219 &= 146\times 1 + 73 \\ 146 &= 73\times 2 + 0 \end{aligned}$$

따라서 위 과정을 반대로 되돌아가면 다음을 얻을수 있다.

$$\begin{aligned}73 &= 219-146\times 1\\ &= 219-(365-219)\times 1\\ &= 219\times 2-365\times 1\\ &= (584-365)\times 2-365\times 1\\ &= 584\times 2-365\times 3\\ &= 584\times 2-(1533-584\times 2)\times 3\\ &= 584\times 8-1533\times 3\\ &= (6716-1533\times 4)\times 8-1533\times 3\\ &= 6716\times 8-1533\times 35\\ &= 6716\times 8-(14965-6716\times 2)\times 35\\ &= 6716\times 78-14965\times 35\\ &= (51611-14965\times 3)\times 78-14965\times 35\\ &= 51611\times 78-14965\times 269\end{aligned}$$

따라서 주어진 방정식의 하나의 정수해는 $x=-269,\ y=78$ 이다. ■

(b). $\gcd(345465, 6455)=5$ 를 얻기 위해 사용한 알고리즘은 다음과 같다.

$$\begin{aligned}345465 &= 6455\times 53+3350\\ 6455 &= 3350\times 1+3105\\ 3350 &= 3105\times 1+245\\ 3105 &= 245\times 12+165\\ 245 &= 165\times 1+80\\ 165 &= 80\times 2+5\\ 80 &= 5\times 16+0\end{aligned}$$

따라서 위 과정을 반대로 되돌아가면 다음을 얻을수 있다.

$$\begin{aligned}5 &= 165-80\times 2\\ &= 165-(245-165\times 1)\times 2\\ &= 165\times 3-245\times 2\\ &= (3105-245\times 12)\times 3-245\times 2\\ &= 3105\times 3-245\times 38\\ &= 3105\times 3-(3350-3105\times 1)\times 38\\ &= 3105\times 41-3350\times 38\\ &= (6455-3350\times 1)\times 41-3350\times 38\\ &= 6455\times 41-3350\times 79\\ &= 6455\times 41-(345465-6455\times 53)\times 79\\ &= 6455\times 4228-345465\times 79\end{aligned}$$

양변에 2를 곱하면 $10=6455\times 8456-345465\times 158$ 이므로 주어진 방정식의 하나의 정수해는 $x=-158,\ y=8456$ 이다. ■

(c). $\gcd(198, 288)=18$ 을 얻기 위해 사용한 알고리즘은 다음과 같다.

$$\begin{aligned}288 &= 198\times 1+90\\ 198 &= 90\times 2+18\\ 90 &= 18\times 5+0\end{aligned}$$

따라서 위 과정을 반대로 되돌아가면 다음을 얻을수 있다.

$$\begin{aligned}18 &= 198-90\times 2\\ &= 198-(288-198\times 1)\times 2\\ &= 198\times 3-288\times 2\end{aligned}$$

그리고 $\gcd(18,512)=2$ 을 얻기 위해 사용한 알고리즘은 다음과 같다.

$$512 = 18 \times 28 + 8$$
$$18 = 8 \times 2 + 2$$
$$8 = 2 \times 4 + 0$$

따라서 위 과정을 반대로 되돌아가면 다음을 얻을수 있다.

$$\begin{aligned} 2 &= 18 - 8 \times 2 \\ &= 18 - (512 - 18 \times 28) \times 2 \\ &= 18 \times 57 - 512 \times 2 \end{aligned}$$

$18 = 198 \times 3 - 288 \times 2$ 이므로 이것을 대입하면 다음을 얻는다.

$$\begin{aligned} 2 &= (198 \times 3 - 288 \times 2) \times 57 - 512 \times 2 \\ &= 198 \times 171 - 288 \times 114 - 512 \times 2 \end{aligned}$$

그러므로 주어진 방정식의 하나의 정수해는 $x = 171,\ y = -114,\ z = -2$ 이다. ■

이제 $ax + by = c$ 이런 형태의 디오판토스 방정식의 일반해에 대해 이야기하겠습니다.

Theorem 1.3.2 0이 아닌 임의의 $a, b \in \mathbb{Z}$ 와 임의의 $c \in \mathbb{Z}$ 가 주어져있다고 할 때 $d = \gcd(a,b)$ 라고 하자. 이때 $ax + by = c$ 를 만족하는 정수 x, y 가 존재할 필요충분조건은 $d \mid c$ 이다.

그리고 정수해가 존재하는 방정식 $ax + by = c$ 한 정수해를 $x = x_0,\ y = y_0$ 라고 하면 $ax + by = c$ 를 만족하는 모든 정수해는 다음과 같이 표현된다.

$$x = x_0 + \left(\frac{b}{d}\right)n,\ y = y_0 - \left(\frac{a}{d}\right)n \ (n \in \mathbb{Z}) \tag{17}$$

(증명)

1.2절의 Corollary 1.2.1에 의하면 $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ 이다. 따라서 $ax + by = c$ 를 만족하는 정수 x, y 가 존재하면 c는 d의 배수이므로 $d \mid c$ 이다.

역으로 $d \mid c$ 이면 적당한 $k \in \mathbb{Z}$ 가 존재해서 $c = kd$ 를 만족하고 $d = \gcd(a,b)$ 이므로 적당한 정수 x_0, y_0 가 존재해서 $ax_0 + by_0 = d$ 를 만족한다.

따라서 $x = kx_0,\ y = ky_0$ 는 방정식 $ax + by = c$ 의 정수해가 되고 그러므로 $d \mid c$ 이면 정수해가 존재한다. 이제 일반해를 구하자.

조건에 의하면 $ax_0 + by_0 = c$ 를 만족한다. $ax + by = c$ 라고 하면 $ax + by = ax_0 + by_0$ 이므로 $a(x - x_0) = b(y_0 - y)$ 를 얻는다.

$d \mid a,\ d \mid b$ 이므로 적당한 정수 r, s 가 존재해서 $a = dr,\ b = ds$ 를 만족하고 이때 $\gcd(r,s) = 1$ 이다. 그리고 대입하면 $r(x - x_0) = s(y_0 - y)$ 를 얻는다.

따라서 $r \mid s(y_0 - y)$ 인데 $\gcd(r,s) = 1$ 이므로 Corollary 1.2.2에 의하면
$r \mid y_0 - y$ 를 얻는다. 그러므로 적당한 정수 n이 존재해서 $y_0 - y = rn$ 을 만족하고
$r(x - x_0) = s(y_0 - y)$ 인데 r, s 는 모두 0이 아니므로 $x - x_0 = sn$ 을 얻는다.

마지막으로 $r = \frac{a}{d},\ s = \frac{b}{d}$ 이므로 $x = x_0 + \left(\frac{b}{d}\right)n,\ y = y_0 - \left(\frac{a}{d}\right)n$ 이 성립한다.

역으로 임의의 $n \in \mathbb{Z}$ 에 대하여 $x = x_0 + \left(\frac{b}{d}\right)n,\ y = y_0 - \left(\frac{a}{d}\right)n$ 는 다음을 만족한다.

$$\begin{aligned} ax + by &= a\left(x_0 + \left(\frac{b}{d}\right)n\right) + b\left(y_0 - \left(\frac{a}{d}\right)n\right) \\ &= (ax_0 + by_0) + a \times \left(\frac{b}{d}\right)n - b \times \left(\frac{a}{d}\right)n \\ &= c \end{aligned}$$

그러므로 정수해가 존재하는 방정식 $ax + by = c$ 의 모든 정수해는
$x = x_0 + \left(\frac{b}{d}\right)n,\ y = y_0 - \left(\frac{a}{d}\right)n\ (n \in \mathbb{Z})$ 으로 표현된다. ■

$n \in \mathbb{Z}$ 과 $-n \in \mathbb{Z}$ 는 동치이므로 (17)을 다음과 같이 부호만 바꿔도 일반해가 됩니다.

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

그리고 Theorem 1.3.2에서 $d = 1$ 이면 모든 $c \in \mathbb{Z}$ 에 대하여 $ax + by = c$ 의 정수해는 존재하고 일반해는 다음과 같이 좀 더 간단하게 표현할수 있습니다.

$$x = x_0 + bn,\ y = y_0 - an\ (n \in \mathbb{Z})$$

정수해가 존재하는 방정식 $ax + by = c$ 의 정수해를 구하는 일반적인 방법은 먼저
유클리드 호제법을 사용해서 $d = \gcd(a,b)$ 를 구하고 그 과정을 반대로 되돌아가서
$ax_0 + by_0 = d$ 를 만족하는 정수 x_0, y_0 를 구한 다음 (17)에 대입하는겁니다.

Problem 1.3.4 다음 디오판토스 방정식의 해가 존재한다면 일반해를 구하시오.
(a). $1769x + 2378y = 29$
(b). $14965x + 51611y = 73$
(c). $345465x + 6455y = 10$

(풀이)
Problem 1.3.1, 1.3.2와 Theorem 1.3.2에 의하면 (a)~(c)의 방정식은 정수해를 갖는다.
그러므로 일반해만 구하면 충분하다.

(a). (16)에 의하면 주어진 방정식의 한 해는 $x_0 = 39,\ y_0 = -29$ 이다.
그러므로 (17)에 의하면 일반해는 $x = 39 + 82n,\ y = -29 - 61n\ (n \in \mathbb{Z})$ 이다. ■

(b). Problem 1.3.3에 의하면 주어진 방정식의 한 해는 $x_0 = -269,\ y_0 = 78$ 이다.
그러므로 (17)에 의하면 일반해는 $x = -269 + 707n,\ y = 78 - 205n\ (n \in \mathbb{Z})$ 이다.
■

(c). Problem 1.3.3에 의하면 주어진 방정식의 한 해는 $x_0 = -158,\ y_0 = 8456$ 이다.
그러므로 (17)에 의하면 일반해는 $x = -158 + 1291n,\ y = 8456 - 69093n\ (n \in \mathbb{Z})$ 이다. ■

2문제만 더 풀고 1.3절을 마치겠습니다.

Problem 1.3.5 음이 아닌 정수 k에 대하여 다항식 $f_k(x) \in \mathbb{Z}[x]$를 다음과 같이 정의하자.

$$f_k(x) = \begin{cases} 0 & (k = 0) \\ 1 + x + x^2 + \cdots + x^{k-1} & (k \geq 1) \end{cases}$$

자연수 m, n에 대하여 $d = \gcd(m,n)$ 라고 하면 $\gcd\big(f_m(a), f_n(a)\big)$ 가 잘 정의되도록 하는 모든 $a \in \mathbb{Z}$ 에 대하여 $\gcd\big(f_m(a), f_n(a)\big) = f_d(a)$ 임을 증명하시오.

(증명)
$m = n$ 이면 $d = m = n$ 이므로 $\gcd\big(f_m(a), f_n(a)\big) = f_d(a)$ 는 명백하다.
따라서 $m \neq n$ 을 가정하자. 이 경우 $m > n$ 이라고 해도 일반성을 잃지 않는다.

$d = \gcd(m,n)$ 이므로 유클리드 호제법에 의하면

$$\begin{aligned} m &= nq_1 + r_1 \ (0 < r_1 < n) \\ n &= r_1 q_2 + r_2 \ (0 < r_2 < r_1) \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n \ (0 < r_n < r_{n-1}) \\ r_{n-1} &= q_{n+1} r_n + 0 \end{aligned}$$

에서 $r_n = d$ 이다. 그리고 위 알고리즘은 큰 자연수를 작은 자연수로 나누므로 몫은 모두 자연수임을 쉽게 알수 있다. 즉, $q_1, q_2, \ldots, q_{n+1}$ 은 모두 자연수이다.

$m = nq_1 + r_1$ 이므로 다음 등식을 얻는다.

$$\begin{aligned} f_m(a) &= f_{nq_1 + r_1}(a) \\ &= 1 + a + a^2 + \cdots + a^{nq_1 + r_1 - 1} \\ &= 1 + a + a^2 + \cdots + a^{r_1 - 1} + a^{r_1} + \cdots + a^{r_1 + nq_1 - 1} \\ &= f_{r_1}(a) + a^{r_1}\big(1 + a + a^2 + \cdots + a^{nq_1 - 1}\big) \end{aligned} \tag{18}$$

여기서 $1 + a + a^2 + \cdots + a^{nq_1 - 1}$ 은 항이 nq_1개 있으므로 다음과 같이 표현할수 있다.

$$\begin{aligned} &1 + a + a^2 + \cdots + a^{nq_1 - 1} \\ &= \big(1 + \cdots + a^{n-1}\big) + \big(a^n + \cdots + a^{2n-1}\big) + \cdots + \big(a^{(q_1 - 1)n} + \cdots + a^{nq_1 - 1}\big) \\ &= f_n(a) + a^n f_n(a) + \cdots + a^{(q_1 - 1)n} f_n(a) \\ &= \big(1 + a^n + \cdots + a^{(q_1 - 1)n}\big) f_n(a) \end{aligned}$$

(18)에 의하면 적당한 $k\in\mathbb{Z}$ 에 대하여 $f_m(a)=kf_n(a)+f_{r_1}(a)$ 이런 형태로 표현되고 따라서 Lemma 1.3.1에 의하면 $\gcd\left(f_m(a),f_n(a)\right)=\gcd\left(f_n(a),f_{r_1}(a)\right)$ 를 얻는다.

$n=r_1q_2+r_2$ 이므로 같은 방법으로 $\gcd\left(f_n(a),f_{r_1}(a)\right)=\gcd\left(f_{r_1}(a),f_{r_2}(a)\right)$도 얻을수 있다. 이 과정을 $r_{n-1}=q_{n+1}r_n+0$ 을 사용할때까지 반복하면 다음을 얻는다.

$$\gcd\left(f_m(a),f_n(a)\right)=\gcd\left(f_n(a),f_{r_1}(a)\right)=\cdots=\gcd\left(f_{r_n}(a),f_0(a)\right)=f_d(a)$$

그러므로 $\gcd\left(f_m(a),f_n(a)\right)=f_d(a)$ 이다. ■

Problem 1.3.6 a는 $a\geq 2$ 를 만족하는 자연수이다. 자연수 m,n에 대하여 $d=\gcd(m,n)$ 라고 하면 $\gcd\left(a^m-1,a^n-1\right)=a^d-1$ 임을 증명하시오.

(증명)
조건에 의하면 적당한 자연수 r,s 가 존재해서 $m=dr,\ n=ds$ 를 만족하고 이때 $\gcd(r,s)=1$ 이다. 그리고 다음 등식을 얻는다.

$$a^m-1=\left(a^d\right)^r-1=\left(a^d-1\right)\left(a^{d(r-1)}+a^{d(r-2)}+\cdots+a^{2d}+a^d+1\right)$$
$$a^n-1=\left(a^d\right)^s-1=\left(a^d-1\right)\left(a^{d(s-1)}+a^{d(s-2)}+\cdots+a^{2d}+a^d+1\right)$$

따라서 $a^d-1\mid a^m-1,\ a^d-1\mid a^n-1$ 이다. 이제 음이 아닌 정수 k에 대하여 다항식 $f_k(x)\in\mathbb{Z}[x]$를 다음과 같이 정의하고

$$f_k(x)=\begin{cases}0 & (k=0)\\ 1+x+x^2+\cdots+x^{k-1} & (k\geq 1)\end{cases}$$

$u=a^d$ 라고 하면 $\gcd(r,s)=1$ 이므로 Problem 1.3.5에 의해 다음을 얻는다.

$$\gcd\left(1+a^d+\cdots+a^{d(r-1)},1+a^d+\cdots+a^{d(s-1)}\right)=\gcd\left(f_r(u),f_s(u)\right)=1$$

그러므로 $\gcd\left(a^m-1,a^n-1\right)=a^d-1$ 이다. ■

1.4 산술의 기본정리

작성자 : 네냐플(Nenyaffle)

1.4절에서는 대학 입학 전에 배운 소수와 합성수를 더 엄밀하고 자세하게 소개하려고 합니다.

제목에 있는 산술의 기본정리는 2 이상의 자연수는 소수의 곱으로 표현할수 있고 곱하는 순서를 무시하면 유일하게 표현할수 있다는 정리입니다. 쉽게 말하면 2 이상의 모든 자연수는 소인수분해를 할수 있다는 정리입니다. 먼저 소수와 합성수를 정의하겠습니다.

Definition 1.4.1 소수(Prime Number), 합성수(Composite Number)
2 이상의 자연수 n에 대하여 n의 양의 약수가 $1, n$ 2개이면 n을 **소수(Prime Number)**라고 정의하고 n이 소수가 아니면 n을 **합성수(Composite Number)**라고 정의한다.

위 정의에 의하면 모든 자연수는 1, 소수, 합성수 셋중 하나입니다. 그리고 합성수의 정의에 의하면 n이 합성수인것과 $1 < a \leq b < n$ 을 만족하는 적당한 자연수 a, b 가 존재해서 $n = ab$ 를 만족하는 것은 동치임을 쉽게 알수 있습니다.

그리고 소수의 정의에 의하면 짝수인 소수는 2가 유일하다는 것도 쉽게 알수 있습니다. $n \geq 3$ 일 때 n이 짝수이면 n은 2를 약수로 갖고 $1 < 2 < n$ 이므로 n은 소수가 될수 없습니다.

산술의 기본정리를 증명하기 위해 먼저 다음 보조정리를 증명하겠습니다.

Lemma 1.4.1 다음이 성립한다.
(a). 임의의 소수 p와 임의의 $a, b \in \mathbb{Z}$ 가 주어져있을 때 $p \mid ab$ 이면 $p \mid a$ 또는 $p \mid b$ 이다.
(b). 임의의 소수 p와 임의의 $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ 가 주어져있을 때 $p \mid a_1 a_2 \cdots a_n$ 이면 $1 \leq k \leq n$ 인 적당한 자연수 k에 대하여 $p \mid a_k$ 이다.
(c). 임의의 소수 $p, q_1, q_2, \ldots q_n$ 가 주어져있을 때 $p \mid q_1 q_2 \cdots q_n$ 이면 $1 \leq k \leq n$ 인 적당한 자연수 k에 대하여 $p = q_k$ 이다.

(증명)
(a). 만약 $p \mid a$ 이면 참이다. $p \nmid a$ 를 가정하자.

$d = \gcd(a, p)$ 라고 하면 $d \mid p$ 인데 p는 소수이므로 $d = 1, p$ 이다.
그런데 $d = p$ 이면 $\gcd(a, p) = p$ 에서 $p \mid a$ 인데 이것은 모순이다.
그러므로 $\gcd(a, p) = 1$ 이다.

따라서 1.2절 Corollary 1.2.2에 의하면 $p \mid b$ 이다. ■

(b). 주어진 명제가 참이 되도록 하는 자연수의 집합을 S 라고 하자.
그러면 $1 \in S$ 임은 명백하다. 이제 임의의 자연수 n에 대하여 $n \in S$ 라고 가정하자.

임의의 $a_1, a_2, ..., a_n, a_{n+1} \in \mathbb{Z}$ 에 대하여 $p \mid a_1 a_2 \cdots a_n a_{n+1}$ 라고 하자.
그러면 (1)에 의해 $p \mid a_1 a_2 \cdots a_n$ 또는 $p \mid a_{n+1}$ 이고 $n \in S$ 이므로 결국
$p \mid a_1, p \mid a_2,$ ..., $p \mid a_{n+1}$ 중 하나가 성립한다.

그러므로 $n+1 \in S$ 이다. 따라서 수학적 귀납법에 의하면 $S = \mathbb{N}$ 이므로
모든 자연수 n에 대하여 주어진 명제는 참이다. ■

(c). (b)에 의하면 $1 \le k \le n$ 인 적당한 자연수 k에 대하여 $p \mid q_k$ 를 만족하고
q_k는 소수이므로 $p = 1$ 또는 $p = q_k$ 인데 p도 소수이므로 $p = q_k$ 가 되어야 한다. ■

Lemma 1.4.1에서 (a)를 **유클리드의 보조정리(Euclid's Lemma)**라고 부릅니다.

Lemma 1.4.1에서 주의할 점은 (a)에서 a, b, (b)에서 $a_1, a_2, ..., a_n$, (c)에서 $q_1, q_2, ..., q_n$
이게 모두 다를 필요는 없습니다. 같은게 있을수도 있습니다. 실제로 3은 소수이고 $3 \mid 3^2$
이므로 Lemma 1.4.1의 (c)에 의해 $3 = 3$ 이라고 해도 됩니다.

Lemma 1.4.2 n이 2 이상의 자연수이면 n의 양의 약수중 소수인 것은 항상 존재한다.

(증명)
n이 소수이면 n의 양의 약수중 소수인 것은 n이므로 명백하다. 따라서 n이 합성수인
경우를 가정하자. 그러면 집합 $S = \{a \in \mathbb{N} : a \mid n, 1 < a < n\}$ 는 공집합이
아니고 자연수 집합의 부분집합이므로 정렬원리에 의하면 가장 작은 원소가 존재한다.

그것을 p라고 하면 p는 n의 약수이다. 이제 p가 소수임을 보이자.

S 의 정의에 의하면 $p \ge 2$ 이다. 따라서 p가 소수가 아니라고 가정하면 p는 합성수이고
그러므로 $1 < q < p < n$ 를 만족하는 적당한 자연수 q가 존재해서 $q \mid p$ 를 만족한다.
그리고 $p \mid n$ 이므로 $q \mid n$ 에서 $q \in S$ 를 얻는다.

이것은 p가 집합 S 의 가장 작은 원소라는 것에 모순이다.
따라서 p는 소수이다. 그러므로 소수인 약수는 항상 존재한다. ■

이제 산술의 기본정리를 증명하겠습니다.

Theorem 1.4.1 산술의 기본정리(Fundamental Theorem of Arithmetic)
n이 2 이상의 자연수이면 n은 소수이거나 소수의 곱으로 표현 가능하다.
그리고 n이 소수의 곱으로 표현될 경우 곱하는 순서를 무시하면 표현방법은 유일하다.

(증명)
n이 소수이면 주어진 정리는 참이므로 n이 합성수인 경우를 가정하자.
그러면 다음 과정으로 n을 소수의 곱으로 표현할수 있다.

1단계 : Lemma 1.4.2에 의하면 n의 양의 약수중 소수인 것이 존재한다. 그것을 p_1 이라고 하면 $1 < n_1 < n$ 을 만족하는 적당한 자연수 n_1이 존재해서 $n = p_1 n_1$ 을 만족한다.

2단계 : 만약 n_1이 소수이면 n은 소수의 곱으로 표현되었다. 만약 n_1이 소수가 아니면 $1 < n_1 < n$ 이므로 n_1은 합성수이고 따라서 Lemma 1.4.2에 의하면 n_1의 양의 약수중 소수인 것이 존재한다. 그것을 p_2라고 하면 $1 < n_2 < n_1$ 을 만족하는 적당한 자연수 n_2가 존재해서 $n_1 = p_2 n_2$ 를 만족한다. 따라서 $n = p_1 p_2 n_2$ 이다.

3단계 : 만약 n_2가 소수이면 n은 소수의 곱으로 표현되었다. 만약 n_2가 소수가 아니면 $1 < n_2 < n_1$ 이므로 n_2는 합성수이고 따라서 Lemma 1.4.2에 의하면 n_2의 양의 약수중 소수인 것이 존재한다. 그것을 p_3이라고 하면 $1 < n_3 < n_2$ 를 만족하는 적당한 자연수 n_3이 존재해서 $n_2 = p_3 n_3$ 을 만족한다. 따라서 $n = p_1 p_2 p_3 n_3$ 이다.

…

위 과정을 반복하면 $n > n_1 > n_2 > n_3 > \cdots > 1$ 이고 $n, n_1, n_2, n_3, \ldots$ 은 자연수이므로 위 과정은 언젠가 종료되어야 한다. 그러므로 n_k가 소수가 되도록 하는 자연수 k는 존재하고 $n_k = p_k$ 라고 하면 $n = p_1 p_2 \cdots p_k$ 이다.

따라서 합성수 n은 소수의 곱으로 표현된다. 이제 곱하는 순서를 무시했을 때 표현방법이 유일함을 보이자.

n을 소수의 곱으로 표현한 것을 $n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ 라고 하자. 여기서 r, s 는 자연수이고 $p_1 \le p_2 \le \cdots \le p_r$, $q_1 \le q_2 \le \cdots \le q_s$ 를 만족한다고 가정한다.

그러면 $p_1 \mid q_1 q_2 \cdots q_s$ 이므로 Lemma 1.4.1에 의하면 $1 \le i \le s$ 를 만족하는 적당한 자연수 i에 대하여 $p_1 = q_i \ge q_1$ 을 만족한다. 마찬가지로 $q_1 \mid p_1 p_2 \cdots p_r$ 이므로 $1 \le j \le r$ 을 만족하는 적당한 자연수 j에 대하여 $q_1 = p_j \ge p_1$ 을 만족한다.

따라서 $p_1 = q_1$ 이다. 그러므로 $p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s$ 이고 위 과정을 똑같이 반복하면 $p_2 = q_2$ 를 얻는다. 이것을 계속 반복하자. 그러면 $r = s$ 가 되어야 한다.

만약 $r \neq s$ 이면 $r > s$ 일 경우 위 과정을 s번 반복했을 때 $p_{s+1} p_{s+2} \cdots p_r = 1$ 이므로 모순이고 $r < s$ 일 경우 위 과정을 r번 반복했을 때 $q_{r+1} q_{r+2} \cdots q_s = 1$ 이므로 모순이다. 따라서 $r = s$ 이고 $p_1 = q_1, p_2 = q_2, \ldots, p_r = q_r$ 을 얻는다.

즉, 곱하는 순서를 무시하면 합성수를 소수의 곱으로 표현하는 방법은 유일하다. ■

Corollary 1.4.1 n이 2 이상의 자연수이면 적당한 서로 다른 소수 $p_1,p_2,...,p_r$ 과 적당한 자연수 $k_1,k_2,...,k_r$ 이 존재해서 $n=p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ 를 만족한다.

(증명)
산술의 기본정리에 의하면 명백하다. ■

산술의 기본정리 증명과정을 보고 n을 소인수분해 하면 소수의 거듭제곱꼴이 안나온다고 오해하는 경우가 있는데 증명과정을 잘 보면 다음 부등식에 등호가 포함되어 있습니다.

$$p_1 \le p_2 \le \cdots \le p_r,\ q_1 \le q_2 \le \cdots \le q_s$$

즉, 저 소수중엔 같은 소수가 있을수도 있고 같은 소수를 곱하면 거듭제곱꼴이 나옵니다.

산술의 기본정리에서 곱하는 순서를 무시하는 이유는 간단합니다. 순서를 무시하지 않으면 $21=3\times7=7\times3$ 처럼 소수의 곱으로 유일하게 표현할수 없는 경우가 발생합니다.

1을 소수로 정의하지 않는 이유도 마찬가지인데 1을 소수로 정의하면 $21=1\times3\times7=1^2\times3\times7=1^3\times3\times7=\cdots$ 이므로 소수의 곱으로 유일하게 표현할수 없기 때문입니다.

산술의 기본정리도 유클리드 호제법처럼 알고리즘을 유한번 반복해서 증명하는데 산술의 기본정리에서 사용한 알고리즘은 유클리드 호제법과 달리 실제로 어떤 자연수를 소인수분해 할 때 사용하기가 불편합니다.

산술의 기본정리 알고리즘은 정렬원리를 사용하는데 정렬원리는 가장 작은 원소가 존재한다는 것만 알려주고 그것을 찾는 방법을 알려주지 않기 때문입니다. 그래서 실제로 2 이상의 자연수 n을 소인수분해 하려면 n 이하의 소수로 일일이 나눠볼 수밖에 없습니다.

그런데 어떤 자연수가 소수인지 판정하는 것도 쉬운게 아니라서 어떤 자연수를 소인수분해 하는것도 쉬운게 아닙니다. 실제로 어떤 자연수가 소수인지 판정하는게 어렵기 때문에 그것을 이용해서 만든 RSA 암호가 많이 사용되고 있는겁니다.

2 이상의 자연수 n이 주어져있을 때 기계의 도움 없이 손계산으로 n보다 작거나 같은 소수를 찾는 방법은 사실상 고대 그리스 시대에 나온 **에라토스테네스의 체(Sieve of Eratosthenes)**가 유일합니다. 원리는 단순한데 소개하기 전에 먼저 다음을 증명하겠습니다.

Theorem 1.4.2 n이 합성수이면 다음을 만족하는 소수 p가 존재한다.

$$p \mid n,\ p \le \sqrt{n} \tag{19}$$

(증명)
조건에 의하면 $1<a\le b<n$ 을 만족하는 적당한 자연수 a,b 가 존재해서 $n=ab$ 를 만족한다. 따라서 $n=ab\ge a^2$ 이므로 $a\le\sqrt{n}$ 이다.

a가 소수이면 a는 (19)를 만족한다. a가 합성수이면 Lemma 1.4.2에 의해 $p\mid a$ 를 만족하는 소수 p는 존재하고 이때 $p\le a\le\sqrt{n}$ 이므로 p는 (19)를 만족한다. ■

Theorem 1.4.2는 2 이상의 자연수 n이 소수인지 확인하는 수고를 조금 덜어주는 역할을 해줍니다. $\sqrt{n}$ 보다 작은 어떤 소수도 n을 나누지 않으면 Theorem 1.4.2에 의해 n은 소수라는 것을 알수 있습니다.

예를 들어 97이 소수인지 확인하려면 $9 < \sqrt{97} < 10$ 이므로 10보다 작은 소수 $2, 3, 5, 7$ 가 97을 나누는지 확인하면 충분합니다. 실제로 나눠보면 나누지 못한다는 것을 알수 있고 그러므로 97은 소수입니다. 97보다 작은 모든 소수로 나누어볼 필요가 없습니다.

에라토스테네스의 체는 이런식으로 n보다 작거나 같은 소수를 찾는 방법입니다.

원리는 단순합니다. 2 이상의 자연수 n이 임의로 주어져있을 때 $a \leq n$ 을 만족하는 합성수 a를 임의로 하나 택합니다. 그러면 Theorem 1.4.2에 의해 $p \mid a, p \leq \sqrt{a}$ 를 만족하는 소수 p가 존재하고 $\sqrt{a} \leq \sqrt{n}$ 이므로 $p \leq \sqrt{n}$ 입니다.

즉, n 이하의 모든 합성수는 $\sqrt{n}$ 보다 작은 소수에 의해 나누어지기 때문에 1부터 n까지 나열해놓고 1을 지운뒤 $\sqrt{n}$ 보다 작은 소수의 배수도 다 지우면 결국 n보다 작거나 같은 소수만 남아있게 됩니다.

$n = 50$ 이면 $7 < \sqrt{50} < 8$ 이므로 8보다 작은 소수는 $2, 3, 5, 7$ 이고 1부터 50까지의 자연수중 2의 배수, 3의 배수, 5의 배수, 7의 배수와 추가로 1을 전부 다 지우면 다음을 얻습니다.

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
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~~

그러므로 남는건 $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47$ 이고 이게 50 이하의 모든 소수입니다. 기계의 도움 없이 손계산으로 소수를 구하는 방법은 사실상 에라토스테네스의 체가 유일합니다.

이제 소수 그 자체에 대한 이야기를 하겠습니다. 처음에 어떤 자연수가 소수인지 판정하는 것은 쉬운게 아니라고 이야기했는데 여기서 소수는 무한하다는 것을 어느정도 눈치챌수 있습니다. 소수가 유한하다면 컴퓨터를 사용하는 현대에는 모든 소수를 다 구해놓았을겁니다.

소수가 무한하다는 것을 수학적으로 처음 증명한 수학자는 유클리드입니다.

Theorem 1.4.3 소수의 개수는 무한하다.

(증명)
결론을 부정해서 소수의 개수가 유한하다고 하자. 소수의 개수를 k라고 하고 모든 소수를 $p_1,p_2,...,p_k$ 라고 하자. 그리고 $n=1+p_1p_2\cdots p_k$ 라고 하자.

그러면 $n\geq 2$ 이므로 Lemma 1.4.2에 의하면 $p\mid n$ 을 만족하는 소수 p가 존재하고 따라서 적당한 $i\in\{1,2,...,k\}$ 에 대하여 $p=p_i$ 를 만족한다.

그러므로 $p=p_i\mid p_1p_2\cdots p_k$ 이고 $p\mid n$ 이므로 $p\mid n-p_1p_2\cdots p_k=1$ 인데 이것은 p가 소수라는 것에 모순이다. 따라서 소수의 개수는 무한하다. ■

Theorem 1.4.3의 증명에 의하면 다음을 알수 있습니다. 소수를 작은 순서대로 나열했을 때 n번째 소수를 p_n 이라고 정의하면 $a=1+p_1p_2\cdots p_n$ 라고 할 때 $a>p_n$ 입니다.

그리고 $\{p_n\}$이 증가수열임은 명백하므로 a는 $p_1,p_2,...,p_n$ 보다 큰 자연수입니다.
따라서 a가 소수이면 $n+1$ 번째 소수는 a보다 작거나 같으므로 $p_{n+1}\leq a$ 입니다.

a가 합성수이면 Lemma 1.4.2에 의해 $p\mid a$ 를 만족하는 소수 p가 존재합니다.
그런데 a는 $p_1,p_2,...,p_n$ 으로 나누지 못하므로 $p\geq p_{n+1}$ 이어야 하고 $p\mid a$ 이므로 $p_{n+1}\leq p\leq a$ 를 만족합니다.

따라서 모든 자연수 n에 대하여 $p_{n+1}\leq 1+p_1p_2\cdots p_n$ 을 만족합니다.
이 부등식을 가지고 다음을 증명할수 있습니다.

Theorem 1.4.4 n번째 소수를 p_n 이라고 하면 $p_n\leq 2^{2^{n-1}}$ 가 성립한다.

(증명)
집합 S 를 $S=\left\{n\in\mathbb{N}:p_n\leq 2^{2^{n-1}}\right\}$ 라고 하자. 그러면 $p_1=2$ 이므로 $1\in S$ 이다.
이제 임의의 자연수 n에 대하여 $1,2,...,n\in S$ 라고 가정하자.
그러면 $p_{n+1}\leq 1+p_1p_2\cdots p_n$ 이므로 다음을 얻는다.

$$\begin{aligned}
p_{n+1} &\leq 1+p_1p_2\cdots p_n \\
&\leq 1+2\times 2^2\times\cdots\times 2^{2^{n-1}} \\
&= 1+2^{1+2+2^2+\cdots+2^{n-1}} \\
&= 1+2^{2^n-1} \\
&\leq 2^{2^n-1}+2^{2^n-1} \\
&= 2^{2^n}
\end{aligned}$$

따라서 $n+1 \in S$ 이다. 그러므로 강한 귀납법에 의하면 $S = \mathbb{N}$ 이고
모든 자연수 n에 대하여 $p_n \leq 2^{2^{n-1}}$ 가 성립한다. ■

Theorem 1.4.4는 p_n은 어떤 값보다 작다는 사실을 알려주는데 $2^{2^{n-1}}$ 은 너무 큰 수라서 좋은 정리는 아닙니다. $p_5 = 11$ 인데 $2^{2^{5-1}} = 2^{16} = 65536$ 이라서 그렇습니다.

베르트랑의 공준(Bertrand's Postulate)이라고 부르는 정리를 이용하면 부등식을 좀 더 좋게 만들수 있습니다. 베르트랑의 공준은 $n \geq 2$ 인 모든 자연수 n에 대하여 $n < p < 2n$ 을 만족하는 소수 p가 항상 존재한다는 정리입니다.

베르트랑의 공준을 이용하면 다음을 증명할수 있습니다.

Theorem 1.4.5 n번째 소수를 p_n 이라고 하면 $p_n \leq 2^n$ 가 성립한다.

(증명)
모든 자연수 n에 대하여 $p_n \geq 2$ 이므로 베르트랑의 공준에 의하면 모든 자연수 n에 대하여 $p_n < p < 2p_n$ 를 만족하는 소수 p가 존재한다. 따라서 적당한 자연수 k에 대하여 $p = p_k$ 이므로 $p_n < p_k < 2p_n$ 이고 $\{p_n\}$은 증가수열이므로 $k \geq n+1$ 이다.

그러므로 $p_n < p_{n+1} \leq p_k < 2p_n$ 에서 $p_{n+1} < 2p_n$ 을 얻는다.
이제 집합 S 를 $S = \{n \in \mathbb{N} : p_n \leq 2^n\}$ 라고 하자. 그러면 $p_1 = 2$ 이므로 $1 \in S$ 이다. 임의의 자연수 n에 대하여 $n \in S$ 라고 하자.

그러면 $p_n \leq 2^n$ 이므로 $p_{n+1} < 2p_n \leq 2^{n+1}$ 에서 $p_{n+1} \leq 2^{n+1}$ 을 얻는다.
$a \leq b$ 는 '$a = b$ 또는 $a < b$' 와 동치이므로 $p_{n+1} < 2^{n+1}$ 이면 $p_{n+1} \leq 2^{n+1}$ 가 성립한다고 말할수 있다.

따라서 $n+1 \in S$ 이므로 수학적 귀납법에 의하면 $S = \mathbb{N}$ 이다.
즉, 모든 자연수 n에 대하여 $p_n \leq 2^n$ 가 성립한다. ■

$2^{2^{n-1}}$은 2^n에 비하면 굉장히 큰 수이므로 $p_n \leq 2^{2^{n-1}}$ 를 $p_n \leq 2^n$ 로 바꾼것도 의미있는 결과입니다. 그런데 2^n도 나름대로 큰 수라서 $p_{10} = 29$ 인데 $2^{10} = 1024$ 가 됩니다. 여전히 큰 차이가 있습니다.

베르트랑의 공준에 의하면 $n \geq 2$ 일 때 n과 $2n$ 사이에는 소수가 항상 존재합니다.
즉, 2와 4 사이, 3과 6 사이, 4와 8 사이, 5와 10 사이, ..., 99와 198 사이, 100과 200 사이, 101과 202 사이, ... 에는 소수가 항상 존재합니다.

그래서 $k \geq 2$ 일 때 합성수가 k번 연속으로 나오게 만드는 자연수 k가 존재하지 않을수도 있다고 생각할수 있는데 실제로는 그렇지 않습니다.

$k \geq 2$ 를 만족하는 임의의 자연수 k에 대하여 다음 k개의 자연수를 생각하면

$$2+(k+1)!, 3+(k+1)!, \ldots, (k+1)+(k+1)! \tag{20}$$

$2 \leq j \leq k+1$ 일 때 $j \mid j+(k+1)!$ 이므로 (20)은 모두 합성수입니다.
즉, $k \geq 2$ 를 만족하는 임의의 k에 대하여 연속한 k개의 합성수는 항상 존재합니다.

Problem 1.4.1 p_n을 n번째 소수라고 할 때 다음을 증명하시오.

(a). $p_n \geq 2n-1$ 이다.

(b). $n \geq 4$ 이면 $p_{n+1}^2 < p_1 p_2 \cdots p_n$ 이다.

(c). $1+p_1 p_2 \cdots p_n$ 은 완전제곱수가 될수 없다.

(d). $\frac{1}{p_1}+\frac{1}{p_2}+\cdots+\frac{1}{p_n}$ 은 자연수가 될수 없다.

(풀이)

(a). 짝수인 소수는 2가 유일하다. 즉, $n \geq 2$ 이면 p_n은 모두 홀수이므로 $n \geq 2$ 이면 $p_{n+1}-p_n \geq 2$ 가 성립한다는 것을 쉽게 알수 있다.

집합 S 를 $S=\{n \in \mathbb{N} : p_n \geq 2n-1\}$ 라고 하자. 그러면 $p_1 = 2$ 이므로 $1 \in S$ 이다. 이제 임의의 자연수 n에 대하여 $n \in S$ 라고 가정하면 $p_n \geq 2n-1$ 이다.

$n=1$ 이면 $p_2 = 3$ 이므로 $2 \in S$ 이다. $n \geq 2$ 이면 $p_{n+1}-p_n \geq 2$ 이므로 $p_{n+1} \geq p_n+2 \geq (2n-1)+2 = 2n+1$ 에서 $n+1 \in S$ 이다.

따라서 어느 경우든 $n+1 \in S$ 이다. 그러므로 수학적 귀납법에 의하면 $S=\mathbb{N}$ 이므로 $p_n \geq 2n-1$ 가 성립한다. ■

(b). 집합 S 를 $S=\{n \in \mathbb{N} : p_{n+1}^2 < p_1 p_2 \cdots p_n\}$ 라고 하자. 그러면 $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, p_5 = 11$ 이므로 간단한 계산에 의해 $1, 2, 3 \notin S$ 이고 $4 \in S$ 임을 쉽게 알수 있다.

이제 $n \geq 4$ 를 만족하는 임의의 자연수 n에 대하여 $n \in S$ 라고 가정하자.
그러면 $p_{n+1}^2 < p_1 p_2 \cdots p_n$ 이고 Theorem 1.4.5의 증명과정에서 $p_{n+2} < 2p_{n+1}$ 이다. 그리고 $n \geq 4$ 이면 $p_{n+1} > 4$ 이므로 다음을 얻는다.

$$p_{n+2}^2 < 4p_{n+1}^2 < 4p_1 p_2 \cdots p_n < p_1 p_2 \cdots p_{n+1}$$

따라서 $n+1 \in S$ 이다. 그러므로 수학적 귀납법의 원리에 의하면 $S = \mathbb{N} - \{1,2,3\}$ 이다. 즉, $n \geq 4$ 이면 $p_{n+1}^2 < p_1 p_2 \cdots p_n$ 가 성립한다.

(c). $p_1 = 2$ 이고 $n \geq 2$ 이면 p_n은 홀수이므로 모든 자연수 n에 대하여 $p_1 p_2 \cdots p_n$ 은 짝수이고 4의 배수는 아니다. 그러므로 $k \in \mathbb{Z}$ 에 대하여 $p_1 p_2 \cdots p_n = 4k+2$ 이런 형태로 표현되고 따라서 $1 + p_1 p_2 \cdots p_n = 4k+3$ 이다.

즉, $1 + p_1 p_2 \cdots p_n$ 은 4로 나누면 나머지가 3이므로 완전제곱수가 될수 없다. ■

(d). 결론을 부정해서 적당한 자연수 n에 대하여 $s = \frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_n}$ 가 자연수라고 가정하자. 그러면 $s = \frac{p_2 p_3 \cdots p_n + p_1 p_3 \cdots p_n + \cdots + p_1 p_2 \cdots p_{n-1}}{p_1 p_2 \cdots p_n}$ 가 자연수이므로 $p_1 p_2 \cdots p_n \mid p_2 p_3 \cdots p_n + p_1 p_3 \cdots p_n + \cdots + p_1 p_2 \cdots p_{n-1}$ 이다.

그러면 $p_1 \mid p_1 p_2 \cdots p_n$ 이므로 $p_1 \mid p_2 p_3 \cdots p_n + p_1 p_3 \cdots p_n + \cdots + p_1 p_2 \cdots p_{n-1}$ 이고 우변에서 p_1을 포함한 식은 p_1에 의해 나누어지므로 결국 $p_1 \mid p_2 p_3 \cdots p_n$ 을 얻는다.

그런데 $p_1 = 2$ 이고 $p_2 p_3 \cdots p_n$ 은 홀수이므로 이것은 모순이다.
따라서 주어진 식은 자연수가 될수 없다. ■

Problem 1.4.2 다음을 증명하시오.

(a). $a \geq 2$ 인 자연수 a와 $n \geq 2$ 인 자연수 n이 임의로 주어져있을 때 $a^n - 1$ 이 소수이면 $a = 2$ 이고 n은 소수이다.

(b). 자연수 n이 임의로 주어져있을 때 $2^n + 1$ 이 소수이면 음이 아닌 정수 m이 존재해서 $n = 2^m$ 을 만족한다.

(증명)

(a) $a^n - 1 = (a-1)\left(a^{n-1} + a^{n-2} + \cdots + a^2 + a + 1\right)$ 이므로 조건에 의하면 $a - 1 = 1$ 또는 $a^{n-1} + a^{n-2} + \cdots + a^2 + a + 1 = 1$ 인데 $a \geq 2$ 이므로 $a^{n-1} + a^{n-2} + \cdots + a^2 + a + 1 > 1$ 이다. 따라서 $a - 1 = 1$ 이므로 $a = 2$ 이다.

결론을 부정해서 n이 소수가 아니라고 하자. 그러면 $n \geq 2$ 이므로 n은 합성수이고 따라서 $1 < r \leq s < n$ 을 만족하는 적당한 자연수 r, s 에 대하여 $n = rs$ 이다. 그러므로 다음을 얻는다.

$$\begin{aligned} 2^n - 1 &= \left(2^r\right)^s - 1 \\ &= \left(2^r - 1\right)\left(2^{r(s-1)} + 2^{r(s-2)} + \cdots + 2^{2r} + 2^r + 1\right) \end{aligned}$$

$r>1$ 이므로 $2^r-1>1$ 이고 $2^r-1 \mid 2^n-1$ 인데 이것은 2^n-1 이 소수라는 조건에 모순이다. 따라서 n은 소수이다. ■

(b). 산술의 기본정리에 의하면 적당한 음이 아닌 정수 m과 적당한 홀수 k가 존재해서 $n=2^m k$ 라고 표현할수 있고 k는 홀수이므로 다음을 얻는다.

$$\begin{aligned} 2^n+1 &= \left(2^{2^m}\right)^k+1 \\ &= \left(2^{2^m}+1\right)\left(2^{2^m(k-1)}+2^{2^m(k-2)}+\cdots+2^{2^m}+1\right) \end{aligned}$$

m은 음이 아닌 정수이므로 $2^{2^m}+1 \geq 3$ 이다. 따라서 조건에 의하면 $2^{2^m(k-1)}+2^{2^m(k-2)}+\cdots+2^{2^m}+1=1$ 이 되어야 한다.

만약 $k \neq 1$ 이면 $k \geq 3$ 이므로 $2^{2^m(k-1)} \geq 4$ 이고 이 경우 $2^{2^m(k-1)}+2^{2^m(k-2)}+\cdots+2^{2^m}+1>1$ 이므로 조건에 모순이다.
따라서 $k=1$ 이고 그러므로 $n=2^m$ 이다. ■

Problem 1.4.2에서 $n \geq 2$ 일 때 2^n-1 형태의 소수를 **메르센 소수(Mersenne Prime)** 라고 부르고 n이 음이 아닌 정수일 때 $2^{2^n}+1$ 형태의 소수를 **페르마 소수(Fermat Prime)** 라고 부릅니다.

메르센 소수는 현재까지 발견된 가장 큰 소수를 발표할 때 많이 등장합니다.
2018년 1월 기준으로 현재까지 발견된 가장 큰 소수는 $2^{77232917}-1$ 입니다. 이 소수는 23249425 자리 자연수이고 따라서 표현하려면 숫자를 2천만개 이상 써야합니다.

소수의 개수는 무한하지만 어떤 자연수가 소수인지 아닌지 판정하는 것이 어렵기 때문에 현재까지 발견된 가장 큰 소수를 찾으면 컴퓨터의 계산능력을 자랑할수 있게 되고 그래서 현재까지 발견된 가장 큰 소수보다 더 큰 소수를 계속 발견해서 발표하려고 하는겁니다.

수학에서도 중요하다고 생각할수 있는데 효율적인 알고리즘을 만드는것도 수학의 영역과 겹치는 부분이 있기 때문입니다.

한편 **완전수(Perfect Number)**라고 부르는 자연수가 있는데 자연수 n이 완전수인 것은 n의 양의 약수의 합이 $2n$이 되는 수로 정의합니다. 예를 들면 6의 양의 약수는 $1,2,3,6$ 이고 $1+2+3+6=12$ 이므로 6은 완전수입니다.

수학자 오일러가 n이 짝수일 때 n이 완전수일 필요충분조건은 2^m-1 이 소수가 되도록 하는 적당한 소수 m이 존재해서 $n=2^{m-1}\left(2^m-1\right)$ 을 만족하는 것임을 증명했습니다. 따라서 짝수인 완전수와 메르센 소수는 일대일 대응이 됩니다.

메르센 소수의 개수가 유한하지 무한한지는 아직 증명되지 않았기 때문에 짝수인 완전수의 개수도 유한하지 무한한지 아직 증명되지 않았습니다. 그리고 홀수인 완전수의 존재성은 아직 밝혀지지 않았습니다.

페르마 소수는 작도가능성과 관련이 있습니다. 이것은 체론을 배우면 증명할수 있는데 $n \geq 3$ 일 때 정n각형이 눈금없는 자와 컴퍼스만 가지고 작도가능할 필요충분조건은 적당한 음이 아닌 정수 k와 $F(m)=2^{2^m}+1$ 이 소수가 되도록 하는 서로 다른 자연수 $m_1, m_2, ..., m_r$ 가 존재해서 $n=2^k$ 또는 $n=2^k F(m_1)F(m_2)\cdots F(m_r)$ 입니다.

Problem 1.4.2의 역은 성립하지 않습니다. $M(n)=2^n-1$ 라고 하면 $n=2,3,5,7$ 일 때 $M(n)$ 은 소수인데 $M(11)=2^{11}-1=2047=23\times 89$ 이므로 $n=11$ 일 때 소수가 아닙니다.

마찬가지로 $n=0,1,2,3,4$ 일 때 $F(n)$은 소수인데 $F(5)=2^{32}+1=4294967297=641\times 6700417$ 이므로 $n=5$ 일 때 소수가 아닙니다. $F(5)$의 소인수분해를 발견한 수학자는 오일러입니다.

현대에는 컴퓨터를 이용하면 4294967297 을 소인수분해 하는건 어렵지 않지만 오일러가 살던 시대에는 컴퓨터가 없었기 때문에 이것을 소인수분해 하는 것은 어려운 일이었습니다. 손계산으로 $641 \mid F(5)$ 임을 좀 더 간단하게 보이는 방법중 하나는 다음과 같습니다.

$a=2^7$, $b=5$ 라고 하면 $1+ab=641$ 이고 $1+ab-b^4=2^4$ 입니다.
그러므로 다음 등식을 얻습니다.

$$\begin{aligned} F(5) &= 2^{32}+1 \\ &= 2^4a^4+1 \\ &= (1+ab-b^4)a^4+1 \\ &= (1+ab)a^4+1-a^4b^4 \\ &= (1+ab)\left(a^4+(1-ab)(1+a^2b^2)\right) \end{aligned}$$

$1+ab=641$ 이므로 $641 \mid F(5)$ 임을 알수 있습니다.

현재까지 알려진 페르마 소수는 다음 5개밖에 없습니다.

$$\begin{aligned} F(0)&=2^{2^0}+1=2+1=3 \\ F(1)&=2^{2^1}+1=2^2+1=5 \\ F(2)&=2^{2^2}+1=2^4+1=17 \\ F(3)&=2^{2^3}+1=2^8+1=257 \\ F(4)&=2^{2^4}+1=2^{16}+1=65537 \end{aligned}$$

2018년 1월 기준으로 $5 \leq n \leq 32$ 일 때 $F(n)$이 합성수라는 것이 밝혀졌고 이들중 소인수분해가 완벽하게 된 경우는 $5 \leq n \leq 11$ 까지입니다. 합성수임을 알지만 소인수분해가 완벽하게 안된 경우가 있다는 것이 이상하다고 생각할수 있는데 페르마 소수는 매우 큰 수이기 때문에 소인수분해를 하는게 쉽지 않습니다.

페르마 소수의 개수도 유한한지 무한한지 아직 밝혀지지 않았지만 페르마 소수는 너무 크기 때문에 다루기가 쉽지 않습니다. 그래서 페르마 소수는 5개밖에 없을거라고 부정적인 추측을 하는 수학자들도 많습니다.

현재 가장 큰 소수를 계산해서 발표하는게 주목을 받는 이유도 자연수를 대입했을 때 소수만 나오는 계산하기 쉬운 함수식이 아직 발견되지 않았기 때문입니다. 메르센 소수의 식과 페르마 소수의 식도 항상 소수만 나오는건 아닙니다.

함수식중 계산하기 쉬운 것은 다항식인데 정수를 대입했을 때 소수만 나오는 정수 계수 다항식은 상수다항식밖에 없어서 의미가 없습니다. 그 사실을 증명하기 전에 알아야 하는 정리가 있는데 바로 **대수학의 기본정리(Fundamental Theorem of Algebra)**입니다.

대수학의 기본정리는 대학 입학 전에 들어본적이 있을겁니다. 임의의 다항식 $f(x)\in\mathbb{C}[x]$ 에 대하여 $f(x)$가 상수다항식이 아니면 $f(a)=0$ 을 만족하는 $a\in\mathbb{C}$ 가 존재한다는 것이 대수학의 기본정리입니다. 이것은 복소해석학을 배우면 증명할수 있습니다.

대수학의 기본정리로 다음을 얻을수 있는데 상수다항식이 아닌 다항식 $f(x)\in\mathbb{C}[x]$가

$$f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n\ (a_n\neq 0)$$

이면 적당한 $z_1,z_2,\ldots,z_n\in\mathbb{C}$ 가 존재해서 다음을 만족합니다.

$$f(x)=a_n(x-z_1)(x-z_2)\cdots(x-z_n) \tag{21}$$

다음 정리를 증명하려면 (21)을 이용해야 합니다.

Theorem 1.4.6 정수계수 다항식 $f(x)\in\mathbb{Z}[x]$가 모든 $n\in\mathbb{Z}$ 에 대해 $f(n)$이 소수라는 조건을 만족하면 $f(x)$는 상수다항식이다.

(증명)

정수계수 다항식 $f(x)\in\mathbb{Z}[x]$가 다음과 같다고 하자.

$$f(x)=a_0+a_1x+a_2x^2+\cdots+a_mx^m\ (a_m\neq 0)$$

적당한 정수 n_0와 소수 p에 대하여 $f(n_0)=a_0+a_1n_0+a_2n_0^2+\cdots+a_mn_0^m=p$

라고 하면 이항정리에 의해 적당한 $g(x)\in\mathbb{Z}[x]$가 존재해서 모든 $n\in\mathbb{Z}$ 에 대하여 다음 등식이 성립한다는 것을 쉽게 알수 있다.

$$\begin{aligned}f(n_0+pn)&=a_0+a_1(n_0+pn)+a_2(n_0+pn)^2+\cdots+a_m(n_0+pn)^m\\&=(a_0+a_1n_0+a_2n_0^2+\cdots+a_mn_0^m)+pg(n)\\&=f(n_0)+pg(n)\\&=p(1+g(n))\end{aligned}$$

따라서 $p\mid f(n_0+pn)$ 이고 p는 소수인데 조건에 의하면 $f(n_0+pn)$ 은 소수이므로 Lemma 1.4.1에 의하면 $p=f(n_0+pn)$ 이다. 즉, 모든 정수 n에 대하여 $x=n_0+pn$ 이것은 방정식 $f(x)=p$ 의 해가 된다.

그러므로 $f(x)$는 상수다항식이 되어야 한다. 만약 $f(x)$가 상수다항식이 아니면 $h(x)\in\mathbb{Z}[x]$를 $h(x)=f(x)-p$ 라고 정의할 때 $h(x)$는 상수다항식이 아니고 $h(x)\in\mathbb{C}[x]$이므로 (21)에 의하면 $h(x)=0$ 즉, $f(x)=p$ 의 해의 개수는 유한하다.

그런데 방정식 $f(x)=p$ 는 모든 $n\in\mathbb{Z}$ 에 대하여 $x=n_0+pn$ 를 해로 가지므로 방정식 $f(x)=p$ 의 해의 개수는 무한하다. 이것은 모순이므로 $f(x)$는 상수다항식이다. ■

재미있는 사실은 연속한 40개의 음이 아닌 정수를 대입했을 때 소수만 나오는 다항식이 있습니다. $f(n)=n^2+n+41$ 은 $0\le n\le 39$ 이면 모두 소수이고 $f(40)=41^2$ 이므로 소수가 아닙니다.

정수를 대입했을 때 소수가 나오는 계산하기 쉬운 함수식에 대해 현재까지 알려진 것은 다음 정리 뿐입니다.

Theorem 1.4.7 디리클레의 정리(Dirichlet's Theorem)
a,b 가 $\gcd(a,b)=1$ 을 만족하는 자연수이면 첫항이 a이고 공차가 b인 다음 등차수열의 항에는 소수가 무한한 횟수로 나타난다.

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

디리클레의 정리는 쉽게 말하면 $\gcd(a,b)=1$ 일 때 $a+bn$ 이 소수가 되도록 하는 음이 아닌 정수 n의 개수가 무한하다는 것을 말해줍니다. 정리는 간단하지만 증명은 간단하지 않습니다. Stein 푸리에해석 책에 증명이 나와있으니 궁금하면 참고하길 바랍니다.

디리클레의 정리는 소수의 개수가 무한하다는 것보다 더 강한 결과를 줍니다. 디리클레의 정리에 의하면 소수의 개수가 무한하다는 것은 명백하기 때문입니다.

디리클레의 정리에 의하면 일의 자리의 숫자가 3인 소수의 개수가 무한하다는 것도 쉽게 알수 있습니다. $a=10,\ b=3$ 이라고 하면 $\gcd(a,b)=1$ 이므로 디리클레의 정리에 의해 $10n+3$ 이 소수가 되도록 하는 음이 아닌 정수 n의 개수는 무한하고 n이 음이 아닌 정수이면 $10n+3$ 은 일의 자리의 숫자가 3인 자연수입니다.

자연수를 대입했을 때 소수만 나오는 다항식은 존재하지 않는다는 것을 증명했는데 대입하는 자연수의 개수가 유한하면 소수만 주는 다항식은 얼마든지 만들 수 있고 심지어 등차수열로 만들 수 있습니다.

수학자 벤 그린과 테렌스 타오가 증명한 **그린-타오 정리(Green-Tao Theorem)**가 있는데 정리 자체는 간단합니다. 임의의 자연수 k가 주어졌을 때 k번 연속으로 소수만 나오는 유한한 등차수열이 항상 존재한다는 정리입니다. 예를 들면 다음과 같습니다.

$k=1$ 이면 2
$k=2$ 이면 $2,3$, 이 경우 공차는 1
$k=3$ 이면 $3,5,7$, 이 경우 공차는 2
$k=4$ 이면 $5,11,17,23$, 이 경우 공차는 6

$k=5$ 이면 $5, 11, 17, 23, 29$, 이 경우 공차는 6
$k=6$ 이면 $7, 37, 67, 97, 127, 157$, 이 경우 공차는 30
$k=7$ 이면 $7, 157, 307, 457, 607, 757, 907$, 이 경우 공차는 150
$\vdots$

테렌스 타오는 2006년에 이 정리를 증명한 공로로 필즈메달을 받았습니다. 하지만 이 정리도 만능은 아닌게 그린-타오 정리는 소수만 나오는 유한한 등차수열을 찾는 방법을 구체적으로 제시해주지 않습니다. 그래서 소수만 k번 등장하는 등차수열을 찾는건 다른 문제입니다.

지금까지 발견된 등차수열중 소수만 나오는 횟수가 가장 큰 것은 다음 수열이라고 합니다.

$$43142746595714191 + 5283234035979900n \ (0 \le n \le 25)$$

위 수열의 공차 5283234035979900 를 소인수분해한 결과는 다음과 같은데

$$2^2 \times 3 \times 5^2 \times 7^2 \times 11 \times 13 \times 17 \times 19 \times 23 \times 373 \times 907$$

잘 보면 26보다 작은 모든 소수를 약수로 갖는다는 것을 알수 있습니다.
이것을 일반화한게 다음 정리입니다.

Theorem 1.4.8 n은 $n \ge 3$ 을 만족하는 자연수이고 d는 자연수, p는 소수일 때 다음 유한한 n개의 등차수열의 모든 항이 소수라고 가정하자.

$$p, p+d, p+2d, \ ..., p+(n-1)d \tag{22}$$

그러면 d는 $q < n$ 을 만족하는 모든 소수 q를 약수로 갖는다.

(증명)
결론을 부정해서 $q < n$ 과 $q \nmid d$ 를 동시에 만족하는 소수 q가 존재한다고 하자.
그리고 다음 q개의 등차수열의 서로 다른 항은 q로 나누었을 때 나머지가 모두 다르다는 것을 증명하자.

$$p, p+d, p+2d, \ ..., p+(q-1)d \tag{23}$$

만약 $0 \le j < k \le q-1$ 을 만족하는 적당한 정수 j, k 가 존재해서 $p+jd, p+kd$ 를 q로 나눈 나머지가 같다면 $q \mid (p+kd)-(p+jd) = (k-j)d$ 인데 q는 소수이고 $q \nmid d$ 이므로 $q \mid k-j$ 를 만족한다.

따라서 $q \le k-j$ 인데 이것은 $0 \le j < k \le q-1$ 에 모순이다. 그러므로 (22)의 q개의 항은 q로 나누었을 때 나머지가 서로 다르고 정수를 q로 나눈 나머지는 $0,1,...,q-1$ 중 하나이므로 (23)의 항 중에는 q로 나누어지는 항이 존재한다.

그러므로 $0 \le t \le q-1$ 을 만족하는 적당한 정수 t가 존재해서 $q \mid p+td$ 를 만족한다.

한편 가정에 의하면 (22)의 모든 항은 소수이다. 그러므로 $n \le p$ 가 되어야 한다.
만약 $p < n$ 이면 $p \le n-1$ 이므로 $p+pd = p(1+d)$ 가 (22)의 항에 포함되고
d는 자연수이므로 $p+pd$ 는 소수가 될수 없다. 따라서 $n \le p$ 이다.

그러므로 $q < n \leq p \leq p + td$ 를 만족한다. 그리고 $q < n$ 이므로 (23)의 모든 항도 소수이고 따라서 $q \mid p + td$ 이면 $p + td = q$ 인데 이것은 $q < n \leq p \leq p + td$ 에 모순이다.

그러므로 $q < n$ 을 만족하는 소수 q는 $q \mid d$ 를 만족한다. 즉, q는 d의 약수이다. ■

사실 모든 자연수를 대입했을 때 소수만 나오는 식 자체는 많이 알려져 있습니다.
그중 가장 유명한 식은 **윌런스의 공식(Willans's Formula)**이라고 부르는 다음 식입니다.

$$p_n = 1 + \sum_{m=1}^{2^n} \left\lfloor \sqrt[n]{n} \left(\sum_{k=1}^{m} \left\lfloor \cos^2 \frac{(1+(k-1)!)\pi}{k} \right\rfloor \right)^{-\frac{1}{n}} \right\rfloor$$

실제로 윌런스의 공식에서 우변에 자연수 n을 대입하면 n번째 소수가 나옵니다.
그런데 윌런스의 공식으로 소수를 찾는 것은 에라토스테네스의 체를 사용해서 소수를 찾는것보다 훨씬 비효율적이라서 의미있는 공식은 아닙니다.

참고로 윌런스의 공식에서 $\lfloor x \rfloor$ 는 **바닥 함수(Floor Function)**라고 부르는 기호인데 x가 실수일 때 $\lfloor x \rfloor$ 는 x를 넘지 않는 최대의 정수로 정의됩니다. 고등학교에서는 가우스 함수라고 부르는 그 함수인데 실제로는 바닥 함수라는 용어를 더 많이 사용합니다.
몇가지 예를 들면 $\lfloor 1 \rfloor = 1,\ \left\lfloor \frac{5}{2} \right\rfloor = 2,\ \lfloor \pi \rfloor = 3,\ \left\lfloor -\frac{3}{2} \right\rfloor = -2$ 입니다.

바닥 함수와 반대되는 함수는 **천장 함수(Ceiling Function)**가 있고 이것은 기호로 $\lceil x \rceil$ 이렇게 씁니다. x가 실수일 때 $\lceil x \rceil$ 는 x보다 작지 않은 최소의 정수로 정의됩니다.

한편 소수는 다음과 같은 해석적인 성질도 가지고 있습니다. 실수 x에 대하여 $\pi(x)$를 x보다 작거나 같은 소수의 개수라고 하면 $\lim_{x \to \infty} \frac{\pi(x) \ln x}{x} = 1$ 이 성립합니다.

$\lim_{x \to \infty} \frac{\pi(x) \ln x}{x} = 1$ 이 등식을 **소수 정리(Prime Number Theorem)**라고 부르는데 현대 해석적 수론은 소수 정리가 없으면 할수 있는게 아무것도 없을 정도로 현대 해석적 수론의 기반이 되는 정리라고 합니다.

소수 정리는 보통 복소해석학의 내용을 가지고 증명합니다. 이것도 증명은 간단하지 않은데 Stein 복소해석 책에 증명이 나와있으니 궁금하면 참고하길 바랍니다.

소수가 가지고 있는 또다른 해석적인 성질은 p_n이 n번째 소수일 때 $\sum_{n=1}^{\infty} \frac{1}{p_n}$ 이 무한급수가 발산한다는 것입니다. 이것도 수학자 오일러가 증명했습니다.

이제 디리클레의 정리에서 조건을 좀 더 강하게 만든 정리의 초등적인 증명을 소개하고 문제를 몇 개 풀고 마치겠습니다.

Theorem 1.4.9 $n \in \mathbb{Z}$ 일 때 $4n+3$ 형태를 갖는 소수의 개수는 무한하다.

(증명)

먼저 $4n+1$ 형태의 두 정수를 곱하면 그것도 여전히 $4n+1$ 형태임을 보이자. (24)

$a = 4n+1,\ b = 4m+1$ 이면 $ab = 4(4mn+m+n)+1$ 이므로

ab도 $4n+1$ 형태이다.

이제 정리를 증명하자. 결론을 부정해서 $4n+3$ 형태를 갖는 소수의 개수가 유한한다고 가정하고 그것을 $q_1, q_2, ..., q_s$ 라고 하자. 이때 $N = 4q_1q_2 \cdots q_s - 1$ 이라고 하면 $N = 4(q_1q_2 \cdots q_s - 1) + 3$ 이므로 N 은 $4n+3$ 형태의 자연수이다.

N 을 소수의 곱으로 나타낸 것을 $N = r_1r_2 \cdots r_t$ 라고 하자. 그러면 N 은 $4n+3$ 형태의 자연수이므로 (24)에 의하면 $r_1, r_2, ..., r_t$ 중 적어도 하나는 $4n+3$ 형태의 소수가 되어야 한다.

따라서 적당한 $i \in \{1,2,...,t\}$ 에 대하여 $r_i \mid q_1q_2 \cdots q_s$ 이고 $r_i \mid N$ 이므로 $r_i \mid 4q_1q_2 \cdots q_s - N = 1$ 인데 이것은 모순이다. 그러므로 $4n+3$ 형태를 갖는 소수의 개수는 무한하다. ■

Problem 1.4.3 $n \geq 2$ 일 때 다음을 증명하시오.

(a). n^4+4 는 합성수이다.

(b). n^4+n^2+1 은 합성수이다.

(증명)

(a). $n^4+4 = (n^4+4n^2+4) - 4n^2 = (n^2+2n+2)(n^2-2n+2)$ 이고

$n \geq 2$ 이면 $n^2+2n+2 \geq n^2-2n+2 \geq 2$ 이므로 n^4+4 는 합성수이다. ■

(b). $n^4+n^2+1 = (n^4+2n^2+1) - n^2 = (n^2-n+1)(n^2+n+1)$ 이고

$n \geq 2$ 이면 $n^2+n+1 \geq n^2-n+1 \geq 3$ 이므로 n^4+n^2+1 은 합성수이다. ■

Problem 1.4.4 $n \geq 2$ 일 때 다음을 증명하시오.

(a). $1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}$ 은 자연수가 될수 없다.

(b). $1+\frac{1}{3}+\frac{1}{5}+\cdots+\frac{1}{2n-1}$ 은 자연수가 될수 없다.

(증명)

p_n을 n번째 소수라고 하자. 그러면 $p_{n+1} < 2p_n$ 가 성립한다.

$n \geq 2$ 이면 $p \leq n$ 을 만족하는 소수 p는 존재하므로 $p \leq n$ 을 만족하는 가장 큰 소수가 존재한다. 그것을 p_M 이라고 하면 $p_M \leq n < P_{M+1}$ 을 만족하고 $p_{M+1} < 2p_M$ 이므로 $p_M \leq n < 2p_M$ 이 성립한다. 이것을 이용하자. (25)

(a). 결론을 부정해서 $n \geq 2$ 를 만족하는 적당한 자연수 n에 대하여 $s = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$ 가 자연수라고 가정하고 s를 통분한 것을 다음과 같이 쓰자.

$$s = \frac{s_1 + s_2 + \cdots + s_n}{n!}$$

여기서 s_k는 다음과 같이 k를 제외한 나머지를 모두 곱한 것이다.

$$\begin{aligned} s_1 &= n! \\ s_2 &= 3 \times 4 \times \cdots \times n \\ s_3 &= 2 \times 4 \times \cdots \times n \\ &\vdots \\ s_n &= 2 \times 3 \times \cdots \times (n-1) \end{aligned}$$

(25)에 의하면 $p_M \leq n < 2p_M$ 을 만족한다. 그러므로 $r \geq 2$ 인 자연수 r에 대하여 $p_M \leq n < 2p_M \leq rp_M$ 을 만족하고 따라서 n보다 작거나 같은 자연수 중에서 p_M 의 배수는 p_M 하나뿐이다.

그리고 p_M 은 소수이므로 Lemma 1.4.1에 의하면 $p_M \nmid s_k$ 을 만족하는 $k \in \{1,2,...,n\}$ 는 $k = p_M$ 이 유일하다는 것을 쉽게 알수 있다. 즉, $k \neq p_M$ 이면 $p_M \mid s_k$ 이다. (26)

가정에 의하면 s는 자연수이다. 그러므로 $n! \mid s_1 + s_2 + \cdots + s_n$ 이고 $p_M \mid n!$ 이므로 $p_M \mid s_1 + s_2 + \cdots + s_n$ 을 만족하고 $k \neq p_M$ 이면 $p_M \mid s_k$ 이므로 다음을 얻는다.

$$p_M \mid (s_1 + s_2 + \cdots + s_n) - s_{p_M}$$

따라서 $p_M \mid s_{p_M}$ 을 얻는데 이것은 (26)에 모순이다. 그러므로 s는 자연수가 될수 없다. ■

(b). $n \geq 2$ 이므로 $2n-1 \geq 3$ 이다. 따라서 $p \leq 2n-1$ 를 만족하는 가장 큰 소수는 존재하고 그것을 p_M 이라고 하면 (a)의 풀이와 같은 방법으로 $r \geq 2$ 인 자연수 r에 대하여 $p_M \leq 2n-1 < rp_M$ 을 보일수 있고 $2n-1 \geq 3$ 이므로 p_M 은 홀수이다.

결론을 부정해서 $n \geq 2$ 를 만족하는 적당한 자연수 n에 대하여 $s = 1 + \frac{1}{3} + \frac{1}{5} + \cdots + \frac{1}{2n-1}$ 가 자연수라고 가정하고 s를 통분한 것을 다음과 같이 쓰자.

$$s = \frac{s_1 + s_2 + \cdots + s_n}{1 \times 3 \times 5 \times \cdots \times (2n-1)}$$

여기서 s_k는 다음과 같이 k번째 홀수를 제외한 나머지를 모두 곱한 것이다.

$$\begin{aligned} s_1 &= 3\times 5\times\cdots\times(2n-1)\\ s_2 &= 1\times 5\times\cdots\times(2n-1)\\ s_3 &= 3\times 7\times\cdots\times(2n-1)\\ &\vdots\\ s_n &= 1\times 3\times\cdots\times(2n-3) \end{aligned}$$

p_M 은 홀수이고 $r\geq 2$ 인 자연수 r에 대하여 $p_M \leq 2n-1 < rp_M$ 이므로 (a)와 같은 논리로 $p_M \nmid s_k$ 을 만족하는 $k\in\{1,2,...,n\}$는 $k=p_M$ 이 유일하다는 것을 쉽게 알수 있다. 즉, $k\neq p_M$ 이면 $p_M \mid s_k$ 이다. (27)

가정에 의하면 s는 자연수이다. 그러므로 $1\times 3\times 5\times\cdots\times(2n-1)\mid s_1+s_2+\cdots+s_n$ 이고 $p_M \mid 1\times 3\times 5\times\cdots\times(2n-1)$ 이므로 $p_M \mid s_1+s_2+\cdots+s_n$ 을 만족하고 $k\neq p_M$ 이면 $p_M \mid s_k$ 이므로 다음을 얻는다.

$$p_M \mid (s_1+s_2+\cdots+s_n)-s_{p_M}$$

따라서 $p_M \mid s_{p_M}$ 을 얻는데 이것은 (27)에 모순이다. 그러므로 s는 자연수가 될수 없다. ■

Problem 1.4.4의 풀이에서 $p_{n+1}<2p_n$ 이 부등식을 사용했는데 이 부등식은 베르트랑의 공준에 의해 유도됩니다. Problem 1.4.4는 베르트랑의 공준을 사용하지 않는 초등적인 풀이도 있는데 저는 그 풀이를 좋아하지 않아서 베르트랑의 공준을 사용해서 풀었습니다.

초등적인 풀이는 구글에 검색해보면 바로 나옵니다. Problem 1.4.4의 널리 알려진 풀이가 베르트랑의 공준을 사용하지 않은 풀이라서 그렇습니다.

Problem 1.4.5 p는 소수이고 a는 $a\leq p-1$ 를 만족하는 자연수일 때 다음을 증명하시오.

(a). $p \mid \binom{p}{a}$ 이다.

(b). $n\geq 2$ 를 만족하는 모든 자연수 n에 대하여 $p^n \nmid \binom{p}{a}$ 이다.

(증명)

(a). 이항계수는 정수이므로 $a!(p-a)! \mid p\times(p-1)!$ 인데 p는 소수이고 $a\leq p-1$ 이므로 $p\nmid a!(p-a)!$ 에서 $\gcd(p, a!(p-a)!)=1$ 을 얻는다.

따라서 $a!(p-a)! \mid (p-1)!$ 이므로 $\dfrac{(p-1)!}{a!(p-a)!}$ 는 정수이고 $p \mid \binom{p}{a}$ 를 얻는다. ■

(b). 결론을 부정해서 $n\geq 2$ 인 적당한 자연수 n이 존재해서 $p^n \mid \binom{p}{a}$ 를 만족한다고 가정하자. 그러면 (a)의 풀이과정에서 $\dfrac{(p-1)!}{a!(p-a)!}$ 는 정수이고 $p^{n-1} \mid \dfrac{(p-1)!}{a!(p-a)!}$ 이다.

그리고 $p \mid p^{n-1}$ 이므로 결국 $p \mid \dfrac{(p-1)!}{a!(p-a)!}$ 를 얻는다.

$\dfrac{(p-1)!}{a!(p-a)!} \mid (p-1)!$ 는 명백하므로 $p \mid (p-1)!$ 인데 p는 소수이므로 $p \nmid (p-1)!$ 이다. 이것은 모순이므로 $p^n \mid \binom{p}{a}$ 을 만족하는 $n \geq 2$ 인 자연수 n은 존재하지 않는다.

즉, $n \geq 2$ 이면 $p^n \nmid \binom{p}{a}$ 이다. ■

Problem 1.4.6 상수가 아닌 다항식 $f(x) \in \mathbb{Z}[x]$가 다음과 같다고 하자.

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \ (a_n \neq 0)$$

$\gcd(r,s) = 1$ 을 만족하는 0이 아닌 정수 r, s 에 대하여 $f\left(\dfrac{r}{s}\right) = 0$ 이면 $r \mid a_0$, $s \mid a_n$ 임을 증명하시오. 이것을 **유리근 정리(Rational Root Theorem)**라고 부른다.

(증명)

$f\left(\dfrac{r}{s}\right) = 0$ 이므로 $a_0 s^n + a_1 r s^{n-1} + \cdots + a_n r^n = 0$ 인데 이 식을 다음과 같이 2가지 방식으로 표현할수 있다.

$$r\left(a_1 s^{n-1} + \cdots + a_n r^{n-1}\right) = -a_0 s^n \tag{28}$$

$$s\left(a_0 s^{n-1} + \cdots + a_{n-1} r^{n-1}\right) = -a_n r^n \tag{29}$$

(28)에서 $r \mid a_0 s^n$ 을 얻는데 $\gcd(r,s) = 1$ 이므로 $\gcd\left(r, s^n\right) = 1$ 이다.
따라서 $r \mid a_0$ 를 얻는다.

마찬가지로 (29)에서 $s \mid a_n r^n$ 을 얻는데 $\gcd(r,s) = 1$ 이므로 $\gcd\left(r^n, s\right) = 1$ 에서 $s \mid a_n$ 을 얻을수 있다. ■

고등학교에서 가르쳐주는 3차 이상의 정수계수 다항식을 인수분해하는 방법은

$x = \pm \dfrac{\text{상수항의 약수}}{\text{최고차항 계수의 약수}}$ 를 대입해봐서 0이 되는 x를 찾는 것입니다.

그렇게 찾은 근이 $x = a$ 이면 $x - a$ 를 인수로 갖는다는 것을 이용해서 인수분해합니다.

이때 근을 저렇게 찾을수 있는 이유가 고등학교에서는 정수계수 다항식을 인수분해 할 때 유리수 근을 갖는 다항식만 문제로 출제하기 때문입니다. 다항식이 유리수 근을 가지면 유리근 정리에 의해 고등학교에서 가르쳐주는 방법으로 근을 구할수 있는겁니다.

Problem 1.4.7 다음을 증명하시오. 여기서 $\lfloor x \rfloor$ 는 바닥함수이다.

(a). a는 정수이고 b는 자연수일 때 a를 b로 나눈 몫은 $\left\lfloor \frac{a}{b} \right\rfloor$ 이다.

(b). a, b가 $a \geq b$ 를 만족하는 자연수일 때 a 이하의 자연수 중에서 b의 배수의 개수는 $\left\lfloor \frac{a}{b} \right\rfloor$ 이다.

(증명)

(a). a를 b로 나눈 몫을 q, 나머지를 r이라고 하면 $a = bq + r$ 을 만족하고 $b > 0$ 이므로 $0 \leq r < b$ 이다. 따라서 $0 \leq \frac{r}{b} < 1$ 이고 q는 정수이므로 바닥함수의 정의에 의하면

$$\begin{aligned} \left\lfloor \frac{a}{b} \right\rfloor &= \left\lfloor \frac{bq+r}{b} \right\rfloor \\ &= \left\lfloor q + \frac{r}{b} \right\rfloor \\ &= q \end{aligned}$$

를 얻는다. 그러므로 $\left\lfloor \frac{a}{b} \right\rfloor$ 는 a를 b로 나눈 몫이다. ■

(b). a를 b로 나눈 몫을 q, 나머지를 r이라고 하면 $a = bq + r$ 을 만족하고 $b > 0$ 이므로 $0 \leq r < b$ 이다. 그리고 $a \geq b$ 에서 $bq = a - r > a - b \geq 0$ 이고 b는 자연수이므로 q도 자연수가 되어야 한다.

$r = a - bq \geq 0$ 이므로 $nb \leq a$ 를 만족하는 자연수 n은 $n = q$ 로 존재한다. 이제 q가 $nb \leq a$ 를 만족하는 가장 큰 자연수임을 보이기 위해 결론을 부정해서 $q' > q$ 를 만족하는 적당한 자연수 q'에 대하여 $q'b \leq a$ 를 만족한다고 하자.

그러면 q, q' 은 자연수이므로 $q' \geq q + 1$ 이고 $r < b$ 이므로 다음을 얻는다.

$$\begin{aligned} a - q'b &= a - ((q' - q) + q)b \\ &= r - (q' - q)b \\ &< (1 + q - q')b \\ &\leq 0 \end{aligned}$$

따라서 $a < q'b$ 인데 이것은 모순이다. 그러므로 q는 $nb \leq a$ 를 만족하는 가장 큰 자연수이고 a 이하의 자연수 중에서 b의 배수는 $b, 2b, 3b, \ldots, qb$ 이렇게 q개 있다.

b는 자연수이므로 (a)에 의하면 $q = \left\lfloor \frac{a}{b} \right\rfloor$ 이고 따라서 조건을 만족하는 자연수의 개수는 $\left\lfloor \frac{a}{b} \right\rfloor$ 이다. ■

Problem 1.4.8 $n \geq 2$ 를 만족하는 자연수 n이 임의로 주어져있을 때 $n!$을 소인수분해하면 $n! = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ 가 된다고 하자. 여기서 $p_1, p_2, ..., p_r$ 은 서로 다른 소수이고 $k_1, k_2, ..., k_r$ 은 자연수이다.

그러면 각각의 $i = 1, 2, ..., r$ 에 대하여 다음을 증명하시오.

$$k_i = \sum_{m=1}^{\infty} \left\lfloor \frac{n}{p_i^m} \right\rfloor \tag{30}$$

여기서 $\lfloor x \rfloor$ 는 바닥함수이다. 그리고 $p_i \geq 2$ 이므로 $p_i^{m_0} > n$ 을 만족하는 자연수 m_0는 존재하고 이때 $m \geq m_0$ 이면 $p_i^m \geq p_i^{m_0} > n$ 이므로 $\left\lfloor \frac{n}{p_i^m} \right\rfloor = 0$ 이다.

따라서 (30)의 급수는 유한개의 자연수의 합과 같으므로 수렴하는 무한급수이다.

(증명)

$n!$을 소인수분해 했을 때 p_i는 p_i의 거듭제곱의 배수에서만 나온다. 따라서 n 이하의 자연수 중에서 p_i의 거듭제곱의 배수만 고려하면 충분하다.

n은 고정된 자연수이므로 $\left\lfloor \frac{n}{p_i^s} \right\rfloor \neq 0$ 을 만족하는 가장 큰 자연수 s는 존재한다.

따라서 Problem 1.4.7에 의하면 n 이하의 자연수 중에서 p_i의 거듭제곱의 배수인 것은 $p_i, p_i^2, ..., p_i^s$ 의 배수밖에 없다.

편의상 각각의 $m = 1, 2, ..., s$ 에 대하여 $e_m = \left\lfloor \frac{n}{p_i^m} \right\rfloor$ 라고 하자. 그러면 n개의 자연수 $1, 2, ..., n$ 를 소인수분해 했을 때 p_i^m만 나오는 자연수의 개수는 $m \neq s$ 인 경우 p_i^m의 배수이면서 p_i^{m+1}의 배수가 아닌 자연수의 개수와 같고 $m = s$ 이면 p_i^s의 배수의 개수와 같다.

따라서 Problem 1.4.7에 의하면 n개의 자연수 $1, 2, ..., n$ 를 소인수분해 했을 때 p_i^m만 나오는 자연수의 개수는 $m \neq s$ 인 경우 $e_m - e_{m+1}$ 이고 $m = s$ 인 경우 e_s 이다.

그리고 $e_m - e_{m+1}$ 개의 p_i^m을 모두 곱하면 $p_i^{m(e_m - e_{m+1})}$ 이고 e_s개의 p_i^s를 모두 곱하면 $p_i^{se_s}$ 이다. 따라서 다음이 성립한다.

case1) $s = 1$

이 경우 $m \geq 2$ 이면 $e_m = 0$ 이므로 $k_i = e_1 = \sum_{m=1}^{\infty} e_m$ 이다.

case2) $s \geq 2$

이 경우 $m \geq s+1$ 이면 $e_m = 0$ 이므로 다음을 얻는다.

$$\begin{aligned} k_i &= \sum_{m=1}^{s-1} m(e_m - e_{m+1}) + se_s \\ &= (e_1 - e_2) + 2(e_2 - e_3) + 3(e_3 - e_4) + \cdots + (s-1)(e_{s-1} - e_s) + se_s \\ &= e_1 + e_2 + \cdots + e_s \\ &= \sum_{m=1}^{s} e_m \\ &= \sum_{m=1}^{\infty} e_m \end{aligned}$$

정리하면 $k_i = \sum_{m=1}^{\infty} e_m = \sum_{m=1}^{\infty} \left\lfloor \frac{n}{p_i^m} \right\rfloor$ 를 얻을수 있다. ■

Problem 1.4.8를 이용해서 $50!$을 소인수분해 하려면 다음과 같이 하면 됩니다.

50 이하의 소수는 $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47$ 이고 (30)에 의하면 $50!$을 소인수분해 했을 때 25보다 큰 소수는 지수가 모두 1이라는 것을 쉽게 알수 있습니다. 따라서 25 이하의 소수만 살펴보면 됩니다.

$$\left\lfloor \frac{50}{2} \right\rfloor = 25, \left\lfloor \frac{50}{2^2} \right\rfloor = 12, \left\lfloor \frac{50}{2^3} \right\rfloor = 6,$$
$$\left\lfloor \frac{50}{2^4} \right\rfloor = 3, \left\lfloor \frac{50}{2^5} \right\rfloor = 1, \left\lfloor \frac{50}{2^6} \right\rfloor = 0$$

$$\left\lfloor \frac{50}{3} \right\rfloor = 16, \left\lfloor \frac{50}{3^2} \right\rfloor = 5, \left\lfloor \frac{50}{3^3} \right\rfloor = 1, \left\lfloor \frac{50}{3^4} \right\rfloor = 0$$

$$\left\lfloor \frac{50}{5} \right\rfloor = 10, \left\lfloor \frac{50}{5^2} \right\rfloor = 2, \left\lfloor \frac{50}{5^3} \right\rfloor = 0$$

$$\left\lfloor \frac{50}{7} \right\rfloor = 7, \left\lfloor \frac{50}{7^2} \right\rfloor = 1, \left\lfloor \frac{50}{7^3} \right\rfloor = 0$$

$$\left\lfloor \frac{50}{11} \right\rfloor = 4, \left\lfloor \frac{50}{11^2} \right\rfloor = 0$$

$$\left\lfloor \frac{50}{13} \right\rfloor = 3, \left\lfloor \frac{50}{13^2} \right\rfloor = 0$$

$$\left\lfloor \frac{50}{17} \right\rfloor = 2, \ \left\lfloor \frac{50}{17^2} \right\rfloor = 0$$

$$\left\lfloor \frac{50}{19} \right\rfloor = 2, \ \left\lfloor \frac{50}{19^2} \right\rfloor = 0$$

$$\left\lfloor \frac{50}{23} \right\rfloor = 2, \ \left\lfloor \frac{50}{23^2} \right\rfloor = 0$$

그러므로 (30)에 의하면 $50!$을 소인수분해한 결과는 다음과 같습니다.

$$\begin{aligned} 50! = \ & 2^{47} \times 3^{22} \times 5^{12} \times 7^8 \times 11^4 \times 13^3 \times 17^2 \times 19^2 \\ & \times 23^2 \times 29 \times 31 \times 37 \times 41 \times 43 \times 47 \end{aligned}$$

Problem 1.4.9 다음을 증명하시오.

(a). $p \geq 5$ 를 만족하는 모든 소수 p에 대하여 $3 \mid p^2+2$ 이다.

(b). $p \neq 5$ 을 만족하는 모든 홀수 소수 p에 대하여 $10 \mid p^2-1$ 또는 $10 \mid p^2+1$ 이다.

(c). $p \neq 3$ 을 만족하는 모든 소수 p에 대하여 $3 \mid p^2+8$ 이다.

(증명)

(a). p는 $p \geq 5$ 를 만족하는 소수이므로 6으로 나누면 나머지가 1 또는 5이다.
따라서 p는 적당한 음이 아닌 정수 k에 대하여 $6k+1$ 또는 $6k+5$ 로 표현된다.

$p = 6k+1$ 이면 $p^2+2 = 3(12k^2+4k+1)$ 이므로 $3 \mid p^2+2$ 이고
$p = 6k+5$ 이면 $p^2+2 = 3(12k^2+20k+9)$ 이므로 $3 \mid p^2+2$ 이다.

그러므로 $3 \mid p^2+2$ 가 성립한다. ■

(b). p는 $p \neq 5$ 를 만족하는 홀수 소수이므로 10으로 나누면 나머지가 $1, 3, 7, 9$ 이다.
따라서 p는 적당한 음이 아닌 정수 k에 대하여 $10k+1, 10k+3, 10k+7, 10k+9$
로 표현된다.

$p = 10k+1$ 이면 $p^2-1 = 10(10k^2+2k)$ 이므로 $10 \mid p^2-1$
$p = 10k+3$ 이면 $p^2+1 = 10(10k^2+6k+1)$ 이므로 $10 \mid p^2+1$
$p = 10k+7$ 이면 $p^2+1 = 10(10k^2+14k+5)$ 이므로 $10 \mid p^2+1$
$p = 10k+9$ 이면 $p^2-1 = 10(10k^2+18k+8)$ 이므로 $10 \mid p^2-1$

따라서 $10 \mid p^2-1$ 또는 $10 \mid p^2+1$ 이다. ■

(c). p는 $p \neq 3$ 을 만족하는 소수이므로 3으로 나누면 나머지가 $1, 2$ 이다.
따라서 p는 적당한 음이 아닌 정수 k에 대하여 $3k+1, 3k+2$ 로 표현된다.

$p=3k+1$ 이면 $p^2+8=3(3k^2+2k+3)$ 이므로 $3 \mid p^2+8$
$p=3k+2$ 이면 $p^2+8=3(3k^2+4k+4)$ 이므로 $3 \mid p^2+8$

그러므로 $3 \mid p^2+8$ 가 성립한다. ■

Problem 1.4.10 다음 두 명제 p, q는 서로 동치임을 증명하시오.

p : 2보다 큰 모든 짝수는 2개의 소수의 합으로 표현된다.
q : 5보다 큰 모든 자연수는 3개의 소수의 합으로 표현된다.

(증명)
$(p \Rightarrow q)$
$n>5$ 를 만족하는 자연수 n을 임의로 하나 택하자.

case1) n은 짝수
n이 짝수이면 적당한 자연수 k가 존재해서 $n=2k$ 이고 $n>5$ 이므로 $k \geq 3$ 이다.

따라서 $2(k-1) \geq 4$ 이므로 가정에 의하면 적당한 소수 r, s 가 존재해서 $2(k-1)=r+s$ 를 만족한다. 그러므로 $n=2k=2+r+s$ 이고 $2, r, s$ 는 소수이므로 q는 참이다.

case2) n은 홀수
n이 홀수이면 적당한 자연수 k가 존재해서 $n=2k-1$ 이고 $n>5$ 이므로 $k \geq 4$ 이다. 따라서 $2(k-2) \geq 4$ 이므로 가정에 의하면 적당한 소수 r, s 가 존재해서 $2(k-2)=r+s$ 를 만족한다.

그러므로 $n=2k-1=3+2(k-2)=3+r+s$ 이고 $3, r, s$ 는 소수이므로 q는 참이다. 정리하면 어느 경우든 q는 참이다.

$(q \Rightarrow p)$
$n>2$ 를 만족하는 짝수 n을 임의로 하나 택하자. 그러면 $n+2 \geq 6$ 이므로 가정에 의하면 $n+2=u+v+w$ 를 만족하는 소수 u, v, w 가 존재한다.

그리고 $n+2$ 는 짝수이므로 u, v, w 셋중 적어도 하나는 짝수가 되어야 한다.
만약 u, v, w 가 모두 홀수이면 $u+v+w=n+2$ 는 홀수이므로 모순이다.

짝수인 소수는 2가 유일하고 이때 $u=2$ 라고 가정해도 일반성을 잃지 않는다. 그러면 $n+2=2+v+w$ 에서 $n=v+w$ 를 얻고 v, w 는 소수이므로 p는 참이다. ■

Problem 1.4.10에서 명제 p를 **골드바흐의 추측(Goldbach's Conjecture)**이라고 부릅니다. 원래 골드바흐가 제시한 명제는 q인데 오일러가 q가 p와 동치임을 증명했고 현대에는 명제 p를 골드바흐의 추측이라고 부릅니다.

4 이상의 짝수를 2개의 소수의 합으로 표현할 때 2개의 소수는 같을수도 있습니다. 간단한 예로 $4 = 2 + 2$ 이고 2는 소수입니다.

골드바흐의 추측은 아직까지 증명되지 않았습니다. 컴퓨터로 계산해본 결과 4×10^{18} 이하 즉, 400경 이하의 짝수에 대해서는 골드바흐의 추측이 참이라고 합니다.

골드바흐의 약한 추측(Goldbach's Weak Conjecture)이라고 부르는 명제도 있는데 5보다 큰 모든 홀수는 3개의 소수의 합으로 표현된다는 명제입니다.

약한 추측이라고 부르는 이유는 골드바흐의 추측이 참이면 골드바흐의 약한 추측도 참이기 때문입니다. $n > 2$ 인 임의의 짝수 n이 적당한 소수 p, q 에 대하여 $n = p + q$ 로 표현되면 $n + 3 = 3 + p + q$ 인데 $n + 3 > 5$ 이고 $n + 3$ 은 홀수, 그리고 3은 소수이므로 골드바흐의 추측이 참이면 골드바흐의 약한 추측은 참입니다.

골드바흐의 약한 추측은 2013년에 증명되었습니다. 그래서 더 이상 추측이라고 할수 없지만 여전히 골드바흐의 약한 추측이라고 부릅니다.

2. 합동식

2.1 합동의 정의와 성질

작성자 : 네냐플(Nenyaffle)

2장에서는 새로운 등호를 사용하는 식을 소개하려고 합니다. 지금까지 본 등호는 두 정수 a, b 에 대하여 $a = b$ 라고 나타내는 것 하나뿐인데 $a = b$ 이것은 두 정수 a, b 가 수학적으로 완벽하게 동일하다는 것을 나타낼 때 사용하는 기호입니다.

예를 들어 두 정수 $1, 2$ 는 다르기 때문에 $1 \neq 2$ 라고 나타냅니다. 그리고 1과 1은 완벽하게 같은 정수이므로 $1 = 1$ 이라고 나타냅니다. 따라서 $=$ 이 기호는 굉장히 강력한 조건이 됩니다. 두 정수가 완벽하게 같을때만 같다고 말하기 때문입니다.

2장에서는 두 정수가 같다는 개념을 조금 약하게 정의하려고 합니다. Corollary 1.1.1에 의하면 모든 정수는 나머지만 가지고 분류할수 있다는 것을 알수 있고 기초 정수론에서는 정수로 나눈 나머지만 가지고 해결할수 있는 문제가 많기 때문에 나머지가 같은 정수를 서로 같은 정수라고 간주하는 것은 의미가 있습니다.

두 정수 a, b를 자연수 n으로 나눈 나머지가 같으면 $n \mid a-b$ 를 만족합니다.
따라서 새로운 등호 $\equiv$ 를 다음과 같이 정의합니다.

Definition 2.1.1 정수 a, b와 자연수 n이 임의로 주어져있을 때 $n \mid a-b$ 를 만족하면 a, b는 법 n에 대하여 합동이라고 정의하고 기호로는 $a \equiv b \pmod{n}$ 라고 나타낸다.
a, b가 법 n에 대하여 합동이 아니면 기호로는 $a \not\equiv b \pmod{n}$ 라고 나타낸다.

등호 $=$ 가 포함된 식을 등식이라고 부르는것처럼 $\equiv$ 이 합동기호가 포함된 식을 합동식이라고 부릅니다. 그리고 합동식에서는 n이 자연수인 경우만 논의하는데 n이 0이 아닌 정수이면 $n \mid a-b$ 와 $(-n) \mid a-b$ 는 동치가 되기 때문입니다.

그리고 Definition 2.1.1은 $n = 1$ 일때도 정의는 가능하지만 $n = 1$ 이면 임의의 정수 a, b에 대하여 $1 \mid a-b$ 이므로 모든 정수가 법 n에 대하여 합동이 되기 때문에 의미가 없습니다. 그래서 합동식은 $n \geq 2$ 가 되어야 의미가 있습니다.

몇가지 예를 들면 $2 \mid 6-4$ 이므로 $6 \equiv 4 \pmod{2}$, $3 \mid 71-23$ 이므로 $71 \equiv 23 \pmod{3}$ 입니다. 그리고 $5 \nmid 40-7$ 이므로 $40 \not\equiv 7 \pmod{5}$ 입니다.

Theorem 2.1.1 정수 a, b와 자연수 n에 대하여 $a \equiv b \pmod{n}$ 일 필요충분조건은 a를 n으로 나눈 나머지와 b를 n으로 나눈 나머지가 같은 것이다.

(증명)
$(\Longrightarrow)$ $a \equiv b \pmod{n}$ 이므로 적당한 $k \in \mathbb{Z}$ 가 존재해서 $a = nk + b$ 를 만족한다.
따라서 Corollary 1.1.2에서 다항식을 $f(x) = x$ 로 택하면 a를 n으로 나눈 나머지와 b를 n으로 나눈 나머지가 같다는 것을 쉽게 알수 있다.

$(\Leftarrow)$ a, b를 n으로 나눈 나머지가 같으므로 그것을 r이라고 하자. 그러면 나눗셈 정리에 의해 $a = nk_1 + r,\ b = nk_2 + r$ 을 만족하는 $k_1, k_2 \in \mathbb{Z}$ 가 존재하고
이때 $a - b = (k_1 - k_2)n$ 을 만족한다.

그러므로 $n \mid a - b$ 이고 따라서 $a \equiv b \pmod{n}$ 이다. ■

Theorem 2.1.1에 의하면 n으로 나눈 나머지가 다른 정수는 서로 합동이 될수 없습니다. 그리고 나눗셈 정리에 의하면 n으로 나눈 나머지는 $0,1,2,...,n-1$ 이렇게 n개이므로 서로 합동이 아닌 정수가 최대 n개 존재한다는 것을 알수 있습니다.

이것을 다음과 같이 정의합니다.

Definition 2.1.2 완전잉여계(Complete Residue System)
자연수 n에 대하여 n개의 정수 $a_1, a_2, ..., a_n$ 가 다음을 만족한다고 하자.

$$a_i \equiv a_j \pmod{n} \text{ 이면 } i = j \text{ 이다.}$$

그러면 집합 $\{a_1, a_2, ..., a_n\}$을 법 n에 대한 **완전잉여계(Complete Residue System)** 라고 정의한다.

법 n에 대한 가장 자연스러운 완전잉여계는 $\{0,1,2,...,n-1\}$ 인데 이것을 편의상 기호로 $\mathbb{Z}_n = \{0,1,2,...,n-1\}$ 라고 나타냅니다.

법 n에 대한 완전잉여계는 하나만 있는건 아닙니다. $n = 5$ 일 때 $\mathbb{Z}_5 = \{0,1,2,3,4\}$는 법 5에 대한 완전잉여계인데 $\{5,6,8,9,12\}$ 이것도 법 5에 대한 완전잉여계가 됩니다.

$\{a_1, a_2, ..., a_n\}$이 법 n에 대한 완전잉여계이면 나머지의 유일성과 Theorem 2.1.1에 의해 $\{a_1, a_2, ..., a_n\}$과 $\mathbb{Z}_n$은 법 n에 대해 합동인 원소들 사이에 일대일 대응이 존재한다는 것을 쉽게 알수 있습니다.

예를 들어 법 5에 대한 2개의 완전잉여계 $\mathbb{Z}_5, \{5,6,8,9,12\}$은 법 5에 대해

$$0 \equiv 5,\ 1 \equiv 6,\ 2 \equiv 12,\ 3 \equiv 8,\ 4 \equiv 9$$

이므로 일대일 대응이 됩니다. 따라서 완전잉여계를 생각할땐 $\mathbb{Z}_n$만 생각해도 충분합니다.

다음은 $\equiv$ 이 기호가 등호 $=$ 와 굉장히 유사한 성질을 가지고 있다는 것을 알려줍니다. 대학 입학 전에 배운 등식의 성질을 생각해보면 이해하기 쉬울겁니다.

Theorem 2.1.2 임의의 자연수 n과 임의의 정수 a, b, c, d 에 대하여 다음이 성립한다.
(a). $a \equiv a \pmod{n}$ 이다.
(b). $a \equiv b \pmod{n}$ 이면 $b \equiv a \pmod{n}$ 이다.
(c). $a \equiv b \pmod{n}$ 이고 $b \equiv c \pmod{n}$ 이면 $a \equiv c \pmod{n}$ 이다.
(d). $a \equiv b \pmod{n}$ 이고 $c \equiv d \pmod{n}$ 이면 $a + c \equiv b + d \pmod{n}$ 이고 $ac \equiv bd \pmod{n}$ 이다.

(증명)
(a). $n \mid 0 = a - a$ 이므로 $a \equiv a \pmod{n}$ 이다. ■

(b). $a \equiv b \pmod{n}$ 이면 $n \mid a - b$ 이고 $a - b \mid b - a$ 이므로 $n \mid b - a$ 이다.
따라서 $b \equiv a \pmod{n}$ 이다. ■

(c). 조건에 의하면 $n \mid a - b,\ n \mid b - c$ 이다. 따라서 $n \mid (a-b) + (b-c) = a - c$
이므로 $a \equiv c \pmod{n}$ 이다. ■

(d). 조건에 의하면 $n \mid a - b,\ n \mid c - d$ 이다. 따라서
$n \mid (a-b) + (c-d) = (a+c) - (b+d)$ 이므로 $a + c \equiv b + d \pmod{n}$ 이다.

한편 적당한 정수 k_1, k_2 가 존재해서 $a - b = nk_1,\ c - d = nk_2$ 를 만족한다.
그러므로 다음 등식을 얻는다.

$$\begin{aligned} ac &= (b + nk_1)(d + nk_2) \\ &= bd + n(bk_2 + dk_1 + nk_1k_2) \end{aligned}$$

따라서 $n \mid ac - bd$ 이므로 $ac \equiv bd \pmod{n}$ 이다. ■

a, b, c, d 가 정수일 때 등호에서는 Theorem 2.1.2의 (a)~(d)가 성립하는 것이 명백합니다.
따라서 $\equiv$ 이것도 등호 $=$ 와 굉장히 유사한 성질을 가지고 있다는 것을 알수 있습니다.

Theorem 2.1.2의 (d)에서 $c = d$ 이면 $a \equiv b \pmod{n}$ 일 때 양변에 같은 것을 더해도
같다는 $a + c \equiv b + c \pmod{n}$ 이 성질과 같은 것을 곱해도 같다는 $ac \equiv bc \pmod{n}$
이 성질을 얻을수 있습니다. 이것은 대학 입학 전에 배운 등식의 성질입니다.

그리고 $a - b = a + (-b)$ 이고 $x \equiv y \pmod{n}$ 이면 $-x \equiv -y \pmod{n}$ 이므로
뺄셈에 대해서도 Theorem 2.1.2의 (d)가 성립한다는 것을 쉽게 알수 있습니다.
그러므로 $a \equiv b \pmod{n}$ 이면 $a - c \equiv b - c \pmod{n}$ 도 성립합니다.

Theorem 2.1.2의 (c)를 일반화하면 각각의 $i = 1, 2, \ldots, m$ 에 대하여 $a_i \equiv b_i \pmod{n}$
일 때 $a_1 + a_2 + \cdots + a_m \equiv b_1 + b_2 + \cdots + b_m \pmod{n}$ 와
$a_1 a_2 \cdots a_m \equiv b_1 b_2 \cdots b_m \pmod{n}$ 가 성립하는데 이것은 수학적 귀납법을 사용하면
증명할수 있습니다.

Corollary 1.1.2에 의하면 $a \equiv b \pmod{n}$ 일 때 임의의 $f(x) \in \mathbb{Z}[x]$ 에 대하여
$f(a) \equiv f(b) \pmod{n}$ 가 성립하는 것도 쉽게 알수 있습니다.

그리고 a가 정수이고 m, n이 자연수일 때 $a^{m+n} = a^m a^n,\ (a^m)^n = a^{mn}$ 이므로
합동식에서도 $a^{m+n} \equiv a^m a^n \pmod{r},\ (a^m)^n \equiv a^{mn} \pmod{r}$ 가 성립합니다.

지금까지 얻은 사실을 이용하면 나머지를 좀 더 쉽게 구할수 있습니다.

Problem 2.1.1 다음을 계산하시오.

(a). $2^{20}-1$ 을 41로 나눈 나머지.

(b). $1!+2!+3!+\cdots+100!$ 을 12로 나눈 나머지.

(c). $1^{2017}+2^{2017}+3^{2017}+\cdots+100^{2017}$ 을 4로 나눈 나머지.

(d). 6^{48}을 13으로 나눈 나머지.

(e). $111^{333}+333^{111}$ 을 7로 나눈 나머지.

(풀이)

(a). $2^5 \equiv 32 \equiv -9 \pmod{41}$ 이다. 따라서 $2^{20} \equiv (-9)^4 \equiv 3^8 \pmod{41}$ 이고 $3^4 \equiv 81 \equiv -1 \pmod{41}$ 이므로 $3^8 \equiv (-1)^2 \equiv 1 \pmod{41}$ 이다.

그러므로 $2^{20} \equiv 1 \pmod{41}$ 이고 $2^{20}-1$ 을 41로 나눈 나머지는 0이다. ■

(b). $4! = 24$ 이므로 $4! \equiv 0 \pmod{12}$ 이다. 따라서 $n \geq 4$ 이면 $n! \equiv 0 \pmod{12}$ 이므로 $1!+2!+3!+\cdots+100! \equiv 1+2+6 \equiv 9 \pmod{12}$ 이다.
그러므로 12로 나눈 나머지는 9이다. ■

(c). 먼저 n이 짝수이면 $n^{2017} \equiv 0 \pmod{4}$ 임을 쉽게 알수 있다.
따라서 밑이 홀수일때만 고려하면 충분하다.

그리고 모든 정수 k에 대하여 $4k+1 \equiv 1 \pmod{4}$, $4k+3 \equiv 3 \pmod{4}$ 이고 $1^{2017}=1$, 그리고 $3^2 \equiv 1 \pmod{4}$ 이므로 $3^{2016} \equiv 1^{1008} \equiv 1 \pmod{4}$ 에서 $3^{2017} \equiv 3 \pmod{4}$ 를 얻는다. 따라서 다음이 성립한다.

$$\begin{aligned} 1^{2017}+2^{2017}+3^{2017}+\cdots+100^{2017} &\equiv 1^{2017}+3^{2017}+\cdots+99^{2017} \\ &\equiv (1+3)+(1+3)+\cdots+(1+3) \\ &\equiv 0 \pmod{4} \end{aligned}$$

그러므로 주어진 자연수를 4로 나눈 나머지는 0이다. ■

(d). $6^2 \equiv -3 \pmod{13}$ 이므로 $6^8 \equiv 3^4 \equiv 3 \pmod{13}$ 이다.
따라서 $6^{48} \equiv 3^6 \pmod{13}$ 인데 $3^4 \equiv 3 \pmod{13}$ 이므로
$3^6 \equiv 3^3 \equiv 1 \pmod{13}$ 을 얻는다.

즉, $6^{48} \equiv 1 \pmod{13}$ 이므로 6^{48}을 13으로 나눈 나머지는 1이다. ■

(e). 112는 7의 배수이므로 $111 \equiv -1 \pmod{7}$ 이다. 따라서 $111^{333} \equiv -1 \pmod{7}$ 을 얻는다. 그리고 $333 \equiv 4 \pmod{7}$ 이고 $4^3 \equiv 1 \pmod{7}$ 이므로 $333^{111} \equiv \left(4^3\right)^{37} \equiv 1 \pmod{7}$ 이다. 둘을 더하면 $111^{333}+333^{111} \equiv 0 \pmod{7}$ 이므로 주어진 자연수를 7로 나눈 나머지는 0이다. ■

등식의 성질중에는 0이 아닌 같은 것을 나눌수 있다는 것도 있습니다. 즉, $c \neq 0$ 이면 $ca = cb$ 일 때 $a = b$ 가 성립한다는 것입니다.

그런데 양변을 c로 나눈다는 것은 양변에 c의 곱셈에 대한 역원 $\frac{1}{c}$ 을 곱하는 겁니다. 0이 아닌 모든 복소수는 곱셈에 대한 역원이 존재하기 때문에 양변을 같은 것으로 나누는 등식의 성질을 얼마든지 사용할수 있는겁니다.

복소수는 0이 아니면 곱셈에 대한 역원이 항상 존재합니다. 그리고 0이 아닌 $z \in \mathbb{C}$ 에 대하여 z의 곱셈에 대한 역원이라는 것은 $zw = 1$ 을 만족하는 $w \in \mathbb{C}$ 이고 이것을 기호로 $w = \frac{1}{z}$ 라고 나타냅니다.

따라서 합동식에서는 곱셈에 대한 역원을 다음과 같이 정의합니다.

Definition 2.1.3 $n \in \mathbb{N}$ 이 임의로 주어져있다고 하자. 이때 $a \in \mathbb{Z}$ 에 대하여 $ax \equiv 1 \pmod{n}$ 를 만족하는 $x \in \mathbb{Z}$ 를 법 n에서 a의 곱셈에 대한 역원이라고 정의한다.

정수의 곱은 교환법칙이 성립하므로 $ax \equiv 1 \pmod{n}$ 이면 $xa \equiv 1 \pmod{n}$ 입니다.

합동식을 사용하게 되면 다양한 정수를 가지고 곱셈에 대한 역원을 생각할수 있다는 것이 장점중 하나입니다. 원래 정수집합에서 곱셈에 대한 역원이 존재하는 원소는 $-1, 1$ 둘뿐인데 합동식에서는 곱셈에 대한 역원을 생각할수 있는 정수가 더 많이 있기 때문입니다.

예를 들면 $2 \times 2 \equiv 1 \pmod{3}$ 이므로 법 3에서 2의 곱셈에 대한 역원은 2이고 $3 \times 2 \equiv 1 \pmod{5}$ 이므로 법 5에서 3의 곱셈에 대한 역원은 2입니다.

곱셈에 대한 역원이 항상 존재하는건 아닙니다. $6x \equiv 1 \pmod{4}$ 를 만족하는 $x \in \mathbb{Z}$ 는 존재하지 않는데 만약 존재한다고 가정하면 합동의 정의에 의해 $6x - 4y = 1$ 을 만족하는 정수 x, y 가 존재하고 $\gcd(6,-4) = 2 \nmid 1$ 이므로 Theorem 1.3.2에 의하면 이것은 모순입니다. 따라서 $6x \equiv 1 \pmod{4}$ 를 만족하는 $x \in \mathbb{Z}$ 는 존재하지 않습니다.

그러므로 법 n에서 곱셈에 대한 역원이 존재하려면 어떤 조건이 필요하다는 것을 알수 있습니다. 한편 다루는 합동식이 법 n에 대한 합동식이라는 것이 명백한 경우에는 법 n에서라는 표현을 생략하고 그냥 곱셈에 대한 역원이라고 쓰기도 합니다.

Theorem 2.1.3 자연수 n과 정수 a가 임의로 주어져있다고 하자.
그러면 다음이 성립한다.

(a). 법 n에서 a의 곱셈에 대한 역원이 존재할 필요충분조건은 $\gcd(a,n) = 1$ 이다.
(b). $\gcd(a,n) = 1$ 이고 정수 x, y 에 대하여 $ax \equiv ay \pmod{n}$ 이면 $x \equiv y \pmod{n}$ 이다.

(증명)
(a). $(\Rightarrow)$ $d=\gcd(a,n)$ 라고 하자. 조건에 의하면 $ax\equiv 1 \pmod n$ 를 만족하는 정수 x가 존재한다. 따라서 적당한 정수 y가 존재해서 $ax-ny=1$ 을 만족하므로 Theorem 1.3.2에 의하면 $\gcd(a,-n)\mid 1$ 이 되어야 한다.

그리고 $\gcd(a,n)=\gcd(a,-n)$ 이므로 $d=1$ 을 얻는다.

$(\Leftarrow)$ 조건에 의하면 $\gcd(a,n)=\gcd(a,-n)=1$ 이 성립하므로 $ax-ny=1$ 을 만족하는 정수 x,y 가 존재한다. 따라서 $ax\equiv 1 \pmod n$ 을 만족하므로 x는 a의 곱셈에 대한 역원이다. ■

(b). $\gcd(a,n)=1$ 이므로 (a)에 의하면 a의 곱셈에 대한 역원이 존재한다.
그것을 u라고 하면 $ua\equiv 1 \pmod n$ 이므로 다음을 얻는다.
$$x\equiv 1\times x\equiv (ua)x\equiv u(ax)\equiv u(ay)\equiv (ua)y\equiv 1\times y\equiv y \pmod n$$
그러므로 $x\equiv y \pmod n$ 이다. ■

Theorem 2.1.3의 (b)에 의하면 a의 곱셈에 대한 역원이 존재할 경우 그 역원은 법 n에서 유일하다는 것을 의미합니다.

$\gcd(a,n)=1$ 일 때 $ax\equiv 1 \pmod n$, $ay\equiv 1 \pmod n$ 을 만족하면 $ax\equiv ay \pmod n$ 이므로 Theorem 2.1.3의 (b)에 의해 $x\equiv y \pmod n$ 를 얻습니다. 따라서 곱셈에 대한 역원은 법 n에서 유일하므로 기호로 나타낼수 있고 a의 곱셈에 대한 역원은 기호로 a^{-1}라고 나타냅니다.

법 n에서 유일하다고 말하는 이유는 이 말이 없으면 유일하지 않기 때문입니다.
$2\times 2\equiv 2\times 5\equiv 1 \pmod 3$ 이므로 2와 5는 모두 법 3에서 2의 곱셈에 대한 역원이 되기 때문입니다.

그래서 법 3에서 유일하다고 말합니다. $2\equiv 5 \pmod 3$ 이므로 법 3에서 2의 곱셈에 대한 역원 $2,5$가 법 3에 대해 합동이고 따라서 유일합니다.

따라서 법 n에서 a의 곱셈의 역원을 구할때는 기본적인 완전잉여계 $\mathbb{Z}_n$의 n개의 원소를 일일이 곱해봐서 1이 나오는 것을 찾아도 됩니다. n이 작으면 이렇게 하는게 효율적입니다.

그런데 n이 크면 일일이 대입하는게 비효율적입니다. 예를 들어 $n=1000$ 이고 $a=357$ 이면 $\gcd(a,n)=1$ 이므로 a의 곱셈에 대한 역원은 존재하는데 0부터 999 까지의 정수를 일일이 357과 곱해서 1이 나오는 정수를 찾는건 비효율적입니다.

곱셈에 대한 역원을 구하는 일반적인 방법은 1.3절에서 배운 유클리드 호제법을 사용하는겁니다. 357의 곱셈에 대한 역원을 구하는 문제는 결국 $357x-1000y=1$ 을 만족하는 정수 x,y 를 구하는 문제가 되기 때문입니다.

$357x-1000y=1$ 은 $357x+1000\times(-y)=1$ 이라고 할수 있고 따라서 $\gcd(357,1000)=1$ 을 얻기 위한 유클리드 호제법을 사용하고 그 과정을 반대로 되돌아가면 x와 $-y$를 얻을수 있습니다.

여기서 원하는 것은 357의 곱셈에 대한 역원 x이므로 x를 구하면 357의 곱셈에 대한 역원을 구한겁니다. 실제로 구해보면 $x=493$ 이고 이게 357의 곱셈에 대한 역원입니다. 둘을 곱하면 $357\times493=176001$ 이므로 $357\times493\equiv1\pmod{1000}$ 입니다.

n이 자연수이고 a,b는 $\gcd(a,n)=\gcd(b,n)=1$ 을 만족하는 정수이면 법 n에서 a^{-1},b^{-1}은 존재하고 다음이 성립합니다.

$$(ab)(b^{-1}a^{-1})\equiv a(bb^{-1})a^{-1}\equiv aa^{-1}\equiv1\pmod{n}$$

따라서 $b^{-1}a^{-1}$ 는 법 n에서 ab의 곱셈에 대한 역원입니다. 그러므로 법 n에서 곱셈에 대한 역원이 유일하다는 성질에 의하면 $(ab)^{-1}\equiv b^{-1}a^{-1}\pmod{n}$ 가 성립하고 특히 $a=b$ 이면 $\left(a^{-1}\right)^2\equiv\left(a^2\right)^{-1}\pmod{n}$ 가 성립합니다.

그러므로 수학적 귀납법에 의하면 모든 자연수 m에 대하여 $\left(a^{-1}\right)^m\equiv\left(a^m\right)^{-1}\pmod{n}$ 가 성립한다는 것을 쉽게 알수 있습니다. 즉, 모든 자연수 m에 대하여 법 n에서 a^m의 곱셈에 대한 역원이 존재합니다. 그것을 기호로는 $a^{-m}=\left(a^m\right)^{-1}$ 라고 나타냅니다.

여기서 $a^{-m}=\left(a^m\right)^{-1}$ 이것은 정수의 음의 지수를 정의한다는게 아니고 법 n에서 a^m의 곱셈에 대한 역원 $\left(a^m\right)^{-1}$을 a^{-m}이라는 기호로 나타내겠다는 뜻입니다. 그러면 $a^{-m}\equiv\left(a^{-1}\right)^m\pmod{n}$ 가 성립한다는 것도 알수 있습니다.

편의상 $a^0=1$ 이라고 정의하면 $\gcd(a,n)=1$ 일 때 음의 지수의 정의에 의해 다음과 같이 지수법칙이 정수 범위에서도 성립한다는 것을 쉽게 알수 있습니다. 다음 식에서 r,s 는 정수입니다.

$$a^{r+s}\equiv a^ra^s\pmod{n}$$
$$\left(a^r\right)^s\equiv a^{rs}\pmod{n}$$

$\gcd(a,n)=1$ 이면 모든 자연수 p,q 에 대하여 $\gcd\left(a^p,n^q\right)=1$ 이므로 법 n에서 a의 거듭제곱의 곱셈에 대한 역원은 항상 존재하고 따라서 음의 정수의 지수도 잘 정의됩니다.

그리고 $\gcd(a,n)=\gcd(b,n)=1$ 이고 $a\equiv b\pmod{n}$ 이면 모든 정수 m에 대하여 $a^m\equiv b^m\pmod{n}$ 도 성립합니다. 합동은 등호와 유사하다는 것을 알면 쉽습니다.

Corollary 2.1.1 자연수 n과 정수 a,x,y 에 대하여 다음이 성립한다.
(a). n이 소수이고 $a\nmid n$ 일 때 $ax\equiv ay\pmod{n}$ 이면 $x\equiv y\pmod{n}$ 이다.
(b). $d=\gcd(a,n)$ 일 때 $ax\equiv ay\pmod{n}$ 이면 $x\equiv y\left(\mod\frac{n}{d}\right)$ 이다.

(증명)
(a). n이 소수이고 $a \nmid n$ 이면 $\gcd(a,n)=1$ 이므로
Theorem 2.1.3에 의하면 참이다. ■

(b). 조건에 의하면 $n \mid ax-ay$ 이므로 $\frac{n}{d} \mid \frac{a}{d}(x-y)$ 이다.
따라서 $\frac{a}{d}x \equiv \frac{a}{d}y \left(\mathrm{mod}\ \frac{n}{d}\right)$ 이고 $\gcd\left(\frac{a}{d},\frac{n}{d}\right)=1$ 이므로 Theorem 2.1.3에 의하면
$x \equiv y \left(\mathrm{mod}\ \frac{n}{d}\right)$ 를 얻는다. ■

Problem 2.1.2 a, b는 정수이고 m, n은 자연수일 때 다음을 증명하시오.
(a). $a \equiv b \pmod{n}$ 이고 $m \mid n$ 이면 $a \equiv b \pmod{m}$ 이다.
(b). $a \equiv b \pmod{n}$ 이고 c가 자연수이면 $ca \equiv cb \pmod{cn}$ 이다.
(c). $a \equiv b \pmod{n}$ 이고 자연수 d가 a, b, n의 공약수이면 $\frac{a}{d} \equiv \frac{b}{d} \left(\mathrm{mod}\ \frac{n}{d}\right)$ 이다.
(d). $a \equiv b \pmod{n}$ 이면 $\gcd(a,n)=\gcd(b,n)$ 이다.

(증명)
(a). 조건에 의하면 $n \mid a-b$ 이고 $m \mid n$ 이므로 $m \mid a-b$ 이다.
따라서 $a \equiv b \pmod{m}$ 이다. ■

(b). 조건에 의하면 $n \mid a-b$ 이므로 $cn \mid c(a-b)=ca-cb$ 이다.
따라서 $ca \equiv cb \pmod{cn}$ 이다. ■

(c). 조건에 의하면 $n \mid a-b$ 이므로 $\frac{n}{d} \mid \frac{a-b}{d}=\frac{a}{d}-\frac{b}{d}$ 이다.
따라서 $\frac{a}{d} \equiv \frac{b}{d} \left(\mathrm{mod}\ \frac{n}{d}\right)$ 이다. ■

(d). 조건에 의하면 $n \mid a-b$ 이므로 적당한 정수 k가 존재해서 $a=nk+b$ 를
만족한다. 따라서 Lemma 1.3.1에 의하면 $\gcd(a,n)=\gcd(n,b)$ 이므로
$\gcd(a,n)=\gcd(b,n)$ 를 얻는다. ■

Problem 2.1.3 a, b, c, d는 정수이고 m, n은 자연수일 때 다음을 증명하시오.
(a). $n<p<2n$ 을 만족하는 모든 소수 p에 대해 $\binom{2n}{n} \equiv 0 \pmod{p}$ 이다.
(b). (a)에서 $m \geq 2$ 이면 $\binom{2n}{n} \not\equiv 0 \pmod{p^m}$ 이다.
(c). $r=\mathrm{lcm}(m,n)$ 라고 하자. 그러면 $a \equiv b \pmod{m}$ 와 $a \equiv b \pmod{n}$ 가
동시에 성립할 필요충분조건은 $a \equiv b \pmod{r}$ 이다.

특히 $\gcd(m,n)=1$ 이면 $r=mn$ 이므로 $a\equiv b\pmod m$ 와 $a\equiv b\pmod n$ 가 동시에 성립할 필요충분조건은 $a\equiv b\pmod{mn}$ 이다.

(d). $\gcd(b,n)=1$ 일 때 $ab\equiv cd\pmod n$ 이고 $b\equiv d\pmod n$ 이면 $a\equiv c\pmod n$ 이다.
(e). p가 소수이고 $ab\equiv 0\pmod p$ 이면 $a\equiv 0\pmod p$ 또는 $b\equiv 0\pmod p$ 이다.

(증명)
(a). 이항계수는 정수이고 $\binom{2n}{n}=\frac{(2n)!}{(n!)^2}$ 이므로 $(n!)^2\mid(2n)!=p\times\frac{(2n)!}{p}$ 이다.
여기서 p는 $n<p<2n$ 을 만족하는 소수이므로 $\frac{(2n)!}{p}$ 는 자연수이고 $p\nmid(n!)^2$ 이다.

만약 $p\mid(n!)^2$ 이면 p는 소수이므로 $1\le k\le n$ 을 만족하는 적당한 자연수 k에 대하여 $p\mid k$ 를 만족한다. 따라서 $p\le k\le n$ 인데 이것은 $n<p<2n$ 에 모순이다.
그러므로 $p\nmid(n!)^2$ 이고 따라서 $\gcd\left(p,(n!)^2\right)=1$ 이다.

즉, $(n!)^2\mid p\times\frac{(2n)!}{p}$ 인데 $\gcd\left(p,(n!)^2\right)=1$ 이므로 $(n!)^2\mid\frac{(2n)!}{p}$ 이다.
따라서 $\frac{(2n)!}{p(n!)^2}$ 는 자연수이므로 $p\mid\frac{(2n)!}{(n!)^2}=\binom{2n}{n}$ 에서 $\binom{2n}{n}\equiv 0\pmod p$ 이다. ■

(b). 먼저 $m=2$ 일 때 참이라는 것을 증명하자. (a)에 의하면 $p\mid\binom{2n}{n}=\frac{(2n)!}{(n!)^2}$ 이므로 $p\nmid\frac{(2n)!}{p(n!)^2}$ 을 증명하면 충분하다. 결론을 부정해서 $n<p<2n$ 을 만족하는 적당한 소수 p에 대하여 $p\mid\frac{(2n)!}{p(n!)^2}$ 라고 가정하자. 그러면 $\frac{(2n)!}{p(n!)^2}\mid\frac{(2n)!}{p}$ 이므로 $p\mid\frac{(2n)!}{p}$ 에서 $p^2\mid(2n)!$ 을 얻는다.

$n<p<2n$ 이므로 p는 홀수인 소수이다. $p=2$ 이면 $n<2<2n$ 을 만족하는 자연수 n은 존재하지 않아서 모순이다. 그러므로 $p>2$ 에서 $p^2>2p>2n$ 을 얻고 $\left\lfloor\frac{2n}{p^2}\right\rfloor=0$ 이다. 그리고 $1<\frac{2n}{p}<2$ 이므로 $\left\lfloor\frac{2n}{p}\right\rfloor=1$ 이다.

Problem 1.4.7 (b)에 의하면 $2n$ 이하의 자연수 중 p의 배수는 1개이고 p^2의 배수는 존재하지 않는다. 이것은 $p^2\mid(2n)!$ 에 모순이다. 그러므로 $\binom{2n}{n}\not\equiv 0\pmod{p^2}$ 이다.

이제 결론을 부정해서 $m \geq 2$ 인 적당한 자연수 m이 존재해서 $\binom{2n}{n} \equiv 0 \pmod{p^m}$ 를 만족한다고 가정하자. 그러면 $p^2 \mid p^m$ 이므로 Problem 2.1.2 (a)에 의하면 $\binom{2n}{n} \equiv 0 \pmod{p^2}$ 인데 이것은 모순이다.

그러므로 $m \geq 2$ 이면 $\binom{2n}{n} \not\equiv 0 \pmod{p^m}$ 이다. ■

(c). $(\Rightarrow)$ 조건에 의하면 $m \mid a-b,\ n \mid a-b$ 이고 $r = \mathrm{lcm}(m,n)$ 이므로 $r \mid a-b$ 가 성립한다. 따라서 $a \equiv b \pmod{r}$ 이다.

$(\Leftarrow)$ $m \mid r,\ n \mid r$ 이므로 Problem 2.1.2 (a)에 의하면 $a \equiv b \pmod{m}$ 이고 $a \equiv b \pmod{n}$ 이다. ■

(d). Problem 2.1.2 (d)에 의하면 $\gcd(b,n) = \gcd(d,n) = 1$ 이다. 따라서 법 n에서 b, d의 곱셈에 대한 역원은 존재하고 이고 $b \equiv d \pmod{n}$ 이므로 $b^{-1} \equiv d^{-1} \pmod{n}$ 이다. 그리고 $ab \equiv cd \pmod{n}$ 이므로 다음을 얻는다.

$$a \equiv a\left(bb^{-1}\right) \equiv (ab)b^{-1} \equiv (cd)d^{-1} \equiv c\left(dd^{-1}\right) \equiv c \pmod{n}$$

■

(e). 조건에 의하면 $p \mid ab$ 이고 p는 소수이므로 $p \mid a$ 또는 $p \mid b$ 이다. 따라서 $a \equiv 0 \pmod{p}$ 또는 $b \equiv 0 \pmod{p}$ 이다. ■

Problem 2.1.3의 (c)에서 $\gcd(m,n) = 1$ 인 경우의 결과에 해당하는 $a \equiv b \pmod{m}$ 와 $a \equiv b \pmod{n}$ 가 동시에 성립할 필요충분조건이 $a \equiv b \pmod{mn}$ 이라는 것과 (e)의 결과는 나중에 많이 사용하기 때문에 기억해놓으면 편합니다.

Problem 2.1.4 자연수 n과 정수 m, r에 대하여 $\{a_1, a_2, \ldots, a_n\}$이 법 n에 대한 완전잉여계이고 $\gcd(m,n) = 1$ 이면 $\{ma_1 + r, ma_2 + r, \ldots, ma_n + r\}$도 법 n에 대한 완전잉여계임을 증명하시오.

(증명)

$\{a_1, a_2, \ldots, a_n\}$가 법 n에 대한 완전잉여계이고 $\gcd(m,n) = 1$ 이므로 다음을 얻는다.

$$\begin{aligned} & ma_i + r \equiv ma_j + r \pmod{n} \\ \Rightarrow\ & ma_i \equiv ma_j \pmod{n} \\ \Rightarrow\ & a_i \equiv a_j \pmod{n} \\ \Rightarrow\ & i = j \end{aligned}$$

그리고 집합 $\{ma_1 + r, ma_2 + r, \ldots, ma_n + r\}$은 원소의 개수가 n개이므로 $\{ma_1 + r, ma_2 + r, \ldots, ma_n + r\}$도 법 n에 대한 완전잉여계이다. ■

Problem 2.1.4의 결과는 $\gcd(m,n)=1$ 이라는 조건이 없으면 성립하지 않을수도 있습니다. $\mathbb{Z}_4=\{0,1,2,3\}$는 법 4에 대한 완전잉여계인데 $m=2, r=0$ 이면 $\{0,2,4,6\}$은 $2\equiv 6 \pmod 4$ 이므로 법 4에 대한 완전잉여계가 아닙니다.

그러므로 다항식 $f(x)\in\mathbb{Z}[x]$를 다항함수로 봤을 때 단사함수가 된다고 해서 $\{a_1,a_2,...,a_n\}$가 법 n에 대한 완전잉여계일 때 $\{f(a_1),f(a_2),...,f(a_n)\}$가 법 n에 대한 완전잉여계가 되는건 아닙니다.

Problem 2.1.5 자연수 n에 대하여 다음을 증명하시오.
(a). 적당한 자연수 m이 존재해서 모든 $a\in\mathbb{Z}$ 에 대해 $ma\equiv 0 \pmod n$ 을 만족하면 $n \mid m$ 이 성립함을 증명하시오.
(b). $n\geq 3$ 이고 m이 짝수인 자연수이면 $\{0^m,1^m,2^m,...,(n-1)^m\}$은 법 n에 대한 완전잉여계가 될수 없음을 증명하시오.

(증명)
(a). 집합 S 를 $S=\{t\in\mathbb{N} : \text{모든 } a\in\mathbb{Z}\text{에 대하여 } ta\equiv 0 \pmod n\}$ 라고 하자. 그러면 $n\in S$ 이므로 S 는 공집합이 아닌 자연수 집합의 부분집합이다. 따라서 정렬원리에 의하면 가장 작은 원소를 갖는다. 그것을 s라고 하고 $s=n$ 임을 보이자.

$s\in S$ 이므로 $a=1$ 일 때 $s\equiv 0 \pmod n$ 을 만족해야 한다. 따라서 $n \mid s$ 이고 n, s는 자연수이므로 $n\leq s$ 를 얻는다. 그리고 $n\in S$ 이고 s가 S 의 가장 작은 원소이므로 $s\leq n$ 이다. 따라서 $s=n$ 을 얻는다.

이제 $n \mid m$ 을 증명하자. m을 n으로 나누었을때의 몫을 q, 나머지를 r이라고 하면 $m=nq+r\ (0\leq r<n)$ 을 만족한다.

결론을 부정해서 $r\neq 0$ 이라고 가정하면 r은 자연수이고
$ma\equiv 0 \pmod n$, $na\equiv 0 \pmod n$ 이므로 $ra\equiv (m-nq)a\equiv 0 \pmod n$
에서 $r\in S$ 인데 이것은 n이 S 의 가장 작은 원소라는 것에 모순이다.

따라서 $r=0$ 이고 그러므로 $m=nq$ 이다. 즉, $n \mid m$ 이다. ■

(b). $n\geq 3$ 이므로 $a\not\equiv -a \pmod n$ 를 만족하는 $a\in\mathbb{Z}$ 가 존재한다. 결론을 부정해서 모든 $a\in\mathbb{Z}$ 에 대하여 $a\equiv -a \pmod n$ 즉, $2a\equiv 0 \pmod n$ 를 만족한다고 하면 (a)에 의해 $n \mid 2$ 이므로 $n=1,2$ 인데 이것은 모순이다.

그리고 완전잉여계와 합동의 정의에 의하면 $a\not\equiv -a \pmod n$ 를 만족하는 $a\in\mathbb{Z}$ 를 $a\in\mathbb{Z}_n$ 에서 택할수 있다. 따라서 $a\not\equiv -a \pmod n$ 를 만족하는 $a\in\mathbb{Z}_n$ 를 택하자.

$n-a \equiv -a \pmod{n}$ 인데 $a \not\equiv -a \pmod{n}$ 이므로 $a \not\equiv n-a \pmod{n}$ 이다.
그리고 m은 짝수이므로 $(n-a)^m \equiv (-a)^m \equiv a^m \pmod{n}$ 을 얻는다.

즉, $a^m \equiv (n-a)^m \pmod{n}$ 와 $a \not\equiv n-a \pmod{n}$ 를 동시에 만족하는
$a \in \mathbb{Z}_n$ 가 존재하므로 $\{0^m, 1^m, 2^m, ..., (n-1)^m\}$은 법 n에 대한 완전잉여계가
될수 없다. ■

Problem 2.1.6 $a > b$ 인 두 자연수 a, b 가 $\gcd(a,b)=1$ 을 만족한다고 하자.
두 자연수 m, n에 대하여 $d=\gcd(m,n)$ 이면 다음 등식이 성립함을 증명하시오.

$$\gcd(a^m-b^m, a^n-b^n)=a^d-b^d$$

이것은 Problem 1.3.6의 일반화이다.

(증명)
$r=\gcd(a^m-b^m, a^n-b^n)$ 라고 하고 먼저 $\gcd(a,r)=\gcd(b,r)=1$ 임을 보이자.

$t=\gcd(a,r)$ 라고 하면 $t \mid r$ 이고 $r \mid a^m-b^m$ 이므로 $t \mid a^m-b^m$ 이다.
그리고 $t \mid a$ 이므로 $t \mid a^m-(a^m-b^m)=b^m$ 을 얻고 $\gcd(a,b)=1$ 이므로
$\gcd(a,b^m)=1$ 이다.

그러므로 $au+b^mv=1$ 을 만족하는 적당한 정수 u, v 가 존재하고 따라서
$t \mid au+b^mv=1$ 이므로 $t=\gcd(a,r)=1$ 이다. 같은 방법으로 $\gcd(b,r)=1$ 도
얻을수 있다.

$d=\gcd(m,n)$ 이므로 적당한 정수 x, y 가 존재해서 $mx+ny=d$ 를 만족하고
$\gcd(w,z)=1$ 을 만족하는 자연수 w, z 에 대하여 $m=dw, n=dz$ 이다.
따라서 다음 등식을 얻을수 있다.

$$a^m-b^m=(a^d)^w-(b^d)^w=(a^d-b^d)(a^{d(w-1)}+a^{d(w-2)}b^d+\cdots+b^{d(w-1)})$$
$$a^n-b^n=(a^d)^z-(b^d)^z=(a^d-b^d)(a^{d(z-1)}+a^{d(z-2)}b^d+\cdots+b^{d(z-1)})$$

$a^d-b^d \mid a^m-b^m$, $a^d-b^d \mid a^n-b^n$ 이고 $a>b$ 이므로 a^d-b^d 는
자연수이다. 그러므로 $a^d-b^d \le r$ 이다. (1)

한편 $r=\gcd(a^m-b^m, a^n-b^n)$ 이므로 다음을 얻는다.

$$a^m \equiv b^m \pmod{r},\ a^n \equiv b^n \pmod{r}$$

$\gcd(a,r)=\gcd(b,r)=1$ 이므로 a, b 는 법 r에서 곱셈에 대한 역원이 존재한다.
그러므로 합동식에서 정수 지수법칙을 사용할수 있고 따라서 다음을 얻는다.

$$a^d \equiv a^{mx+ny} \equiv (a^m)^x(a^n)^y \equiv (b^m)^x(b^n)^y \equiv b^{mx+ny} \equiv b^d \pmod{r}$$

그러므로 $r \mid a^d - b^d$ 이고 따라서 $r \leq a^d - b^d$ 이다. (2)

(1), (2)에 의하면 $r = a^d - b^d$ 이다. 즉, $\gcd(a^m - b^m, a^n - b^n) = a^d - b^d$ 가 성립한다. ■

1.2절에서 a, b 가 적어도 하나는 0이 아닌 정수일 때 $d = \gcd(a,b)$ 이면 $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ 임을 증명했습니다. 즉, $x, y \in \mathbb{Z}$ 이면 $ax + by$ 는 d의 배수가 됩니다. 특히 $d = 1$ 이면 $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$ 이므로 $ax + by$ 는 모든 정수값을 다 가질수 있습니다.

여기서 x, y 의 범위를 정수 전체가 아니고 음이 아닌 정수로 제한시키면 다음 정리를 얻을수 있습니다. 범위를 제한시켰다는 사실을 생각해보면 신기한 결과입니다.

Theorem 2.1.4 $\gcd(a,b) = 1$ 을 만족하는 자연수 a, b가 임의로 주어져있다고 하자. 그러면 음이 아닌 정수 x, y 에 대하여 $ax + by$ 형태로 표현되지 않는 정수중 가장 큰 정수는 $ab - a - b$ 이다.

즉, 집합 S 를 $S = \{ax + by \in \mathbb{Z} : x, y\text{는 음이 아닌 정수}\}$ 라고 할 때 (3)을 만족하는 음이 아닌 정수 n의 최솟값은 $ab - a - b + 1 = (a-1)(b-1)$ 이고 $n \geq (a-1)(b-1)$ 을 만족하는 모든 정수 n은 (3)을 만족한다.

$$n \in S \text{ 이면 } n + 1 \in S \text{ 이다.} \quad (3)$$

(증명)
다음 두가지를 증명하면 충분하다.

step1) $ax + by = ab - a - b$ 를 만족하는 음이 아닌 정수 x, y 는 존재하지 않는다.
step2) $n \geq (a-1)(b-1)$ 을 만족하는 모든 정수 n에 대하여 $ax + by = n$ 을 만족하는 음이 아닌 정수 x, y 가 존재한다.

step1) 결론을 부정해서 $ax + by = ab - a - b$ 를 만족하는 음이 아닌 정수 x, y 가 존재한다고 가정하자. 그러면 $ax + by - ab + a + b = 0$ 이므로 다음을 얻는다.

$$ax + by - ab + a + b \equiv b(1+y) \equiv 0 \pmod{a}$$

$\gcd(a,b) = 1$ 이므로 a는 법 b에서 곱셈에 대한 역원이 존재한다.
따라서 $1 + y \equiv 0 \pmod{a}$ 이므로 $a \mid 1 + y$ 이고 $a, 1 + y$ 는 자연수이므로 $a \leq 1 + y$ 를 얻는다. 그러므로 $y \geq a - 1$ 이다.

한편 $ax + by - ab + a + b = 0$ 이므로 $a(1+x) \equiv 0 \pmod{b}$ 를 얻고 $\gcd(a,b) = 1$ 이므로 $1 + x \equiv 0 \pmod{b}$ 에서 $b \mid 1 + x$ 이다. 마찬가지로 $b, 1 + x$ 는 자연수이므로 $b \leq 1 + x$ 에서 $x \geq b - 1$ 을 얻는다.

그러므로 $ax+by \geq a(b-1)+b(a-1)=2ab-a-b$ 인데 a,b 는 자연수이므로 $2ab-a-b > ab-a-b$ 에서 $ax+by > ab-a-b$ 이다. 이것은 모순이다. 따라서 $ax+by=ab-a-b$ 를 만족하는 음이 아닌 정수 x,y 는 존재하지 않는다.

step2) $\gcd(a,b)=1$ 이므로 Problem 2.1.4에 의하면 $\{0,a,2a,...,(b-1)a\}$는 법 b에 대한 완전잉여계이다. 따라서 $n \geq (a-1)(b-1)$ 을 만족하는 모든 정수 n에 대하여 $ak \equiv n \pmod{b}$ 를 만족하는 $0 \leq k \leq b-1$ 인 정수 k가 존재한다.

그러므로 $b \mid n-ak$ 이다. 따라서 적당한 정수 s가 존재해서 $ak+bs=n$ 을 만족한다. 그리고 $n \geq (a-1)(b-1)$ 이고 $0 \leq k \leq b-1$ 이므로 다음을 얻는다.

$$n-ak \geq (a-1)(b-1)-(b-1)a = -b+1 > -b$$

$n-ak > -b$ 인데 $b \mid n-ak$ 이므로 $n-ak \geq 0$ 이어야 하고 $bs=n-ak \geq 0$ 인데 b는 자연수이므로 $s \geq 0$ 이다. 즉, $ax+by=n$ 을 만족하는 음이 아닌 정수 x,y 는 $x=k,\ y=s$ 로 존재한다.

따라서 step1), step2)에 의하면 주어진 정리는 참이다. ■

Theorem 2.1.4에서 오해하면 안되는 부분은 $(a-1)(b-1)$ 이 집합 $S=\{ax+by \in \mathbb{Z} : x,y\text{는 음이 아닌 정수}\}$의 가장 작은 원소가 아니라는 것입니다.

예를 들어 $a=3, b=11$ 이면 $\gcd(a,b)=1$ 이고 음이 아닌 정수 x,y 에 대하여 $3x+11y \geq 0$ 입니다. 그리고 $x=y=0$ 이면 $3x+11y=0$ 이므로 S 의 가장 작은 원소는 0입니다. $(a-1)(b-1)=20$ 이 아닙니다.

x,y 의 범위를 자연수로 한정해도 최솟값은 $x=y=1$ 일 때 14이고 이것은 20보다 작은 값입니다. 따라서 $(a-1)(b-1)$ 을 $ax+by$ 의 최솟값으로 오해하면 안됩니다.

법 n에서 a의 곱셈에 대한 역원이 존재할 필요충분조건은 $\gcd(a,n)=1$ 입니다. 즉, 법 n에서는 n과 서로소인 정수만 곱셈에 대한 역원을 갖습니다.

합동식은 완전잉여계에서만 고려해도 충분하기 때문에 $\mathbb{Z}_n=\{0,1,2,...,n-1\}$에서 n 이하의 자연수중 n과 서로소인 자연수만 법 n에서 곱셈에 대한 역원을 갖습니다.

따라서 $\mathbb{Z}_n$에서 곱셈에 대한 역원을 갖는 원소의 개수는 n 이하의 자연수중 n과 서로소인 자연수의 개수와 같습니다. 수학에서는 n 이하의 자연수중 n과 서로소인 자연수의 개수를 다음과 같은 기호로 나타냅니다.

Definition 2.1.4 오일러의 ϕ함수(Euler's ϕ-Function)
n 이하의 자연수중 n과 서로소인 자연수의 개수를 기호로 $\phi(n)$으로 나타내고 $\phi(n)$을 **오일러의 ϕ함수(Euler's ϕ-Function)**라고 부른다.

작은 n에 대해서는 일일이 세보면 $\phi(n)$을 구할수 있습니다. $\phi(1)=1$ 은 명백하고 6 이하의 자연수 $1,2,3,4,5,6$ 중 6과 서로소인 자연수는 $1,5$ 이므로 $\phi(6)=2$ 입니다.

p가 소수이면 1부터 $p-1$ 까지의 자연수는 모두 p와 서로소이므로 $\phi(p)=p-1$ 임을 쉽게 알수 있습니다.

그리고 p가 소수일 때 자연수 k에 대하여 p^k와 서로소인 자연수는 p의 배수가 아닌 것 뿐입니다. $d=\gcd(a,p^k)$ 라고 하고 $d\geq 2$ 라고 가정하면 $q\mid d$ 를 만족하는 소수 q가 존재하므로 $q\mid p^k$ 인데 p도 소수이므로 $q=p$ 입니다.

따라서 $p\mid a$ 이므로 a는 p의 배수입니다. 그러므로 $d=1$ 이면 a는 p의 배수가 아니고 Problem 1.4.7 (b)에 의하면 다음 등식이 성립합니다.

$$\phi(p^k)=p^k-\left\lfloor \frac{p^k}{p} \right\rfloor = p^k-p^{k-1}=p^{k-1}(p-1) \tag{4}$$

그런데 n이 크면 이렇게 일일이 세는 방법으로 구하는게 비효율적입니다.
따라서 오일러의 ϕ함수의 값을 쉽게 계산할수 있는 방법이 필요한데 쉬운 계산법을 유도해주는게 다음 정리입니다.

Theorem 2.1.5 $\gcd(m,n)=1$ 을 만족하는 모든 자연수 m,n에 대하여 $\phi(mn)=\phi(m)\phi(n)$ 가 성립한다.

(증명)
$\phi(1)=1$ 이므로 m,n 둘중 적어도 하나가 1이면 $\phi(mn)=\phi(m)\phi(n)$ 는 명백하다.
따라서 m,n이 모두 2 이상의 자연수라고 가정하자.

Problem 1.2.15 (a)에 의하면 자연수 a에 대하여 $\gcd(a,mn)=1$ 일 필요충분조건은 $\gcd(a,m)=\gcd(a,n)=1$ 인 것이다. 그러므로 mn 이하의 자연수중 mn과 서로소인 자연수는 m,n과 모두 서로소이고 역도 성립한다. (5)

1부터 mn까지의 정수를 다음과 같이 $m\times n$개의 바둑판식으로 배열하자.

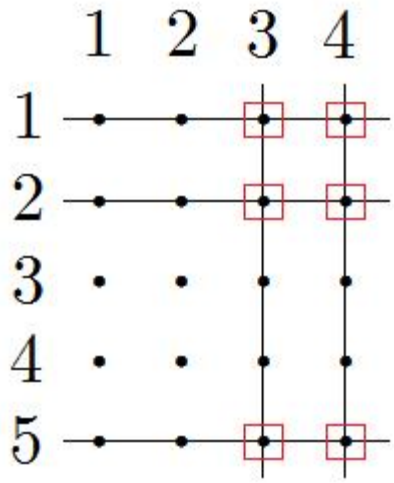
$$\begin{array}{ccccccc} 1 & 2 & \cdots & r & \cdots & n \\ n+1 & n+2 & \cdots & n+r & \cdots & 2n \\ 2n+1 & 2n+2 & \cdots & 2n+r & \cdots & 3n \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ (m-1)n+1 & (m-1)n+2 & \cdots & (m-1)n+r & \cdots & mn \end{array} \tag{6}$$

$0\equiv n \pmod n$ 이므로 (6)의 첫 번째 행 $\{1,2,...,n\}$은 법 n에 대한 완전잉여계이고 첫 번째 행에서 n과 서로소인 자연수의 개수는 $\phi(n)$이다. 그리고 (6)의 각 열은 법 n에 대하여 모두 합동이다. 즉, $0\leq s,t\leq m-1$ 일 때 $sn+r\equiv tn+r \pmod n$ 이다.

따라서 (6)의 각 행은 모두 법 n에 대한 완전잉여계이고 Problem 2.1.2 (d)에 의하면 $\gcd(sn+r,n)=\gcd(tn+r,n)$ 이므로 (6)의 각 행에서 n과 서로소인 자연수의 개수는 첫 번째 행에서 n과 서로소인 자연수의 개수 $\phi(n)$과 같다.

한편 $\{0,1,2,...,m-1\}$은 법 m에 대한 완전잉여계이고 $\gcd(m,n)=1$ 이므로 Problem 2.1.4에 의하면 (6)의 각 열은 법 m에 대한 완전잉여계이다. 그러므로 이 경우에도 각 열에서 m과 서로소인 자연수의 개수는 $\phi(m)$임을 알수 있다.

마지막으로 간단한 사실을 기억하자. 예를 들어 20개의 점이 다음과 같이 배열되어 있으면 $1,2,5$행과 $3,4$열에 있는 점의 개수는 $3\times 2=6$ 으로 계산할수 있다.



따라서 (6)에 있는 자연수중 m,n과 서로소인 자연수의 개수는 $\phi(m)\phi(n)$이고 (5)에 의하면 이것은 $\phi(mn)$과 같다. 그러므로 $\phi(mn)=\phi(m)\phi(n)$ 이다. ■

$\gcd(m,n)=1$ 일 때 $\phi(mn)=\phi(m)\phi(n)$ 가 성립하면 $\phi(n)$을 쉽게 계산할수 있는데 그 이유는 모든 합성수는 소인수분해가 가능하다는 산술의 기본정리 때문입니다.

수학적 귀납법을 이용하면 $i\neq j$ 일 때 $\gcd(m_i,m_j)=1$ 을 만족하는 n개의 자연수 $m_1,m_2,...,m_n$ 가 임의로 주어져있을 때 $\phi(m_1m_2\cdots m_n)=\phi(m_1)\phi(m_2)\cdots\phi(m_n)$ 가 성립한다는 것을 증명할수 있고 이 등식과 소인수분해를 이용하면 됩니다.

자세한 내용은 다음과 같습니다.

Corollary 2.1.2 다음이 성립한다.

(a). $n\geq 2$ 일 때 n을 소인수분해한 결과가 $n=p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ 이면 다음이 성립한다.

$$\begin{aligned}\phi(n)&=\left(p_1^{k_1}-p_1^{k_1-1}\right)\left(p_2^{k_2}-p_2^{k_2-1}\right)\cdots\left(p_r^{k_r}-p_r^{k_r-1}\right)\\&=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)\end{aligned}$$

(b). $n\geq 3$ 이면 $\phi(n)$은 짝수이다.

(증명)

(a). $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ 이면 $i \neq j$ 일 때 p_i, p_j는 서로 다른 소수이므로

$\gcd\left(p_i^{k_i}, p_j^{k_j}\right) = 1$ 이다. 따라서 Theorem 2.1.5와 (4)에 의하면 다음 등식이 성립한다.

$$\begin{aligned}\phi(n) &= \phi\left(p_1^{k_1}\right)\phi\left(p_2^{k_2}\right)\cdots\phi\left(p_r^{k_r}\right)\\ &= \left(p_1^{k_1} - p_1^{k_1-1}\right)\left(p_2^{k_2} - p_2^{k_2-1}\right)\cdots\left(p_r^{k_r} - p_r^{k_r-1}\right)\\ &= p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)\\ &= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)\end{aligned}$$

■

(b). $n \geq 3$ 이고 $\phi(2) = 1$ 이므로 (a)에 의하면 n을 소인수분해 했을 때 $2^k\ (k \geq 2)$를 소인수로 가질 때와 갖지 않을 때 이렇게 두가지 경우만 고려하면 충분하다.

case1) $2^k\ (k \geq 2)$를 소인수로 가짐.

$\phi\left(2^k\right) = 2^k - 2^{k-1} = 2^{k-1}$ 이고 $k \geq 2$ 이므로 $\phi\left(2^k\right)$는 짝수이다.

따라서 (a)에 의하면 $\phi(n)$은 짝수이다.

case2) $2^k\ (k \geq 2)$를 소인수로 갖지 않음.

이 경우 n은 적당한 홀수인 소수 p와 적당한 자연수 m에 대하여 p^m을 소인수로 갖고 $\phi\left(p^m\right) = p^m - p^{m-1} = p^{m-1}(p-1)$ 인데 $p-1$ 은 짝수이므로 (a)에 의하면 $\phi(n)$은 짝수이다.

그러므로 $n \geq 3$ 이면 $\phi(n)$은 짝수이다. ■

$360 = 2^3 \times 3^2 \times 5$ 이므로 $\phi(360) = 360 \times \left(1-\frac{1}{2}\right) \times \left(1-\frac{1}{3}\right) \times \left(1-\frac{1}{5}\right) = 96$

입니다. 따라서 Corollary 2.1.2를 이용하면 $\phi(n)$을 쉽게 계산할수 있습니다.

즉, 법 n에서 곱셈에 대한 역원이 존재하는 자연수의 개수를 쉽게 계산할수 있습니다.

법 n에서 곱셈에 대한 역원이 존재하는 특별한 $\phi(n)$개의 정수를 다음과 같이 정의합니다.

Definition 2.1.5 기약잉여계(Reduced Residue System)

자연수 n에 대하여 $\{a_1, a_2, ..., a_n\}$을 법 n에 대한 완전잉여계라고 할 때 $a_1, a_2, ..., a_n$ 중 n과 서로소인 정수 $b_1, b_2, ..., b_{\phi(n)}$ 를 모은 집합 $\{b_1, b_2, ..., b_{\phi(n)}\}$을 법 n에 대한 **기약잉여계(Reduced Residue System)**라고 정의한다.

정의에 의하면 법 n에 대한 기약잉여계는 적당한 법 n에 대한 완전잉여계의 부분집합이 됩니다. 따라서 기약잉여계를 쉽게 찾는 방법은 완전잉여계를 먼저 찾고 완전잉여계의 원소들 중에서 n과 서로소인 정수를 찾는겁니다.

가장 자연스러운 완전잉여계가 $\mathbb{Z}_n = \{0,1,2,...,n-1\}$이므로 가장 자연스러운 기약잉여계는 $\mathbb{Z}_n$의 원소들 중에서 n과 서로소인 정수를 모은 집합입니다.

이렇게 $\mathbb{Z}_n$에서 찾은 가장 자연스러운 기약잉여계를 기호로는 $\mathbb{Z}_n^{\times}$ 이렇게 씁니다.
좀 더 엄밀하게 정의하면 $\mathbb{Z}_n^{\times} = \{a \in \mathbb{Z}_n : \gcd(a,n) = 1\}$ 입니다.

Problem 2.1.2 (d)에서 $\gcd(a,n) = 1$ 이고 $a \equiv b \pmod{n}$ 이면 $\gcd(b,n) = 1$ 이므로 법 n에 대한 모든 기약잉여계는 $\mathbb{Z}_n^{\times}$과 일대일 대응이 존재한다는 것을 쉽게 알수 있습니다.

이제 정수론에서 많이 사용하는 기호를 정의하겠습니다.

Definition 2.1.6 자연수 n에 대하여 n의 서로 다른 모든 양의 약수를 $d_1, d_2, ..., d_m$ 이라고 하자. 그러면 다음과 같이 정의한다.

$$\sum_{d \mid n} f(d) = f(d_1) + f(d_2) + \cdots + f(d_m)$$
$$\prod_{d \mid n} f(d) = f(d_1) f(d_2) \cdots f(d_m)$$

예를 들면 $\sum_{d \mid 4} f(d) = f(1) + f(2) + f(4)$ 이고 $\prod_{d \mid 4} f(d) = f(1) f(2) f(4)$ 입니다.

그리고 $d \mid n$ 이면 $n = d \times \frac{n}{d}$ 이고 $\frac{n}{d}$ 도 자연수이므로 $\frac{n}{d} \mid n$ 입니다.

따라서 d가 n의 모든 양의 약수를 나타내면 $\frac{n}{d}$도 모든 양의 약수를 나타내므로 다음 등식이 성립함은 명백합니다.

$$\sum_{d \mid n} f(d) = \sum_{d \mid n} f\left(\frac{n}{d}\right)$$
$$\prod_{d \mid n} f(d) = \prod_{d \mid n} f\left(\frac{n}{d}\right) \tag{7}$$

다음 정리는 가우스가 증명한 정리입니다. 이 정리는 나중에 다시 보게 될겁니다.

Theorem 2.1.6 가우스의 정리(Gauss's Theorem)
모든 자연수 n에 대하여 $n = \sum_{d \mid n} \phi(d)$ 이다. 여기서 $\phi(n)$은 오일러의 ϕ함수이다.

(증명)
자연수 n을 임의로 하나 택하고 n의 양의 약수 d에 대하여 S_d 를 다음과 같이 정의하자.

$$S_d = \{m \in \{1,2,...,n\} : \gcd(m,n) = d\}$$

n의 서로 다른 모든 양의 약수를 $d_1, d_2, ..., d_m$ 라고 하자. 그러면 $i \neq j$ 일 때 $d_i \neq d_j$ 이므로 $S_{d_i} \cap S_{d_j} = \varnothing$ 이고 $\bigcup_{i=1}^{m} S_{d_i} \subset \{1,2,...,n\}$ 는 명백하다.

따라서 $\{1,2,...,n\} \subset \bigcup_{i=1}^{m} S_{d_i}$ 를 증명하자.

임의의 $k \in \{1,2,...,n\}$ 를 택하자. 그러면 $\gcd(k,n)$은 n의 양의 약수이므로 $k \in S_{\gcd(k,n)}$ 이다. 따라서 $\{1,2,...,n\} \subset \bigcup_{i=1}^{m} S_{d_i}$ 이므로 정리하면 다음을 얻는다.

(a). $\{1,2,...,n\} = \bigcup_{i=1}^{m} S_{d_i}$

(b). $i \neq j$ 이면 $S_{d_i} \cap S_{d_j} = \varnothing$

그러므로 집합 $\{1,2,...,n\}$의 원소의 개수 n은 각각의 $i = 1,2,...,m$ 에 대하여 S_{d_i}의 원소의 개수를 모두 더한것과 같다. (8)

이제 고정된 n의 양의 약수 d에 대하여 S_d의 원소의 개수를 구하자. $m \in S_d$ 이면 $\gcd(m,n) = d$ 이므로 $d \mid m$, $d \mid n$ 이고 따라서 적당한 자연수 r, s가 존재해서 $m = dr$, $n = ds$, $\gcd(r,s) = 1$ 을 만족한다.

여기서 n과 d는 고정된 자연수이므로 $\gcd(r,s) = 1$ 을 만족하는 r이 결정되면 m도 결정된다. 역으로 m이 결정되면 $\gcd(r,s) = 1$ 을 만족하는 r도 결정된다. 그리고 S_d의 정의에 의하면 $m \leq n$ 이므로 $r \leq s$ 이다.

따라서 S_d의 원소의 개수는 $r \leq s$ 와 $\gcd(r,s) = 1$ 을 만족하는 자연수 r의 개수이고 $s = \frac{n}{d}$ 이므로 결국 자연수 r의 개수는 $\frac{n}{d}$ 이하의 자연수 중 $\frac{n}{d}$와 서로소인 자연수의 개수인 $\phi\left(\frac{n}{d}\right)$와 같다.

(7)에 의하면 $\sum_{d \mid n} \phi\left(\frac{n}{d}\right) = \sum_{d \mid n} \phi(d)$ 이므로 (8)에 의하면 다음 등식을 얻는다.

$$n = \sum_{d \mid n} \phi\left(\frac{n}{d}\right) = \sum_{d \mid n} \phi(d)$$

■

예를 들면 $n=10$ 일 때 10의 양의 약수는 $1,2,5,10$ 이고

$$S_1=\{m\in\{1,2,...,10\}:\gcd(m,10)=1\}=\{1,3,7,9\}$$
$$S_2=\{m\in\{1,2,...,10\}:\gcd(m,10)=2\}=\{2,4,6,8\}$$
$$S_5=\{m\in\{1,2,...,10\}:\gcd(m,10)=5\}=\{5\}$$
$$S_{10}=\{m\in\{1,2,...,10\}:\gcd(m,10)=10\}=\{10\}$$

이므로 원소의 개수의 합은 $4+4+1+1=10$ 입니다.

그리고 $\phi(1)+\phi(2)+\phi(5)+\phi(10)=1+1+4+4=10$ 입니다.

Problem 2.1.7 n이 홀수이면 다음은 법 n에 대한 완전잉여계임을 증명하시오.

$$S=\left\{-\frac{n-1}{2},-\frac{n-3}{2},\ ...,\ -2,-1,0,1,2,\ ...,\ \frac{n-3}{2},\frac{n-1}{2}\right\}$$

(증명)

집합 S 의 원소가 n개 있음은 명백하다. 그리고 다음을 얻는다.

$$-\frac{n-1}{2}\equiv\frac{n+1}{2}\pmod n$$
$$-\frac{n-3}{2}\equiv\frac{n+3}{2}\pmod n$$
$$\vdots$$
$$-1\equiv-\frac{n-(n-2)}{2}\equiv\frac{n+(n-2)}{2}\equiv n-1\pmod n$$

그러므로 S 의 원소는 법 n에 대하여 $\mathbb{Z}_n$과 일대일 대응이 된다.

따라서 S 는 법 n에 대한 완전잉여계이다. ■

Problem 2.1.7은 n이 홀수일 때 사용하기 편한 완전잉여계입니다. 0을 기준으로 좌우 대칭이기 때문에 짝수 거듭제곱만 있는 합동식에서 많이 사용합니다.

$n=13$ 일 때 $x^2\equiv3\pmod{13}$ 을 만족하는 x를 찾아야 하는 경우 $\mathbb{Z}_{13}$ 의 원소를 대입하는것보단 다음 S 의 원소를 대입하는게 계산하기 편합니다.

$$S=\{-6,-5,-4,-3,-2,-1,0,1,2,3,4,5,6\}$$

부호만 다른 것은 제곱하면 같아지므로 $x^2\equiv3\pmod{13}$ 에 $x=0,1,2,3,4,5,6$ 이것만 대입해보면 됩니다. $\mathbb{Z}_{13}$의 원소를 대입하려면 13개를 대입해야 하는데 S 의 원소를 대입하면 확인해야하는 원소의 개수를 7개로 줄일수 있습니다.

실제로 대입해보면 음이 아닌 정수들 중엔 $x=4$ 만 해가 된다는 것을 알수 있습니다.

그러므로 $x=\pm4$ 는 $x^2\equiv3\pmod{13}$ 을 만족하고 따라서 $\mathbb{Z}_{13}$의 원소들 중엔 $x=4,9$ 만 해가 된다는 것을 알수 있습니다.

Problem 2.1.8 자연수 n에 대하여 $\{r_1, r_2, ..., r_{\phi(n)}\}$가 법 n에 대한 기약잉여계이고 $\gcd(a,n)=1$ 이면 $\{ar_1, ar_2, ..., ar_{\phi(n)}\}$도 법 n에 대한 기약잉여계임을 증명하시오.

(증명)
각각의 $i=1,2,...,\phi(n)$ 에 대하여 $\gcd(r_i,n)=1$ 이고 $\gcd(a,n)=1$ 이므로 $\gcd(ar_i,n)=1$ 을 얻는다. 따라서 ar_i는 법 n에서 곱셈에 대한 역원이 존재하고 다음을 얻을수 있다.

$$ar_i \equiv ar_j \pmod{n} \Rightarrow r_i \equiv r_j \pmod{n} \Rightarrow i=j$$

따라서 $\{ar_1, ar_2, ..., ar_{\phi(n)}\}$도 법 n에 대한 기약잉여계이다. ■

Problem 2.1.8에서 기약잉여계의 원소에 덧셈을 한 것은 기약잉여계가 안될 수도 있습니다. $\mathbb{Z}_6^{\times}=\{1,5\}$ 는 법 6에 대한 기약잉여계인데 각각의 원소에 1을 더한 $\{2,6\}$은 $\gcd(2,6)=2, \gcd(6,6)=6$ 이므로 법 6에 대한 기약잉여계가 될수 없습니다.

Problem 2.1.9 $n \geq 2$ 를 만족하는 자연수 n에 대하여 법 n에 대한 기약잉여계 $\mathbb{Z}_n^{\times}$을 $\mathbb{Z}_n^{\times}=\{r_1, r_2, ..., r_{\phi(n)}\}$ 라고 할 때 $r_1+r_2+\cdots+r_{\phi(n)}=\dfrac{n\phi(n)}{2}$ 임을 증명하시오.

(증명)
$a \in \mathbb{Z}_n$ 이면 $\gcd(a,n)=1$ 이므로 $\gcd(n-a,n)=1$ 이다. 그리고 $n \geq 2$ 이므로 $a \in \mathbb{Z}_n^{\times}$ 이면 $1 \leq a \leq n-1$ 이다. 따라서 $1 \leq n-a \leq n-1$ 이므로 $n-a \in \mathbb{Z}_n^{\times}$ 이다. 그러므로 다음 등식이 성립한다.

$$\begin{aligned} r_1+r_2+\cdots+r_{\phi(n)} &= (n-r_1)+(n-r_2)+\cdots+(n-r_{\phi(n)}) \\ &= n\phi(n)-(r_1+r_2+\cdots+r_{\phi(n)}) \end{aligned}$$

정리하면 $2(r_1+r_2+\cdots+r_{\phi(n)})=n\phi(n)$ 이고 $r_1+r_2+\cdots+r_{\phi(n)}=\dfrac{n\phi(n)}{2}$ 을 얻는다. ■

Problem 2.1.10 n은 자연수이고 p는 소수일 때 다음을 증명하시오.
(a). $\phi(pn)=p\phi(n)$ 이 성립할 필요충분조건은 $p \mid n$ 이다.
(b). $\phi(pn)=(p-1)\phi(n)$ 이 성립할 필요충분조건은 $p \nmid n$ 이다.

(증명)
(a). $(\Rightarrow)$ 결론을 부정해서 $p \nmid n$ 라고 가정하자. 그러면 p는 소수이므로 $\gcd(p,n)=1$ 이고 따라서 $\phi(pn)=\phi(p)\phi(n)=(p-1)\phi(n)$ 을 얻는다. 그러므로 조건에 의하면 $\phi(n)=0$ 인데 이것은 모순이다. 따라서 $p \mid n$ 이다.

$(\Leftarrow)$ 조건에 의하면 적당한 자연수 k와 $\gcd(p,m)=1$ 을 만족하는 적당한 자연수 m이 존재해서 $n=p^k m$ 을 만족한다. 따라서 다음 등식을 얻는다.

$$\begin{aligned}\phi(pn) &= \phi\left(p^{k+1}m\right)\\ &= \phi\left(p^{k+1}\right)\phi(m)\\ &= \left(p^{k+1}-p^k\right)\phi(m)\\ &= p(p-1)p^{k-1}\phi(m)\\ &= p\phi\left(p^k\right)\phi(m)\\ &= p\phi\left(p^k m\right)\\ &= p\phi(n)\end{aligned}$$

■

(b). $(\Longrightarrow)$ 결론을 부정해서 $p \mid n$ 이라고 가정하자. 그러면 (a)에 의해 $\phi(pn)=p\phi(n)$ 이므로 조건에 의하면 $\phi(n)=0$ 인데 이것은 모순이다. 따라서 $p \nmid n$ 이다.

$(\Leftarrow)$ (a)의 증명과정에서 $p \nmid n$ 이면 $\phi(pn)=(p-1)\phi(n)$ 임을 증명했다. ■

Problem 2.1.11 자연수 n에 대하여 다음을 증명하시오.

(a). $\phi(n)=\dfrac{n}{2}$ 가 성립할 필요충분조건은 적당한 자연수 k에 대하여 $n=2^k$ 이다.

(b). $\phi(n)=\dfrac{n}{4}$ 을 만족하는 자연수 n은 존재하지 않는다.

(증명)

(a). $(\Longrightarrow)$ 조건에 의하면 $n \geq 2$ 가 되어야 한다. 따라서 적당한 음이 아닌 정수 k와 적당한 홀수 m에 대하여 $n=2^k m$ 라고 할수 있다. 만약 $k=0$ 이면 $n=m$ 이므로 $\phi(m)=\dfrac{m}{2}$ 인데 m은 홀수이므로 우변은 자연수가 아니다. 따라서 모순이다.

그러므로 k는 자연수이고 $\gcd(2,m)=1$ 이므로 조건에 의하면 다음을 얻는다.

$$\phi(n)=\phi\left(2^k\right)\phi(m)=2^{k-1}\phi(m)=2^{k-1}m$$

따라서 $\phi(m)=m$ 을 얻는다. 만약 $m \geq 3$ 이면 m은 합성수이므로 1부터 m까지의 자연수 중엔 m의 약수가 되는 소수가 존재해서 $\phi(m)<m$ 인데 이것은 모순이다. 그러므로 $m=1$ 이고 $n=2^k$ 이다.

$(\Leftarrow)$ $n=2^k$ 이면 $\phi(n)=\phi\left(2^k\right)=2^{k-1}=\dfrac{n}{2}$ 는 명백하다. ■

(b). 결론을 부정해서 $\phi(n)=\frac{n}{4}$ 을 만족하는 자연수 n이 존재한다고 가정하자.

그러면 $n \geq 2$ 이므로 n을 소인수분해한 것을 $n=p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ 라고 하고
편의상 $p_1<p_2<\cdots<p_r$ 라고 가정하자.

그러면 $\phi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)=\frac{n}{4}$ 에서
$\frac{1}{4}=\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)=\frac{(p_1-1)(p_2-1)\cdots(p_r-1)}{p_1p_2\cdots p_r}$ 이므로
$4(p_1-1)(p_2-1)\cdots(p_r-1)=p_1p_2\cdots p_r$ 이다. 따라서 $p_1p_2\cdots p_r$ 은 짝수이다.

그러므로 $p_1,p_2,...,p_r$ 중 적어도 하나는 2가 되어야 하고 $p_1<p_2<\cdots<p_r$ 이므로
$p_1=2$ 이다. 따라서 $2(p_2-1)(p_3-1)\cdots(p_r-1)=p_2p_3\cdots p_r$ 이므로
$p_2p_3\cdots p_r$ 도 짝수인데 $3\leq p_2<p_3<\cdots p_r$ 이므로 $p_2p_3\cdots p_r$ 은 홀수이다.

이것은 모순이므로 $\phi(n)=\frac{n}{4}$ 을 만족하는 자연수 n은 존재하지 않는다. ■

Problem 2.1.12 자연수 n에 대하여 다음을 증명하시오.

(a). $\frac{\sqrt{n}}{2}\leq\phi(n)\leq n$ 이다.

(b). n이 합성수이면 $\phi(n)\leq n-\sqrt{n}$ 이다.

(c). $n\geq 2$ 일 때 n이 서로 다른 r개의 소인수를 가지면 $\phi(n)\geq\frac{n}{2^r}$ 이다.

(증명)

(a). $n=1$ 이면 주어진 부등식이 성립함은 명백하다. 따라서 $n\geq 2$ 를 가정하자.
그리고 $n\geq 2$ 이면 $n>1$ 이고 $\gcd(1,n)=1$ 이므로 $\phi(n)\leq n-1<n$ 도
명백하다. 따라서 $n\geq 2$ 일 때 $\frac{\sqrt{n}}{2}\leq\phi(n)$ 을 증명하면 충분하다.

n을 소인수분해한 것을 $n=p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ 라고 하고 편의상 $p_1<p_2<\cdots<p_r$ 라고 가정하자. 그러면 다음을 얻는다.

$$\begin{aligned}&\phi(n)\geq\frac{\sqrt{n}}{2}\\ &\Leftrightarrow 2\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)\geq\frac{1}{\sqrt{n}}\\ &\Leftrightarrow\frac{2(p_1-1)(p_2-1)\cdots(p_r-1)}{p_1p_2\cdots p_r}\geq\frac{1}{\sqrt{p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}}}\end{aligned}\qquad(9)$$

그리고 $k_1, k_2, ..., k_r$ 은 자연수이므로 $\frac{1}{\sqrt{p_1 p_2 \cdots p_r}} \geq \frac{1}{\sqrt{p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}}}$ 이다.

따라서 $\frac{2(p_1-1)(p_2-1)\cdots(p_r-1)}{p_1 p_2 \cdots p_r} \geq \frac{1}{\sqrt{p_1 p_2 \cdots p_r}}$ 을 증명하면

(9)가 증명된다. 즉, 다음 부등식을 증명하면 충분하다.

$$2(p_1-1)(p_2-1)\cdots(p_r-1) \geq \sqrt{p_1 p_2 \cdots p_r} \qquad (10)$$

$p \geq 3$ 이면 $(p-1)^2 - p = p(p-3)+1 \geq 0$ 이므로 $p-1 \geq \sqrt{p}$ 가 성립한다는 것을 쉽게 알수 있다. 이것을 이용하자.

case1) $p_1 = 2$

이 경우 증명해야 할 부등식은 $2(p_2-1)(p_3-1)\cdots(p_r-1) \geq \sqrt{2p_2 \cdots p_r}$ 이고

각각의 $i = 2,3,...,r$ 에 대해 $p_i \geq 3$ 이고 $2 > \sqrt{2}$ 이다.

따라서 각각의 $i = 2,3,...,r$ 에 대해 $p_i - 1 \geq \sqrt{p_i}$ 이므로 (10)이 성립한다.

그러므로 (9)에 의하면 문제에 주어진 부등식도 성립한다.

case2) $p_1 \geq 3$

이 경우에는 각각의 $i = 1,2,...,r$ 에 대하여 $p_i \geq 3$ 이므로 $p_i - 1 \geq \sqrt{p_i}$ 이다.

따라서 $(p_1-1)(p_2-1)\cdots(p_r-1) \geq \sqrt{p_1 p_2 \cdots p_r}$ 이므로 (10)이 성립하는 것은 명백하다. 그러므로 (9)에 의하면 문제에 주어진 부등식도 성립한다. ■

(b). n이 합성수이므로 $p \mid n$ 과 $p \leq \sqrt{n}$ 을 동시에 만족하는 소수 p가 존재한다.

따라서 $1 - \frac{1}{p} \leq 1 - \frac{1}{\sqrt{n}}$ 이고 q가 소수이면 $1 - \frac{1}{q} \leq 1$ 이므로 Corollary 2.1.2에

의하면 $\phi(n) \leq n\left(1 - \frac{1}{\sqrt{n}}\right) = n - \sqrt{n}$ 임을 쉽게 알수 있다. ■

(c). p가 소수이면 $p \geq 2$ 이므로 $1 - \frac{1}{p} \geq \frac{1}{2}$ 이다. 따라서 n이 서로 다른 r개의

소인수를 가지면 Corollary 2.1.2에 의해 $\phi(n) \geq \frac{n}{2^r}$ 임을 쉽게 알수 있다. ■

Problem 2.1.13 자연수 k가 임의로 주어져있다고 할 때 다음을 증명하시오.

(a). $\phi(n) = k$ 를 만족하는 자연수 n이 존재한다면 그 개수는 유한하다.

(b). $\phi(n) = k$ 를 만족하는 자연수 n이 유일하다면 $4 \mid n$ 이다.

(증명)

(a). Problem 2.1.12 (a)에 의하면 $\frac{\sqrt{n}}{2} \leq \phi(n)$ 이다. 따라서 $\phi(n)=k$ 를 만족하는 자연수 n이 존재한다면 $\frac{\sqrt{n}}{2} \leq k$ 에서 $n \leq 4k^2$ 을 만족하고 $n \leq 4k^2$ 을 만족하는 자연수 n의 개수는 유한하다. ■

(b). Problem 2.1.10에 의하면 n이 홀수일 때 $\phi(2n)=\phi(n)$ 이므로 조건을 만족하는 자연수 n은 유일하지 않다. 따라서 n은 짝수이므로 적당한 자연수 m에 대하여 $n=2m$ 인데 만약 m이 홀수이면 Problem 2.1.10에 의해 $\phi(2m)=\phi(m)$ 이므로 $\phi(n)=\phi(2m)=\phi(m)=k$ 를 얻는다.

이것은 $\phi(n)=k$ 를 만족하는 자연수 n은 유일하다는 것에 모순이다.
그러므로 m은 짝수이고 $n=2m$ 이므로 $4 \mid n$ 이다. ■

1907년에 수학자 로버트 다니엘 카마이클(Robert Daniel Carmichael)이 $\phi(n)=k$ 를 만족하는 자연수 n이 존재할 경우 그 개수는 2개 이상이라는 추측을 제시했는데 아직까지 풀리지 않은 문제입니다. 지금까지 컴퓨터로 계산해본 결과 $\phi(n)=k$ 를 만족하는 n이 유일하다면 그 유일한 n은 $10^{10^{10}}$ 이상이라고 합니다.

Problem 2.1.14 다음 물음에 답하시오.
(a). $\phi(n)=16$ 을 만족하는 자연수 n을 모두 구하시오.
(b). $2p+1$ 이 합성수가 되도록 하는 소수 p에 대하여 $\phi(n)=2p$ 를 만족하는 자연수 n은 존재하지 않는다는 것을 증명하시오.
(c). $\phi(n)=k$ 를 만족하는 자연수 n이 존재하지 않도록 하는 가장 작은 짝수인 자연수 k가 $k=14$ 임을 증명하시오.

(풀이)
(a). $\phi(1)=1$ 이므로 $n \geq 2$ 가 되어야 한다. 따라서 n은 합성수이고 n을 소인수분해한 것을 $n=p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ 라고 하자. 그리고 편의상 $p_1<p_2<\cdots<p_r$ 라고 가정하자.
$\phi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)=16$ 이면 다음을 얻는다.

$$\frac{2^4}{p_1^{k_1-1}p_2^{k_2-1}\cdots p_r^{k_r-1}}=(p_1-1)(p_2-1)\cdots(p_r-1) \qquad (11)$$

따라서 (11)의 좌변은 자연수이고 $p_1,p_2,...,p_r$ 은 소수이므로 n을 소인수분해 했을 때 2 이외의 소수를 소인수로 가질 경우 그 소인수의 지수는 1이 되어야 한다. 즉, 자연수 m에 대하여 $n=2^m$ 이거나 적당한 음이 아닌 정수 m과 적당한 홀수인 소수 $p_1,p_2,...,p_r$ 에 대하여 $n=2^m p_1p_2\cdots p_r$ 이다. 이때도 $p_1<p_2<\cdots<p_r$ 라고 하자.

case1) m이 자연수일 때 $n=2^m$
이 경우 $\phi(n)=2^{m-1}=16$ 이므로 $m=5$ 이다. 따라서 $n=32$ 이다.

case2) m이 음이 아닌 정수일 때 $n=2^m p_1 p_2 \cdots p_r$
이 경우 $m=0$ 이면 $\phi(n)=(p_1-1)(p_2-1)\cdots(p_r-1)=16$ 이고
$1 \le m \le 4$ 이면 $\phi(n)=2^{m-1}(p_1-1)(p_2-1)\cdots(p_r-1)=16$ 이다.

$m=0$ 이면 $\phi(n)=(p_1-1)(p_2-1)\cdots(p_r-1)=16$ 인데 $p_1<p_2<\cdots<p_r$
이므로 가능한 경우는 $r=1$ 일 때 $p_1-1=16$ 뿐이고 $n=17$ 이다.

$m=1$ 이면 $(p_1-1)(p_2-1)\cdots(p_r-1)=16$ 이고 이것은 $m=0$ 일 때와 같은
상황이므로 $r=1$ 이고 $p_1-1=16$ 이다. 따라서 $n=2\times 17=34$ 이다.

$m=2$ 이면 $(p_1-1)(p_2-1)\cdots(p_r-1)=8$ 이고 $p_1<p_2<\cdots<p_r$ 이므로
가능한 경우는 $r=2$ 일 때 $p_1=1=2,\ p_2-1=4$ 뿐이다.
따라서 $n=2^2\times 3\times 5=60$ 이다.

$m=3$ 이면 $(p_1-1)(p_2-1)\cdots(p_r-1)=4$ 이고 $p_1<p_2<\cdots<p_r$ 이므로
가능한 경우는 $r=1$ 일 때 $p_1-1=4$ 뿐이다. 따라서 $n=2^3\times 5=40$ 이다.

$m=4$ 이면 $(p_1-1)(p_2-1)\cdots(p_r-1)=2$ 이고 $p_1<p_2<\cdots<p_r$ 이므로
가능한 경우는 $r=1$ 일 때 $p_1-1=2$ 뿐이다. 따라서 $n=2^4\times 3=48$ 이다.

그러므로 $\phi(n)=16$ 을 만족하는 자연수 n은 $n=17,32,34,40,48,60$ 이다. ■

(b). 결론을 부정해서 $\phi(n)=2p$ 를 만족하는 자연수 n이 존재한다고 가정하자.
그러면 n을 소인수분해한 것을 $n=p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}\ (p_1<p_2<\cdots<p_r)$ 라고 했을 때
(a)의 풀이과정에 의하면 다음 등식을 얻을수 있다.

$$\frac{2p}{p_1^{k_1-1}p_2^{k_2-1}\cdots p_r^{k_r-1}}=(p_1-1)(p_2-1)\cdots(p_r-1) \qquad (12)$$

$p=2$ 이면 $2p+1=5$ 는 소수이므로 조건에 의하면 p는 홀수이다. 그리고 (12)의 좌변은
자연수이므로 n이 $2,p$ 이외의 소인수를 가지면 그 소인수의 지수는 1이어야 한다.

먼저 n이 $2,p$ 이외의 소인수를 갖는 경우를 고려하자. 그럼 다음 3가지 경우가 발생한다.

case1) $n=2^m p_1 p_2 \ldots p_r \left(m\in\mathbb{N},\ 3\le p_1<p_2<\cdots<p_r\right)$ 이고
각각의 $i=1,2,\ldots,r$ 에 대하여 $p_i\neq p$ 인 경우

이 경우 $\phi(n)=2^{m-1}(p_1-1)(p_2-1)\cdots(p_r-1)=2p$ 인데 $2p$의 양의 약수는
$1,2,p,2p$ 가 전부이므로 $m=1$ 이면 $r=1$ 이고 $p_1=1+2p$ 를 얻는다.
그런데 $1+2p$ 는 합성수이므로 모순이다.

따라서 $m\ge 2$ 인데 $m\ge 3$ 이면 2^{m-1}은 4의 배수이므로 $2p$가 4의 배수라서
모순이다. 그러므로 $m=2$ 이고 $(p_1-1)(p_2-1)\cdots(p_r-1)=p$ 인데 좌변은
짝수이고 우변은 홀수이므로 이것도 모순이다. 그러므로 case1)과 같은 형태는 $\phi(n)=2p$
를 만족하지 않는다.

case2) $n=p^m p_1 p_2 \ldots p_r \left(m\in\mathbb{N},\ 3\le p_1<p_2<\cdots<p_r\right)$ 이고
각각의 $i=1,2,\ldots,r$ 에 대하여 $p_i\neq p$ 인 경우

이 경우 $\phi(n)=p^{m-1}(p-1)(p_1-1)(p_2-1)\cdots(p_r-1)=2p$ 인데
$p-1$ 은 짝수이므로 n의 새로운 소인수가 존재하면 $2p$는 4의 배수가 되어서 모순이다.
그러므로 case2)와 같은 형태는 $\phi(n)=2p$ 를 만족하지 않는다.

case3) $n=2^{m_1}p^{m_2}p_1 p_2 \ldots p_r \left(m_1,m_2\in\mathbb{N},\ 3\le p_1<p_2<\cdots<p_r\right)$ 이고
각각의 $i=1,2,\ldots,r$ 에 대하여 $p_i\neq p$ 인 경우

이 경우 $\phi(n)=2^{m_1-1}p^{m_2-1}(p-1)(p_1-1)(p_2-1)\cdots(p_r-1)=2p$ 인데
이때도 case2)와 같은 이유로 $2p$가 4의 배수가 되어서 모순이다.

따라서 case1)~case3)에 의하면 n은 $2,p$ 이외의 소인수를 가질수 없다.
그러므로 남은 경우는 간단하게 계산할수 있다.

case4) $n=2^m\ (m\in\mathbb{N})$
이 경우 $\phi(n)=2^{m-1}=2p$ 인데 $m=1$ 이면 $2p=1$, $m=2$ 이면 $p=1$
$m\ge 3$ 이면 $2p$는 4의 배수이므로 어느 경우든 모순이다.

case5) $n=p^m\ (m\in\mathbb{N})$
이 경우 $\phi(n)=p^{m-1}(p-1)=2p$ 인데 $m=1$ 이면 $p-1=2p$ 에서 $p=-1$,
$m=2$ 이면 $p-1=2$ 에서 $p=3$ 인데 $2p+1=7$ 은 소수, $m\ge 3$ 이면
$p^{m-2}(p-1)=2$ 인데 $p\ge 3$ 이므로 $p^{m-2}(p-1)\ge 6$ 이다. 어느 경우든 모순이다.

case6) $n = 2^{m_1}p^{m_2}\,(m_1, m_2 \in \mathbb{N})$

이 경우 $\phi(n) = 2^{m_1-1}p^{m_2-1}(p-1) = 2p$ 인데 $m_1 = 1$ 이면 case5)와 같은 상황이므로 모순이다. $m_2 = 1$ 이면 $2^{m_1-1}(p-1) = 2p$ 인데 $m_1 \neq 1$ 임은 이미 보였고 $m_1 = 2$ 이면 $p-1 = p$ 이므로 모순, $m_1 \geq 3$ 이면 $2p$는 4의 배수이므로 모순이다.

따라서 m_1, m_2는 모두 2 이상의 자연수인데 이 경우 $2p$는 4의 배수이므로 모순이다.

지금까지의 내용을 정리하면 어느 경우든 모순이 발생했다.
그러므로 $\phi(n) = 2p$ 를 만족하는 자연수 n은 존재하지 않는다. ■

(c). 우선 $p = 7$ 이면 $2p+1 = 15$ 는 합성수이므로 (b)에 의하면 $\phi(n) = 14$ 를 만족하는 자연수 n은 존재하지 않는다. 그리고 $\phi(n)$이 가질수 있는 값은 1 또는 짝수인데

$$\phi(3) = 2, \phi(5) = 4, \phi(7) = 6, \phi(15) = 8, \phi(11) = 10, \phi(13) = 12$$

이므로 14가 조건을 만족하는 가장 작은 짝수인 자연수이다. ■

Problem 2.1.15 모든 자연수 n에 대하여 다음 등식이 성립함을 증명하시오.

$$\sum_{k=1}^{n} \gcd(k,n) = \sum_{d \mid n} d\phi\left(\frac{n}{d}\right) = n\sum_{d \mid n} \frac{\phi(d)}{d}$$

(증명)
n의 서로 다른 모든 양의 약수를 $d_1, d_2, ..., d_m$ 라고 하면 임의의 $k \in \{1,2,...,n\}$ 는 가우스의 정리의 증명과정에서 등장한 m개의 집합 $S_{d_1}, S_{d_2}, ..., S_{d_m}$ 중 정확히 한 집합에만 속해있으므로 $\sum_{k=1}^{n} \gcd(k,n)$ 를 계산한 값은 결국 각각의 $i = 1,2,...,m$ 에 대하여 $d_i\phi\left(\frac{n}{d_i}\right)$를 모두 더한 값과 같다. 따라서 (7)에 의하면 다음 등식이 성립한다.

$$\sum_{k=1}^{n} \gcd(k,n) = \sum_{d \mid n} d\phi\left(\frac{n}{d}\right) = n\sum_{d \mid n} \frac{\phi(d)}{d}$$

■

2.2 페르마, 오일러, 윌슨의 정리

작성자 : 네냐플(Nenyaffle)

2.2절에서는 합동식에서 기본적이면서 중요한 3가지 정리를 소개하려고 합니다.
그 정리는 각각 **페르마의 작은 정리(Fermat's Little Theorem), 오일러의 정리(Euler's Theorem), 윌슨의 정리(Wilson's Theorem)**라고 부르는 정리입니다.

오일러의 정리는 페르마의 작은 정리의 일반화입니다. 따라서 오일러의 정리를 먼저 소개하고 페르마의 작은 정리를 오일러의 정리의 Corollary로 소개하겠습니다.

Theorem 2.2.1 오일러의 정리(Euler's Theorem)
자연수 n이 임의로 주어져있다고 하자. 그러면 $\gcd(a,n)=1$ 을 만족하는 모든 $a\in\mathbb{Z}$ 에 대하여 $a^{\phi(n)} \equiv 1 \pmod{n}$ 이다.

(증명)
법 n에 대한 기약잉여계를 $\{r_1,r_2,...,r_{\phi(n)}\}$라고 하자. 그러면 $\gcd(a,n)=1$ 이므로 Problem 2.1.8에 의해 $\{ar_1,ar_2,...,ar_{\phi(n)}\}$도 법 n에 대한 기약잉여계이다.

따라서 두 집합 $\{r_1,r_2,...,r_{\phi(n)}\}$, $\{ar_1,ar_2,...,ar_{\phi(n)}\}$은 법 n에 대하여 합동인 원소끼리 일대일 대응이 존재한다. 그러므로 각각의 원소들을 모두 곱한 것은 법 n에 대하여 합동이다. 즉, 다음이 성립한다.

$$(ar_1)(ar_2)\cdots(ar_{\phi(n)}) \equiv r_1r_2\cdots r_{\phi(n)} \pmod{n}$$

정리하면 다음을 얻는다.

$$a^{\phi(n)}r_1r_2\cdots r_{\phi(n)} \equiv r_1r_2\cdots r_{\phi(n)} \pmod{n} \tag{13}$$

각각의 $i=1,2,...,\phi(n)$ 에 대하여 $\gcd(r_i,n)=1$ 이므로 $\gcd(r_1r_2\cdots r_{\phi(n)},n)=1$ 이다. 그러므로 $r_1r_2\cdots r_{\phi(n)}$은 법 n에서 곱셈에 대한 역원이 존재하고 (13)의 양변에 그 역원을 곱하면 $a^{\phi(n)} \equiv 1 \pmod{n}$ 을 얻는다. ■

Corollary 2.2.1 페르마의 작은 정리(Fermat's Little Theorem)
소수 p가 임의로 주어져있다고 하자. 그러면 $p\nmid a$ 를 만족하는 모든 $a\in\mathbb{Z}$ 에 대하여 $a^{p-1} \equiv 1 \pmod{p}$ 이다.

(증명)
p가 소수이고 $p\nmid a$ 이므로 $\gcd(a,p)=1$ 이고 $\phi(p)=p-1$ 이다. 따라서 오일러의 정리에 의하면 $a^{p-1} \equiv 1 \pmod{p}$ 이다. ■

Corollary 2.2.2 p가 소수이면 모든 $a\in\mathbb{Z}$ 에 대하여 $a^p \equiv a \pmod{p}$ 이다.

(증명)
$p\mid a$ 이면 명백하다. $p\nmid a$ 이면 $a^{p-1} \equiv 1 \pmod{p}$ 의 양변에 a를 곱해서 얻을수 있다. ■

오일러의 정리에 의하면 $\gcd(a,n)=1$ 일 때 법 n에서 a의 곱셈에 대한 역원은 $a^{\phi(n)-1}$ 가 됩니다. 그런데 이건 기호로 나타내기 좋은 것 뿐이고 실제로 계산할때는 도움이 안됩니다.

$n=15$ 일 때 $\gcd(7,15)=1$ 이므로 $7^{\phi(15)} \equiv 7^8 \equiv 1 \pmod{15}$ 이고 따라서 법 15에서 7의 곱셈에 대한 역원은 7^7인데 이것은 직접 계산하기 힘들어서 도움이 안됩니다. 곱셈에 대한 역원을 기계의 도움 없이 구하려면 유클리드 호제법을 사용하는게 좋습니다.

페르마의 작은 정리를 약자로 쓸때는 Flt로 씁니다. FLT는 **페르마의 마지막 정리(Fermat's Last Theorem)**의 약자로 쓰는 편입니다.

오일러의 정리가 페르마의 작은 정리의 일반화이긴 하지만 실제로는 오일러의 정리보다 페르마의 작은 정리를 더 많이 사용하게 됩니다. 법 n에 대한 합동식을 다룰땐 n이 소수인 경우를 많이 다루기 때문입니다.

Corollary 2.2.2와 오일러의 정리를 보고 모든 $a \in \mathbb{Z}$ 에 대하여 $a^{\phi(n)+1} \equiv a \pmod{n}$ 가 성립한다고 생각할수 있는데 이것은 거짓입니다. $n=16$ 일 때 $\phi(16)=8$ 인데 $2^{8+1} \equiv 512 \equiv 0 \pmod{16}$ 입니다.

오일러의 정리, 페르마의 작은 정리는 모두 역이 거짓입니다.

오일러의 정리의 역이 거짓인 경우는 다음과 같습니다. $7^8 \equiv 1 \pmod{15}$ 가 성립하지만 $7^4 \equiv 2401 \equiv 1 \pmod{15}$ 도 성립하므로 $\gcd(a,n)=1$ 일 때 $a^k \equiv 1 \pmod{n}$ 라고 해서 $k=\phi(n)$ 이 되는건 아닙니다.

페르마의 작은 정리의 역은 $n=561=3\times 11\times 17$ 일 때 반례가 발생합니다. $\gcd(a,561)=1$ 를 만족하는 $a \in \mathbb{Z}$ 를 임의로 택하면 $561=3\times 11\times 17$ 이므로 $\gcd(a,3)=\gcd(a,11)=\gcd(a,17)=1$ 을 만족합니다.

페르마의 작은 정리에 의하면 다음을 얻을수 있습니다.

$$a^2 \equiv 1 \pmod{3},\ a^{10} \equiv 1 \pmod{11},\ a^{16} \equiv 1 \pmod{17}$$

그러므로 다음이 성립합니다.

$$\begin{aligned} a^{560} &\equiv \left(a^2\right)^{280} \equiv 1 \pmod{3} \\ a^{560} &\equiv \left(a^{10}\right)^{56} \equiv 1 \pmod{11} \\ a^{560} &\equiv \left(a^{16}\right)^{35} \equiv 1 \pmod{17} \end{aligned}$$

따라서 Problem 2.1.3 (c)에 의하면 $a^{560} \equiv 1 \pmod{561}$ 가 성립하는데 $561=3\times 11\times 17$ 이므로 소수가 아닙니다.

페르마의 작은 정리와 Corollary 2.2.2의 역이 성립하지 않게 만드는 자연수도 수학에서는 이름을 가지고 있습니다. 이제 그것을 소개하겠습니다.

Definition 2.2.1 유사소수(Pseudoprime)
$2^n \equiv 2 \pmod{n}$ 를 만족하는 합성수 n을 **유사소수(Pseudoprime)**라고 정의한다.

실제로 유사소수는 존재합니다. 위에서 보인 $n = 561$ 이 유사소수의 한 예인데
$\gcd(2,3) = \gcd(2,11) = \gcd(2,17) = 1$ 이므로 $2^{561} \equiv 2 \pmod{561}$ 입니다.

그런데 561이 가장 작은 유사소수가 되는건 아닙니다. 실제로 가장 작은 유사소수는 341인데 341이 유사소수임을 보이는데 도움이 되는 정리를 하나 소개하겠습니다.

Lemma 2.2.1 p, q가 서로 다른 소수이고 $a^p \equiv a \pmod{q}$, $a^q \equiv a \pmod{p}$ 를 만족하면 $a^{pq} \equiv a \pmod{pq}$ 이다.

(증명)
Corollary 2.2.2에 의하면 다음이 성립한다.

$$a^{pq} \equiv (a^q)^p \equiv a^q \pmod{p}$$
$$a^{pq} \equiv (a^p)^q \equiv a^p \pmod{q}$$

따라서 조건에 의하면 $a^{pq} \equiv a \pmod{p}$, $a^{pq} \equiv a \pmod{q}$ 이고 $\gcd(p,q) = 1$ 이므로 $a^{pq} \equiv a \pmod{pq}$ 가 성립한다. ■

$341 = 11 \times 31$ 이고 Corollary 2.2.2에 의하면

$$2^{11} \equiv 2 \pmod{11},\ 2^{31} \equiv 2 \pmod{31}$$

입니다. 그리고 $11, 31$은 서로 다른 소수이므로 Lemma 2.2.1에 의하면
$2^{341} \equiv 2 \pmod{341}$ 가 성립합니다. 따라서 341은 유사소수입니다.

유사소수를 작은 순서대로 4개만 쓰면 $341, 561, 645, 1105$ 라고 합니다.
소인수분해를 하면 다음과 같습니다.

$$341 = 11 \times 31$$
$$561 = 3 \times 11 \times 17$$
$$645 = 3 \times 5 \times 43$$
$$1105 = 5 \times 13 \times 17$$

그리고 짝수인 유사소수도 있는데 최초로 발견된 짝수인 유사소수는 다음과 같다고 합니다.

$$161038 = 2 \times 73 \times 1103$$

다음 정리는 모든 항이 유사소수로 이루어진 증가수열을 만들 수 있고
따라서 유사소수의 개수는 무한하다는 것을 알려줍니다.

Theorem 2.2.2 n이 유사소수이면 $2^n - 1$ 도 유사소수이다.

(증명)

$M_n = 2^n - 1$ 라고 하자. 조건에 의하면 n은 합성수이므로 $1 < a \le b < n$ 을 만족하는 적당한 자연수 a, b가 존재해서 $n = ab$ 를 만족한다.

따라서 $2^n-1=\left(2^a-1\right)\left(2^{a(b-1)}+2^{a(b-2)}+\cdots 2^a+1\right)$ 이므로 $2^a-1 \mid M_n$ 이고 $2^a-1>1$ 이므로 M_n은 합성수이다. 그리고 $2^n \equiv 2 \pmod n$ 이므로 적당한 정수 k가 존재해서 $2^n-2=kn$ 을 만족하고 $2^{M_n-1}=2^{2^n-2}=2^{kn}$ 을 얻는다.

따라서 다음이 성립한다.

$$\begin{aligned} 2^{M_n-1}-1 &\equiv 2^{kn}-1 \\ &\equiv \left(2^n-1\right)\left(2^{n(k-1)}+2^{n(k-2)}+\cdots+2^n+1\right) \\ &\equiv 0 \pmod{M_n} \end{aligned}$$

그러므로 $2^{M_n-1} \equiv 1 \pmod{M_n}$ 이고 양변에 2를 곱하면 $2^{M_n} \equiv 2 \pmod{M_n}$ 이다.
따라서 M_n은 유사소수이다. ■

수학적 귀납법을 이용하면 모든 자연수 n에 대하여 $2^n-1 \geq n$ 가 성립한다는 것을 증명할수 있고 등호가 성립할 필요충분조건은 $n=1$ 이라는 것도 쉽게 증명할수 있습니다.

따라서 n이 합성수이면 $2^n-1>n$ 이므로 n이 유사소수이면 n보다 큰 유사소수가 2^n-1 로 존재합니다. 그러므로 모든 항이 유사소수로 이루어진 증가수열을 만들 수 있고 유사소수의 개수는 무한합니다.

유사소수는 $a=2$ 일 때 $a^n \equiv a \pmod n$ 을 만족하는 합성수 n입니다.
따라서 a가 2가 아닐때도 $a^n \equiv a \pmod n$ 을 만족하는 합성수 n을 생각할수 있는데
$a=3$ 이면 $a^n \equiv a \pmod n$ 을 만족하는 가장 작은 자연수 n은 $n=91$ 이고
$a=5$ 이면 $a^n \equiv a \pmod n$ 을 만족하는 가장 작은 자연수 n은 $n=217$ 입니다.

유사소수보다 좀 더 강력한 조건을 갖는 수로 **카마이클 수(Carmichael Number)**라는게 있는데 이것은 다음과 같이 정의합니다.

Definition 2.2.2 카마이클 수(Carmichael Number)
합성수 n이 $\gcd(a,n)=1$ 을 만족하는 모든 $a \in \mathbb{Z}$ 에 대하여 $a^n \equiv a \pmod n$ 를 만족하면 합성수 n을 **카마이클 수(Carmichael Number)**라고 정의한다.

페르마의 작은 정리의 역이 성립하지 않는 반례를 소개할 때 $n=561$ 을 예로 들었는데 반례임을 보이는 과정을 보면 561이 카마이클 수라는 것을 알수 있습니다.
그리고 561이 가장 작은 카마이클 수라고 합니다.

$\gcd(a,n)=1$ 이므로 $a^n \equiv a \pmod n$ 과 $a^{n-1} \equiv 1 \pmod n$ 은 동치입니다.
따라서 카마이클 수를 정의할 때 $a^{n-1} \equiv 1 \pmod n$ 를 만족하는 합성수 n으로 정의해도 상관없습니다.

카마이클 수를 작은 순서대로 7개만 나열하면 다음과 같습니다.

$$561 = 3 \times 11 \times 17$$
$$1105 = 5 \times 13 \times 17$$
$$1729 = 7 \times 13 \times 19$$
$$2465 = 5 \times 17 \times 29$$
$$2821 = 7 \times 13 \times 31$$
$$6601 = 7 \times 23 \times 41$$
$$8911 = 7 \times 19 \times 67$$

7개의 카마이클 수를 보면 모두 소인수가 3개입니다. 따라서 모든 카마이클 수를 소인수분해 하면 서로 다른 소인수가 3개라고 생각할수 있는데 실제로는 그렇지 않습니다.
다음 6개의 수도 카마이클 수입니다.

$$41041 = 7 \times 11 \times 13 \times 41$$
$$825265 = 5 \times 7 \times 17 \times 19 \times 73$$
$$321197185 = 5 \times 19 \times 23 \times 29 \times 37 \times 137$$
$$5394826801 = 7 \times 13 \times 17 \times 23 \times 31 \times 67 \times 73$$
$$232250619601 = 7 \times 11 \times 13 \times 17 \times 31 \times 37 \times 73 \times 163$$
$$9746347772161 = 7 \times 11 \times 13 \times 17 \times 19 \times 31 \times 37 \times 41 \times 641$$

카마이클 수의 개수도 무한합니다. 이것은 1994년에 증명되었습니다.

합성수 n이 카마이클 수가 되기 위한 필요충분조건도 널리 알려져 있는데
이것은 지금 증명할수 없습니다. 이것을 증명하기 위해서 알아야하는 정의와 정리가 있는데 그 정의와 정리가 뒤에 나옵니다. 따라서 지금은 증명없이 받아들이겠습니다.

Theorem 2.2.3 Korselt의 판정법(Korselt's Criterion)
합성수 n이 카마이클 수가 될 필요충분조건은 다음을 만족하는 것이다.

(a). 모든 소수 p에 대하여 $p^2 \nmid n$ 이다. 즉, $n \geq 2$ 일 때 n을 소인수분해 하면 소인수의 지수는 모두 1이다.
(b). $p \mid n$ 을 만족하는 모든 소수 p에 대하여 $p-1 \mid n-1$ 이다.

수학에서 (a)를 만족하는 정수를 **제곱인수가 없는 정수(Square Free Integer)**라고 부릅니다. 직역한 느낌이지만 실제로 대한수학회에서 이렇게 번역해놓았습니다.

오일러의 정리나 페르마의 작은 정리는 정수의 거듭제곱으로 이루어진 수를 나눈 나머지를 구할 때 유용합니다. 예를 들어 5^{38}을 11로 나눈 나머지를 구하고 싶을 때 페르마의 작은 정리에 의하면 $5^{10} \equiv 1 \pmod{11}$ 이므로 $5^{40} \equiv 1 \pmod{11}$ 입니다.

그리고 $5 \times 9 \equiv 1 \pmod{11}$ 이므로 $5^{38} \equiv 5^{40} \times 81 \equiv 81 \equiv 4 \pmod{11}$ 입니다.
따라서 5^{38}을 11로 나눈 나머지는 4입니다.

Problem 2.2.1 다음을 증명하시오.
(a). $17 \mid 11^{104} + 1$ 이다.
(b). $\gcd(a, 35) = 1$ 을 만족하는 모든 $a \in \mathbb{Z}$ 에 대하여 $a^{12} \equiv 1 \pmod{35}$ 이다.

(c). $\gcd(a,42)=1$ 을 만족하는 모든 $a\in\mathbb{Z}$ 에 대하여 $a^6\equiv 1\pmod{168}$ 이다.
(d). $\gcd(a,133)=\gcd(b,133)=1$ 을 만족하는 모든 $a,b\in\mathbb{Z}$ 에 대하여
$a^{18}\equiv b^{18}\pmod{133}$ 이다.
(e). 모든 음이 아닌 정수 n에 대하여 $13\mid 11^{12n+6}+1$ 이다.

(증명)
(a). 페르마의 작은 정리에 의하면 $11^{16}\equiv 1\pmod{17}$ 이다.
따라서 $11^{96}\equiv\left(11^{16}\right)^6\equiv 1\pmod{17}$ 이다. 그리고 $11^2\equiv 2\pmod{17}$ 이므로
$11^8\equiv\left(11^2\right)^4\equiv 16\equiv -1\pmod{17}$ 이다.

그러므로 $11^{104}\equiv 11^{96}\times 11^8\equiv -1\pmod{17}$ 에서 $17\mid 11^{104}+1$ 을 얻는다. ■

(b). $35=5\times 7$ 이므로 조건에 의하면 $\gcd(a,5)=\gcd(a,7)=1$ 이다.
따라서 페르마의 작은 정리에 의하면 다음을 얻는다.

$$a^4\equiv 1\pmod{5}$$
$$a^6\equiv 1\pmod{7}$$

그러므로 다음을 얻을수 있다.

$$a^{12}\equiv\left(a^4\right)^3\equiv 1\pmod{5}$$
$$a^{12}\equiv\left(a^6\right)^2\equiv 1\pmod{7}$$

그리고 $\gcd(5,7)=1$ 이므로 $a^{12}\equiv 1\pmod{35}$ 를 얻는다. ■

(c). $42=2\times 3\times 7$ 이고 $168=2^3\times 3\times 7$ 이다. 따라서 조건에 의하면
$\gcd(a,2)=\gcd(a,3)=\gcd(a,7)=1$ 이고 페르마의 작은 정리에 의하면

$$a\equiv 1\pmod{2}$$
$$a^2\equiv 1\pmod{3}$$
$$a^6\equiv 1\pmod{7}$$

가 성립한다. 그리고 a가 홀수이면 a는 8의 배수가 될수 없으므로 $a\equiv 1\pmod{8}$
임을 알수 있다. 따라서 다음을 얻는다.

$$a^6\equiv 1\pmod{8}$$
$$a^6\equiv\left(a^2\right)^3\equiv 1\pmod{3}$$
$$a^6\equiv 1\pmod{7}$$

$\gcd(8,3)=\gcd(3,7)=\gcd(7,8)=1$ 이고 $168=2^3\times 3\times 7$ 이므로
$a^6\equiv 1\pmod{168}$ 가 성립한다. ■

(d). $133=7\times 19$ 이다. 따라서 다음을 만족한다.

$$\gcd(a,7)=\gcd(b,7)=\gcd(a,19)=\gcd(b,19)=1$$

그러므로 페르마의 작은 정리에 의하면 다음을 얻는다.

$$a^6 \equiv 1 \equiv b^6 \pmod 7$$
$$a^{18} \equiv 1 \equiv b^{18} \pmod{19}$$

따라서 다음을 얻을수 있다.

$$a^{18} \equiv (a^6)^3 \equiv (b^6)^3 \equiv b^{18} \pmod 7$$
$$a^{18} \equiv b^{18} \pmod{19}$$

그리고 $\gcd(7,19)=1$ 이므로 $a^{18} \equiv b^{18} \pmod{133}$ 이다. ■

(e). 페르마의 작은 정리에 의하면 $11^{12} \equiv 1 \pmod{13}$ 이다. 따라서 n이 음이 아닌 정수이면 $11^{12n} \equiv 1 \pmod{13}$ 을 얻을수 있다. 그리고 $11^2 \equiv 4 \pmod{13}$ 이므로 $11^6 \equiv 64 \equiv -1 \pmod{13}$ 이다.

그러므로 $11^{12n+6} \equiv -1 \pmod{13}$ 이고 따라서 $13 \mid 11^{12n+6}+1$ 이다. ■

Problem 2.2.2 모든 $a \in \mathbb{Z}$ 에 대하여 다음을 증명하시오.

(a). $a^{21} \equiv a \pmod{15}$ 이다.

(b). $a^9 \equiv a \pmod{30}$ 이다.

(증명)

(a). $15 = 3 \times 5$ 이므로 $a^{21} \equiv a \pmod{15}$ 일 필요충분조건은 $a^{21} \equiv a \pmod 3$, $a^{21} \equiv a \pmod 5$ 를 동시에 만족하는 것이다. 이것을 증명하자.

Corollary 2.2.2에 의하면 다음이 성립한다.

$$a^3 \equiv a \pmod 3$$
$$a^5 \equiv a \pmod 5$$

따라서 다음을 얻는다.

$$a^{21} \equiv (a^3)^7 \equiv a^7 \equiv (a^3)^2 a \equiv a \pmod 3$$
$$a^{21} \equiv (a^5)^4 a \equiv a^5 \equiv a \pmod 5$$

그러므로 $a^{21} \equiv a \pmod{15}$ 이다. ■

(b). $30 = 2 \times 3 \times 5$ 이므로 $a^9 \equiv a \pmod{30}$ 일 필요충분조건은 $a^9 \equiv a \pmod 2$, $a^9 \equiv a \pmod 3$, $a^9 \equiv a \pmod 5$ 를 동시에 만족하는 것이다. 이것을 증명하자.

Corollary 2.2.2에 의하면 다음이 성립한다.

$$a^2 \equiv a \pmod 2$$
$$a^3 \equiv a \pmod 3$$
$$a^5 \equiv a \pmod 5$$

따라서 다음을 얻는다.

$$a^9 \equiv (a^2)^4 a \equiv a^5 \equiv (a^2)^2 a \equiv a^3 \equiv a^2 a \equiv a^2 \equiv a \pmod 2$$
$$a^9 \equiv (a^3)^3 \equiv a^3 \equiv a \pmod 3$$
$$a^9 \equiv a^5 a^4 \equiv a^5 \equiv a \pmod 5$$

그러므로 $a^9 \equiv a \pmod{30}$ 이다. ■

Problem 2.2.3 a, b는 정수이고 p는 소수이다. 이때 $\gcd(a^p - b^p, p) \neq 1$ 이면 $a^p \equiv b^p \pmod{p^2}$ 임을 증명하시오.

(증명)

p가 소수이므로 $\gcd(a^p - b^p, p) \neq 1$ 이면 $\gcd(a^p - b^p, p) = p$ 이다.

따라서 $p \mid a^p - b^p$ 이므로 $a^p \equiv b^p \pmod p$ 이고 Corollary 2.2.2에 의하면

$a \equiv a^p \equiv b^p \equiv b \pmod p$ 를 얻는다. (14)

따라서 적당한 정수 k가 존재해서 $a - b = kp$ 를 만족한다.

그러므로 이항정리에 의하면 다음을 얻을수 있다.

$$\begin{aligned} & a^{p-1} + a^{p-2}b + \cdots + ab^{p-2} + b^{p-1} \\ & \equiv (b+kp)^{p-1} + (b+kp)^{p-2}b + \cdots + (b+kp)b^{p-2} + b^{p-1} \\ & \equiv b^{p-1} + b^{p-1} + \cdots + b^{p-1} \ (b^{p-1}\text{이 } p\text{개}) \\ & \equiv pb^{p-1} \\ & \equiv 0 \pmod p \end{aligned} \tag{15}$$

그리고 $a^p - b^p = (a-b)(a^{p-1} + a^{p-2}b + \cdots + ab^{p-2} + b^{p-1})$ 이므로

(14), (15)에 의하면 $p^2 \mid a^p - b^p$ 임을 쉽게 알수 있다. 따라서 $a^p \equiv b^p \pmod{p^2}$ 이다.

■

Problem 2.2.4 홀수인 소수 p에 대하여 다음을 증명하시오.

(a). $1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \pmod p$

(b). $1^p + 2^p + \cdots + (p-1)^p \equiv 0 \pmod p$

(증명)

(a). p가 소수이므로 $1 \leq a \leq p-1$ 이면 페르마의 작은 정리에 의해

$a^{p-1} \equiv 1 \pmod p$ 를 만족한다. 따라서 다음을 얻는다.

$$1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv p - 1 \equiv -1 \pmod p$$

■

(b). p가 소수이므로 $1 \leq a \leq p-1$ 이면 Corollary 2.2.2에 의해

$a^p \equiv a \pmod p$ 를 만족한다. 그리고 p가 홀수인 소수이므로 $\frac{p-1}{2}$ 는 자연수이고

따라서 다음을 얻는다.

$$\begin{aligned} 1^p+2^p+\cdots+(p-1)^p &\equiv 1+2+\cdots+(p-1) \\ &\equiv \frac{p(p-1)}{2} \\ &\equiv 0 \pmod p \end{aligned}$$

■

Problem 2.2.5 $11^{341} \equiv 55 \pmod{341}$ 임을 증명하시오.

따라서 $11^{341} \not\equiv 11 \pmod{341}$ 이므로 가장 작은 유사소수인 341은 가장 작은 카마이클 수가 될수 없다.

(증명)

$341 = 11 \times 31$ 이다. 따라서 다음을 보이면 된다.

$$\begin{aligned} 11^{341} &\equiv 55 \pmod{11} \\ 11^{341} &\equiv 55 \pmod{31} \end{aligned}$$

$11^{341}, 55$는 모두 11의 배수이므로 $11^{341} \equiv 55 \pmod{11}$ 은 명백하다.

따라서 $11^{341} \equiv 55 \pmod{31}$ 임을 보이자.

페르마의 작은 정리에 의하면 $11^{30} \equiv 1 \pmod{31}$ 이므로 다음을 얻는다.

$$11^{341} \equiv \left(11^{30}\right)^{11} \times 11^{11} \equiv 11^{11} \pmod{31}$$

그리고 $11^2 \equiv -3 \pmod{31}$ 이므로 $11^{10} \equiv 5 \pmod{31}$ 이다.

따라서 $11^{11} \equiv 55 \pmod{31}$ 이므로 $11^{341} \equiv 55 \pmod{31}$ 이다.

그러므로 $11^{341} \equiv 55 \pmod{341}$ 이다. ■

Problem 2.2.6 다음을 증명하시오.

(a). 자연수 n과 $\gcd(a,n) = \gcd(a-1,n) = 1$ 을 만족하는 정수 a에 대하여 $1+a+a^2+\cdots+a^{\phi(n)-1} \equiv 0 \pmod n$ 이다.

(b). $\gcd(m,n) = 1$ 이면 $n^{\phi(m)} + m^{\phi(n)} \equiv 1 \pmod{mn}$ 이다.

(증명)

(a). 오일러의 정리에 의하면 $a^{\phi(n)} \equiv 1 \pmod n$ 이다.

그리고 $a^{\phi(n)} - 1 = (a-1)\left(a^{\phi(n)-1} + \cdots + a^2 + a + 1\right)$ 이고 $\gcd(a-1,n) = 1$ 이므로 $a-1$ 은 법 n에서 곱셈에 대한 역원이 존재한다.

따라서 $a^{\phi(n)} \equiv 1 \pmod n$ 에서 $1+a+a^2+\cdots+a^{\phi(n)-1} \equiv 0 \pmod n$ 를 얻을수 있다. ■

(b). $\gcd(m,n) = 1$ 이므로 오일러의 정리와 직관에 의하면 다음을 얻는다.

$$\begin{aligned} n^{\phi(m)} + m^{\phi(n)} &\equiv 1 \pmod m \\ n^{\phi(m)} + m^{\phi(n)} &\equiv 1 \pmod n \end{aligned}$$

따라서 $n^{\phi(m)}+m^{\phi(n)}\equiv 1 \pmod{mn}$ 가 성립한다. ■

이제 마지막으로 윌슨의 정리를 소개하겠습니다.

Theorem 2.2.4 윌슨의 정리(Wilson's Theorem)
$n\geq 2$ 일 때 $(n-1)!\equiv -1 \pmod{n}$ 가 성립할 필요충분조건은 n이 소수인 것이다.

(증명)
$(\Longrightarrow)$ 결론을 부정해서 n이 소수가 아니라고 가정하자. 그러면 $n\geq 2$ 이므로 n은 합성수이고 따라서 $1<a\leq b<n$ 을 만족하는 적당한 자연수 a,b가 존재해서 $n=ab$ 를 만족한다.

조건에 의하면 $n\mid (n-1)!+1$ 이다. 그리고 $a\mid n$ 이므로 $a\mid (n-1)!+1$ 인데 $a\leq n-1$ 이므로 $a\mid (n-1)!$ 이다. 따라서 $a\mid ((n-1)!+1)-(n-1)!=1$ 이므로 $a=1$ 인데 이것은 모순이다. 그러므로 n은 소수이다.

$(\Longleftarrow)$ $n=2,3$ 이면 $(n-1)!\equiv -1 \pmod{n}$ 은 명백하다. $n\geq 5$ 를 가정하자. 그러면 n이 소수이므로 $\mathbb{Z}_n^{\times}=\{1,2,...,n-1\}$ 이다.

$a\in\mathbb{Z}_n^{\times}$ 가 $a^2\equiv 1 \pmod{n}$ 를 만족한다고 하자.
그러면 $(a-1)(a+1)\equiv 0 \pmod{n}$ 이고 n은 소수이므로 $a\equiv 1 \pmod{n}$ 또는 $a\equiv -1 \pmod{n}$ 이다. 따라서 $a^2\equiv 1 \pmod{n}$ 을 만족하는 $a\in\mathbb{Z}_n^{\times}$ 는 $a=1,n-1$ 이다.

그리고 $\mathbb{Z}_n^{\times}=\{1,2,...,n-1\}$은 법 n에 대한 기약잉여계 이므로 $a\in\mathbb{Z}_n^{\times}$ 이면 $a^{-1}\in\mathbb{Z}_n^{\times}$ 이다. $\mathbb{Z}_n^{\times}$의 원소들 중 $1,n-1$ 을 제외한 나머지는 $a^2\not\equiv 1 \pmod{n}$ 이므로 $1,n-1$ 을 제외한 나머지를 모두 곱하면 a와 a^{-1}를 모두 곱하는것과 같다.

2부터 $n-2$ 까지의 자연수는 $n-3$ 개 있고 n은 $n\geq 5$ 인 소수이므로 $n-3$ 은 짝수이다. 따라서 $2,3,\ ...,n-2$ 에는 서로 곱하면 1이 되는 쌍이 $\frac{n-3}{2}$ 개 있다.

그러므로 $2\times 3\times\cdots\times(n-2)\equiv 1 \pmod{n}$ 이고
$(n-1)!\equiv n-1\equiv -1 \pmod{n}$ 가 성립한다. ■

보통 윌슨의 정리라고 하면 p가 소수일 때 $(p-1)!\equiv -1 \pmod{p}$ 가 성립한다는 것만 말하는 편인데 저는 필요충분조건이라는 것을 말하고 싶어서 둘다 썼습니다.

윌슨의 정리는 다음과 같이 일반화할수 있는데 이것은 가우스가 증명했습니다.
일반화된 윌슨의 정리를 증명하려면 대수학에 나오는 내용이 필요합니다.
따라서 이것은 증명없이 받아들이겠습니다.

Theorem 2.2.5 일반화된 윌슨의 정리(Generalized Wilson's Theorem)
자연수 n에 대하여 $\mathbb{Z}_n^{\times} = \{r_1, r_2, ..., r_{\phi(n)}\}$라고 하자. 그러면 홀수인 소수 p와 자연수 k에 대하여 다음이 성립한다.

$$r_1 r_2 \cdots r_{\phi(n)} \equiv \begin{cases} -1 & (n = 2, 4, p^k, 2p^k) \\ 1 & (\text{otherwise}) \end{cases} \pmod{n}$$

n이 소수이면 일반화된 윌슨의 정리에서 $n = p$ 인 경우이고 이때 $\mathbb{Z}_p^{\times} = \{1, 2, ..., p-1\}$ 이므로 $(p-1)! \equiv -1 \pmod{p}$ 가 성립한다는 것을 알수 있습니다.

페르마의 작은 정리와 윌슨의 정리를 가지고 다음을 유도할수 있습니다. 사실 페르마의 작은 정리와 윌슨의 정리는 다음 정리를 유도할수 있기 때문에 중요한 정리이기도 합니다.

$a \in \mathbb{Z}$ 이고 p가 소수일 때 $x^2 \equiv a \pmod{p}$ 을 만족하는 $x \in \mathbb{Z}$ 가 어떤 조건 하에서 존재하냐는 문제는 과거에 수학자들이 오랫동안 고민한 문제였습니다. 지금은 대부분 해결되었고 모든 기초 정수론 책에 나오는 내용입니다. 나중에 소개하겠습니다.

Theorem 2.2.6 p가 홀수인 소수일 때 $x^2 \equiv -1 \pmod{p}$ 를 만족하는 해가 존재할 필요충분조건은 $p \equiv 1 \pmod{4}$ 인 것이다. 그리고 해가 존재할 경우 $x = \left(\frac{p-1}{2}\right)!$ 가 $x^2 \equiv -1 \pmod{p}$ 를 만족하는 하나의 해가 된다.

(증명)
$(\Rightarrow)$ $x^2 \equiv -1 \pmod{p}$ 를 만족하는 해가 $x = a$ 로 존재한다고 하자.
그러면 $a^2 \equiv -1 \pmod{p}$ 이므로 $p \nmid a$ 이다. 그리고 p는 홀수인 소수이므로 $\frac{p-1}{2}$ 는 자연수이다. 따라서 페르마의 작은 정리에 의하면 다음을 얻는다.

$$1 \equiv a^{p-1} \equiv \left(a^2\right)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$

p는 홀수인 소수이므로 $p \equiv 1 \pmod{4}$ 또는 $p \equiv 3 \pmod{4}$ 이다.

만약 $p \equiv 3 \pmod{4}$ 이면 음이 아닌 정수 k에 대하여 $p = 4k + 3$ 형태이고
이 경우 $(-1)^{\frac{p-1}{2}} = (-1)^{2k+1} = -1$ 이므로 $1 \equiv -1 \pmod{p}$ 에서
$2 \equiv 0 \pmod{p}$ 이다. 따라서 $p \mid 2$ 인데 이것은 p가 홀수인 소수라는 것에 모순이다.

그러므로 $p \equiv 1 \pmod{4}$ 가 되어야 한다.

($\Leftarrow$) p가 홀수이므로 Problem 2.1.7에 의하면 다음 S 는 법 p에 대한 완전잉여계이다.

$$S=\left\{-\frac{p-1}{2}, -\frac{p-3}{2}, \ ..., -2, -1, 0, 1, 2, \ ..., \frac{p-3}{2}, \frac{p-1}{2}\right\}$$

따라서 윌슨의 정리와 S 가 법 p에 대한 완전잉여계라는 사실, 그리고 $p \equiv 1 \pmod 4$ 이므로 $\frac{p-1}{2}$ 가 짝수라는 사실에 의해 다음을 얻을수 있다.

$$\begin{aligned} -1 &\equiv (p-1)! \\ &\equiv 1\times(-1)\times 2\times(-2)\times\cdots\times\left(\frac{p-1}{2}\right)\times\left(-\frac{p-1}{2}\right) \\ &\equiv (-1)^{\frac{p-1}{2}}\left(1\times 2\times\cdots\times\frac{p-1}{2}\right)^2 \\ &\equiv \left(\left(\frac{p-1}{2}\right)!\right)^2 \pmod p \end{aligned}$$

그러므로 $x^2 \equiv -1 \pmod p$ 을 만족하는 x는 $x=\left(\frac{p-1}{2}\right)!$ 로 존재한다. ■

Theorem 2.2.6으로 $x^2+1 \equiv 0 \pmod{13}$ 을 만족하는 x가 존재하는지, 그리고 존재하면 하나의 해는 무엇인지 쉽게 알수 있습니다.

$13 \equiv 1 \pmod 4$ 이므로 Theorem 2.2.6에 의하면 $x^2+1 \equiv 0 \pmod{13}$ 을 만족하는 x는 존재하고 하나의 해는 $x=\left(\frac{13-1}{2}\right)! = 720 \equiv 5 \pmod{13}$ 입니다.

그러므로 $x=\pm 5$ 가 $x^2+1 \equiv 0 \pmod{13}$ 을 만족하는 해가 됩니다.
해를 $\mathbb{Z}_{13}$에서 고르면 $x=5, 8$ 입니다.

윌슨의 정리에 의하면 자연수 n에 대하여 $n!+1$ 형태를 갖는 합성수의 개수가 무한하다는 것을 알수 있습니다. 소수의 개수는 무한하고 p가 $p \geq 5$ 를 만족하는 소수이면 $(p-1)!+1 > p$ 이고 $p \mid (p-1)!+1$ 이므로 $(p-1)!+1$ 은 합성수입니다.

그런데 $n!+1$ 형태를 갖는 소수의 개수가 무한한지는 아직 밝혀지지 않았습니다.
$1 \leq n \leq 100$ 일 때 $n!+1$ 이 소수가 되는 경우는 다음과 같고

$$n = 1, 2, 3, 11, 27, 37, 41, 73, 77$$

현재까지 발견된 $n!+1$ 형태를 갖는 가장 큰 소수는 $6380!+1$ 이라고 합니다.

Problem 2.2.7 다음을 계산하시오.
(a). $15!$을 17로 나눈 나머지.
(b). $2\times(26!)$을 29로 나눈 나머지.
(c). $4\times(29!)+5!$을 31로 나눈 나머지.
(d). $18!$을 437로 나눈 나머지.

(풀이)
(a). 17은 소수이므로 윌슨의 정리에 의하면 $16! \equiv -1 \pmod{17}$ 이다.
그리고 $16 \equiv -1 \pmod{17}$ 이므로 양변에 16을 곱하면 $15! \equiv 1 \pmod{17}$ 을
얻는다. 따라서 나머지는 1이다. ■

(b). 29는 소수이므로 윌슨의 정리에 의하면 $28! \equiv -1 \pmod{29}$ 이고
법 29에 대하여 $28 \equiv -1, 27 \equiv -2$ 이므로 $28! \equiv 2 \times (26!) \pmod{29}$ 이다.
따라서 $2 \times (26!) \equiv -1 \equiv 28 \pmod{29}$ 이므로 나머지는 28이다. ■

(c). 31은 소수이므로 윌슨의 정리에 의하면 $30! \equiv -1 \pmod{31}$ 이다.
그리고 $30 \equiv -1 \pmod{31}$ 이므로 양변에 30을 곱하면 $29! \equiv 1 \pmod{31}$ 이다.
따라서 $4 \times (29!) + 5! \equiv 124 \equiv 0 \pmod{31}$ 이므로 나머지는 0이다. ■

(d). $437 = 19 \times 23$ 이다. 윌슨의 정리에 의하면 다음을 얻는다.

$$18! \equiv -1 \pmod{19}$$
$$22! \equiv -1 \pmod{23}$$

그리고 법 23에 대하여 $22 \equiv -1, 21 \equiv -2, 20 \equiv -3, 19 \equiv -4$ 이므로
$22! \equiv 18! \times 4! \equiv 18! \pmod{23}$ 을 얻는다.

따라서 $18! \equiv -1 \pmod{19}$, $18! \equiv -1 \pmod{23}$ 이므로
$18! \equiv -1 \equiv 17 \pmod{437}$ 을 얻는다. 그러므로 나머지는 17이다. ■

Problem 2.2.8 다음 물음에 답하시오.
(a). $x^2 \equiv -1 \pmod{17}$ 을 만족하는 $x \in \mathbb{Z}$ 가 존재하는지 판정하고
존재하면 가장 작은 자연수 해를 구하시오.
(b). $x^2 \equiv -1 \pmod{43}$ 을 만족하는 $x \in \mathbb{Z}$ 가 존재하는지 판정하고
존재하면 가장 작은 자연수 해를 구하시오.
(c). $x^2 \equiv -1 \pmod{731}$ 을 만족하는 $x \in \mathbb{Z}$ 가 존재하는지 판정하고
존재하면 가장 작은 자연수 해를 구하시오.

(풀이)
(a). 17은 소수이고 $17 \equiv 1 \pmod{4}$ 이므로 Theorem 2.2.6에 의하면
해가 존재한다. 그리고 하나의 해는 $x = 8!$ 이다.

법 17에 대하여 $4! \equiv -10, 5 \times 6 \equiv -4, 7 \times 8 \equiv -5$ 이고 $20 \equiv -3$ 이므로
$8! \equiv -20 \times 10 \equiv 30 \equiv -4 \pmod{17}$ 이다. 따라서 가장 작은 자연수 해는
$x = 4$ 이다. ■

(b). 43은 소수이고 $43 \equiv 3 \pmod{4}$ 이므로 Theorem 2.2.6에 의하면
해가 존재하지 않는다. ■

(c). $x^2 \equiv -1 \pmod{731}$ 을 만족하는 $a \in \mathbb{Z}$ 가 존재한다고 가정하자.
그러면 $731 = 17 \times 43$ 이므로 다음을 만족한다.

$$a^2 \equiv -1 \pmod{17}$$
$$a^2 \equiv -1 \pmod{43}$$

이것은 (b)에 모순이다. 따라서 $x^2 \equiv -1 \pmod{731}$ 을 만족하는 $x \in \mathbb{Z}$ 는 존재하지 않는다. ■

Problem 2.2.9 p, q는 서로 다른 소수이고 $p-1 \mid q-1$ 을 만족한다.
그러면 $\gcd(a, pq) = 1$ 일 때 $a^{q-1} \equiv 1 \pmod{pq}$ 임을 증명하시오.

(증명)
$\gcd(a, pq) = 1$ 이므로 $\gcd(a, p) = \gcd(a, q) = 1$ 이다. 따라서 페르마의 작은 정리에 의하면 다음을 얻는다.

$$a^{p-1} \equiv 1 \pmod{p}$$
$$a^{q-1} \equiv 1 \pmod{q}$$

$p-1 \mid q-1$ 이므로 $a^{p-1} \equiv 1 \pmod{p}$ 에서 $a^{q-1} \equiv 1 \pmod{p}$ 가 성립하고 조건에 의하면 $\gcd(p, q) = 1$ 이므로 $a^{q-1} \equiv 1 \pmod{pq}$ 가 성립한다. ■

Problem 2.2.10 다음을 증명하시오.
(a). n이 $n \geq 6$ 을 만족하는 합성수이면 $(n-1)! \equiv 0 \pmod{n}$ 이다.
(b). p가 소수일 때 $(p-1)! + 1 = p^k$ 를 만족하는 자연수 k가 존재할 필요충분조건은 $p = 2, 3, 5$ 이다.

(증명)
(a). n이 합성수이므로 $1 < a \leq b < n$ 을 만족하는 적당한 자연수 a, b가 존재해서 $n = ab$ 를 만족한다. 만약 $a < b$ 이면 $2 \leq a < b \leq n-1$ 이므로 1부터 $n-1$ 까지의 자연수에는 a, b가 모두 있다. 따라서 $(n-1)! \equiv 0 \pmod{n}$ 가 성립한다.

그러므로 $a = b$ 즉, $n = a^2$ 으로 표현되는 경우만 증명하면 충분하다.

$n = a^2$ 으로 표현되는 경우 $n \geq 6$ 이므로 6 이상의 짝수중 가장 작은 제곱수는 $16 = 4^2$ 이다. 그러므로 n이 짝수이면 $a \geq 4$ 이다.

마찬가지로 $n = a^2$ 으로 표현되는 경우 n이 홀수이면 n은 합성수이므로 $n \geq 9$ 이고 $9 = 3^2$ 이므로 9가 조건을 만족하는 가장 작은 홀수 제곱수이다. 그리고 이 경우 $a \geq 3$ 이다. 따라서 어느 경우든 $a \geq 3$ 이어야 한다.

한편 $n=a^2$ 이면 바닥함수의 정의에 의해 $\left\lfloor \frac{n-1}{a} \right\rfloor = \left\lfloor a-\frac{1}{a} \right\rfloor = a-1 \geq 2$ 이므로 $n-1$ 이하의 자연수중 a의 배수는 적어도 2개 있다. 그러므로 이 경우에도 $(n-1)! \equiv 0 \pmod{n}$ 가 성립한다.

정리하면 어느 경우든 $(n-1)! \equiv 0 \pmod{n}$ 가 성립한다.
따라서 n이 $n \geq 6$ 을 만족하는 합성수이면 $(n-1)! \equiv 0 \pmod{n}$ 이다. ■

(b). $(\Rightarrow)$ $p=2,3$ 일땐 각각 $2=2^k, 3=3^k$ 이므로 $k=1$ 이다. 그리고 $p=5$ 이면 $25=5^k$ 이므로 $k=2$ 이다. 따라서 조건을 만족하는 자연수 k가 존재한다.

이제 $p \geq 7$ 일 때 $(p-1)!+1=p^k$ 를 만족하는 자연수 k가 존재하지 않음을 증명하기 위해 결론을 부정해서 존재한다고 가정하자. 그러면 $(p-1)!=p^k-1$ 에서 양변을 $p-1$ 로 나누면 $(p-2)!=1+p+p^2+\cdots+p^{k-1}$ 을 얻는다.

$p-1$ 은 6 이상의 합성수이므로 (a)에 의하면 $(p-2)! \equiv 0 \pmod{p-1}$ 이다.
따라서 $1+p+p^2+\cdots+p^{k-1} \equiv 0 \pmod{p-1}$ 이고 $p \equiv 1 \pmod{p-1}$
이므로 모든 자연수 m에 대하여 $p^m \equiv 1 \pmod{p-1}$ 이다.

그러므로 $1+p+p^2+\cdots+p^{k-1} \equiv k \equiv 0 \pmod{p-1}$ 를 얻는다.

따라서 적당한 자연수 t가 존재해서 $k=(p-1)t$ 를 만족하고 $(p-1)!+1=p^{(p-1)t}$
인데 $1,2,...,p-1$ 은 모두 p보다 작으므로 $(p-1)! < p^{p-1}$ 이다. (16)

그러므로 $p^{p-1} > p^{(p-1)t}-1$ 이다. $x=p^{p-1}$ 라고 하면 $x^t-x-1<0$ 이고
$p \geq 7$ 이므로 $x \geq 7^6$ 이다. 여기서 만약 $t \geq 2$ 이면 다음을 얻는다.

$$x^t-x-1=x\left(x^{t-1}-1\right)-1 \geq 7^6\left(7^6-1\right)-1>0$$

이것은 $x^t-x-1<0$ 에 모순이므로 $t=1$ 이어야 한다. 즉, $k=p-1$ 이므로
$(p-2)!=1+p+p^2+\cdots+p^{p-2}$ 인데 (16)과 같은 논리로 $(p-2)! < p^{p-2}$ 를
얻을수 있고 따라서 $1+p+p^2+\cdots+p^{p-2} < p^{p-2}$ 인데 이것은 모순이다.

그러므로 $p \geq 7$ 이면 $(p-1)!+1=p^k$ 를 만족하는 자연수 k는 존재하지 않는다.
따라서 $p=2,3,5$ 가 되어야 한다.

$(\Leftarrow)$ 이것은 $(\Rightarrow)$ 이 증명과정에서 이미 보였으므로 생략한다. ■

Problem 2.2.10에서 $(p-1)! \equiv -1 \pmod{p^2}$ 을 만족하는 $p \geq 7$ 인 소수 p가 존재하는지 생각해볼수 있는데 $p=13$ 이면 $12!+1 = 13^2 \times 2834329$ 이므로 $12! \equiv -1 \pmod{13^2}$ 을 만족합니다. 추가로 $p=563$ 도 합동식을 만족한다고 합니다.

$(p-1)! \equiv -1 \pmod{p^2}$ 을 만족하는 소수 p를 **윌슨 소수(Wilson Prime)**라고 부르는데 현재까지 발견된 윌슨 소수는 $p=5, 13, 563$ 이게 전부라고 합니다.

Problem 2.2.11 소수 p에 대하여 다음을 증명하시오.

(a). $(p-1)! \equiv p-1 \pmod{1+2+\cdots+(p-1)}$ 이다.

(b). 정수 k가 $0 \leq k \leq p-1$ 이면 $\binom{p-1}{k} \equiv (-1)^k \pmod{p}$ 이다.

(c). 정수 k가 $0 \leq k \leq p-1$ 이면 $k!(p-1-k)! \equiv (-1)^{k+1} \pmod{p}$ 이다.

(증명)

(a). $1+2+\cdots+(p-1) = \dfrac{p(p-1)}{2}$ 이고 $p=2$ 이면 주어진 합동식이 성립함은 명백하다. 따라서 $p \geq 3$ 을 가정하자. 그러면 $\dfrac{p-1}{2}$ 는 자연수이고 윌슨의 정리와 $\dfrac{p-1}{2} \mid p-1$ 에 의하면 다음을 얻을수 있다.

$$(p-1)! \equiv -1 \equiv p-1 \pmod{p}$$
$$(p-1)! \equiv p-1 \pmod{\frac{p-1}{2}}$$

그리고 p는 소수이고 $p > \dfrac{p-1}{2}$ 이므로 $\gcd\left(p, \dfrac{p-1}{2}\right) = 1$ 이다.

따라서 $(p-1)! \equiv p-1 \pmod{1+2+\cdots+(p-1)}$ 가 성립한다. ■

(b). $p=2$ 이면 $\binom{1}{0} = \binom{1}{1} = 1$ 이고 $1 \equiv -1 \pmod{2}$ 이므로 명백하다.

따라서 p가 홀수인 소수일때를 가정하자. 그리고 이때도 $k=0$ 또는 $k=p-1$ 이면 $\binom{p-1}{k} = 1$ 이고 $p-1$ 은 짝수이므로 명백하다.

그러므로 $1 \leq k \leq p-2$ 을 가정하자. 그러면 다음을 얻는다.

$$\begin{aligned}(p-1)(p-2)\cdots(p-k) &\equiv (-1)\times(-2)\times\cdots\times(-k) \\ &\equiv (-1)^k k! \pmod{p}\end{aligned}$$

$1 \leq k \leq p-2$ 이고 p는 소수이므로 $\gcd(p, k!) = 1$ 이다. 따라서 다음이 성립한다.

$$\binom{p-1}{k} \equiv \frac{(p-1)(p-2)\cdots(p-k)}{k!} \equiv (-1)^k \pmod{p}$$

■

(c). (b)에 의하면 $\dfrac{(p-1)!}{k!(p-1-k)!} \equiv (-1)^k \pmod p$ 이므로 양변에 $k!(p-1-k)!$ 을 곱하면 윌슨의 정리에 의해 다음을 얻는다.

$$(-1)^k k!(p-1-k)! \equiv (p-1)! \equiv -1 \pmod p$$

다시 양변에 $(-1)^k$를 곱하면 $k!(p-1-k)! \equiv (-1)^{k+1} \pmod p$ 를 얻는다. ■

Problem 2.2.11 (b)를 풀 때 p가 소수인 경우에는 $p-m \equiv -m \pmod p$ 를 이용해서 다음과 같이 풀어도 됩니다.

$$\begin{aligned} \frac{(p-1)(p-2)\cdots(p-k)}{k!} &\equiv \frac{(-1)\times(-2)\times\cdots\times(-k)}{k!} \\ &\equiv \frac{(-1)^k k!}{k!} \\ &\equiv (-1)^k \pmod p \end{aligned} \tag{17}$$

그런데 p가 소수가 아닌 경우에는 (17)처럼 풀면 안됩니다. p가 소수일 때 (17)처럼 풀수 있는 이유는 $\gcd(p,k!)=1$ 이므로 $k!$이 법 p에서 곱셈에 대한 역원이 존재하기 때문입니다. 따라서 양변을 $k!$으로 나눌수 있는겁니다.

소수가 아닌 경우에는 (17)처럼 풀면 틀립니다. $n=6$ 이고 $k=3$ 이면 $\binom{5}{3} \equiv 2 \pmod 6$ 이므로 $(-1)^3 = -1$ 과 합동이 아닌데 (17)처럼 풀면

$$\frac{5\times4\times3}{3!} \equiv \frac{(-1)\times(-2)\times(-3)}{3!} \equiv -1 \pmod 6$$

이렇게 모순된 결과가 나옵니다. 이때는 $\gcd(6,3!)=6$ 이므로 $3!$은 법 6에서 곱셈에 대한 역원이 존재하지 않고 그래서 분모에 쓰면 안됩니다.

Problem 2.2.12 임의의 서로 다른 소수 p, q와 임의의 정수 a에 대하여 다음이 성립함을 증명하시오.

$$pq \mid a^{pq} - a^p - a^q + a$$

(증명)
Corollary 2.2.2에 의하면 다음을 얻는다.

$$\begin{aligned} a^p \equiv a \pmod p &\Rightarrow a^{pq} \equiv a^q \pmod p \\ a^q \equiv a \pmod q &\Rightarrow a^{pq} \equiv a^p \pmod q \end{aligned}$$

그러므로 다음을 얻을수 있다.

$$\begin{aligned} a^{pq} - a^p &\equiv a^q - a \pmod p \\ a^{pq} - a^q &\equiv a^p - a \pmod q \end{aligned}$$

따라서 다음을 얻는다.

$$\begin{aligned} a^{pq} - a^p - a^q + a &\equiv 0 \pmod p \\ a^{pq} - a^p - a^q + a &\equiv 0 \pmod q \end{aligned}$$

p, q는 서로 다른 소수이므로 $\gcd(p,q)=1$ 이다. 그러므로
$a^{pq}-a^p-a^q+a \equiv 0 \pmod{pq}$ 이고 다음을 얻을수 있다.

$$pq \mid a^{pq}-a^p-a^q+a$$

■

Problem 2.2.13 p가 홀수인 소수일 때 다음을 증명하시오.

$$1^2 \times 3^2 \times \cdots \times (p-2)^2 \equiv 2^2 \times 4^2 \times \cdots \times (p-1)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$$

(증명)
p가 홀수인 소수이므로 $p-2$ 는 자연수이다. 다음 두 단계로 나눠서 증명하자.

step1) $1^2 \times 3^2 \times \cdots \times (p-2)^2 \equiv 2^2 \times 4^2 \times \cdots \times (p-1)^2 \pmod{p}$
법 p에 대하여 다음이 성립한다.

$$\begin{aligned} 1 &\equiv -(p-1) \\ 3 &\equiv -(p-3) \\ &\vdots \\ p-2 &\equiv -2 \end{aligned}$$

따라서 양변을 제곱하면 법 p에 대하여 다음을 얻는다.

$$\begin{aligned} 1^2 &\equiv (p-1)^2 \\ 3^2 &\equiv (p-3)^2 \\ &\vdots \\ (p-2)^2 &\equiv 2^2 \end{aligned} \tag{18}$$

(18)의 양변을 모두 곱하면 step1)의 합동식을 얻을수 있다.

step2) $2^2 \times 4^2 \times \cdots \times (p-1)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$
p가 홀수이므로 Problem 2.1.7에 의하면 다음 S 는 법 p에 대한 완전잉여계이다.

$$S=\left\{-\frac{p-1}{2}, -\frac{p-3}{2}, \ ..., -2, -1, 0, 1, 2, \ ..., \frac{p-3}{2}, \frac{p-1}{2}\right\}$$

따라서 윌슨의 정리와 S 가 법 p에 대한 완전잉여계라는 사실에 의해 다음을 얻을수 있다.

$$\begin{aligned} -1 &\equiv (p-1)! \\ &\equiv 1 \times (-1) \times 2 \times (-2) \times \cdots \times \left(\frac{p-1}{2}\right) \times \left(-\frac{p-1}{2}\right) \\ &\equiv (-1)^{\frac{p-1}{2}} \left(1 \times 2 \times \cdots \times \frac{p-1}{2}\right)^2 \\ &\equiv (-1)^{\frac{p-1}{2}} \left(\frac{2}{2} \times \frac{4}{2} \times \cdots \times \frac{p-1}{2}\right)^2 \\ &\equiv (-1)^{\frac{p-1}{2}} \times \frac{2^2 \times 4^2 \times \cdots \times (p-1)^2}{2^{p-1}} \pmod{p} \end{aligned} \tag{19}$$

한편 p는 홀수인 소수이므로 페르마의 작은 정리에 의하면 $2^{p-1} \equiv 1 \pmod{p}$ 이고
$\left((-1)^{\frac{p-1}{2}}\right)^2 \equiv (-1)^{p-1} \equiv 1 \pmod{p}$ 이므로 양변에 $2^{p-1} \times (-1)^{\frac{p-1}{2}}$ 를 곱하면
$2^2 \times 4^2 \times \cdots \times (p-1)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$ 를 얻는다.

따라서 step1), step2)에 의하면 문제에 주어진 합동식이 성립한다. ■

Problem 2.2.14 p와 $p+2$가 모두 소수일 때 다음을 증명하시오.

$$4((p-1)!+1)+p \equiv 0 \pmod{p(p+2)}$$

(증명)

p는 소수이므로 윌슨의 정리에 의하면 다음이 성립한다는 것은 명백하다.

$$4((p-1)!+1)+p \equiv 0 \pmod{p} \tag{20}$$

마찬가지로 $p+2$ 도 소수이므로 윌슨의 정리에 의하면 다음이 성립한다는 것은 명백하다.

$$2((p+1)!+1)+(p+2) \equiv 0 \pmod{p+2} \tag{21}$$

그리고 $p(p+1) \equiv (-2) \times (-1) \equiv 2 \pmod{p+2}$ 이므로 (21)에서 다음을 얻는다.

$$\begin{aligned} 2((p+1)!+1)+(p+2) &\equiv 2(2(p-1)!+1)+(p+2) \\ &\equiv 4(p-1)!+4+p \\ &\equiv 4((p-1)!+1)+p \\ &\equiv 0 \pmod{p+2} \end{aligned}$$

따라서 $4((p-1)!+1)+p \equiv 0 \pmod{p+2}$ 가 성립한다. (22)

그리고 $\gcd(p, p+2) = 1$ 이므로 (20)과 (22)에 의하면 다음을 얻는다.

$$4((p-1)!+1)+p \equiv 0 \pmod{p(p+2)}$$

■

Problem 2.2.15 소수 p가 $p \equiv 3 \pmod{4}$ 를 만족할 때 정수 a, b가
$a^2+b^2 \equiv 0 \pmod{p}$ 를 만족하면 $a \equiv b \equiv 0 \pmod{p}$ 임을 증명하시오.

(증명)

$2 \not\equiv 3 \pmod{4}$ 이므로 조건에 의하면 p는 홀수이다.

결론을 부정해서 $a^2+b^2 \equiv 0 \pmod{p}$ 을 만족할 때 a, b 둘중 적어도 하나가 p의 배수가 아니라고 가정하자. 이때 a가 p의 배수가 아니라고 가정해도 일반성을 잃지 않는다.

그러면 $\gcd(a, p) = 1$ 이므로 법 p에서 a의 곱셈에 대한 역원은 존재하고 그것을 c라고 하면 조건식의 양변에 c를 곱해서 $1+(cb)^2 \equiv 0 \pmod{p}$ 를 얻을수 있다.

따라서 $x^2 \equiv -1 \pmod{p}$ 를 만족하는 $x \in \mathbb{Z}$ 가 $x = cb$ 로 존재하는데
$p \equiv 3 \pmod{4}$ 이므로 이것은 Theorem 2.2.6에 모순이다.

그러므로 $a \equiv 0 \pmod{p}$ 이고 이 경우 $b^2 \equiv 0 \pmod{p}$ 인데 p는 소수이므로 $b \equiv 0 \pmod{p}$ 이다. 따라서 $a \equiv b \equiv 0 \pmod{p}$ 이다. ■

Problem 2.2.16 다음을 증명하시오.

(a). p가 소수일 때 $2^p - 1$ 이 합성수이면 $2^p - 1$ 은 유사소수이다.

(b). n이 음이 아닌 정수일 때 $2^{2^n} + 1$ 이 합성수이면 $2^{2^n} + 1$ 은 유사소수이다.

(c). $6k+1, 12k+1, 18k+1$ 가 모두 소수가 되도록 하는 자연수 k에 대하여 $n = (6k+1)(12k+1)(18k+1)$ 은 카마이클 수이다.

(증명)

(a). $2^2 - 1 = 3$ 은 소수이므로 조건에 의하면 p는 홀수인 소수이고 Corollary 2.2.2에 의하면 $2^p \equiv 2 \pmod{p}$ 를 만족한다. 따라서 적당한 자연수 k가 존재해서 $2^p - 2 = kp$ 를 만족한다.

$M_p = 2^p - 1$ 라고 하자. 조건에 의하면 M_p 는 합성수이다. 이 다음은 Theorem 2.2.2의 증명과정을 그대로 따라하면 $2^{M_p} \equiv 2 \pmod{M_p}$ 를 얻을수 있다.
따라서 M_p는 유사소수이다. ■

(b). $F_n = 2^{2^n} + 1$ 이라고 하고 $2^{F_n - 1} \equiv 1 \pmod{F_n}$ 임을 보이자.

수학적 귀납법을 이용하면 모든 자연수 n에 대하여 $2^n \geq n+1$ 임을 쉽게 증명할수 있다.
따라서 $2^{n+1} \mid 2^{2^n} = F_n - 1$ 이므로 $2^{2^{n+1}} - 1 \mid 2^{F_n - 1} - 1$ 이다.

그리고 Problem 1.2.12에 의하면 $F_n \mid 2^{2^{n+1}} - 1$ 이다. 따라서 $F_n \mid 2^{F_n - 1} - 1$ 이므로 $2^{F_n - 1} \equiv 1 \pmod{F_n}$ 이고 양변에 2를 곱하면 $2^{F_n} \equiv 2 \pmod{F_n}$ 을 얻는다.

조건에 의하면 F_n은 합성수이므로 정의에 의하면 F_n은 유사소수이다. ■

(c). Korselt의 판정법을 사용하자. 조건에 의하면 n은 제곱인수가 없는 정수이다.
그리고 n을 전개하면

$$\begin{aligned} n &= 6 \times 12 \times 18k^3 + (6 \times 12 + 12 \times 18 + 18 \times 6)k^2 + (6 + 12 + 18)k + 1 \\ &= 6 \times 12 \times 18k^3 + 2^2 \times 3^2 \times 11k^2 + 2^2 \times 3^2 k + 1 \end{aligned}$$

이므로 다음을 만족한다는 것도 쉽게 알수 있다.

$$\begin{aligned} 6k &\mid n-1 \\ 12k &\mid n-1 \\ 18k &\mid n-1 \end{aligned}$$

따라서 Korselt의 판정법에 의하면 n은 카마이클 수이다. ■

Problem 2.2.17 다음을 증명하시오.

(a). p가 홀수인 소수일 때 $n=2p$ 라고 하자. 그러면 모든 $a\in\mathbb{Z}$ 에 대하여 $a^{n-1}\equiv a\pmod{n}$ 임을 증명하시오.

(b). 모든 $a\in\mathbb{Z}$ 에 대하여 $a^{193}\equiv a\pmod{195}$ 임을 증명하시오.

(증명)

(a). Corollary 2.2.2에 의하면 다음을 얻는다.

$$a^2\equiv a\pmod{2}$$
$$a^p\equiv a\pmod{p}$$

수학적 귀납법에 의하면 모든 자연수 m에 대하여 $a^{m+1}\equiv a\pmod{2}$ 임을 쉽게 증명할수 있다. 따라서 $m=p-1$ 이면 m은 자연수이므로 $a^p\equiv a\pmod{2}$ 이고 $\gcd(2,p)=1$ 이므로 $a^p\equiv a\pmod{n}$ 가 성립한다.

양변에 a^{p-1} 을 곱하면 $a^{2p-1}\equiv a^p\equiv a\pmod{n}$ 을 얻고 $2p-1=n-1$ 이므로 $a^{n-1}\equiv a\pmod{n}$ 가 성립한다. ■

(b). $195=3\times5\times13$ 이고 Corollary 2.2.2에 의하면 다음을 얻는다.

$$a^3\equiv a\pmod{3}$$
$$a^5\equiv a\pmod{5}$$
$$a^{13}\equiv a\pmod{13}$$

수학적 귀납법에 의하면 모든 자연수 m에 대하여 다음이 성립한다는 것을 쉽게 증명할수 있다.

$$\begin{aligned} a^{2m+1}&\equiv a\pmod{3}\\ a^{4m+1}&\equiv a\pmod{5}\\ a^{12m+1}&\equiv a\pmod{13}\end{aligned} \tag{23}$$

그리고 $192=2^6\times3$ 이므로 다음을 만족하는 자연수 r,s,t 는 존재한다.

$$193=2r+1$$
$$193=4s+1$$
$$193=12t+1$$

따라서 (23)에 의하면 다음을 얻을수 있다.

$$a^{193}\equiv a\pmod{3}$$
$$a^{193}\equiv a\pmod{5}$$
$$a^{193}\equiv a\pmod{13}$$

그리고 $\gcd(3,5)=\gcd(5,13)=\gcd(13,3)=1$ 이므로 $a^{193}\equiv a\pmod{195}$ 이다. ■

2.3 중국인의 나머지 정리

작성자 : 네냐플(Nenyaffle)

2.3절부터 합동방정식의 해법을 소개하려고 합니다. $x^3-2x^2+4x+1=0$ 처럼 등식에 미지수 x가 포함된 식을 방정식이라고 부르는것처럼 합동식에 미지수 x가 포함된 식을 합동방정식 이라고 부릅니다. 예를 들면 $2x\equiv 3\pmod 5$ 는 합동방정식 입니다.

2.2절에서도 합동방정식을 이미 소개했습니다. p가 홀수인 소수일 때 $x^2\equiv -1\pmod p$ 의 해가 존재할 필요충분조건은 $p\equiv 1\pmod 4$ 인 것이고 $p\equiv 1\pmod 4$ 이면 $x=\left(\frac{p-1}{2}\right)!$ 가 하나의 해가 된다는 정리였습니다.

일반적인 방정식을 다룰땐 다항함수만 나오는게 아니고 초월함수도 나옵니다.
$\ln(x-1)+\ln x=\ln 2$ 이것도 방정식이고 $e^{2x}-3e^x+2=0$ 이것도 방정식입니다.

그런데 초월함수의 함숫값은 정수가 아닐 가능성이 높아서 일반적인 방정식과 달리 합동방정식은 정수계수 다항식 $f(x)\in\mathbb{Z}[x]$에 대하여 $f(x)\equiv 0\pmod n$ 만 고려합니다.

그리고 $f(x)\in\mathbb{Z}[x]$이면 $a\equiv b\pmod n$ 일 때 $f(a)\equiv f(b)\pmod n$ 이므로 $x=a$ 가 합동방정식 $f(x)\equiv 0\pmod n$ 의 해이고 $a\equiv b\pmod n$ 이면 $x=b$ 도 합동방정식 $f(x)\equiv 0\pmod n$ 의 해가 됩니다.

따라서 합동방정식 $f(x)\equiv 0\pmod n$ 의 해의 개수를 이야기할땐 법 n에 대하여 합동이 아닌 해의 개수로 이야기합니다. $\gcd(a,n)=1$ 일 때 법 n에서 a의 곱셈에 대한 역원은 합동방정식 $ax\equiv 1\pmod n$ 을 만족하는 $x\in\mathbb{Z}$ 이고 a의 곱셈에 대한 역원은 법 n에서 유일하다고 말하는 것을 생각해보면 됩니다.

먼저 가장 쉬운 일차합동방정식 $ax\equiv b\pmod n$ 의 해법을 소개하겠습니다.
일반적인 방정식에서 일차방정식이라고 하면 $ax=b$ 에서 $a\neq 0$ 이라는 조건을 줍니다.
따라서 일차합동방정식 이라고 하면 보통 $a\not\equiv 0\pmod n$ 을 가정합니다.

일차합동방정식 $ax\equiv b\pmod n$ 을 푸는 것은 합동의 정의에 의하면 $ax-ny=b$ 를 만족하는 정수 x,y를 구하는 것과 같습니다.

Theorem 2.3.1 정수 a,b와 자연수 n에 대하여 $d=\gcd(a,n)$ 라고 하자. 그러면 일차합동방정식 $ax\equiv b\pmod n$ 의 해가 존재할 필요충분조건은 $d\mid b$ 인 것이다.

그리고 일차합동방정식 $ax\equiv b\pmod n$ 의 해가 존재하면 그 해는 법 n에서 정확히 d개 존재한다.

(증명)
합동의 정의에 의하면 $ax \equiv b \pmod{n}$ 의 해가 존재하는것과 $ax - ny = b$ 를 만족하는 정수 x, y가 존재하는 것은 동치이다. 그리고 $ax - ny = b$ 를 만족하는 정수 x, y가 존재할 필요충분조건은 $\gcd(a, -n) \mid b$ 이다.

$d = \gcd(a,n) = \gcd(a,-n)$ 이므로 해가 존재할 필요충분조건은 $d \mid b$ 이다.

일차합동방정식 $ax \equiv b \pmod{n}$ 의 해가 존재할 때 하나의 해를 $x = x_0$ 라고 하자. 그러면 적당한 정수 y_0가 존재해서 $ax_0 - ny_0 = b$ 를 만족하고 따라서 디오판토스 방정식 $ax - ny = b$ 의 일반해는 다음과 같다.

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

즉, 모든 정수 t에 대해 $x = x_0 + \left(\frac{n}{d}\right)t$ 는 합동방정식 $ax \equiv b \pmod{n}$ 을 만족한다. 이제 $x = x_0 + \left(\frac{n}{d}\right)t$ 중 법 n에 대하여 합동이 아닌 것을 분류하자.

t를 d로 나눈 나머지를 r 이라고 하자. 그러면 $0 \le r < d$ 이고 적당한 정수 q가 존재해서 $t = dq + r$ 를 만족한다. 따라서 다음을 얻는다.

$$\begin{aligned} x_0 + \left(\frac{n}{d}\right)t &\equiv x_0 + \left(\frac{n}{d}\right)(qd + r) \\ &\equiv x_0 + \left(\frac{n}{d}\right)r + qn \\ &\equiv x_0 + \left(\frac{n}{d}\right)r \pmod{n} \end{aligned}$$

그러므로 주어진 일차합동방정식의 해는 다음 d개만 고려해도 충분하다.

$$x_0,\ x_0 + \frac{n}{d},\ x_0 + \frac{2n}{d},\ \ldots,\ x_0 + \frac{(d-1)n}{d} \tag{24}$$

이제 (24)에 있는 서로 다른 d개의 정수가 법 n에 대하여 합동이 아님을 보이자.
$\gcd\left(\frac{n}{d}, n\right) = \frac{n}{d}$ 이고 $n \times \frac{d}{n} = d$ 이므로 $0 \le t_1 < d,\ 0 \le t_2 < d$ 를 만족하는 적당한 정수 t_1, t_2 에 대하여

$$\begin{aligned} & x_0 + \left(\frac{n}{d}\right)t_1 \equiv x_0 + \left(\frac{n}{d}\right)t_2 \pmod{n} \\ \Rightarrow & \left(\frac{n}{d}\right)t_1 \equiv \left(\frac{n}{d}\right)t_2 \pmod{n} \\ \Rightarrow & t_1 \equiv t_2 \pmod{d} \\ \Rightarrow & t_1 = t_2 \ (\because\ -d < t_1 - t_2 < d) \end{aligned}$$

를 얻는다. 따라서 (24)에 있는 서로 다른 d개의 정수는 법 n에 대하여 합동이 아니고 그러므로 주어진 일차합동방정식은 법 n에서 정확히 d개의 해를 갖는다. ■

Corollary 2.3.1 정수 a, b와 자연수 n에 대하여 일차합동방정식 $ax \equiv b \pmod{n}$ 이 법 n에서 유일한 해를 가질 필요충분조건은 $\gcd(a,n)=1$ 이고 유일한 해를 가지면 $x \equiv a^{-1}b \pmod{n}$ 이다. 여기서 a^{-1}는 법 n에서 a의 곱셈에 대한 역원이다.

(증명)

Theorem 2.3.1 에 의하면 해가 유일하게 존재할 필요충분조건이 $\gcd(a,n)=1$ 임은 명백하다. 그리고 $\gcd(a,n)=1$ 이므로 법 n에서 a의 곱셈에 대한 역원이 존재하고 $x \equiv (a^{-1}a)x \equiv a^{-1}(ax) \equiv a^{-1}b \pmod{n}$ 를 만족한다. ■

일차방정식 $ax=b$ 의 해를 구하는 방법은 $a \neq 0$ 이므로 양변에 a의 곱셈에 대한 역원 $\frac{1}{a}$를 곱하는겁니다. 그러면 $x=\frac{b}{a}$ 가 해가 됩니다.

그런데 법 n에서는 a의 곱셈에 대한 역원이 존재하지 않는 경우가 많아서 일차합동방정식 $ax \equiv b \pmod{n}$ 을 풀 때 양변에 a의 곱셈에 대한 역원을 곱하려고 하면 안됩니다. 곱셈에 대한 역원이 존재해야 양변에 역원을 곱해서 풀수 있습니다.

Corollary 2.3.1에 의하면 법 n에서 곱셈에 대한 역원이 존재할 경우 해는 유일합니다.

Problem 2.3.1 다음 일차합동방정식의 해가 존재하면 해를 $\mathbb{Z}_n$에서 모두 구하시오.

(a). $18x \equiv 30 \pmod{42}$

(b). $9x \equiv 21 \pmod{30}$

(c). $140x \equiv 133 \pmod{301}$

(풀이)

(a). $\gcd(18,42)=6 \mid 30$ 이므로 주어진 일차합동방정식은 해가 존재한다.

그리고 $\gcd(18,42)=6$ 을 유클리드 호제법을 사용해서 얻는 과정은 다음과 같다.

$$42=18\times 2+6$$
$$18=6\times 3+0$$

따라서 $6=42-18\times 2$ 이므로 $30=42\times 5-18\times 10$ 이고

$18\times(-10)-30=42\times(-5)$ 에서 하나의 해는 $x=-10$ 이다.

그리고 $-10 \equiv 32 \pmod{32}$ 이므로 하나의 해를 $\mathbb{Z}_{42}$에서 찾으면 $x=32$ 이다.

그러므로 Theorem 2.3.1과 (24)에 의하면 일차합동방정식의 6개의 해는 다음과 같다.

$$32, 39, 46, 53, 60, 67$$

해를 $\mathbb{Z}_{42}$에 있도록 하기 위해 42를 넘는 것은 42를 빼면 다음을 얻는다.

$$x=4, 11, 18, 25, 32, 39$$

■

(b). $\gcd(9,30)=3 \mid 21$ 이므로 주어진 일차합동방정식은 해가 존재한다.
그리고 이 경우에는 $x=-1$ 이 한 해가 된다는 것을 쉽게 알수 있다.

$\frac{30}{3}=10$ 이므로 일차합동방정식의 3개의 해는 $-1, 9, 19$ 이고
$\mathbb{Z}_{30}$에 있도록 만들면 $x=9, 19, 29$ 이다. ■

(c). 유클리드 호제법을 사용하자.

$$\begin{aligned} 301 &= 140\times 2+21 \\ 140 &= 21\times 6+14 \\ 21 &= 14\times 1+7 \\ 14 &= 7\times 2+0 \end{aligned}$$

이므로 $\gcd(140,301)=7$ 이다. 그리고 $133=7\times 19$ 이므로 $7 \mid 133$ 이고
따라서 주어진 일차합동방정식은 해가 존재한다.

이제 유클리드 호제법의 과정을 반대로 되돌아가면

$$\begin{aligned} 7 &= 21-14\times 1 \\ &= 21-(140-21\times 6)\times 1 \\ &= 21\times 7-140\times 1 \\ &= (301-140\times 2)\times 7-140\times 1 \\ &= 301\times 7-140\times 15 \end{aligned}$$

이므로 $133=301\times 19-140\times 285$ 이다. 따라서 주어진 일차합동방정식의
하나의 해는 $x=-285$ 이고 $-285\equiv 16 \pmod{301}$ 이므로 하나의 해를
$x=16$ 으로 택할수 있다. 그리고 $\frac{301}{7}=43$ 이므로 7개의 해는 다음과 같다.

$$16, 59, 102, 145, 188, 231, 274$$

이것은 모두 $\mathbb{Z}_{301}$의 원소이다. 따라서 $\mathbb{Z}_{301}$에 있는 해는 다음과 같다.

$$x=16, 59, 102, 145, 188, 231, 274$$

■

일차합동방정식은 이렇게 풀어도 됩니다. $18x\equiv 30 \pmod{42}$ 에서 $\gcd(18,42)=6$
이므로 양변을 6으로 나누면 $3x\equiv 5 \pmod{7}$ 을 얻고 $\gcd(3,7)=1$ 이므로 이것을
만족하는 해는 유일하고 $3\times 5\equiv 1 \pmod{7}$ 이므로 $x\equiv 5\times 5\equiv 4 \pmod{7}$ 입니다.

따라서 하나의 해를 $x=4$ 로 찾았고 Theorem 2.3.1의 증명과정에 의하면
4에 $\frac{42}{6}=7$을 $6-1=5$번 더해서 6개의 해를 얻을수 있습니다.
따라서 $\mathbb{Z}_{42}$에서 해를 찾으면 $x=4, 11, 18, 25, 32, 39$ 입니다.

숫자가 작으면 이렇게 푸는게 좀 더 편할수도 있습니다.

이제 2.3절에서 가장 중요한 중국인의 나머지 정리를 소개할건데 정리를 소개하기 전에 다음 두문제를 먼저 생각하겠습니다.

Q1) 일차합동방정식 $17x \equiv 9 \pmod{276}$ 을 다른 방법으로 풀어보려고 한다.

$276 = 2^2 \times 3 \times 23$ 이므로 $\gcd(17,276)=1$ 이고 따라서 일차합동방정식의 해는 법 276에서 유일하게 존재한다. 그리고 $17x \equiv 9 \pmod{276}$ 가 성립할 필요충분조건은

$$\begin{aligned} 17x &\equiv 9 \pmod{3} \\ 17x &\equiv 9 \pmod{4} \\ 17x &\equiv 9 \pmod{23} \end{aligned} \tag{25}$$

가 동시에 성립하는 것이고 (25)에 있는 3개의 일차합동방정식을 풀면 다음을 얻는다.

$$\begin{aligned} x &\equiv 0 \pmod{3} \\ x &\equiv 1 \pmod{4} \\ x &\equiv 10 \pmod{23} \end{aligned} \tag{26}$$

이때 (26)을 이용해서 일차합동방정식 $17x \equiv 9 \pmod{276}$ 의 유일한 해를 구하는 방법이 존재할까? 존재한다면 그 방법은 무엇일까?

Q2) 물건이 몇 개 있는지 알수 없다. 다만 3개씩 세면 2개가 남고 5개씩 세면 3개가 남고 7개씩 세면 2개가 남는다고 한다. 물건은 총 몇 개 있을까?

중국인의 나머지 정리는 Q1), Q2)를 해결할수 있는 하나의 방법입니다.

실제로 Q2)는 기원후 3~4세기 중국의 고전 수학서 산경십서(算經十書)중 하나인 손자산경(孫子算經)에 나온 문제입니다. 이 문제와 해법을 서양의 수학자들도 관심을 갖게 되었고 문제의 해법이 다음과 같이 정립되었습니다.

Theorem 2.3.2 중국인의 나머지 정리(Chinese Remainder Theorem)

n개의 자연수 $m_1, m_2, \ldots, m_n$ 가 $i \neq j$ 일 때 $\gcd(m_i, m_j)=1$ 을 만족한다고 하자. 그러면 n개의 정수 $a_1, a_2, \ldots, a_n$ 가 임의로 주어져있을 때

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned} \tag{27}$$

를 동시에 만족하는 정수 x는 법 $m_1 m_2 \cdots m_n$ 에서 유일하게 존재한다.

(증명)

먼저 존재성을 증명하자. 각각의 $k = 1,2,\ldots,n$ 에 대하여 M_k를 다음과 같이 정의하자.

$$\begin{aligned} M_1 &= m_2 m_3 \cdots m_n \\ M_2 &= m_1 m_3 \cdots m_n \\ &\vdots \\ M_n &= m_1 m_2 \cdots m_{n-1} \end{aligned}$$

즉, M_k는 $m_1 m_2 \cdots m_n$ 에서 m_k를 제외한 나머지를 모두 곱한 자연수이다.

그러면 $i \neq j$ 일 때 $\gcd(m_i, m_j)=1$ 이므로 $\gcd(m_k, M_k)=1$ 을 만족한다.

따라서 M_k는 법 m_k에서 곱셈에 대한 역원이 존재한다. 그 역원을 x_k라고 하고
이때 정수 x를 $x = a_1M_1x_1 + a_2M_2x_2 + \cdots + a_nM_nx_n$ 라고 정의하자. (28)

그러면 M_k의 정의에 의해 $s \neq k$ 일땐 $M_sx_s \equiv 0 \pmod{m_k}$ 를 만족하고
$s = k$ 일땐 x_k가 법 m_k에서 M_k의 곱셈에 대한 역원이므로 $M_kx_k \equiv 1 \pmod{m_k}$
를 만족한다. 따라서 (28)에서 정의한 정수 x는 (27)을 만족한다는 것을 쉽게 알수 있다.

해의 존재성이 증명되었다. 이제 유일성을 증명하자. a, b가 (27)을 만족하는 해라고 하면
다음을 만족한다.

$$\begin{aligned} a &\equiv b \pmod{m_1} \\ a &\equiv b \pmod{m_2} \\ &\vdots \\ a &\equiv b \pmod{m_n} \end{aligned}$$

그리고 $i \neq j$ 일 때 $\gcd(m_i, m_j) = 1$ 이므로 다음을 얻을수 있다.

$$a \equiv b \pmod{m_1m_2 \cdots m_n}$$

따라서 (27)을 만족하는 해는 법 $m_1m_2 \cdots m_n$ 에서 유일하다. ■

중국인의 나머지 정리는 증명과정도 같이 기억하는게 좋습니다. 증명과정에서 (27)을
만족하는 해를 구하는 방법을 알려주기 때문입니다.

이제 중국인의 나머지 정리를 사용해서 Q1), Q2)를 풀어보겠습니다. 먼저 Q1)에서
(26)을 만족하는 해를 구하겠습니다. 이 경우 $m_1 = 3, m_2 = 4, m_3 = 23$ 이므로

$$\begin{aligned} M_1 &= 4 \times 23 = 92 \\ M_2 &= 3 \times 23 = 69 \\ M_3 &= 3 \times 4 = 12 \end{aligned}$$

이고 법 m_1, m_2, m_3 에서 M_1, M_2, M_3 의 곱셈에 대한 역원을 하나만 구하면

$$\begin{aligned} M_1x_1 \equiv 2x_1 \equiv 1 \pmod{3} &\Rightarrow x_1 = 2 \\ M_2x_2 \equiv x_2 \equiv 1 \pmod{4} &\Rightarrow x_2 = 1 \\ M_3x_3 \equiv 12x_3 \equiv 1 \pmod{23} &\Rightarrow x_3 = 2 \end{aligned}$$

입니다. 따라서 $x = M_2x_2 + 10M_3x_3 = 309$ 가 $17x \equiv 9 \pmod{276}$ 을 만족하는
하나의 해가 되고 $309 \equiv 33 \pmod{276}$ 이므로 $x = 33$ 이 $\mathbb{Z}_{276}$에 있는 해가 됩니다.

Q2)는 결국 다음을 만족하는 정수 x를 구하는 문제입니다.

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 2 \pmod{7} \end{aligned}$$

$m_1 = 3, m_2 = 5, m_3 = 7$ 이므로 $M_1 = 35,\ M_2 = 21,\ M_3 = 15$ 이고
곱셈에 대한 역원을 하나만 구하면 $x_1 = 2, x_2 = 1, x_3 = 1$ 입니다.
따라서 하나의 해는 다음과 같습니다.

$$x = 2M_1x_1 + 3M_2x_2 + 2M_3x_3 = 233$$

그리고 $233 \equiv 23 \pmod{105}$ 이므로 $\mathbb{Z}_{105}$에 있는 해는 $x = 23$ 입니다. 그러므로 물건의 개수로 가능한 자연수는 $23, 128, 233, 338, \ldots$ 인데 고대 중국에서는 이 문제의 답을 23으로 기록했다고 합니다.

학부 수준의 대수학을 공부할 때 중국인의 나머지 정리를 다시 볼 기회가 있을겁니다. 그리고 중국인의 나머지 정리를 알면 이해할 때 도움이 되는 대수학적인 어떤 성질도 있으므로 수학을 계속 공부할거라면 알고있는게 공부할 때 도움이 됩니다.

Problem 2.3.2 $n \geq 2$ 인 자연수 n에 대하여 다음 조건을 만족하는 n개의 정수 $a_1, a_2, \ldots, a_n$ 가 존재함을 증명하시오.

(a). 각각의 $i = 1, 2, \ldots, n-1$ 에 대하여 $a_{i+1} - a_i = 1$ 이다.

(b). 각각의 $i = 1, 2, \ldots, n$ 에 대하여 $b_i^2 \mid a_i$ 를 만족하는 2 이상의 자연수 b_i가 존재한다.

(증명)

n개의 서로 다른 소수 $p_1, p_2, \ldots, p_n$ 를 임의로 택하자. 그러면 $i \neq j$ 일 때 $\gcd\left(p_i^2, p_j^2\right) = 1$ 임은 명백하다. 그러므로 중국인의 나머지 정리에 의하면 다음을 만족하는 x는 법 $p_1^2 p_2^2 \cdots p_n^2$ 에서 유일하다.

$$\begin{aligned} x &\equiv 0 \pmod{p_1^2} \\ x &\equiv -1 \pmod{p_2^2} \\ &\vdots \\ x &\equiv -(n-1) \pmod{p_n^2} \end{aligned} \tag{29}$$

(29)를 만족하는 법 $p_1^2 p_2^2 \cdots p_n^2$ 에서 유일한 정수를 a라고 하고 각각의 $i = 1, 2, \ldots, n$ 에 대하여 $a_i = a + (i-1)$ 라고 정의하자. 그러면 $a_1, a_2, \ldots, a_n$ 이 조건 (a)를 만족함은 명백하고 a가 (29)를 만족하므로 $a_i \equiv a + (i-1) \equiv 0 \pmod{p_i^2}$ 이다.

따라서 $a_1, a_2, \ldots, a_n$ 는 (b)도 만족한다. 그러므로 조건을 만족하는 n개의 정수는 항상 존재한다. ■

Problem 2.3.3 자연수 m, n에 대하여 $d = \gcd(m, n)$, $s = \operatorname{lcm}(m, n)$ 라고 하자. 그러면 정수 a, b에 대하여 (30)을 만족하는 해가 존재할 필요충분조건은 $a \equiv b \pmod{d}$ 임을 증명하고 그 해는 법 s에서 유일함을 증명하시오.

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned} \tag{30}$$

(증명)

$(\Longrightarrow)$ $d \mid m$, $d \mid n$ 이므로 (30)의 해가 존재하면 다음을 얻는다.

$$\begin{aligned} x &\equiv a \pmod{d} \\ x &\equiv b \pmod{d} \end{aligned}$$

따라서 $a \equiv x \equiv b \pmod{d}$ 이므로 $a \equiv b \pmod{d}$ 이다.

$(\Leftarrow)$ 합동의 정의에 의하면 $a+mk_1=b+nk_2$ 를 만족하는 정수 k_1,k_2의 존재성을 증명하면 충분하다. 조건에 의하면 적당한 정수 k_3이 존재해서 $a-b=dk_3$ 을 만족하고 $d=\gcd(m,n)$ 이므로 $nk_2-mk_1=dk_3$ 을 만족하는 정수 k_1,k_2는 존재한다.

따라서 $a+mk_1=b+nk_2$ 를 만족하므로 $x=a+mk_1=b+nk_2$ 라고 하면 이것은 (30)을 만족하는 해가 된다.

해가 존재할 필요충분조건이 증명되었다. 이제 (30)을 만족하는 해가 존재할 경우 법 s에서 유일함을 보이자. $(\Leftarrow)$ 증명과정에서 $np-mq=dk_3$ 을 만족하는 정수 p,q가 $p=k_2, q=k_1$ 으로 존재하므로 $np-mq=dk_3$ 의 일반해는 다음과 같다.

$$p=k_2+\left(\frac{m}{d}\right)t,\ q=k_1+\left(\frac{n}{d}\right)t\ (t\in\mathbb{Z})$$

그러므로 (30)을 만족하는 x는 모든 정수 t에 대하여 다음과 같은 형태를 갖는다.

$$x=a+mk_1+\left(\frac{mn}{d}\right)t=b+nk_2+\left(\frac{mn}{d}\right)t$$

그리고 $\frac{mn}{d}=s$ 이므로 (30)을 만족하는 하나의 해 $y=a+mk_1=b+nk_2$ 에 대하여 $x\equiv y\pmod{s}$ 가 성립한다. 즉, 법 s에서 (30)을 만족하는 해는 유일하다. ■

Problem 2.3.4 다음 합동방정식의 해가 존재하면 해를 하나만 구하시오.
(a). $x\equiv 4\pmod{6},\ x\equiv 7\pmod{15}$
(b). $x\equiv 9\pmod{10},\ x\equiv 4\pmod{15}$

(풀이)
(a). $\gcd(6,15)=3$ 이고 $4\equiv 7\pmod{3}$ 이므로 Problem 2.3.3에 의하면 주어진 합동방정식의 해가 존재한다. 그리고 해를 구하기 위해 $4+6a=7+15b$ 를 만족하는 정수 a,b를 구하면 충분하다.

$6a-15b=3$ 을 만족하는 정수 a,b는 $a=3,b=1$ 가 있고 따라서 주어진 합동방정식을 만족하는 하나의 해는 $x=4+6a=7+15b=22$ 이다. ■

(b). $\gcd(10,15)=3$ 이고 $9\not\equiv 4\pmod{3}$ 이므로 Problem 2.3.3에 의하면 주어진 합동방정식의 해가 존재하지 않는다. ■

Problem 2.3.5 다음 합동방정식을 만족하는 정수를 $\mathbb{Z}_{210}$에서 모두 구하시오.

$$\begin{aligned} 2x&\equiv 3\pmod{5}\\ 4x&\equiv 2\pmod{6}\\ 3x&\equiv 2\pmod{7}\end{aligned} \tag{31}$$

(풀이)

$2\times 3\equiv 1\,(\mathrm{mod}\,5),\ 3\times 5\equiv 1\,(\mathrm{mod}\,7)$ 이므로 다음을 얻는다.

$$2x\equiv 3\,(\mathrm{mod}\,5)\Rightarrow x\equiv 4\,(\mathrm{mod}\,5)$$
$$3x\equiv 2\,(\mathrm{mod}\,7)\Rightarrow x\equiv 3\,(\mathrm{mod}\,7)$$

그리고 $4x\equiv 2\,(\mathrm{mod}\,6)$ 의 해는 직접 대입해보면 $x\equiv 2\,(\mathrm{mod}\,6)$ 또는 $x\equiv 5\,(\mathrm{mod}\,6)$ 임을 쉽게 알수 있다. 따라서 (31)의 해는 다음 2개의 합동방정식에서 모두 얻을수 있다.

$$\begin{aligned} x&\equiv 4\,(\mathrm{mod}\,5)\\ x&\equiv 2\,(\mathrm{mod}\,6)\\ x&\equiv 3\,(\mathrm{mod}\,7)\end{aligned}\tag{32}$$

$$\begin{aligned} x&\equiv 4\,(\mathrm{mod}\,5)\\ x&\equiv 5\,(\mathrm{mod}\,6)\\ x&\equiv 3\,(\mathrm{mod}\,7)\end{aligned}\tag{33}$$

먼저 (32)를 풀자. $M_1=42, M_2=35, M_3=30$ 이고

$$M_1x_1\equiv 2x_1\equiv 1\,(\mathrm{mod}\,5)\Rightarrow x_1=3$$
$$M_2x_2\equiv 5x_2\equiv 1\,(\mathrm{mod}\,6)\Rightarrow x_2=5$$
$$M_3x_3\equiv 2x_3\equiv 1\,(\mathrm{mod}\,7)\Rightarrow x_3=4$$

이므로 $x=4M_1x_1+2M_2x_2+3M_3x_3=1214$ 가 하나의 해가 된다.

$1214\equiv 164\,(\mathrm{mod}\,210)$ 이므로 $\mathbb{Z}_{210}$에서 구하면 $x=164$ 이다.

(32)를 푼 과정에 의하면 (33)의 하나의 해는 다음과 같다는 것을 쉽게 알수 있다.

$$x=4M_1x_1+5M_2x_2+3M_3x_3=1739$$

그리고 $1739\equiv 59\,(\mathrm{mod}\,210)$ 이므로 $\mathbb{Z}_{210}$에서 구하면 $x=59$ 이다.

그러므로 주어진 합동방정식의 해를 $\mathbb{Z}_{210}$에서 구하면 $x=59, 164$ 이다. ■

Problem 2.3.6 합동방정식 $x^2\equiv 1\,(\mathrm{mod}\,56)$ 의 해를 $\mathbb{Z}_{56}$에서 모두 구하시오.

(풀이)

$56=2^3\times 7$ 이므로 다음 합동방정식의 해를 구하면 된다.

$$\begin{aligned} x^2&\equiv 1\,(\mathrm{mod}\,7)\\ x^2&\equiv 1\,(\mathrm{mod}\,8)\end{aligned}\tag{34}$$

$x^2\equiv 1\,(\mathrm{mod}\,7)$ 의 해는 $\mathbb{Z}_7$의 원소를 직접 대입해보면 $x\equiv 1\,(\mathrm{mod}\,7)$ 또는 $x\equiv 6\,(\mathrm{mod}\,7)$ 이고 $x^2\equiv 1\,(\mathrm{mod}\,8)$ 의 해는 $\mathbb{Z}_8$의 원소를 직접 대입해보면 $x\equiv 1,3,5,7\,(\mathrm{mod}\,8)$ 임을 쉽게 알수 있다.

따라서 (34)의 첫 번째 합동식에서 나오는 경우가 2가지고 두 번째 합동식에서 나오는 경우가 4가지이므로 전체 경우의 수는 $2\times 4=8$가지이다. 그러므로 다음 8개의 합동방정식을 풀면 해를 구할수 있다.

$$\begin{cases} x \equiv 1 \pmod 7 \\ x \equiv 1 \pmod 8 \end{cases}, \begin{cases} x \equiv 6 \pmod 7 \\ x \equiv 1 \pmod 8 \end{cases}, \begin{cases} x \equiv 1 \pmod 7 \\ x \equiv 3 \pmod 8 \end{cases}$$

$$\begin{cases} x \equiv 6 \pmod 7 \\ x \equiv 3 \pmod 8 \end{cases}, \begin{cases} x \equiv 1 \pmod 7 \\ x \equiv 5 \pmod 8 \end{cases}, \begin{cases} x \equiv 6 \pmod 7 \\ x \equiv 5 \pmod 8 \end{cases} \tag{35}$$

$$\begin{cases} x \equiv 1 \pmod 7 \\ x \equiv 7 \pmod 8 \end{cases}, \begin{cases} x \equiv 6 \pmod 7 \\ x \equiv 7 \pmod 8 \end{cases}$$

(35)에 있는 8개의 합동식을 중국인의 나머지 정리를 사용해서 해를 구하고 그 해를 $\mathbb{Z}_{56}$에서 찾으면 $x = 1, 13, 15, 27, 29, 41, 43, 55$ 이다. ■

Problem 2.3.6에 의하면 다음을 알수 있습니다. $n \geq 2$ 인 자연수 n과 정수계수 다항식 $f(x) \in \mathbb{Z}[x]$가 임의로 주어져있을 때 자연수 n을 소인수분해한 결과가 $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ 이면 합동방정식 $f(x) \equiv 0 \pmod n$ 의 해를 구하기 위해서 각각의 $i = 1,2,...,r$ 에 대하여 합동방정식 $f(x) \equiv 0 \left(\mathrm{mod}\ p_i^{k_i}\right)$ 의 해를 구하면 됩니다.

이것은 합동방정식 $f(x) \equiv 0 \pmod n$ 을 푸는 하나의 방법이고 Problem 2.3.6의 풀이과정을 보면 r개의 합동방정식 $f(x) \equiv 0 \left(\mathrm{mod}\ p_i^{k_i}\right)$ 을 풀 때 새로운 합동방정식이 여러개 나온다는 것을 알수 있습니다.

따라서 새로운 합동방정식의 해는 중국인의 나머지 정리를 이용해서 풀게 되고 이것은 중국인의 나머지 정리가 수학적으로 중요한 이유가 됩니다.

2.4 다항합동방정식의 해법

작성자 : 네냐플(Nenyaffle)

2.4절에서는 p가 소수이고 m이 자연수일 때 정수계수 다항식 $f(x)\in\mathbb{Z}[x]$에 대하여 합동방정식 $f(x)\equiv 0 \pmod{p^m}$ 의 해법을 소개하려고 합니다. 2.3절의 마지막에서 합동방정식 $f(x)\equiv 0 \pmod{n}$ 을 풀기 위해 합동방정식 $f(x)\equiv 0 \pmod{p^m}$ 만 풀면 충분하다는 이야기를 했습니다.

그런데 합동방정식 $f(x)\equiv 0 \pmod{p^m}$ 을 그냥 풀기는 힘듭니다. 합동방정식의 해가 될수 있는 후보는 $\mathbb{Z}_{p^m}$에 모두 있으니 $\mathbb{Z}_{p^m}$의 원소를 다 대입해서 확인하는 방법도 있는데 이것은 숫자가 커지면 하기 힘듭니다.

따라서 다른 방법을 찾아야 합니다. 해가 될수 있는 후보를 줄일수 있으면 좋은데 후보를 줄이는 아이디어는 간단합니다. 정수 a에 대하여 $f(a)\equiv 0 \pmod{p^{m+1}}$ 이면 $p^m \mid p^{m+1}$ 이므로 $f(a)\equiv 0 \pmod{p^m}$ 을 만족한다는 성질을 이용하는겁니다.

즉, $f(x)\equiv 0 \pmod{p^{m+1}}$ 의 해가 될수 있는 후보는 $f(x)\equiv 0 \pmod{p^m}$ 을 만족하는 해에 모두 있습니다. 그래서 $f(x)\equiv 0 \pmod{p^m}$ 의 해를 알고 있을 때 $f(x)\equiv 0 \pmod{p^{m+1}}$ 의 해를 구하는 방향으로 접근하는게 좀 더 편합니다.

여기서 주의할 점은 $f(x)\equiv 0 \pmod{p^{m+1}}$ 의 해는 $f(x)\equiv 0 \pmod{p^m}$ 의 해에서 나와도 합동식에서는 다르게 표현될수 있다는 것입니다.

예를 들어 $f(x)=x^2-x+1$ 이면 $f(3)\equiv 0 \pmod{7}$ 이므로 $x\equiv 3 \pmod{7}$ 을 만족하는 모든 정수 x는 $f(x)\equiv 0 \pmod{7}$ 를 만족합니다.
그리고 $f(31)=931=7^2\times 19$ 이므로 $f(31)\equiv 0 \pmod{7^2}$ 입니다. 따라서 $x\equiv 31 \pmod{7^2}$ 을 만족하는 모든 정수 x는 $f(x)\equiv 0 \pmod{7^2}$ 을 만족합니다.

$x\equiv 3 \pmod{7}$ 과 $x\equiv 31 \pmod{7^2}$ 을 비교해보면 다르게 보입니다.
그런데 $x\equiv 31 \pmod{7^2}$ 이면 $x\equiv 31\equiv 3 \pmod{7}$ 이므로 결국 $f(x)\equiv 0 \pmod{7^2}$ 의 해는 $f(x)\equiv 0 \pmod{7}$ 의 해가 된다는 것을 알수 있습니다.

$f(x)\equiv 0 \pmod{p^m}$ 의 해는 $x\equiv a \pmod{p^m}$ 로 쓰고 $f(x)\equiv 0 \pmod{p^{m+1}}$ 의 해는 $x\equiv b \pmod{p^{m+1}}$ 로 써서 다르게 보이는겁니다.

따라서 $f(x)\equiv 0 \pmod{p^{m+1}}$ 의 해가 $x=a \pmod{p^{n+1}}$ 로 존재한다면 그 해는 적당한 정수 k에 대하여 $x=a+p^m k$ 형태로 나온다고 이해하는게 편합니다.
$3=3+7\times 0$ 이고 $31=3+7\times 4$ 인 것을 생각해보면 쉽습니다.

먼저 다항합동식을 풀기 위해 필요한 정의와 정리를 소개하겠습니다.

Definition 2.4.1 형식적 도함수(Formal Derivative)
정수계수 다항식 $f(x)\in\mathbb{Z}[x]$가 다음과 같다고 할 때

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_2x^2+a_1x+a_0$$

새로운 다항식 $f'(x)$를 다음과 같이 정의하자.

$$f'(x)=na_nx^{n-1}+(n-1)a_{n-1}x^{n-2}+\cdots+2a_2x+a_1$$

이때 $f'(x)$를 $f(x)$의 **형식적 도함수(Formal Derivative)**라고 정의한다.

그리고 음이 아닌 정수 m에 대하여 $f(x)$의 형식적 m계도함수를 기호로는 $f^{(m)}(x)$로 나타내고 다음과 같이 정의한다.

(a). $f^{(0)}(x)=f(x)$ 이다.
(b). m이 음이 아닌 정수이면 $f^{(m+1)}(x)=\left(f^{(m)}(x)\right)'$ 이다.

원래 미분은 해석학에 나오는 극한의 개념이 필요한 정의입니다. 그런데 다항식으로 한정하면 미분을 극한을 생각하지 않고 x^n 이라는 다항식을 nx^{n-1} 이라는 다항식으로 대응시키는 새로운 함수의 개념으로 생각할수 있습니다.

이런 관점에서 다항식을 미분한 것이 형식적 도함수입니다. 즉, 정수계수 다항식 $f(x)\in\mathbb{Z}[x]$가 주어져있을 때 미분을 다항식 $f(x)$를 다항식 $f'(x)$로 대응시키는 새로운 함수로 보는겁니다. 그리고 형식적 도함수는 다항식에서만 정의하는 편입니다.

형식적 m계도함수에서 $m=1,2,3$ 일땐 $f^{(1)}(x),f^{(2)}(x),f^{(3)}(x)$ 보다 $f'(x),f''(x),f'''(x)$ 로 자주 쓰는 편입니다.

형식적 도함수는 다항식에 한정할 경우 해석학에서 정의한 도함수와 동일한 결과가 나오게 정의한 개념이기 때문에 다음이 성립하는 것은 명백합니다. 따라서 증명은 생략하겠습니다.

Theorem 2.4.1 임의의 정수계수 다항식 $f(x),g(x)\in\mathbb{Z}[x]$에 대하여 다음 등식이 성립한다.

(a). $f(x)$가 상수다항식이면 $f'(x)=0$ 이다.
(b). 모든 정수 c에 대하여 $(cf(x))'=cf'(x)$ 이다.
(c). $(f(x)\pm g(x))'=f'(x)\pm g'(x)$ 이다.
(d). $(f(x)g(x))'=f'(x)g(x)+f(x)g'(x)$ 이다.
(e). $(f(g(x)))'=f'(g(x))g'(x)$ 이다.
(f). 모든 자연수 m에 대하여 $\left((f(x))^m\right)'=m(f(x))^{m-1}f'(x)$ 이다.

$f(x),g(x)$가 다항식이고 $g(x)\neq 0$ 일 때 $\dfrac{f(x)}{g(x)}$는 일반적으로 다항식이 아니기 때문에 형식적 도함수에서는 몫의 미분법을 생각하지 않습니다.

이제 다항식에서 성립하는 테일러의 정리를 소개하려고 합니다. 테일러의 정리를 증명하려면 2개의 보조정리가 필요합니다. 그것을 먼저 소개하고 증명하겠습니다.

Lemma 2.4.1 임의의 정수계수 다항식 $f(x),g(x)\in\mathbb{Z}[x]$에 대하여 다음이 성립한다.
(a). a는 정수일 때 모든 음이 아닌 정수 m에 대하여 $f^{(m)}(a)=0$ 이면 $f(x)=0$ 이다.
(b). a는 정수일 때 모든 음이 아닌 정수 m에 대하여 $f^{(m)}(a)=g^{(m)}(a)$ 이면 $f(x)=g(x)$ 이다.

(증명)

(a). 자연수 n에 대하여 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_2x^2+a_1x+a_0$ 라고 하자.
그러면 조건에 의해 $f^{(n)}(a)=n!a_n=0$ 이므로 $a_n=0$ 을 얻는다.

따라서 $f(x)=a_{n-1}x^{n-1}+\cdots+a_2x^2+a_1x+a_0$ 이다. 그리고 조건에 의하면
$f^{(n-1)}(a)=(n-1)!a_{n-1}=0$ 이므로 $a_{n-1}=0$ 을 얻는다.
그러므로 $f(x)=a_{n-2}x^{n-2}+\cdots+a_2x^2+a_1x+a_0$ 이다.

이 과정을 계속 반복하면 $a_0=a_1=a_2=\cdots=a_n=0$ 을 얻을수 있다.
따라서 $f(x)=0$ 이다. ■

(b). $h(x)=f(x)-g(x)$ 라고 하면 $h(x)\in\mathbb{Z}[x]$이고 조건에 의하면
$h^{(m)}(a)=0$ 이다. 따라서 (a)에 의하면 $h(x)=0$ 이므로 $f(x)=g(x)$ 이다. ■

Lemma 2.4.2 정수 a와 정수계수 다항식 $f(x)\in\mathbb{Z}[x]$가 임의로 주어져있다고 하자.
그러면 모든 음이 아닌 정수 m에 대하여 $\dfrac{f^{(m)}(a)}{m!}$ 는 정수이다.

(증명)

자연수 n에 대하여 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_2x^2+a_1x+a_0$ 라고 하자.
$m>n$ 이면 $f^{(m)}(x)=0$ 이므로 $\dfrac{f^{(m)}(a)}{m!}=0$ 을 얻고 이것은 정수이다.
그리고 $f(a)$는 정수이므로 $m=0$ 일때도 명백하다.

따라서 $1\le m\le n$ 인 경우를 가정하자. 그러면 다음을 얻는다.

$$\begin{aligned} f^{(m)}(x)= & \ n(n-1)(n-2)\cdots(n-m+1)a_nx^{n-m} \\ & +(n-1)(n-2)\cdots(n-m)a_{n-1}x^{n-m-1} \\ & +\cdots+(m+2)(m+1)m\cdots4\times3a_{m+2}x^2 \\ & +(m+1)!a_{m+1}x+m!a_m \end{aligned} \tag{36}$$

이제 m개의 연속한 자연수의 곱은 $m!$의 배수임을 보이자. 자연수 b에 대하여 m개의 연속한 자연수를 $b, b+1, b+2, \ldots, b+m-1$ 라고 하면 이항계수의 정의에 의해 다음을 얻는다.

$$\begin{aligned} b(b+1)(b+2)\cdots(b+m-1) &= m! \times \frac{(b+m-1)(b+m-2)\cdots(b+1)b}{m!} \\ &= m! \times \frac{(b+m-1)!}{m!(b-1)!} \\ &= m!\binom{b+m-1}{m} \end{aligned}$$

이항계수는 정수이므로 $b(b+1)(b+2)\cdots(b+m-1)$ 는 $m!$의 배수이다.
그리고 (36)의 계수와 상수항은 모두 m개의 연속한 자연수의 곱으로 이루어져 있다.
따라서 $\dfrac{f^{(m)}(a)}{m!}$ 는 정수이다. ■

Theorem 2.4.2 테일러의 정리(Taylor's Theorem)
정수 a와 정수계수 n차다항식 $f(x) \in \mathbb{Z}[x]$가 임의로 주어져있다고 하자.
그러면 다음 등식이 성립한다.

$$f(x) = f(a) + f'(a)(x-a) + \frac{f''(a)}{2!}(x-a)^2 + \cdots + \frac{f^{(n)}(a)}{n!}(x-a)^n$$

(증명)

$g(x) = f(a) + f'(a)(x-a) + \dfrac{f''(a)}{2!}(x-a)^2 + \cdots + \dfrac{f^{(n)}(a)}{n!}(x-a)^n$ 라고 하면
이항정리와 Lemma 2.4.2에 의해 $g(x) \in \mathbb{Z}[x]$이다. 그리고 $f(x)$의 최고차항의 계수를 a_n이라고 하면 $a_n \neq 0$ 이므로 $f^{(n)}(a) = n!a_n \neq 0$ 이다. 따라서 $f(x), g(x)$는 모두 n차다항식 이므로 $m > n$ 이면 $f^{(m)}(a) = g^{(m)}(a) = 0$ 이다.

그리고 $0 \leq m \leq n$ 일 때 $f^{(m)}(a) = g^{(m)}(a)$ 가 성립한다는 것도 쉽게 알수 있다.
따라서 Lemma 2.4.1에 의하면 $f(x) = g(x)$ 이고 그러므로 다음 등식이 성립한다.

$$f(x) = f(a) + f'(a)(x-a) + \frac{f''(a)}{2!}(x-a)^2 + \cdots + \frac{f^{(n)}(a)}{n!}(x-a)^n$$

■

테일러의 정리를 사용하면 소수 p와 자연수 m에 대하여 $f(x) \equiv 0 \pmod{p^m}$ 의 해를 알고 있을 때 $f(x) \equiv 0 \pmod{p^{m+1}}$ 의 해를 쉽게 구할수 있습니다.

따라서 계속 반복하면 $f(x) \equiv 0 \pmod{p}$ 의 해를 모두 알고 있어야 한다는 결론이 나오는데 아쉽게도 $f(x) \equiv 0 \pmod{p}$ 을 푸는 일반적인 방법은 알려져있지 않습니다.

$f(x) \equiv 0 \pmod{p}$ 의 해법에 대해 현재까지 알려진 경우는 $f(x)$가 $1,2$차 다항식인 경우밖에 없습니다. 일차합동방정식은 이미 소개했으므로 나머지는 나중에 소개하겠습니다.

Theorem 2.4.3 p는 소수이고 m은 자연수, n은 $n \geq 2$ 를 만족하는 자연수이다.
이때 정수 a와 정수계수 n차다항식 $f(x) \in \mathbb{Z}[x]$에 대하여 해가 존재하는 합동방정식 $f(x) \equiv 0 \pmod{p^m}$ 의 하나의 해를 $x \equiv a \pmod{p^m}$ 라고 하자.

그러면 정수 k에 대하여 $x = a + p^m k$ 가 합동방정식 $f(x) \equiv 0 \pmod{p^{m+1}}$ 의 해가 될 필요충분조건은 정수 k가 다음 합동식을 만족하는 것이다.

$$f'(a)k \equiv -\frac{f(a)}{p^m} \pmod{p}$$

(증명)

$x = a + p^m k$ 이면 테일러의 정리에 의해 다음 등식을 얻을수 있다.

$$f(x) = f(a) + f'(a)kp^m + \frac{f''(a)}{2!}k^2p^{2m} + \cdots + \frac{f^{(n)}(a)}{n!}k^n p^{mn} \tag{37}$$

그리고 m은 자연수이므로 $mn \geq 2m \geq m+1$ 이다. 따라서 $p^{2m}, p^{3m}, \ldots, p^{mn}$ 은 모두 p^{m+1}의 배수이다. 그러므로 (37)에서 다음을 얻을수 있다.

$$f(x) \equiv f(a) + f'(a)kp^m \pmod{p^{m+1}} \tag{38}$$

$(\Rightarrow)$ 조건에 의하면 $f(x) \equiv 0 \pmod{p^{m+1}}$ 이므로 (38)에서 다음을 얻는다.

$$f'(a)kp^m \equiv -f(a) \pmod{p^{m+1}} \tag{39}$$

마찬가지로 조건에 의하면 $f(a)$는 p^m의 배수이고 $\gcd(p^m, p^{m+1}) = p^m$ 이므로 (39)의 양변을 p^m으로 나누면 $f'(a)k \equiv -\frac{f(a)}{p^m} \pmod{p}$ 를 얻는다.

$(\Leftarrow)$ $f'(a)k \equiv -\frac{f(a)}{p^m} \pmod{p}$ 이므로 $p \mid f'(a)k + \frac{f(a)}{p^m}$ 이고
따라서 $p^{m+1} \mid f(a) + f'(a)kp^m$ 을 얻는다. 그러므로 (38)에 의하면
$f(x) \equiv 0 \pmod{p^{m+1}}$ 이다. ■

Theorem 2.4.3에서 $f'(a) \equiv 0 \pmod{p}$ 이 될수도 있습니다. 그래서 $0 \times k \equiv 0 \pmod{p}$ 이런 합동방정식이 나올수도 있는데 이 경우에는 모든 정수 k에 대하여 $x = a + p^m k$ 가 $f(x) \equiv 0 \pmod{p^{m+1}}$ 의 해가 되는겁니다.

Theorem 2.4.3을 이용해서 $f(x) = x^2 - x + 1$ 일 때 $f(x) \equiv 0 \pmod{7^2}$ 의 해를 구해보겠습니다. $f(x) \equiv 0 \pmod{7}$ 에 $\mathbb{Z}_7$의 원소를 전부 대입해보면 해는 $x \equiv 3 \pmod{7}$ 또는 $x \equiv 5 \pmod{7}$ 가 나옵니다.

$x \equiv 3 \pmod{7}$ 이므로 $x = 3 + 7k$ 라고 하고 $f(3) = 7, f'(3) = 5$ 이므로 $5k \equiv -1 \pmod{7}$ 이 합동방정식을 풀면 $k \equiv 4 \pmod{7}$ 를 얻습니다.

따라서 $x=3+7k$ 에 대입하면 $...,-18,31,80,129,...$ 를 얻는데 이들중 $\mathbb{Z}_{49}$에 있는 해는 $x=31$ 입니다. 그러므로 $x\equiv 31 \pmod{7^2}$ 이 하나의 해가 됩니다.

이제 다른 해를 구하겠습니다. $x\equiv 5 \pmod 7$ 이므로 $x=5+7k$ 라고 하고 $f(5)=21, f'(5)=9$ 이므로 $9k\equiv -3 \pmod 7$ 즉, $3k\equiv -1 \pmod 7$ 을 풀면 $k\equiv 2 \pmod 7$ 를 얻습니다.

$x=5+7k$ 에 대입하면 $...,-30,19,68,117,...$ 를 얻는데 이들중 $\mathbb{Z}_{49}$에 있는 해는 $x=19$ 입니다. 그러므로 다른 해는 $x\equiv 19 \pmod{7^2}$ 입니다.

정리하면 합동방정식 $f(x)\equiv 0 \pmod{7^2}$ 의 해는 $x\equiv 19,31 \pmod{7^2}$ 입니다.
소수 p에 대하여 $f(x)\equiv 0 \pmod p$ 의 해를 모두 알고 있다면 똑같이 풀면 됩니다.

Problem 2.4.1 다음 합동방정식의 해를 $\mathbb{Z}_n$에서 모두 구하시오.

(a). $2x^3-x-1\equiv 0 \pmod 9$

(b). $x^4+2x+4\equiv 0 \pmod{27}$

(c). $x^2+3x+2\equiv 0 \pmod{36}$

(풀이)

(a). $f(x)=2x^3-x-1$ 라고 하자. 그러면 $f(x)\equiv 0 \pmod 3$ 의 해는 $x\equiv 1 \pmod 3$ 이 유일하다는 것을 쉽게 알수 있다. $x=1+3k$ 라고 하면 $f(1)=0, f'(1)=5$ 이고 $5k\equiv 0 \pmod 3$ 의 해는 $k\equiv 0 \pmod 3$ 이다.

따라서 주어진 합동방정식의 해는 $x\equiv 1 \pmod 9$ 이므로 $\mathbb{Z}_9$에서 구하면 $x=1$ 이다. ■

(b). $f(x)=x^4+2x+4$ 라고 하자. 그러면 $f(x)\equiv 0 \pmod 3$ 의 해는 $x\equiv 2 \pmod 3$ 가 유일하다는 것을 쉽게 알수 있다. $x=2+3k$ 라고 하면 $f(2)=24, f'(2)=34$ 이고 $34k\equiv k\equiv -8 \pmod 3$ 의 해는 $k\equiv 1 \pmod 3$ 이다.

따라서 $f(x)\equiv 0 \pmod 9$ 의 해는 $x\equiv 5 \pmod 9$ 이다. 다시 $x=5+9k$ 라고 하면 $f(5)=639, f'(5)=502$ 이고 $502k\equiv -71 \pmod 3$ 즉, $k\equiv -71 \pmod 3$ 의 해는 $k\equiv 1 \pmod 3$ 이다.

따라서 $f(x)\equiv 0 \pmod{27}$ 의 해는 $x\equiv 14 \pmod{27}$ 이고 $\mathbb{Z}_{27}$에서 구하면 $x=14$ 이다. ■

(c). $36=2^2\times 3^2$ 이므로 $f(x)=x^2+3x+2$ 라고 하고 다음 합동방정식을 풀자.

$$f(x)\equiv 0\ (\mathrm{mod}\ 4)$$
$$f(x)\equiv 0\ (\mathrm{mod}\ 9)$$

case1) $f(x)\equiv 0\ (\mathrm{mod}\ 4)$
$f(x)\equiv 0\ (\mathrm{mod}\ 2)$ 의 해는 $x\equiv 0,1\ (\mathrm{mod}\ 2)$ 임을 쉽게 알수 있다.
그리고 $f(0)=2, f'(0)=3, f(1)=6, f'(1)=5$ 이다.

$x=2k$ 라고 하고 $3k\equiv -1\ (\mathrm{mod}\ 2)$ 을 풀면 $k\equiv 1\ (\mathrm{mod}\ 2)$ 이고
$x=1+2k$ 라고 하고 $5k\equiv -3\ (\mathrm{mod}\ 2)$ 를 풀면 $k\equiv 1\ (\mathrm{mod}\ 2)$ 이다.

따라서 $f(x)\equiv 0\ (\mathrm{mod}\ 4)$ 의 해는 $x\equiv 2,3\ (\mathrm{mod}\ 4)$ 이다.

case2) $f(x)\equiv 0\ (\mathrm{mod}\ 9)$
$f(x)\equiv 0\ (\mathrm{mod}\ 3)$ 의 해는 $x\equiv 1,2\ (\mathrm{mod}\ 3)$ 임을 쉽게 알수 있다.
그리고 $f(1)=6, f'(1)=5, f(2)=12, f'(2)=7$ 이다.

$x=1+3k$ 라고 하고 $5k\equiv -2\ (\mathrm{mod}\ 3)$ 을 풀면 $k\equiv 2\ (\mathrm{mod}\ 3)$ 이고
$x=2+3k$ 라고 하고 $7k\equiv -4\ (\mathrm{mod}\ 3)$ 를 풀면 $k\equiv 2\ (\mathrm{mod}\ 3)$ 이다.

따라서 $f(x)\equiv 0\ (\mathrm{mod}\ 9)$ 의 해는 $x\equiv 7,8\ (\mathrm{mod}\ 9)$ 이다.

case1), case2)에 의하면 다음 4개의 합동방정식을 얻을수 있다.

$$\begin{cases} x\equiv 2\ (\mathrm{mod}\ 4) \\ x\equiv 7\ (\mathrm{mod}\ 9) \end{cases}, \quad \begin{cases} x\equiv 2\ (\mathrm{mod}\ 4) \\ x\equiv 8\ (\mathrm{mod}\ 9) \end{cases}$$

$$\begin{cases} x\equiv 3\ (\mathrm{mod}\ 4) \\ x\equiv 7\ (\mathrm{mod}\ 9) \end{cases}, \quad \begin{cases} x\equiv 3\ (\mathrm{mod}\ 4) \\ x\equiv 8\ (\mathrm{mod}\ 9) \end{cases}$$

각각의 합동방정식을 중국인의 나머지 정리를 사용해서 풀면 $\mathbb{Z}_{36}$에 있는 해는
$x=7,26,34,35$ 임을 알수 있다. ■

Problem 2.4.2 p는 홀수인 소수이고 정수 a는 $p\nmid a$ 를 만족할 때 합동방정식
$x^2\equiv a\ (\mathrm{mod}\ p)$의 해가 존재한다고 하자. 그러면 모든 자연수 n에 대하여 합동방정식
$x^2\equiv a\ (\mathrm{mod}\ p^n)$은 법 p^n에서 해가 2개만 존재한다는 것을 증명하시오.

(증명)
자연수 n에 대하여 수학적 귀납법을 사용하자. $n=1$ 이면 조건에 의해
$x^2\equiv a\ (\mathrm{mod}\ p)$의 해가 존재하고 $p\nmid a$ 이므로 p의 배수는 해가 될수 없다.

$x^2\equiv y^2\ (\mathrm{mod}\ p)$ 라고 하면 $(x+y)(x-y)\equiv 0\ (\mathrm{mod}\ p)$ 에서 p가 소수이므로
$x\equiv -y\ (\mathrm{mod}\ p)$ 또는 $x\equiv y\ (\mathrm{mod}\ p)$ 이다. (40)

$x^2 \equiv a \pmod{p}$의 하나의 해를 k라고 하면 $p \nmid k$ 이다. 그리고 $-k$도 $x^2 \equiv a \pmod{p}$의 해가 된다는 것은 명백한데 $p \nmid k$ 이고 p는 홀수인 소수이므로 $-k \not\equiv k \pmod{p}$ 이다.

따라서 (40)에 의하면 $x^2 \equiv a \pmod{p}$의 해는 $x \equiv -k, k \pmod{p}$ 로 법 p에서 2개만 존재한다. 그러므로 $n = 1$ 이면 참이다.

이제 임의의 자연수 n에 대하여 문제에 주어진 명제가 참이라고 가정하자.
$f(x) = x^2 - a$ 라고 하면 조건에 의해 적당한 정수 k가 존재해서 $f(k) \equiv 0 \pmod{p^n}$을 만족하고 이때 $f(-k) \equiv 0 \pmod{p^n}$임은 명백하다.

조건에 의하면 법 p^n에서 서로 다른 2개의 해를 가지므로 $-k \not\equiv k \pmod{p^n}$ 이다.
이제 Theorem 2.4.3을 이용해서 $x^2 \equiv a \pmod{p^{n+1}}$의 해를 구하자.

$x = k + p^n m$ 라고 하자. p는 홀수인 소수이므로 $\gcd(2, p) = 1$ 이고 $f'(k) = 2k$ 인데 $2km \equiv -\dfrac{f(k)}{p^n} \pmod{p}$ 를 만족하는 m은 법 p에서 유일하게 존재한다. 그 해를 $m \equiv r \pmod{p}$ 라고 하면 $x \equiv k + p^n r \pmod{p^{n+1}}$ 가 $x^2 \equiv a \pmod{p^{n+1}}$의 해가 된다.

마찬가지로 $x = -k + p^n m$ 라고 하자. p는 홀수인 소수이므로 $\gcd(2, p) = 1$ 이고 $f'(-k) = -2k$ 인데 $-2km \equiv -\dfrac{f(-k)}{p^n} \pmod{p}$ 를 만족하는 m은 법 p에서 유일하게 존재한다. 그 해를 $m \equiv s \pmod{p}$ 라고 하면 $x \equiv -k + p^n s \pmod{p^{n+1}}$ 가 $x^2 \equiv a \pmod{p^{n+1}}$의 해가 된다.

정리하면 $x^2 \equiv a \pmod{p^{n+1}}$ 의 해는 $x \equiv k + p^n r \pmod{p^{n+1}}$ 와 $x \equiv -k + p^n s \pmod{p^{n+1}}$ 이다. 마지막으로 $-k + p^n s \not\equiv k + p^n r \pmod{p^{n+1}}$ 임을 보이면 충분하다.

결론을 부정해서 $-k + p^n s \equiv k + p^n r \pmod{p^{n+1}}$ 라고 가정하자.
그러면 $2k \equiv p^n(s - r) \pmod{p^{n+1}}$ 이고 s, r은 각각 다음을 만족하는 정수이다.

$$2kr \equiv -\frac{f(k)}{p^n} \pmod{p}$$

$$2ks \equiv \frac{f(-k)}{p^n} \pmod{p}$$

따라서 각각의 양변에 p^n을 곱하면 $f(-k) = f(k)$ 이므로 다음을 얻을수 있다.

$$2krp^n \equiv -f(k) \pmod{p^{n+1}}$$
$$2ksp^n \equiv f(k) \pmod{p^{n+1}}$$

그러므로 $2kp^n(s-r) \equiv 2f(k) \pmod{p^{n+1}}$ 인데 $2k \equiv p^n(s-r) \pmod{p^{n+1}}$
이므로 $4k^2 \equiv 2f(k) \pmod{p^{n+1}}$ 이고 $\gcd(2,p)=1$ 이므로 다음을 얻는다.

$$2k^2 \equiv f(k) \equiv k^2 - a \pmod{p^{n+1}}$$

따라서 $k^2 \equiv -a \pmod{p^{n+1}}$ 이고 $p^n \mid p^{n+1}$ 이므로 $k^2 \equiv -a \pmod{p^n}$ 이다.
그리고 가정에 의하면 $k^2 \equiv a \pmod{p^n}$ 이므로 $2a \equiv 0 \pmod{p^n}$ 을 얻고
마찬가지로 $\gcd(2,p)=1$ 이므로 $a \equiv 0 \pmod{p^n}$ 이다.

$p \mid p^n$ 이므로 $a \equiv 0 \pmod{p}$ 를 얻을수 있는데 이것은 $p \nmid a$ 라는 조건에 모순이다.
그러므로 $-k+p^n s \not\equiv k+p^n r \pmod{p^{n+1}}$ 가 되어야 한다.
따라서 $x^2 \equiv a \pmod{p^{n+1}}$도 법 p^{n+1}에서 해가 2개만 존재한다.

정리하면 수학적 귀납법에 의해 모든 자연수 n에 대하여 합동방정식 $x^2 \equiv a \pmod{p^n}$은
법 p^n에서 해를 2개만 갖는다. ■

2.5 다항식의 합동

작성자 : 네냐플(Nenyaffle)

2.5절에서는 다항식의 합동에 대해 이야기하려고 합니다. 지금까지는 두 정수의 합동만 이야기했는데 두 다항식의 합동도 정의할수 있습니다.

Definition 2.5.1 n은 자연수이고 정수계수 다항식 $f(x)\in\mathbb{Z}[x]$가 다음과 같이 주어져있다고 하자.

$$f(x)=a_0+a_1x+\cdots+a_mx^m$$

그러면 집합 $S=\{k\in\{0,1,...,m\}:a_k\not\equiv 0\pmod n\}$ 가 공집합이 아닐 때 집합 S 의 가장 큰 원소를 법 n에서 $f(x)$의 차수라고 정의하고 기호로는 $\deg_n(f(x))$ 또는 $\deg_n(f)$로 나타낸다.

예를 들어 $f(x)=35x^4+7x^2+2x+1$ 이면 $n=2$ 일땐 $35\not\equiv 0\pmod 2$ 이므로 $\deg_2(f(x))=4$ 이고 $n=5$ 일땐 $35\equiv 0\pmod 5$, $7\not\equiv 0\pmod 5$ 이므로 $\deg_5(f(x))=2$ 입니다. 같은 이유로 $n=7$ 일땐 $\deg_7(f(x))=1$ 입니다.

물론 $\deg_n(f(x))=0$ 이 될수도 있습니다. $n=2$ 일 때 $f(x)=1$ 이라고 하면 $\deg_2(f(x))=0$ 입니다.

$f(x)=35x^4+7x^2+2x+1$ 이면 대학 입학 전에는 $\deg(f(x))=4$ 라고 했는데 합동식에서는 자연수 n에 따라서 다항식의 차수가 달라질수도 있습니다.

그리고 Definition 2.5.1을 보면 집합 S 가 공집합이 아닌 것을 가정하고 있는데 $S=\varnothing$ 이 될수도 있습니다. n이 자연수일 때 $f(x)=0$ 이면 $S=\varnothing$ 임은 명백하고 $f(x)=n(x^2-3x+4)$ 일때도 $S=\varnothing$ 임은 명백합니다.

대수학에서는 이런 경우 차수를 $-\infty$으로 정의하는 편인데 이 책에서는 이런 경우를 고려하지 않겠습니다. 즉, 법 n에서의 차수를 이 책에서 이야기할땐 Definition 2.5.1에서 정의된 집합 S 가 공집합이 아니라고 가정하겠습니다.

Definition 2.5.2 n은 자연수이고 정수계수 다항식 $f(x),g(x)\in\mathbb{Z}[x]$가 다음과 같이 주어져있다고 하자.

$$f(x)=a_0+a_1x+a_2x^2+\cdots$$
$$g(x)=b_0+b_1x+b_2x^2+\cdots$$

그러면 모든 음이 아닌 정수 i에 대하여 $a_i\equiv b_i\pmod n$ 를 만족하면 두 다항식 $f(x),g(x)$는 법 n에 대하여 합동이라고 정의하고 기호로는 $f(x)\equiv {}_x g(x)\pmod n$ 로 나타낸다. 두 다항식 $f(x),g(x)$가 법 n에 대하여 합동이 아니면 기호로는 $f(x)\not\equiv {}_x g(x)\pmod n$로 나타낸다.

Definition 2.5.2에서 다항식을 끝까지 안쓴 이유는 다음과 같습니다. 다항식은 차수가 달라도 합동이 될수 있어서 말로 하는게 편하기 때문입니다. 예를 들면 다음과 같습니다.

$$x^3+x^2+x+1 \equiv_x 4x^5+8x^4+x^3+x^2+x+1 \pmod 4$$

대학 입학 전에 차수가 다르다고 배운 다항식도 법 4에 대하여 합동이 됩니다. 그래서 두 다항식의 합동을 정의할 때 모든 것을 수식으로 쓰는게 쉽지 않습니다.

합동의 정의에 의하면 두 정수계수 다항식 $f(x), g(x)$가 합동인 것과 적당한 정수계수 다항식 $h(x)$가 존재해서 $f(x)-g(x)=nh(x)$ 를 만족하는 것은 동치임을 쉽게 알수 있습니다.

그리고 n이 자연수일 때 임의의 정수계수 다항식 $f(x)$에 대하여 적당한 다항식 $g(x)\in\mathbb{Z}_n[x]$가 존재해서 $f(x)\equiv_x g(x) \pmod n$ 을 만족하는것도 명백합니다.

직관에 의하면 Theorem 2.1.2와 유사한 합동식의 기본성질은 다항식의 합동에서도 똑같이 성립한다는 것을 쉽게 알수 있습니다. 그리고 합동은 등호와 유사하다는 것을 생각해보면 다음이 성립하는것도 명백합니다.

Theorem 2.5.1 자연수 n과 정수계수 다항식 $f(x), g(x)\in\mathbb{Z}[x]$가 임의로 주어져있을 때 $f(x)\equiv_x g(x) \pmod n$ 이면 다음이 성립한다.

(a). $\deg_n(f(x))=\deg_n(g(x))$ 이다.

(b). 모든 정수 a에 대하여 $f(a)\equiv g(a) \pmod n$ 이다.

(c). $f'(x)\equiv_x g'(x) \pmod n$ 이다.

(증명)

(a). 두 다항식 $f(x), g(x)$의 m차항 계수를 각각 a_m, b_m이라고 하자.

이때 a_0, b_0는 두 다항식 $f(x), g(x)$의 상수항이다.

$\deg_n(f(x))=k$ 라고 하자. 그러면 $a_k \not\equiv 0 \pmod n$ 을 만족하고 $i>k$ 이면 $a_i \equiv 0 \pmod n$ 을 만족한다. 그리고 $f(x)\equiv_x g(x) \pmod n$ 이므로 합동의 정의에 의하면 $b_k \equiv a_k \not\equiv 0 \pmod n$ 과 $i>k$ 일 때 $b_i \equiv a_i \equiv 0 \pmod n$ 을 만족한다는 것은 명백하다.

차수의 정의에 의하면 $\deg_n(g(x))=k$ 이므로 $\deg_n(f(x))=\deg_n(g(x))$ 이다. ■

(b). 조건에 의하면 적당한 정수계수 다항식 $h(x)$가 존재해서 $f(x)-g(x)=nh(x)$ 를 만족한다. 따라서 $f(a)-g(a)=nh(a)$ 이므로 $f(a)\equiv g(a) \pmod n$ 을 얻는다. ■

(c). 조건에 의하면 적당한 정수계수 다항식 $h(x)$가 존재해서 $f(x)-g(x)=nh(x)$ 를 만족한다. 따라서 $f'(x)-g'(x)=nh'(x)$ 이고 $h'(x)\in\mathbb{Z}[x]$ 이므로 $f'(x)\equiv_x g'(x) \pmod n$ 을 얻는다. ■

Theorem 2.5.1의 역은 성립하지 않습니다. $n=6$ 일 때 정수계수 다항식 $f(x), g(x)$가 다음과 같이 주어져있으면

$$\begin{aligned} f(x) &= x^4 + 2x^2 \\ g(x) &= 4x^4 + 5x^2 \end{aligned} \tag{41}$$

$\deg_6(f(x)) = \deg_6(g(x)) = 4$ 임은 명백하고

$$\begin{aligned} f'(x) &= 4x^3 + 4x \\ g'(x) &= 16x^3 + 10x \end{aligned}$$

에서 $4 \equiv 16 \pmod 6, 4 \equiv 10 \pmod 6$ 이므로 $f'(x) \equiv_x g'(x) \pmod 6$ 을 만족합니다. 그리고 $a = 0,1,2,3,4,5$ 는 다음 합동식을 만족합니다.

$$a^4 + 2a^2 \equiv 4a^4 + 5a^2 \pmod 6$$

따라서 모든 정수 a에 대하여 $f(a) \equiv g(a) \pmod 6$ 를 만족합니다.

그런데 $1 \not\equiv 4 \pmod 6$ 이므로 $f(x) \not\equiv_x g(x) \pmod 6$ 입니다.
그러므로 (41)은 Theorem 2.5.1의 역이 성립하지 않는 반례가 됩니다.

(41)은 Theorem 2.5.1의 역에 다음 조건을 추가했을때도 반례가 됩니다.

모든 자연수 m에 대하여 $f^{(m)}(x) \equiv_x g^{(m)}(x) \pmod n$ 이다. (42)

(41)의 다항식은 $f'(x) \equiv_x g'(x) \pmod 6$ 을 만족하므로 Theorem 2.5.1에 의하면 (42)가 성립한다는 것을 쉽게 알수 있습니다. 그리고 $f(x) \not\equiv_x g(x) \pmod 6$ 입니다.

대학 입학 전에 사용한 등호에서는 조건 (b)와 비슷하게 모든 정수 a에 대하여 $f(a) = g(a)$ 가 성립하면 대수학의 기본정리에 의해 $f(x) = g(x)$ 를 유도할수 있는데 합동식에서는 조건 (b) 이외에 (a),(c)를 추가해도 두 다항식이 합동이 아닐수 있습니다.

해석학에 나오는 평균값정리에 의하면 조건 (b),(c)와 비슷하게 $f'(x) = g'(x)$ 이고 적당한 정수 a가 존재해서 $f(a) = g(a)$ 라는 조건이 있을 때 $f(x) = g(x)$ 가 성립합니다.

그래서 (a),(b),(c)가 모두 성립해도 합동이 아닐수 있다는 것과 대학 입학 전에 알고있던 세계에서 약한 조건만 가지고 두 다항식이 같다는 것을 유도할수 있다는 것은 신기한 일입니다. 이것은 해석학에서 평균값 정리가 중요한 정리인 이유가 되기도 합니다.

Theorem 2.5.1의 역은 다음과 같이 비슷한 형태로 만들 수 있습니다.

Theorem 2.5.2 n은 자연수이고 정수계수 다항식 $f(x), g(x) \in \mathbb{Z}[x]$는 차수가 n과 서로소가 되는 단항식의 합으로만 이루어져있다고 하자. 예를 들어 $n=6$ 이면

$$\begin{aligned} f(x) &= x^{11} - 3x^7 + 2x^5 + 4x \\ g(x) &= 2x^{19} - 5x^5 \end{aligned}$$

는 조건을 만족하는 다항식이다. 그러면 $f'(x) \equiv_x g'(x) \pmod n$ 가 성립하면 $f(x) \equiv_x g(x) \pmod n$ 도 성립한다.

(증명)
$n=1$ 이면 모든 정수가 법 n에 대하여 합동이므로 명백하다. 따라서 $n \geq 2$ 를 가정하자.
그러면 $\gcd(0,n)=n \geq 2$ 이므로 조건에 의하면 두 다항식 $f(x), g(x) \in \mathbb{Z}[x]$의
상수항을 0으로 가정해도 일반성을 잃지 않는다.

다항식 $f(x), g(x)$의 의 k차항 계수를 각각 a_k, b_k 라고 하면 k는 자연수이고
$f'(x) \equiv_x g'(x) \pmod{n}$ 이므로 $ka_k \equiv kb_k \pmod{n}$ 을 만족하는데
$\gcd(k,n)=1$ 이므로 $a_k \equiv b_k \pmod{n}$ 을 얻을수 있다.

따라서 합동의 정의에 의하면 $f(x) \equiv_x g(x) \pmod{n}$ 가 성립한다. ■

Corollary 2.5.1 p가 소수일 때 법 p에서 차수가 $p-1$ 이하이고 상수가 아닌 임의의 정수계수 다항식 $f(x), g(x) \in \mathbb{Z}[x]$에 대하여 $f'(x) \equiv_x g'(x) \pmod{p}$ 이고 $f(0) \equiv g(0) \pmod{p}$ 이면 $f(x) \equiv_x g(x) \pmod{p}$ 이다.

(증명)
법 p에서 차수가 $p-1$ 이하이므로 다항식을 다음과 같이 가정해도 일반성을 잃지 않는다.

$$f(x)=a_{p-1}x^{p-1}+a_{p-2}x^{p-2}+\cdots+a_2x^2+a_1x+a_0$$
$$g(x)=b_{p-1}x^{p-1}+b_{p-2}x^{p-2}+\cdots+b_2x^2+b_1x+b_0$$

이때 다항식 $h(x), k(x) \in \mathbb{Z}[x]$을 다음과 같이 정의하자.

$$h(x)=f(x)-a_0$$
$$k(x)=g(x)-b_0$$

그러면 $h'(x)=f'(x), k'(x)=g'(x)$ 이므로 조건에 의하면
$h'(x) \equiv_x k'(x) \pmod{p}$ 이고 p는 소수이므로 1부터 $p-1$ 까지의 자연수는 모두
p와 서로소이다. 따라서 Theorem 2.5.2에 의하면 $h(x) \equiv_x k(x) \pmod{p}$ 이다.

그러므로 $f(x)-a_0 \equiv_x g(x)-b_0 \pmod{p}$ 이고 양변에 $x=0$ 을 대입하면
조건에 의해 $a_0 \equiv b_0 \pmod{p}$ 를 얻는다. 따라서 $f(x) \equiv_x g(x) \pmod{p}$ 이다. ■

정수계수 다항식 $f(x), g(x)$가 주어져있을 때 대학 입학 전에 배운 내용에 의하면
지수법칙에 의해 $\deg(f(x)g(x))=\deg(f(x))+\deg(g(x))$ 가 성립했습니다.

예를 들어 $f(x)=2x+1,\ g(x)=3x+1$ 이면 $f(x)g(x)=6x^2+5x+1$ 이므로
$\deg(f(x)g(x))=\deg(f(x))+\deg(g(x))$ 가 성립한다는 것은 명백합니다.

그런데 합동식에서는 $\deg_n(f(x)g(x))=\deg_n(f(x))+\deg_n(g(x))$ 가 일반적으로
성립하지 않습니다. $n=6$ 일 때 $f(x)=2x+1,\ g(x)=3x+1$ 이면
$\deg_6(f(x))=\deg_6(g(x))=1$ 인데 $f(x)g(x)=6x^2+5x+1$ 이므로
$\deg_6(f(x)g(x))=1$ 입니다. 따라서 등호가 성립하지 않습니다.

법 n에서는 $\deg_n(f(x)g(x)) \le \deg_n(f(x)) + \deg_n(g(x))$ 이렇게 부등식으로 유도됩니다. 이것의 증명은 간단합니다. (43)

정수계수 다항식 $f(x), g(x)$의 법 n에서 최고차항의 계수를 각각 a_m, b_k라고 하면 $f(x)g(x)$는 법 n에 대하여 다음을 만족합니다.

$$f(x)g(x) \equiv a_m b_k x^{m+k} + \cdots \pmod{n}$$

따라서 $a_m b_k \equiv 0 \pmod{n}$ 이면 $\deg_n(f(x)g(x)) < \deg_n(f(x)) + \deg_n(g(x))$ 이고 $a_m b_k \not\equiv 0 \pmod{n}$ 이면 $\deg_n(f(x)g(x)) = \deg_n(f(x)) + \deg_n(g(x))$ 입니다. 그러므로 $\deg_n(f(x)g(x)) \le \deg_n(f(x)) + \deg_n(g(x))$ 입니다.

p가 소수일 때 정수 a, b에 대하여 $ab \equiv 0 \pmod{p}$ 이면 $a \equiv 0 \pmod{p}$ 또는 $b \equiv 0 \pmod{p}$ 입니다. 즉, $a \not\equiv 0 \pmod{p}$ 이고 $b \not\equiv 0 \pmod{p}$ 이면 $ab \not\equiv 0 \pmod{p}$ 이므로 p가 소수일땐 다음과 같이 등호가 성립합니다.

$$\deg_p(f(x)g(x)) = \deg_p(f(x)) + \deg_p(g(x)) \quad (44)$$

이제 합동식에서 다항식의 인수분해를 소개하겠습니다. 대학 입학 전에는 $x^2 - 3x + 2 = (x-1)(x-2)$ 이렇게 좌변과 우변이 완벽하게 같은 다항식일 때 좌변을 인수분해한 것을 우변이라고 했는데 합동식에서는 형태가 다를수도 있습니다.

예를 들어 $n = 3$ 이면 $(x-1)(x-2) \equiv_x x^2 - 3x + 2 \equiv_x x^2 - 1 \pmod{3}$ 이므로 $x^2 - 1 \equiv_x (x-1)(x-2) \pmod{3}$ 입니다. 좌변과 우변을 비교해보면 대학 입학 전에 알고있던 세계에서는 두 다항식 $x^2 - 1, (x-1)(x-2)$ 은 다릅니다. 그런데 법 3에서는 같은 다항식입니다.

2.5절에서는 법 n에서 다항식을 인수분해하는 것을 소개할겁니다. 물론 인수분해하는 것을 소개한다는 말이 인수분해를 하는 방법을 알려준다는 말은 아닙니다. 일반적으로 다항식을 인수분해하는 것은 어려운 일입니다.

대학 입학 전에 다항식을 인수분해하기 위해서 $f(x) = 0$ 을 만족하는 x를 먼저 찾았을겁니다. 마찬가지로 합동식에서도 인수분해를 하기 위해서 $f(x) \equiv 0 \pmod{n}$ 을 만족하는 x를 먼저 찾아야하는데 x를 찾는 일반적인 방법은 알려져있지 않습니다.

다음 보조정리는 대학 입학 전에 다항식의 나머지정리를 소개할 때 한번쯤 들어봤을겁니다.

Lemma 2.5.1 음이 아닌 정수 m에 대하여 정수계수 다항식 $f(x) \in \mathbb{Z}[x]$가 다음과 같이 주어져있다고 하자.

$$f(x) = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_2 x^2 + a_1 x + a_0 \ (a_m \not\equiv 0)$$

그러면 모든 정수 a에 대하여

$$f(x) = (x-a)q(x) + f(a)$$

를 만족하는 정수계수 다항식 $q(x) \in \mathbb{Z}[x]$가 존재한다. (45)

(증명)
$m=0$ 이면 $q(x)=0$ 으로 택하면 (45)를 만족한다. 따라서 m이 자연수라고 가정하고 집합 S 를 $S=\{m\in\mathbb{N} : f(x)\in\mathbb{Z}[x]$가 (43)를 만족한다.$\}$ 라고 정의하자.

$f(x)=a_1x+a_0$ 이면 $f(a)=a_1a+a_0$ 이므로 다음 등식이 성립한다.

$$\begin{aligned} f(x)-f(a) &= (a_1x+a_0)-(a_1a+a_0) \\ &= a_1(x-a) \end{aligned}$$

따라서 $q(x)=a_1$ 으로 택하면 (45)를 만족한다. 그러므로 $1\in S$ 이다.

이제 모든 자연수 m에 대하여 $1,2,...,m\in S$ 라고 가정하고 정수계수 다항식 $f(x)$가 다음과 같이 주어져있을 때

$$f(x)=a_{m+1}x^{m+1}+a_mx^m+\cdots+a_2x^2+a_1x+a_0\ (a_{m+1}\neq 0)$$

정수계수 다항식 $g(x)$를 다음과 같이 정의하자.

$$\begin{aligned} g(x) &= f(x)-a_{m+1}x^m(x-a) \\ &= (a_m+aa_{m+1})x^m+a_{m-1}x^{m-1}+\cdots+a_0 \end{aligned}$$

그러면 $\deg(g(x))\leq m$ 이므로 가정에 의하면 정수계수 다항식 $q_1(x)\in\mathbb{Z}[x]$가 존재해서 $g(x)=(x-a)q_1(x)+g(a)$ 를 만족하고 $g(x)$의 정의에 의하면 $g(a)=f(a)$ 이므로 다음 등식을 얻는다.

$$\begin{aligned} f(x) &= g(x)+a_{m+1}x^m(x-a) \\ &= (x-a)\left(q_1(x)+a_{m+1}x^m\right)+f(a) \end{aligned}$$

따라서 $q(x)=q_1(x)+a_{m+1}x^m$ 라고 하면 $f(x)=(x-a)q(x)+f(a)$ 이므로 $m+1\in S$ 이다. 그러므로 강한 귀납법에 의하면 $S=\mathbb{N}$ 이다.

정리하면 모든 자연수 m에 대하여 (45)를 만족하고 $m=0$ 일때도 (45)를 만족하므로 모든 음이 아닌 정수 m에 대하여 (45)를 만족한다. ■

Theorem 2.5.3 $n\geq 2$ 인 자연수 n과 정수 a, 법 n에서 상수가 아닌 정수계수 다항식 $f(x)\in\mathbb{Z}[x]$가 임의로 주어져있다고 하자. 그러면 $f(a)\equiv 0\pmod n$ 일 필요충분조건은 정수계수 다항식 $q(x)\in\mathbb{Z}[x]$가 존재해서 다음을 만족하는 것이다.

$$f(x)\equiv_x (x-a)q(x)\pmod n \tag{46}$$

그리고 (46)에서 $\deg_n(q(x))=\deg_n(f(x))-1$ 이다.

(증명)
$(\Rightarrow)$ Lemma 2.5.1에 의하면 다음을 만족하는 정수계수 다항식 $q(x)$가 존재한다.

$$f(x)=(x-a)q(x)+f(a)$$

따라서 $f(a)\equiv 0\pmod n$ 이면 $f(x)\equiv_x (x-a)q(x)\pmod n$ 이다.

$(\Leftarrow)$ 이 경우에는 (46)의 양변에 $x=a$ 를 대입하면 명백하다.

이제 (46)에서 $\deg_n(q(x))=\deg_n(f(x))-1$ 임을 보이자. Theorem 2.5.1에 의하면 $\deg_n(f(x))=\deg_n((x-a)q(x))$ 이고 1은 곱셈에 대한 항등원이므로 (43)을 증명하는 과정을 그대로 따라하면 다음 등식을 얻을수 있다.

$$\deg_n((x-a)q(x))=\deg_n((x-a))+\deg_n(q(x))=1+\deg_n(q(x))$$

따라서 $\deg_n(f(x))=1+\deg_n(q(x))$ 이므로 $\deg_n(q(x))=\deg_n(f(x))-1$ 이다. ■

Theorem 2.5.3에 의하면 합동방정식 $f(x)\equiv 0\pmod n$ 의 해를 모두 알고 있을 경우 법 n에 대하여 합동이 아닌 해를 $x_1,x_2,...,x_m$ 라고 하면 법 n에서 $f(x)$의 최고차항의 계수를 a_k 라고 할 때 다음과 같이 인수분해가 될거라고 오해할수 있습니다.

$$f(x)\equiv a_k(x-x_1)(x-x_2)\cdots(x-x_m)\pmod n$$

하지만 이것은 거짓입니다. 그 반례는 법 8에서의 다항식 x^2-1 이 있는데 합동방정식 $x^2-1\equiv 0\pmod 8$ 의 해는 $\mathbb{Z}_8$에서 찾으면 $x=1,3,5,7$ 입니다.

그런데 $\deg_8(x^2-1)=2$ 이고 $\deg_8((x-1)(x-3)(x-5)(x-7))=4$ 이므로 Theorem 2.5.1에 의하면 $x^2-1\neq_x(x-1)(x-3)(x-5)(x-7)\pmod 8$ 입니다. 따라서 합동식에서는 대학 입학 전에 배운 방식대로 인수분해할수 없는 경우가 발생합니다.

실제로 x^2-1 을 법 8에서 인수분해하면 최고차항의 계수를 1로 고정시켰을 때 다음 두가지 형태로 나옵니다. 즉, 인수분해의 형태가 유일하지 않습니다.

$$x^2-1\equiv_x(x-1)(x-7)\pmod 8$$
$$x^2-1\equiv_x(x-3)(x-5)\pmod 8$$

인수분해의 형태가 유일하지 않다는 말은 $x-1,x-3,x-5,x-7$ 이 다항식은 법 8에서 서로 합동이 아니므로 법 8에 대한 합동식에서 4개 모두 다른 다항식인데 x^2-1 은 $(x-1)(x-7),(x-3)(x-5)$ 이렇게 서로 다른 다항식으로 표현된다는 말입니다.

대학 입학 전에는 다항식의 인수분해가 서로 다른 형태로 나오는것과 차수와 해의 개수가 다를수 있다는 것은 상상하지 못했을겁니다. 합동식에서는 이런 결과가 생각보다 잘 나옵니다. 나중에 대수학에서 환의 분류를 공부할 때 2.5절을 다시 보길 바랍니다.

Theorem 2.5.4 라그랑주의 정리(Lagrange's Theorem)

p는 소수이고 n은 자연수일 때 $\deg_p(f(x))=n$ 을 만족하는 정수계수 다항식 $f(x)\in\mathbb{Z}[x]$가 임의로 주어져있다고 하자. 그러면 합동방정식 $f(x)\equiv 0\pmod p$ 의 법 p에서 서로 다른 해의 개수는 $\min(p,n)$ 이하이다.

여기서 $\min(p,n)=\begin{cases}p & (p\leq n)\\ n & (p\geq n)\end{cases}$ 이다.

(증명)
실수 a,b에 대하여 $x \le \min(a,b)$ 는 $x \le a,\ x \le b$ 가 동시에 성립하는 것과 동치이다. 그리고 합동방정식의 해가 될수 있는 후보는 모두 $\mathbb{Z}_p$에 있으므로 법 p에서 서로 다른 해의 개수가 p개 이하임은 명백하다. 따라서 법 p에서 서로 다른 해의 개수가 n개 이하임을 보이면 충분하다. (47)

집합 S 를 다음과 같이 정의하자.

$$S=\{n\in\mathbb{N} : \deg_p(f(x))=n \text{ 이면 } (46)\text{이 성립한다.}\}$$

$\deg_p(f(x))=1$ 이면 $f(x)=a_1x+a_0\ (a_1 \not\equiv 0 \pmod p)$ 라고 가정해도 충분하다. 그러면 p가 소수이므로 $\gcd(a_1,p)=1$ 이고 따라서 $a_1x \equiv -a_0 \pmod p$ 의 해는 법 p에서 유일하다. 즉, $1\in S$ 이다.

이제 임의의 자연수 n에 대하여 $n\in S$ 라고 가정하고 $\deg_p(f(x))=n+1$ 을 만족하는 정수계수 다항식 $f(x)$를 임의로 택하자.

만약 $f(x)\equiv 0 \pmod p$ 의 해가 존재하지 않으면 $n+1\in S$ 임은 명백하고 법 p에서 하나만 있으면 $1 \le n+1$ 이므로 $n+1\in S$ 임은 명백하다. 따라서 $f(x)\equiv 0 \pmod p$ 의 해가 법 p에서 2개 이상 존재한다고 가정하자.

$f(x)\equiv 0 \pmod p$ 의 하나의 해를 $x=a$ 라고 하면 Theorem 2.5.3에 의해 $f(x)\equiv_x (x-a)q(x) \pmod p$ 과 $\deg_p(q(x))=n$ 을 만족하는 다항식 $q(x)$가 존재한다. 그리고 법 p에서 a와 다른 해를 b라고 하면 $(b-a)q(b)\equiv 0 \pmod p$ 이다.

$b-a \not\equiv 0 \pmod p$ 이고 p는 소수이므로 $q(b)\equiv 0 \pmod p$ 를 얻는다.
즉, $f(x)\equiv 0 \pmod p$ 의 해 중 법 p에서 a와 다른 해는 모두 $q(x)\equiv 0 \pmod p$ 의 해가 된다.

$n\in S$ 이고 $\deg_p(q(x))=n$ 이므로 $q(x)\equiv 0 \pmod p$ 의 해는 법 p에서 n개 이하이다. 따라서 $f(x)\equiv 0 \pmod p$ 의 해는 법 p에서 $n+1$개 이하가 되고 그러므로 (47)을 만족한다. 즉, $n+1\in S$ 이다.

수학적 귀납법에 의하면 $S=\mathbb{N}$ 이다. 따라서 모든 자연수 n에 대하여 (47)이 성립하므로 법 p에서 서로 다른 해의 개수는 n 이하이다. 그리고 그 개수는 p 이하이기도 하므로 결국 법 p에서 서로 다른 해의 개수는 $\min(p,n)$ 이하이다. ■

한편 p가 소수일 때 법 p에서 인수분해를 하면 인수분해한 결과는 합동방정식 $f(x)\equiv 0 \pmod p$ 의 해를 모두 포함합니다. $n=8$ 일 때 $x^2-1\equiv_x (x-1)(x-7) \pmod 8$ 이므로 소수가 아니면 인수분해한 결과가 합동방정식의 해를 모두 포함하지 않을수 있는데 소수이면 모두 다 포함합니다.

Theorem 2.5.5 소수 p와 법 p에서 상수가 아닌 정수계수 다항식 $f(x)\in\mathbb{Z}[x]$가 임의로 주어져있다고 하자. k가 $k\le p$ 를 만족하는 자연수일 때 법 p에서 합동방정식 $f(x)\equiv 0\pmod p$ 의 서로 다른 해가 $x_1,x_2,\ldots,x_k$ 이면 다음을 만족하는 정수계수 다항식 $q(x)\in\mathbb{Z}[x]$가 존재한다.

$$f(x)\equiv_x (x-x_1)(x-x_2)\cdots(x-x_k)q(x)\pmod p \tag{48}$$

그리고 (48)에서 $\deg_p(q(x))=\deg_p(f(x))-k$ 이다.

(증명)

정수계수 다항식 $f(x)$가 $\deg_p(f(x))=n$ 을 만족한다고 하자. 라그랑주의 정리에 의하면 $n\ge k$ 임을 쉽게 알수 있다.

Theorem 2.5.3에 의하면 다음을 만족하는 정수계수 다항식 $q_1(x)$가 존재해서

$$f(x)\equiv_x (x-x_1)q_1(x)\pmod p$$
$$\deg_p(q_1(x))=n-1$$

을 만족한다. 그리고 $x_1\not\equiv x_2\pmod p$ 이고 p가 소수이므로 $q_1(x_2)\equiv 0\pmod p$ 을 얻을수 있고 따라서 Theorem 2.5.3에 의하면 다음을 만족하는 정수계수 다항식 $q_2(x)$가 존재한다.

$$f(x)\equiv_x (x-x_1)(x-x_2)q_2(x)$$
$$\deg_p(q_2(x))=n-2$$

이것을 k번 반복하면 다음을 만족하는 정수계수 다항식 $q(x)$가 존재한다는 결론을 얻는다.

$$f(x)\equiv_x (x-x_1)(x-x_2)\cdots(x-x_k)q(x)\pmod p$$
$$\deg_p(q(x))=n-k=\deg_p(f(x))-k$$

따라서 (48)을 만족하는 정수계수 다항식 $q(x)$가 존재한다. ■

Theorem 2.5.3에서 주의할 점은 $x_1,x_2,\ldots,x_k$ 가 $q(x)\equiv 0\pmod p$ 의 해가 될수도 있다는 것입니다. 정리 내용만 보면 $x_1,x_2,\ldots,x_k$ 가 $q(x)\equiv 0\pmod p$ 의 해가 될수 없다는 것으로 오해할수 있는데 그렇지 않습니다. 다음 합동식도 모순이 없는 합동식입니다.

$$x^3-3x^2+3x-1\equiv_x (x-1)^3\pmod 5$$

한편 p가 소수일 때 페르마의 작은 정리에서 유도되는 모든 정수 a에 대하여 $a^p\equiv a\pmod p$ 가 성립한다는 성질을 이용하면 다항합동방정식의 차수를 언제나 $p-1$ 이하로 만들 수 있습니다.

예를 들어 $p=5$ 이고 $f(x)=x^{35}-x^{10}+x-3$ 일 때 합동방정식 $f(x)\equiv 0\pmod p$ 을 풀려고 합니다. 그런데 $\deg_5(f(x))=35$ 라서 $x=0,1,2,3,4$ 를 대입해서 푸는게 조금 불편합니다.

여기서 $a^p \equiv a \pmod{p}$ 를 이용해서 합동방정식의 차수를 작게 만드는게 가능합니다.
$p=5$ 이므로 모든 정수 a에 대하여 $a^5 \equiv a \pmod{5}$ 이므로 다음을 얻을수 있습니다.

$$a^{35} \equiv (a^5)^7 \equiv a^7 \equiv a^5 a^2 \equiv a^3 \pmod{5}$$
$$a^{10} \equiv (a^5)^2 \equiv a^2 \pmod{5}$$

그러므로 모든 정수 a에 대하여 다음 합동식이 성립합니다.

$$f(a) \equiv a^3 - a^2 + a - 3 \pmod{5}$$

따라서 $g(x)= x^3 - x^2 + x - 3$ 라고 할 때 두 합동방정식 $f(x) \equiv 0 \pmod{p}$ 과 $g(x) \equiv 0 \pmod{p}$ 는 해가 같습니다. 그러므로 $g(x) \equiv 0 \pmod{p}$ 을 풀면 됩니다.

이때 주의할 점은 $f(x) \neq_x g(x) \pmod{5}$ 라는 것입니다. 즉, 차수를 작게 만들 수 있어도 두 다항식이 합동이 되는건 아닙니다.

Problem 2.5.1 다음 합동방정식의 해가 존재하면 $\mathbb{Z}_n$에서 모두 구하시오.

(a). $x^{14} + 12x^2 \equiv 0 \pmod{13}$

(b). $2x^{17} + 3x^2 + 1 \equiv 0 \pmod{5}$

(c). p는 소수이고 n은 자연수, $a \in \mathbb{Z}_p$ 일 때 $x^{p^n} \equiv a \pmod{p}$

(풀이)

(a). 모든 정수 a에 대하여 $a^{13} \equiv a \pmod{13}$ 이므로 $a^{14} \equiv a^2 \pmod{13}$ 이다.
따라서 모든 정수 a에 대하여 $a^{14} + 12a^2 \equiv a^2 + 12a^2 \equiv 0 \pmod{13}$ 이므로
합동방정식의 해를 $\mathbb{Z}_{13}$에서 구하면 $x = 0,1,2,3,4,5,6,7,8,9,10,11,12$ 이다. ■

(b). 모든 정수 a에 대하여 $a^5 \equiv a \pmod{5}$ 이므로
$a^{17} \equiv (a^5)^3 a^2 \equiv a^5 \equiv a \pmod{5}$ 이다. 그러므로 $g(x)= 3x^2 + 2x + 1$ 에 대하여
$g(x) \equiv 0 \pmod{5}$ 을 풀자.

$x = 0,1,2,3,4$ 를 $g(x) \equiv 0 \pmod{5}$ 에 대입해보면 만족하는 것이 없다.
따라서 주어진 합동방정식은 해가 존재하지 않는다. ■

(c). 모든 정수 b에 대하여 $b^p \equiv b \pmod{p}$ 이므로 수학적 귀납법을 이용하면 모든 자연수 n에 대하여 $b^{p^n} \equiv b \pmod{p}$ 임을 보일수 있다. 따라서 주어진 합동방정식의 해는 결국 합동방정식 $x \equiv a \pmod{p}$ 의 해와 같고 $a \in \mathbb{Z}_p$ 이므로 $x = a$ 가 조건을 만족하는 해가 된다. ■

Problem 2.5.2 $f(x)= x^4 - 6x^3 - 3x^2 - 7x + 2$ 일 때 합동방정식
$f(x) \equiv 0 \pmod{13}$ 을 만족하는 모든 해는 $x \equiv -1, 1 \pmod{13}$ 이다.
이때 $f(x) \equiv_x (x-1)(x+1)g(x) \pmod{13}$ 을 만족하는 다항식 $g(x)$를
하나만 구하시오.

(풀이)

우선 $f(1)=-13$ 이고 다음 등식이 성립한다는 것은 쉽게 확인할수 있다.

$$f(x)-f(1)=(x-1)(x^3-5x^2-8x-15)$$

따라서 $f(x)\equiv_x (x-1)(x^3-5x^2-8x-15) \pmod{13}$ 이다.

$q(x)=x^3-5x^2-8x-15$ 라고 하면 $q(-1)=-13$ 이고 이때도 다음 등식이 성립한다는 것은 쉽게 확인할수 있다.

$$q(x)-q(-1)=(x+1)(x^2-6x-2)$$

따라서 $q(x)\equiv_x (x+1)(x^2-6x-2) \pmod{13}$ 이다.

그러므로 $f(x)\equiv_x (x-1)(x+1)(x^2-6x-2) \pmod{13}$ 에서 조건을 만족하는 다항식은 $g(x)=x^2-6x-2$ 이다. ■

사실 13이 소수이므로 Problem 2.5.2에서 조건을 만족하는 다항식 $g(x)$는 법 13에서 x^2-6x-2 가 유일합니다. 나중에 소개할 Theorem 2.5.6을 보면 알수 있습니다.

Problem 2.5.3 p가 소수일 때 다음 합동식이 성립함을 증명하시오.

(a). $x^p-x\equiv_x x(x-1)(x-2)\cdots(x-p+1) \pmod{p}$ 이다.

(b). $x^{p-1}-1\equiv_x (x-1)(x-2)\cdots(x-p+1) \pmod{p}$ 이다.

(c). p가 홀수인 소수이면 다음을 만족한다.

$$1+x+x^2+\cdots+x^{p-2}\equiv_x (x-2)(x-3)\cdots(x-p+1) \pmod{p}$$

(증명)

(a). $f(x)=x^p-x$ 라고 하면 p가 소수이므로 모든 정수 a에 대하여 $f(a)\equiv 0 \pmod{p}$ 이다. 즉, 0부터 $p-1$ 까지의 정수가 모두 $f(x)\equiv 0 \pmod{p}$ 을 만족하므로 Theorem 2.5.5에 의하면 다음을 만족하는 정수계수 다항식 $q(x)$가 존재한다.

$$f(x)\equiv_x x(x-1)(x-2)\cdots(x-p+1)q(x) \pmod{p}$$
$$\deg_p(q(x))=\deg_p(f(x))-p=0$$

따라서 $q(x)$는 상수다항식이고 합동식이 성립하도록 하는 다항식은 $q(x)=1$ 로 택하면 충분하다. 그러므로 주어진 합동식이 성립한다. ■

(b). $f(x)=x^{p-1}-1$ 라고 하면 p가 소수이므로 페르마의 작은 정리에 의하면 $\gcd(a,p)=1$ 인 모든 정수 a에 대하여 $f(a)\equiv 0 \pmod{p}$ 이다. 즉, 1부터 $p-1$ 까지의 자연수가 모두 $f(x)\equiv 0 \pmod{p}$ 을 만족한다. 그러므로 (a)의 풀이과정과 같은 방법으로 주어진 합동식이 성립한다는 것을 쉽게 알수 있다. ■

(c). $a \neq 1$ 이면 $1+a+a^2+\cdots+a^{p-2}=\dfrac{a^{p-1}-1}{a-1}$ 이다. 그리고 $2 \leq a \leq p-1$ 이므로 페르마의 작은 정리에 의해 $a^{p-1}-1 \equiv 0 \pmod{p}$ 가 성립한다.

$\gcd(a-1,p)=1$ 이므로 $a^{p-1}-1 \equiv 0 \pmod{p}$ 의 양변을 $a-1$ 로 나누면 다음을 얻는다.

$$1+a+a^2+\cdots+a^{p-2} \equiv 0 \pmod{p}$$

따라서 (a)의 풀이과정과 같은 방법으로 주어진 합동식이 성립한다는 것을 쉽게 알수 있다. ■

소수 p에 대한 합동식을 Problem 2.5.3을 이용해서 쉽게 증명할수 있는 경우가 있습니다. Problem 2.5.3의 결과에서 양변의 계수를 비교하는겁니다.

Problem 2.5.4 p가 소수일 때 다음을 증명하시오.

(a). $(p-1)! \equiv -1 \pmod{p}$ 이다.

(b). $p \geq 3$ 이면 $1+2+\cdots+(p-1) \equiv 0 \pmod{p}$ 이다.

(c). $p \geq 5$ 이면 다음이 성립한다.

$$1\times 2+1\times 3+\cdots+1\times(p-1)+2\times 3+\cdots+2\times(p-1)$$
$$+3\times 4+\cdots+3\times(p-1)+\cdots+(p-2)(p-1) \equiv 0 \pmod{p}$$

(d). $p \geq 5$ 이면 다음이 성립한다.

$$2\times 3\times\cdots\times(p-1)+1\times 3\times\cdots\times(p-1)+1\times 2\times 4\times\cdots\times(p-1)$$
$$+\cdots+1\times 2\times\cdots\times(p-3)(p-2) \equiv 0 \pmod{p}$$

(증명)

Problem 2.5.3 (b)에 의하면 p가 소수일 때 다음이 성립한다.

$$x^{p-1}-1 \equiv {}_x(x-1)(x-2)\cdots(x-p+1) \pmod{p} \tag{49}$$

(a). $p=2$ 이면 명백하다. 따라서 $p \geq 3$ 일때를 가정하자. 이 경우 $p-1$ 은 짝수이다. (49)의 상수항을 비교하면 좌변은 -1이고 우변은 $(-1)^{p-1}(p-1)!=(p-1)!$ 이므로 $p \geq 3$ 이면 $(p-1)! \equiv -1 \pmod{p}$ 가 성립한다. ■

(b). $p \geq 3$ 이므로 (49)의 우변에서 $p-2$ 차항은 상수항이 아니다. 그리고 $p-2$ 차항의 계수를 구하면 좌변은 0이고 우변은 $1+2+\cdots+(p-1)$ 이다.
그러므로 $1+2+\cdots+(p-1) \equiv 0 \pmod{p}$ 가 성립한다. ■

(c). $p \geq 5$ 이므로 (49)의 우변에서 $p-3$ 차항은 상수항이 아니다. 그리고 $p-3$ 차항의 계수를 구하면 좌변은 0이고 우변은 (c)에 주어진 합동식과 같다. 그러므로 주어진 합동식이 성립한다. ■

(d). $p \geq 5$ 이므로 (49)의 우변에서 일차항은 최고차항이 아니다. 이때 $p-2$ 는 홀수이므로 (49)의 우변에서 일차항의 계수는 (d)에 주어진 식에 -1을 곱한것과 같다. 그리고 좌변에서 일차항의 계수는 0이므로 주어진 합동식은 성립한다. ■

이제 2가지 성질을 소개하고 마치겠습니다.

Theorem 2.5.6 p가 소수일 때 임의의 정수계수 다항식 $f(x),g(x),h(x)\in\mathbb{Z}[x]$에 대하여 다음이 성립한다.
(a). $f(x)g(x)\equiv_x 0\pmod p$ 이면 $f(x)\equiv_x 0\pmod p$ 또는 $g(x)\equiv_x 0\pmod p$ 이다.
(b). $f(x)h(x)\equiv_x g(x)h(x)\pmod p$ 이고 $h(x)\not\equiv_x 0\pmod p$ 이면 $f(x)\equiv_x g(x)\pmod p$ 이다.

(증명)
(a). 결론을 부정해서 $f(x)\not\equiv_x 0\pmod p$, $g(x)\not\equiv_x 0\pmod p$ 이라고 가정하자.
그러면 법 p에서 $f(x),g(x)$의 차수는 잘 정의되고 음이 아닌 정수 m,n에 대하여 각각의 최고차항의 계수를 a_m,b_n 라고 하면 $a_m\not\equiv 0\pmod p$, $b_n\not\equiv 0\pmod p$ 이다.

법 p에서 $f(x)g(x)$의 최고차항의 계수는 a_mb_n 이고 조건에 의하면 $a_mb_n\equiv 0\pmod p$ 이다. 그리고 p는 소수이므로 $a_m\equiv 0\pmod p$ 또는 $b_n\equiv 0\pmod p$ 인데 이것은 모순이다.

따라서 $f(x)\equiv_x 0\pmod p$ 또는 $g(x)\equiv_x 0\pmod p$ 이다. ■

(b). 조건에 의하면 $(f(x)-g(x))h(x)\equiv_x 0\pmod p$ 이고 $h(x)\not\equiv_x 0\pmod p$ 이므로 (a)에 의하면 $f(x)-g(x)\equiv_x 0\pmod p$ 이다.
따라서 $f(x)\equiv_x g(x)\pmod p$ 이다. ■

소수가 아닐때의 반례는 다음과 같습니다. $n=6$ 일 때 $f(x)=2x,g(x)=3x$ 라고 하면 $f(x)g(x)\equiv_x 6x^2\equiv_x 0\pmod 6$ 입니다.
그런데 $f(x)\not\equiv_x 0\pmod 6$, $g(x)\not\equiv_x 0\pmod 6$ 이므로 반례가 됩니다.

이제 새로운 기호를 소개하겠습니다. n 이하의 자연수중 n과 서로소인 자연수를 원소로 갖는 집합을 기호로 $\mathbb{Z}_n^{\times}$ 로 나타냈고 이렇게 나타낸 이유는 법 n에서 곱셈에 대한 역원이 존재한다는 것을 강조하기 위해서입니다.

실제로 수학에서는 집합 A의 원소들 중 곱셈에 대한 역원이 존재하는 원소만 모은 집합을 $A^{\times}$로 쓰기도 합니다. 예를 들어 복소수 집합을 전체집합으로 고려할땐 $\mathbb{C}^{\times}=\mathbb{C}-\{0\}$ 가 되고 정수 집합을 전체집합으로 고려할땐 $\mathbb{Z}^{\times}=\{-1,1\}$ 가 됩니다.

대학 입학 전에 알고있던 세계에서는 $(\mathbb{C}[x])^{\times}=\mathbb{C}^{\times}$ 가 성립합니다. 이것은 직관적으로 생각해봐도 당연한데 $f(x)$가 상수가 아닌 다항식이면 $\dfrac{1}{f(x)}$는 다항식이 아닙니다.
그러므로 2개의 다항식을 곱해서 1이 나오려면 모두 0이 아닌 상수다항식이 되어야 합니다.

p가 소수인 경우 법 p에서는 다음과 같이 비슷한 결과를 얻을수 있습니다. p의 배수는 법 p에서 0과 합동이라는 사실을 생각해보면 됩니다.

Theorem 2.5.7 p가 소수일 때 정수계수 다항식 $f(x),g(x)\in\mathbb{Z}[x]$에 대하여 $f(x)g(x)\equiv_x 1 \pmod p$ 을 만족하면 $f(x),g(x)$는 모두 p의 배수가 아닌 상수다항식이다.

(증명)
만약 정수계수 다항식 $f(x),g(x)$ 둘중 적어도 하나가 법 p에 대하여 0과 합동이면 $f(x)g(x)\equiv_x 0 \pmod p$ 이므로 이것은 조건에 모순이다.

따라서 $f(x)\not\equiv_x 0 \pmod p$, $g(x)\not\equiv_x 0 \pmod p$ 을 만족해야 하고 이 경우 $\deg_p(f(x)), \deg_p(g(x))$는 잘 정의된다.

p는 소수이므로 (44)에 의하면 다음을 얻는다.

$$0=\deg_p(1)=\deg_p(f(x)g(x))=\deg_p(f(x))+\deg_p(g(x))$$

그러므로 $\deg_p(f(x))=\deg_p(g(x))=0$ 이고 따라서 $f(x),g(x)$는 모두 p의 배수가 아닌 상수다항식이다. ■

소수가 아니면 반례가 있습니다. $n=4$ 일 때 $f(x)=2x+1$ 이라고 하면 $(f(x))^2=4x^2+4x+1$ 이므로 $(f(x))^2\equiv_x 1 \pmod 4$ 이고 이때 $f(x)$는 법 4에서 상수다항식이 아닙니다.

일반적으로 법 n에서 다항식 $f(x)$의 곱셈에 대한 역원이 존재할 필요충분조건이 있는데 그 필요충분조건은 나중에 대수학을 공부할 때 만나게 될겁니다. 그 정리를 소개하려면 미리 소개해야 하는 개념과 성질이 많아서 이 책에 소개하는 것은 생략하겠습니다.

3. 위수와 원시근

3.1 위수, 원시근의 정의와 성질

작성자 : 네냐플(Nenyaffle)

n이 자연수이고 a는 $\gcd(a,n)=1$ 을 만족하는 정수이면 오일러의 정리에 의해 $a^{\phi(n)} \equiv 1 \pmod{n}$ 가 성립합니다. 그런데 실제로는 $\phi(n)$만큼 거듭제곱하지 않아도 법 n에서 1과 합동인 경우가 발생합니다.

$n=8$ 이고 $a=3$ 이면 $\gcd(a,n)=1$ 이고 $\phi(8)=4$ 이므로 오일러의 정리에 의하면 $3^4 \equiv 1 \pmod{8}$ 인데 $3^2 \equiv 1 \pmod{8}$ 도 만족합니다.

3장에서는 $\gcd(a,n)=1$ 일 때 $a^k \equiv 1 \pmod{n}$ 를 만족하는 가장 작은 자연수 k를 이야기하려고 합니다. $\gcd(a,n)=1$ 일 때 집합 S 를 다음과 같이 정의하면

$$S=\{k \in \mathbb{N} : a^k \equiv 1 \pmod{n}\}$$

$\phi(n) \in S$ 이므로 S 는 공집합이 아닌 자연수 집합의 부분집합입니다. 그러므로 정렬원리에 의하면 S 는 가장 작은 원소를 갖습니다. 그 원소를 다음과 같이 정의합니다.

Definition 3.1.1 위수(Order)
자연수 n과 $\gcd(a,n)=1$ 을 만족하는 정수 a가 임의로 주어져있다고 하자. 이때 $a^k \equiv 1 \pmod{n}$ 을 만족하는 가장 작은 자연수 k를 법 n에 대한 a의 **위수(Order)** 라고 정의하고 기호로는 $\mathrm{ord}_n(a)$ 로 나타낸다.

위수를 정의하기 위해서는 $\gcd(a,n)=1$ 이라는 조건이 필요합니다. $a^k \equiv 1 \pmod{n}$ 이므로 a는 법 n에서 곱셈에 대한 역원이 a^{k-1}로 존재해야 하기 때문입니다.

수학에서 Order라는 영어단어는 여러 가지 뜻으로 쓰입니다. 순서를 나타낼때도 쓰고 정수론에서는 Definition 3.1.1처럼 쓰고 대수학에서는 유한군의 원소의 개수로 쓰기도 합니다.

적당한 정수의 위수를 하나 구해보면 $n=8$ 일 때 $\gcd(3,8)=1$ 이고 $3 \not\equiv 1 \pmod{8}, 3^2 \equiv 1 \pmod{8}$ 이므로 $\mathrm{ord}_8(3)=2$ 입니다.

그런데 이렇게 하나하나 대입해서 찾는 것은 불편합니다. 물론 위수는 정의에 의하면 위수는 $\phi(n)$보다 작거나 같은 자연수인데 n이 숫자가 크면 $\phi(n)$도 마찬가지라서 1부터 $\phi(n)$ 까지의 자연수를 일일이 대입해서 위수를 찾는 것은 불편합니다.

따라서 위수가 될 자연수의 후보를 줄일 필요가 있는데 다음 정리가 그 역할을 해줍니다.

Theorem 3.1.1 n은 자연수이고 a는 $\gcd(a,n)=1$ 을 만족하는 정수일 때 자연수 h에 대하여 $a^h \equiv 1 \pmod{n}$ 을 만족할 필요충분조건은 $\mathrm{ord}_n(a) \mid h$ 이다. 그러므로 $\mathrm{ord}_n(a) \mid \phi(n)$ 가 성립한다.

(증명)
편의상 $k = \mathrm{ord}_n(a)$ 라고 하자.

$(\Longrightarrow)$ 나눗셈 정리에 의해 $h = kq + r$ 을 만족하는 정수 q와 $0 \le r < k$ 를 만족하는 정수 r이 존재하고 다음을 얻는다.

$$a^h \equiv a^{kq+r} \equiv (a^k)^q a^r \equiv a^r \equiv 1 \pmod{n}$$

따라서 $a^r \equiv 1 \pmod{n}$ 이다. 이제 $r = 0$ 임을 보이자.

결론을 부정해서 $r \neq 0$ 이라고 가정하자. 그러면 r은 k보다 작은 자연수인데 이것은 $k = \mathrm{ord}_n(a)$에 모순이다. 따라서 $r = 0$ 이고 이때 $h = kq$ 이므로 $k \mid h$ 를 얻는다.

$(\Longleftarrow)$ 조건에 의하면 적당한 정수 s가 존재해서 $h = ks$ 를 만족한다.
그리고 $a^k \equiv 1 \pmod{n}$ 이므로 $a^h \equiv (a^k)^s \equiv 1 \pmod{n}$ 이다.

이제 $k \mid \phi(n)$ 를 증명하자. 오일러의 정리에 의하면 $a^{\phi(n)} \equiv 1 \pmod{n}$ 이므로 이것은 $h = \phi(n)$ 인 경우이다. 따라서 $k \mid \phi(n)$ 이 성립한다. ■

Theorem 3.1.1에 의하면 위수가 될수 있는 자연수는 $\phi(n)$의 양의 약수에 모두 있습니다. 따라서 정수의 위수를 찾을때는 $\phi(n)$을 먼저 구하고 $\phi(n)$의 양의 약수를 가지고 거듭제곱 해보면 됩니다.

$n = 13$ 일 때 $\phi(13) = 12$ 이고 12의 양의 약수는 $1,2,3,4,6,12$ 이므로 3의 위수는 6개중 하나입니다. 실제로 계산해보면 법 13에 대하여 $3^1 \equiv 3, 3^2 \equiv 9, 3^3 \equiv 1$ 이므로 $\mathrm{ord}_{13}(3) = 3$ 입니다.

여기서 주의할 점은 $\phi(n)$의 양의 약수가 모두 어떤 정수의 위수가 되는건 아니라는 것입니다. $n = 12$ 이면 $\phi(12) = 4$ 이고 4의 양의 약수는 $1,2,4$ 인데 12와 서로소인 자연수 $1,5,7,11$중 위수가 4인 것은 존재하지 않습니다. 다음이 성립하기 때문입니다.

$$1^1 \equiv 5^2 \equiv 7^2 \equiv 11^2 \equiv 1 \pmod{12}$$

한편 위수의 정의에 의하면 $\mathrm{ord}_n(a) \le \phi(n)$ 임은 명백합니다. 따라서 위수가 가질수 있는 최댓값은 $\phi(n)$인지 관심을 가져볼수 있는데 $\mathrm{ord}_n(a) = \phi(n)$ 이 성립하는 경우도 얼마든지 있습니다.

$n = 5$ 일 때 $\phi(5) = 4$ 이고 $\gcd(2,5) = 1$ 입니다. 그리고 다음이 성립합니다.

$$2^1 \equiv 2 \pmod{5}$$
$$2^2 \equiv 4 \pmod{5}$$
$$2^4 \equiv 1 \pmod{5}$$

따라서 $\mathrm{ord}_5(2) = 4 = \phi(5)$ 입니다. 즉, $\mathrm{ord}_n(a) = \phi(n)$ 가 성립하는 경우입니다.

위수가 $\phi(n)$인 정수를 수학에서는 다음과 같이 정의합니다.

Definition 3.1.2 원시근(Primitive Root)
n은 자연수이고 a는 $\gcd(a,n)=1$ 을 만족하는 정수일 때 정수 a가
$\mathrm{ord}_n(a)=\phi(n)$ 을 만족하면 a를 법 n의 **원시근(Primitive Root)**이라고 정의한다.

법 n의 원시근이 항상 존재하는 것은 아닙니다. $n=12$ 일 때 $\phi(12)=4$ 인데

$$1^1 \equiv 5^2 \equiv 7^2 \equiv 11^2 \equiv 1 \pmod{12}$$

이므로 위수가 4인 정수가 존재하지 않습니다. 즉, 법 12의 원시근은 존재하지 않습니다.

이제 법 n에서 원시근이 존재할 경우 원시근은 몇 개인지 조사해보겠습니다.
원시근이 몇 개 있는지 조사할땐 $\mathbb{Z}_n^{\times}$에서만 조사해도 충분한데 그 이유는 다음 문제를 풀어보면 알수 있습니다.

Problem 3.1.1 자연수 n과 $\gcd(a,n)=1$ 을 만족하는 정수 a가 임의로 주어져있다고 하자. 정수 b가 $a \equiv b \pmod{n}$ 을 만족하면 $\mathrm{ord}_n(a)=\mathrm{ord}_n(b)$ 임을 증명하시오.

(증명)
$a \equiv b \pmod{n}$ 이므로 $\gcd(b,n)=\gcd(a,n)=1$ 이다. 따라서 법 n에서 b의 위수는 잘 정의된다. 편의상 $k_1=\mathrm{ord}_n(a)$, $k_2=\mathrm{ord}_n(b)$ 라고 하자.
그러면 $a^{k_1} \equiv b^{k_2} \equiv 1 \pmod{n}$ 이 성립한다.

$a \equiv b \pmod{n}$ 이므로 $a^{k_1} \equiv b^{k_1} \equiv 1 \pmod{n}$ 이고 따라서 Theorem 3.1.1에 의하면 $k_2 \mid k_1$ 이다. 그러므로 $k_2 \le k_1$ 를 얻는다.

마찬가지로 $a \equiv b \pmod{n}$ 이므로 $a^{k_2} \equiv b^{k_2} \equiv 1 \pmod{n}$ 이고 Theorem 3.1.1에 의하면 $k_1 \mid k_2$ 이다. 그러므로 $k_1 \le k_2$ 를 얻는다.

따라서 $k_1=k_2$ 이다. 그러므로 $\mathrm{ord}_n(a)=\mathrm{ord}_n(b)$ 가 성립한다. ■

Problem 3.1.1에 의하면 법 n에서 합동인 정수는 같은 위수를 갖습니다.
따라서 특정한 위수를 갖는 정수가 얼마나 있는지 조사할땐 $\mathbb{Z}_n^{\times}$에서만 조사해도 충분합니다.
그러므로 원시근이 얼마나 있는지 조사할때도 $\mathbb{Z}_n^{\times}$에서만 조사하면 됩니다.

Theorem 3.1.2 n은 자연수이고 a는 $\gcd(a,n)=1$ 을 만족하는 정수일 때
$k=\mathrm{ord}_n(a)$ 라고 하면 다음이 성립한다.
(a). $a^i \equiv a^j \pmod{n}$ 가 성립할 필요충분조건은 $i \equiv j \pmod{k}$ 이다.
(b). $a, a^2, a^3, \ldots, a^k$ 는 법 n에서 서로 합동이 아니다.
(c). a가 법 n의 원시근이면 $\{a, a^2, a^3, \ldots, a^{\phi(n)}\}$은 법 n에 대한 기약잉여계이다.

(증명)
(a). $(\Rightarrow)$ $i \geq j$ 라고 가정해도 일반성을 잃지 않는다. $i = j$ 이면 명백하므로 $i > j$ 를 가정하자. 그러면 $a^{i-j} \equiv 1 \pmod{n}$ 이고 $i-j$ 는 자연수이므로 Theorem 3.1.1에 의하면 $k \mid i-j$ 이다. 따라서 $i \equiv j \pmod{k}$ 가 성립한다.

$(\Leftarrow)$ 조건에 의하면 적당한 정수 q가 존재해서 $i = j+qk$ 를 만족한다.
따라서 다음이 성립한다.

$$a^i \equiv a^{j+qk} \equiv a^j(a^k)^q \equiv a^j \pmod{n}$$

■

(b). $1 \leq i \leq j \leq k$ 일 때 $a^i \equiv a^j \pmod{n}$ 이면 (a)에 의해 $i \equiv j \pmod{k}$ 인데 $1 \leq i \leq j \leq k$ 이므로 $i \equiv j \pmod{k}$ 이면 $i = j$ 이다. 따라서 $i \neq j$ 이면 $a^i \not\equiv a^j \pmod{n}$ 이므로 $a, a^2, a^3, \ldots, a^k$ 는 법 n에서 서로 합동이 아니다. ■

(c). (b)에 의하면 $a, a^2, a^3, \ldots, a^{\phi(n)}$ 은 법 n에서 서로 합동이 아니다. 그리고 $\{a, a^2, a^3, \ldots, a^{\phi(n)}\}$의 원소의 개수는 $\phi(n)$이고 $\gcd(a,n) = 1$ 이므로 각각의 $i = 1, 2, \ldots, \phi(n)$ 에 대하여 $\gcd(a^i, n) = 1$ 이다.

따라서 $\{a, a^2, a^3, \ldots, a^{\phi(n)}\}$는 법 n에 대한 기약잉여계이다. ■

Theorem 3.1.3 n은 자연수이고 a는 $\gcd(a,n) = 1$ 을 만족하는 정수일 때 $\mathrm{ord}_n(a) = k$ 이면 모든 자연수 h에 대하여 $\mathrm{ord}_n(a^h) = \dfrac{k}{\gcd(k,h)}$ 이다.

(증명)
$d = \gcd(k,h), r = \mathrm{ord}_n(a^h)$ 라고 하자. 그러면 $\dfrac{h}{d}$ 는 자연수이므로

$(a^h)^{\frac{k}{d}} \equiv \left(a^{\frac{h}{d}}\right)^k \equiv 1 \pmod{n}$ 을 얻는다. 따라서 Theorem 3.1.1에 의하면 $r \mid \dfrac{k}{d}$ 이므로 $r \leq \dfrac{k}{d}$ 이다.

마찬가지로 $(a^h)^r \equiv a^{hr} \equiv 1 \pmod{n}$ 이므로 Theorem 3.1.1에 의하면 $k \mid hr$ 이고 따라서 $\dfrac{k}{d} \mid \left(\dfrac{h}{d}\right) \times r$ 인데 $\gcd\left(\dfrac{k}{d}, \dfrac{h}{d}\right) = 1$ 이므로 $\dfrac{k}{d} \mid r$ 을 얻는다.
그러므로 $\dfrac{k}{d} \leq r$ 이다.

정리하면 $r = \dfrac{k}{d}$ 를 얻는다. 따라서 $\mathrm{ord}_n(a^h) = \dfrac{k}{\gcd(k,h)}$ 이다. ■

Theorem 3.1.3은 많이 쓰이는 공식이므로 기억해놓으면 편합니다. 실제로 확인해보면
법 13에서 1부터 12까지의 위수는 다음과 같고

정수	1	2	3	4	5	6	7	8	9	10	11	12
위수	1	12	3	6	4	12	12	4	3	6	12	2

법 13에서 2^2의 위수는 $\frac{12}{\gcd(12,2)}=6$, 2^3의 위수는 $\frac{12}{\gcd(12,3)}=4$ 입니다.

Theorem 3.1.3에 의하면 $\mathrm{ord}_n(a)=k$ 일 때 $\mathrm{ord}_n(a^h)=k$ 일 필요충분조건은
$\gcd(k,h)=1$ 인 것임을 쉽게 알수 있습니다. 따라서 a가 법 n의 원시근일 때
a^h가 법 n의 원시근이 될 필요충분조건은 $\gcd(\phi(n),h)=1$ 입니다. (1)

이것을 이용하면 원시근이 존재할 경우 $\mathbb{Z}_n^{\times}$에 있는 원시근의 개수는
다음과 같이 구할수 있습니다.

Theorem 3.1.4 n이 자연수일 때 법 n에서 원시근이 존재할 경우 그 원시근은 $\mathbb{Z}_n^{\times}$에 $\phi(\phi(n))$개 있다.

(증명)
a를 법 n의 원시근이라고 하자. 그러면 Theorem 3.1.2에 의해 $\{a,a^2,a^3,\ldots,a^{\phi(n)}\}$은
법 n에 대한 기약잉여계이다. 따라서 법 n에서 a와 다른 원시근 b가 존재한다면
그 b는 $a,a^2,a^3,\ldots,a^{\phi(n)}$ 중 정확히 한 정수와 법 n에 대해 합동이 된다.

그러므로 법 n에 대한 기약잉여계는 모든 원시근을 포함하고 있다.
즉, 법 n의 원시근은 $a,a^2,a^3,\ldots,a^{\phi(n)}$ 중 하나이다.

따라서 (1)에 의하면 법 n의 원시근의 개수는 1부터 $\phi(n)$까지의 자연수 중
$\phi(n)$과 서로소인 자연수의 개수와 같고 그 개수는 $\phi(\phi(n))$이다. ■

Theorem 3.1.4의 증명과정을 이용하면 하나의 원시근을 알고 있을 경우 다른 원시근도
모두 구할수 있습니다. $n=9$ 일 때 $\phi(9)=6$ 이고 6의 양의 약수 $1,2,3,6$ 만큼
거듭제곱을 해보면 5는 법 9의 원시근임을 알수 있습니다.

따라서 $\{5,5^2,5^3,5^4,5^5,5^6\}$은 법 9에 대한 기약잉여계입니다.
실제로 계산해보면 법 9에서 다음과 같이 나옵니다.

$$5^1\equiv 5, 5^2\equiv 7, 5^3\equiv 8, 5^4\equiv 4, 5^5\equiv 2, 5^6\equiv 1$$

그리고 Theorem 3.1.4에 의하면 법 9의 원시근은 $\phi(\phi(9))=\phi(6)=2$개 있고
나머지 하나를 직접 구하기 위해 $\mathrm{ord}_9(5^k)=\frac{6}{\gcd(6,k)}=6$ 이라고 하면
$\gcd(6,k)=1$ 이므로 이것을 만족하는 6 이하의 자연수 k는 $k=1,5$ 입니다.

$k=1$ 이면 5이고 $k=5$ 이면 $5^5 \equiv 2 \pmod 9$ 이므로 법 9의 원시근을 $\mathbb{Z}_9^{\times}$에서 찾으면 $2,5$ 입니다. 즉, 나머지 하나의 원시근은 2입니다.

이제 위수가 $\phi(n)$인 정수를 법 n의 원시근이라고 부르는 이유를 설명하겠습니다. 자연수 n에 대하여 합동방정식 $x^{\phi(n)} \equiv 1 \pmod n$ 의 해를 구해보면 법 n에 대한 기약잉여계의 모든 원소가 해가 됩니다.

$x^{\phi(n)} \equiv 1 \pmod n$ 의 해가 될수 있는 후보는 $\mathbb{Z}_n^{\times}$에 있는데 거듭제곱한 것이 1과 합동이므로 법 n에서 곱셈에 대한 역원이 존재합니다. 따라서 해가 될수 있는 후보는 모두 법 n에 대한 기약잉여계에 있습니다.

그리고 오일러의 정리에 의하면 $\gcd(a,n)=1$ 일 때 $a^{\phi(n)} \equiv 1 \pmod n$ 을 만족하므로 기약잉여계의 모든 원소는 합동방정식 $x^{\phi(n)} \equiv 1 \pmod n$ 의 해가 됩니다. 따라서 합동방정식 $x^{\phi(n)} \equiv 1 \pmod n$ 의 해는 기약잉여계에만 있습니다.

Theorem 3.1.2에 의하면 a가 법 n의 원시근일 때 $\{a,a^2,a^3,...,a^{\phi(n)}\}$은 법 n에 대한 기약잉여계가 됩니다. 이것은 합동방정식 $x^{\phi(n)} \equiv 1 \pmod n$ 의 모든 해는 a를 가지고 표현할수 있다는 뜻입니다. 그래서 위수가 $\phi(n)$인 정수를 법 n의 원시근이라고 부릅니다.

문제를 몇 개 풀고 3.1절을 마치겠습니다.

Problem 3.1.2 $n \geq 2$ 일 때 $F_n = 2^{2^n}+1$ 이 소수이면 2는 법 F_n의 원시근이 될수 없음을 증명하시오.

(증명)
수학적 귀납법을 이용하면 $n \geq 2$ 일 때 $2^n > n+1$ 임을 쉽게 증명할수 있다.

$2^{2^{n+1}}-1 = \left(2^{2^n}-1\right)\left(2^{2^n}+1\right) = \left(2^{2^n}-1\right)F_n$ 이므로 $2^{2^{n+1}} \equiv 1 \pmod{F_n}$ 이다.
따라서 $\mathrm{ord}_{F_n}(2)=k$ 라고 하면 Theorem 3.1.1에 의해 $k \mid 2^{n+1}$ 이므로 $k \leq 2^{n+1}$ 이다. 그런데 F_n은 소수이므로 $\phi(F_n)=2^{2^n}$ 이고 $n \geq 2$ 이면 $2^n > n+1$ 이므로 $k \leq 2^{n+1} < 2^{2^n} = \phi(F_n)$ 을 얻는다.

그러므로 2는 법 F_n의 원시근이 될수 없다. ■

Problem 3.1.3 n은 자연수이고 $\gcd(a,n)=1$ 일 때 법 n에서 a의 곱셈에 대한 역원을 x라고 하자. 그러면 $\mathrm{ord}_n(a)=\mathrm{ord}_n(x)$ 임을 증명하시오.

(증명)
이 경우 $\gcd(x,n)=1$ 임은 명백하므로 x의 위수는 잘 정의된다.
편의상 $k_1 = \mathrm{ord}_n(a),\ k_2 = \mathrm{ord}_n(x)$ 라고 하자. 그러면 다음을 만족한다.

$$a^{k_1} \equiv x^{k_2} \equiv 1 \pmod{n}$$

$ax \equiv 1 \pmod{n}$ 이므로 $(ax)^{k_1} \equiv a^{k_1}x^{k_1} \equiv x^{k_1} \equiv 1 \pmod{n}$ 이다.
따라서 Theorem 3.1.1에 의하면 $k_2 \mid k_1$ 이므로 $k_2 \le k_1$ 이다.

마찬가지로 $ax \equiv 1 \pmod{n}$ 에서 $(ax)^{k_2} \equiv a^{k_2}x^{k_2} \equiv a^{k_2} \equiv 1 \pmod{n}$ 이므로
Theorem 3.1.1에 의하면 $k_1 \mid k_2$ 이다. 따라서 $k_1 \le k_2$ 이다.

정리하면 $k_1 = k_2$ 를 얻을수 있고 그러므로 $\mathrm{ord}_n(a) = \mathrm{ord}_n(x)$ 이다. ■

Problem 3.1.4 다음을 증명하시오. 각각의 문제에서 용어는 잘 정의된다고 가정한다.
(a). n이 자연수일 때 법 n에 대한 a의 위수가 hk이면 a^h의 위수는 k이다.
(b). p가 홀수인 소수일 때 법 p에 대한 a의 위수가 $2k$이면 $a^k \equiv -1 \pmod{p}$ 이다.
(c). p가 홀수인 소수일 때 법 p에 대한 a의 위수가 2일 필요충분조건은
$a \equiv -1 \pmod{p}$ 을 만족하는 것이다.
(d). n이 $n \ge 2$ 인 자연수일 때 법 n에 대한 a의 위수가 $n-1$ 이면 n은 소수이다.

(증명)
(a). $h \mid hk$ 이므로 $\gcd(hk,h) = h$ 이다. 따라서 Theorem 3.1.3에 의하면
$\mathrm{ord}_n(a^h) = \dfrac{hk}{\gcd(hk,h)} = k$ 이다. ■

(b). 조건에 의하면 $a^{2k} \equiv 1 \pmod{p}$ 이므로 $(a^k-1)(a^k+1) \equiv 0 \pmod{p}$ 를
만족하고 p가 소수이므로 $a^k \equiv 1 \pmod{p}$ 또는 $a^k \equiv -1 \pmod{p}$ 인데
법 p에 대한 a의 위수가 $2k$이므로 $a^k \equiv -1 \pmod{p}$ 이어야 한다. ■

(c). $(\Rightarrow)$ (b)에 의하면 명백하다.

$(\Leftarrow)$ 조건에 의하면 $a^2 \equiv 1 \pmod{p}$ 이므로 Theorem 3.1.1에 의하면 a의 위수는
2의 양의 약수 $1,2$ 둘중 하나인데 $a \equiv -1 \pmod{p}$ 이므로 a의 위수는 2이다. ■

(d). Theorem 3.1.1에 의하면 $n-1 \mid \phi(n)$ 이므로 $n-1 \le \phi(n)$ 을 만족하고
오일러 ϕ함수의 정의에 의하면 $\phi(n) \le n-1$ 은 명백하다. 따라서 $\phi(n) = n-1$
을 만족하고 이것은 1부터 $n-1$ 까지의 모든 자연수가 n과 서로소라는 것을 의미한다.

결론을 부정해서 n이 합성수라고 가정하자. 그러면 $1 < a \leq b < n$ 을 만족하는 적당한 자연수 a, b가 존재해서 $n = ab$ 를 만족하고 $\gcd(a,n) = a \geq 2$ 이므로 이 경우 $\phi(n) \leq n-2$ 인데 이것은 모순이다. 따라서 n은 소수이다. ■

Problem 3.1.5 n이 자연수일 때 다음을 증명하시오.
(a). $\mathrm{ord}_{2^n-1}(2) = n$ 이다.
(b). 자연수 n에 대하여 $n \mid \phi(2^n-1)$ 이다.

(증명)
(a). n이 자연수이면 $\gcd(2, 2^n-1) = 1$ 이므로 법 2^n-1 에서 2의 위수는 잘 정의된다. $\mathrm{ord}_{2^n-1}(2) = k$ 라고 하면 $2^n \equiv 1 \pmod{2^n-1}$ 은 명백하므로 Theorem 3.1.1에 의하면 $k \mid n$ 이다. 그러므로 $k \leq n$ 이다.

그리고 $2^k \equiv 1 \pmod{2^n-1}$ 이므로 $2^n-1 \mid 2^k-1$ 이다.
따라서 $\gcd(2^n-1, 2^k-1) = 2^{\gcd(n,k)}-1 = 2^n-1$ 이므로 $\gcd(n,k) = n$ 에서 $n \mid k$ 를 얻는다. 그러므로 $n \leq k$ 이다.

정리하면 $k = n$ 이므로 $\mathrm{ord}_{2^n-1}(2) = n$ 이다. ■

(b). (a)에서 $\mathrm{ord}_{2^n-1}(2) = n$ 이므로 Theorem 3.1.1에 의하면 $n \mid \phi(2^n-1)$ 이다. ■

Problem 3.1.6 n은 자연수이고 a, b는 정수일 때 $\mathrm{ord}_n(a) = h$, $\mathrm{ord}_n(b) = k$ 이면 $\mathrm{ord}_n(ab) \mid hk$ 이고 만약 $\gcd(h,k) = 1$ 이면 $\mathrm{ord}_n(ab) = hk$ 임을 증명하시오. 여기서 모든 기호는 잘 정의된다고 가정한다.

(증명)
$\mathrm{ord}_n(ab) = r$ 라고 하자. 조건에 의하면 $a^h \equiv b^k \equiv 1 \pmod{n}$ 이므로 $(ab)^{hk} \equiv a^{hk}b^{hk} \equiv (a^h)^k (b^k)^h \equiv 1 \pmod{n}$ 이다. 따라서 Theorem 3.1.1에 의하면 $r \mid hk$ 를 얻는다. 그러므로 $\mathrm{ord}_n(ab) \mid hk$ 이다.

이제 $\gcd(h,k) = 1$ 라고 가정하자. $(ab)^r \equiv a^r b^r \equiv 1 \pmod{n}$ 이므로 Problem 3.1.3에 의하면 $\mathrm{ord}_n(a^r) = \mathrm{ord}_n(b^r)$ 이다. 따라서 Theorem 3.1.3에 의하면

$$\frac{h}{\gcd(h,r)} = \frac{k}{\gcd(k,r)}$$ 가 성립한다.

$\mathrm{ord}_n(a^r) = \mathrm{ord}_n(b^r) = m$ 라고 하자. 그러면 $h = m\gcd(h,r), k = m\gcd(k,r)$ 에서 $m \mid h, m \mid k$ 이고 $\gcd(h,k) = 1$ 이므로 적당한 정수 x, y가 존재해서 $hx + ky = 1$ 을 만족한다. 따라서 $m \mid hx + ky = 1$ 이므로 $m = 1$ 이다.

그러므로 $\mathrm{ord}_n(a^r)=\mathrm{ord}_n(b^r)=1$ 에서 $a^r\equiv b^r\equiv 1\pmod n$ 을 얻고
Theorem 3.1.1에 의하면 $h\mid r, k\mid r$ 인데 $\gcd(h,k)=1$ 이므로 $hk\mid r$ 을 얻는다.

정리하면 $\gcd(h,k)=1$ 일 때 $r\mid hk$ 과 $hk\mid r$ 가 모두 성립하므로
$r\le hk, hk\le r$ 이 성립하고 따라서 $r=hk$ 이다. 즉, $\mathrm{ord}_n(ab)=hk$ 이다. ■

Problem 3.1.6에서 $\mathrm{ord}_n(a)=h$, $\mathrm{ord}_n(b)=k$ 이면 $\mathrm{ord}_n(ab)=\mathrm{lcm}(h,k)$ 가 된다고 생각할수 있는데 이것은 거짓입니다. 반례는 다음과 같습니다.

$n=5$ 일 때 $a=2, b=3$ 라고 하면 $\gcd(2,5)=\gcd(3,5)=1$ 이므로 a,b의 위수는 잘 정의되고 $\mathrm{ord}_5(2)=\mathrm{ord}_5(3)=4$ 임을 쉽게 알수 있습니다.

그런데 $ab=6$ 이고 $6\equiv 1\pmod 5$ 이므로 $\mathrm{ord}_5(6)=1$ 입니다.
따라서 $\mathrm{ord}_5(6)\neq \mathrm{lcm}\big(\mathrm{ord}_5(2),\mathrm{ord}_5(3)\big)$ 입니다.

한편 Problem 3.1.6의 증명과정과 비슷한 방법으로 $\mathrm{ord}_n(a)=h$, $\mathrm{ord}_n(b)=k$ 일 때 $\mathrm{ord}_n(ab)\mid \mathrm{lcm}(h,k)$ 가 성립한다는 것은 쉽게 알수 있습니다.

Problem 3.1.7 p가 홀수인 소수이고 a는 $\gcd(a,p)=\gcd(a+1,p)=1$ 을 만족하는 정수일 때 $\mathrm{ord}_p(a)=3$ 이면 $\mathrm{ord}_p(a+1)=6$ 임을 증명하시오.

(증명)
조건에 의하면 $a^3\equiv 1\pmod p$ 이다. 따라서 $(a-1)\big(a^2+a+1\big)\equiv 0\pmod p$
인데 p는 소수이고 $\mathrm{ord}_p(a)=3$ 이므로 $a^2+a+1\equiv 0\pmod p$ 이다.
따라서 다음을 얻을수 있다.

$$\begin{aligned}(a+1)^2&\equiv a^2+2a+1\\&\equiv a+1\pmod p\end{aligned}$$

$$\begin{aligned}(a+1)^3&\equiv a^3+3a^2+3a+1\\&\equiv 3\big(a^2+a\big)+2\\&\equiv -1\pmod p\end{aligned}$$

그러므로 $(a+1)^6\equiv 1\pmod p$ 가 성립하고 $\gcd(a,p)=1$ 이므로
$a+1\not\equiv 1\pmod p$ 이다. 따라서 $(a+1)^2\equiv a+1\not\equiv 1\pmod p$ 이고
$(a+1)^3\equiv -1\not\equiv 1\pmod p$ 이므로 Theorem 3.1.1에서 $\mathrm{ord}_p(a+1)=6$ 이다. ■

Problem 3.1.8 n이 자연수일 때 다음을 증명하시오.
(a). n^2+1 의 약수중 홀수인 소수가 존재하면 그것은 $4k+1$ 형태이다.
(b). n^4+1 의 약수중 홀수인 소수가 존재하면 $8k+1$ 형태이다.
(c). n^2+n+1 의 약수중 3이 아닌 홀수 소수가 존재하면 그것은 $6k+1$ 형태이다.

(증명)

(a). n^2+1 의 약수중 홀수인 소수를 p라고 하자. 그러면 $n^2 \equiv -1 \pmod{p}$ 이므로 $n^4 \equiv 1 \pmod{p}$ 을 얻는다.

p가 홀수인 소수이므로 $-1 \not\equiv 1 \pmod{p}$ 이고 $n^2 \equiv -1 \pmod{p}$ 이므로 $n \not\equiv 1 \pmod{p}$ 이다. 따라서 Theorem 3.1.1에 의하면 $\mathrm{ord}_p(n)=4$ 이므로 $4 \mid \phi(p)=p-1$ 을 얻는다. 그러므로 적당한 정수 k가 존재해서 $p-1=4k$ 를 만족하고 $p=4k+1$ 이다. ■

(b). n^4+1 의 약수중 홀수인 소수를 p라고 하자. 그러면 $n^4 \equiv -1 \pmod{p}$ 이므로 $n^8 \equiv 1 \pmod{p}$ 을 얻는다.

p가 홀수인 소수이므로 $-1 \not\equiv 1 \pmod{p}$ 이고 $n^4 \equiv -1 \pmod{p}$ 이므로 다음을 만족한다.

$$n \not\equiv 1 \pmod{p},\ n^2 \not\equiv 1 \pmod{p}$$

따라서 Theorem 3.1.1에 의하면 $\mathrm{ord}_p(n)=8$ 이므로 $8 \mid \phi(p)=p-1$ 을 얻는다. 그러므로 적당한 정수 k가 존재해서 $p-1=8k$ 를 만족하고 $p=8k+1$ 이다. ■

(c). n^2+n+1 의 약수중 3이 아닌 홀수 소수를 p라고 하자. 그러면 $n^2+n+1 \equiv 0 \pmod{p}$ 이고 양변에 $n-1$ 을 곱하면 $n^3 \equiv 1 \pmod{p}$ 를 얻는다.

이제 $n \not\equiv 1 \pmod{p}$ 임을 보이자. 결론을 부정해서 $n \equiv 1 \pmod{p}$ 라고 가정하면 적당한 정수 k가 존재해서 $n=pk+1$ 을 만족하고 다음을 얻는다.

$$n^2+n+1=p^2k^2+3pk+3$$

조건에 의하면 $p \mid n^2+n+1$ 이므로 $p \mid 3$ 을 얻고 p는 소수이므로 $p=3$ 인데 이것은 조건에 모순이다. 따라서 $n \not\equiv 1 \pmod{p}$ 이다.

그리고 p는 홀수인 소수이므로 $-1 \not\equiv 1 \pmod{p}$ 이고 $n^3 \equiv 1 \pmod{p}$ 이므로 Theorem 3.1.1에 의하면 $\mathrm{ord}_p(n)=3$ 이다. 그러므로 $3 \mid \phi(p)=p-1$ 이다.

따라서 적당한 정수 m이 존재해서 $p-1=3m$ 를 만족하므로 $p=3m+1$ 이다. 만약 m이 홀수이면 $m=2k+1$ 에서 $p=6k+4=2(3k+2)$ 를 얻는데 p는 홀수인 소수이므로 이것은 모순이다. 그러므로 m은 짝수이고 $m=2k$ 이면 $p=6k+1$ 이다. ■

Problem 3.1.8을 이용해서 다음을 증명할수 있습니다.

Theorem 3.1.5 $k \in \mathbb{Z}$ 일 때 다음이 성립한다.

(a). $4k+1$ 형태를 갖는 소수의 개수는 무한하다.

(b). $6k+1$ 형태를 갖는 소수의 개수는 무한하다.

(c). $8k+1$ 형태를 갖는 소수의 개수는 무한하다.

(증명)
(a). 결론을 부정해서 $4k+1$ 형태를 갖는 소수의 개수가 유한하다고 가정하고 그것을 $p_1,p_2,...,p_r$ 라고 하자. 그리고 $N=(2p_1p_2\cdots p_r)^2+1$ 라고 하자.

그러면 N은 n^2+1 형태를 갖는 3 이상의 홀수이다. 따라서 약수들 중 홀수인 소수 p가 존재하고 Problem 3.1.8 (a)에 의하면 p는 $4k+1$ 형태이다.

따라서 적당한 $i=1,2,...,r$ 에 대하여 $p=p_i$ 를 만족하고 $p \mid N$ 인데 $p \mid (2p_1p_2\cdots p_r)^2$ 이므로 $p \mid 1$ 을 얻는다. 이것은 p가 소수라는 것에 모순이다. 그러므로 $4k+1$ 형태를 갖는 소수의 개수는 무한하다. ■

(b). 결론을 부정해서 $6k+1$ 형태를 갖는 소수의 개수가 유한하다고 가정하고 그것을 $p_1,p_2,...,p_r$ 라고 하자. 그리고 $N=(3p_1p_2\cdots p_r)^2+(3p_1p_2\cdots p_r)+1$ 라고 하자.

그러면 N은 n^2+n+1 형태이고 $p_1,p_2,...,p_r$ 은 모두 홀수이므로 N은 3 이상의 홀수이다. 따라서 N의 약수들 중 홀수인 소수 p가 존재하고 $3 \nmid N$ 은 명백하므로 p는 3이 아닌 홀수인 소수이다.

따라서 Problem 3.1.8 (c)에 의하면 p는 $6k+1$ 형태이다. 그러므로 적당한 $i=1,2,...,r$ 에 대하여 $p=p_i$ 를 만족하고 $p \mid N$ 인데 $p \mid (3p_1p_2\ ...\ p_r)^2+(3p_1p_2\ ...\ p_r)$ 이므로 $p \mid 1$ 을 얻는다.

이것은 p가 소수라는 것에 모순이므로 $6k+1$ 형태를 갖는 소수의 개수는 무한하다. ■

(c). 결론을 부정해서 $8k+1$ 형태를 갖는 소수의 개수가 유한하다고 가정하고 그것을 $p_1,p_2,...,p_r$ 라고 하자. 그리고 $N=(2p_1p_2\cdots p_r)^4+1$ 라고 하자.

그러면 N은 n^4+1 형태를 갖는 3 이상의 홀수이다. 따라서 약수들 중 홀수인 소수 p가 존재하고 Problem 3.1.8 (b)에 의하면 p는 $8k+1$ 형태이다.

따라서 적당한 $i=1,2,...,r$ 에 대하여 $p=p_i$ 를 만족하고 $p \mid N$ 인데 $p \mid (2p_1p_2\cdots p_r)^4$ 이므로 $p \mid 1$ 을 얻는다. 이것은 p가 소수라는 것에 모순이다. 그러므로 $8k+1$ 형태를 갖는 소수의 개수는 무한하다. ■

Problem 3.1.9 다음 물음에 답하시오.
(a). p,q는 서로 다른 홀수 소수이고 a는 정수일 때 $q \mid a^{p-1}+a^{p-2}+\cdots+a^2+a+1$ 이면 적당한 정수 k가 존재해서 $q=2pk+1$ 을 만족함을 증명하시오.
(b). p가 홀수인 소수이면 2^p-1 의 소수인 약수는 $2pk+1$ 형태임을 증명하시오.

(증명)

(a). 조건에 의하면 $a^{p-1}+a^{p-2}+\cdots+a^2+a+1\equiv 0 \pmod q$ 이다. 따라서 양변에 $a-1$ 을 곱하면 $a^p\equiv 1 \pmod q$ 이므로 Theorem 3.1.1에 의하면 $\mathrm{ord}_q(a)\mid p$ 를 얻고 p는 소수이므로 $\mathrm{ord}_q(a)=1$ 또는 $\mathrm{ord}_q(a)=p$ 이다.

$\mathrm{ord}_q(a)=1$ 이면 $a\equiv 1 \pmod q$ 이므로 조건에 의하면 $p\equiv 0 \pmod q$ 를 얻고 $q\mid p$ 인데 p,q는 모두 소수이므로 $p=q$ 가 되어야 한다. 이것은 조건에 모순이므로 $\mathrm{ord}_q(a)=p$ 가 되어야 한다.

이제 정수 k에 대하여 $q=2pk+1$ 임을 증명하자. $\mathrm{ord}_q(a)=p$ 이므로 Theorem 3.1.1에 의하면 $p\mid\phi(q)=q-1$ 이다. 따라서 적당한 정수 m이 존재해서 $q=pm+1$ 을 만족한다.

만약 m이 홀수이면 $m=2k+1$ 에서 $q=2pk+p+1$ 이고 p는 홀수이므로 q는 짝수인데 이것은 조건에 모순이다. 그러므로 m은 짝수이고 $m=2k$ 에서 $q=2pk+1$ 을 얻는다. ■

(b). p가 홀수인 소수이면 2^p-1 은 3 이상의 홀수이므로 홀수인 소수 약수를 갖는다. 그것을 q라고 하면 $q\mid 2^p-1=2^{p-1}+2^{p-2}+\cdots+2^2+2+1$ 이다. 이제 $p\neq q$ 임을 보이자.

결론을 부정해서 $p=q$ 라고 가정하자. 그러면 조건에 의해 $2^p\equiv 2\equiv 1 \pmod p$ 이므로 $p\mid 1$ 인데 이것은 모순이다. 따라서 p,q는 서로 다른 홀수 소수이다. 그러므로 (a)에 의하면 적당한 정수 k가 존재해서 $q=2pk+1$ 을 만족한다. ■

Problem 3.1.9 (a)를 이용해서 다음을 증명할수 있습니다.

Theorem 3.1.6 홀수인 소수 p가 임의로 주어져있다고 하자. 그러면 $k\in\mathbb{Z}$ 일 때 $2pk+1$ 형태를 갖는 소수의 개수는 무한하다.

(증명)

결론을 부정해서 $2pk+1$ 형태를 갖는 소수의 개수가 유한하다고 가정하고 그것을 $q_1,q_2,\ldots,q_r$ 라고 하자. 그리고 $a=q_1q_2\cdots q_r$ 라고 할 때 자연수 N을 다음과 같이 정의하자.

$$N=a^{p-1}+a^{p-2}+\cdots+a^2+a+1$$

a는 홀수이므로 N은 p개의 홀수를 더한 값이고 p는 홀수이므로 N도 홀수이다.

이제 N은 p와 다른 소수를 약수로 갖는다는 것을 증명하자. 결론을 부정해서 N의 약수들 중 소수인 것은 p가 유일하다고 가정하면 적당한 자연수 m이 존재해서 $N=p^m$을 만족한다.

$a^{p-1}+a^{p-2}+\cdots+a^2+a+1\equiv 0\pmod p$ 이므로 양변에 $a-1$ 을 곱하면 $a^p\equiv 1\pmod p$ 에서 $a^p\equiv a\equiv 1\pmod p$ 를 얻는다. 따라서 적당한 정수 r이 존재해서 $a=pr+1$ 을 만족한다.

그리고 이항정리에 의하면 $f(0)=f'(0)=0$ 을 만족하는 적당한 정수계수 다항식 $f(x)$가 존재해서 다음 등식을 만족한다.

$$\begin{aligned} N=\ & a^{p-1}+a^{p-2}+\cdots+a^2+a+1 \\ & =(pr+1)^{p-1}+(pr+1)^{p-2}+\cdots+(pr+1)^2+(pr+1)+1 \\ & =f(p)+\left(\binom{p-1}{1}+\binom{p-2}{1}+\cdots+\binom{2}{1}+\binom{1}{1}\right)rp+p \\ & =f(p)+\frac{rp^2(p-1)}{2}+p \\ & =p^m \end{aligned} \tag{2}$$

$f(x)$는 $f(0)=f'(0)=0$ 을 만족하는 다항식이므로 $p^2\mid f(p)+\dfrac{rp^2(p-1)}{2}$ 이다.

따라서 (2)를 만족하려면 $m=1$ 이 되어야 한다. 만약 $m\geq 2$ 이면 $p^2\mid p^m$ 이므로 (2)에서 $p^2\mid p$ 를 얻는데 이것은 모순이다.

$m=1$ 이면 $N=p$ 인데 $q_1,q_2,\ldots,q_r$ 은 $2pk+1$ 형태를 갖는 소수이고 $2pk+1$ 이 소수이면 k는 자연수이므로 $2pk+1\geq 2p+1>p$ 이다. 따라서 $a=q_1q_2\cdots q_r>p$ 이므로 $N>p$ 인데 이것은 $N=p$ 에 모순이다.

그러므로 N은 p와 다른 소수를 약수로 갖고 N은 홀수이므로 p와 다른 홀수인 소수를 약수로 갖는다. 그것을 q라고 하면 Problem 3.1.9 (a)에 의해 적당한 $i=1,2,\ldots,r$ 가 존재해서 $q=q_i$ 를 만족한다.

그러면 $q\mid N$ 이고 $q\mid a$ 이므로 $q\mid 1$ 을 얻는데 이것은 q가 소수라는 것에 모순이다. 따라서 $2pk+1$ 형태를 갖는 소수의 개수는 무한하다. ■

3.2 소수 p의 원시근

작성자 : 네냐플(Nenyaffle)

3.2절과 3.3절에서는 자연수 n이 어떤 조건을 만족할 때 원시근을 갖는지 소개하려고 합니다. 3.2절에서는 소수의 원시근이 항상 존재한다는 것을 소개하는게 목표이고 3.3절에서는 원시근을 갖는 자연수가 어떤 자연수인지 소개하는게 목표입니다.

Lemma 3.2.1 p는 소수이고 d는 $d \mid p-1$ 을 만족하는 자연수이면 합동방정식 $x^d \equiv 1 \pmod p$ 은 법 p에서 정확히 d개의 해를 갖는다.

(증명)

조건에 의하면 $p-1$ 은 자연수이므로 적당한 자연수 k가 존재해서 $p-1=dk$ 를 만족한다. 이때 정수계수 다항식 $f(x)$가 다음과 같다고 하자.

$$f(x)=x^{d(k-1)}+x^{d(k-2)}+\cdots+x^{2d}+x^d+1$$

그러면 $x^{p-1}-1=(x^d-1)f(x)$ 가 성립한다. (3)

p가 소수이므로 페르마의 작은 정리에 의하면 $1,2,...,p-1$ 은 모두 합동방정식 $x^{p-1} \equiv 1 \pmod p$ 의 해가 되고 p는 소수이므로 (3)에 의하면 $1,2,...,p-1$ 은 모두 다음 2개의 합동방정식중 하나를 만족한다.

$$\begin{aligned} x^d &\equiv 1 \pmod p \\ f(x) &\equiv 0 \pmod p \end{aligned} \tag{4}$$

이제 (4)에 있는 합동방정식이 공통해를 갖지 않음을 보이자. 결론을 부정해서 공통해를 갖는다고 가정하고 그것을 a라고 하면 $a^d \equiv 1 \pmod p$ 이고 $f(a) \equiv 0 \pmod p$ 이므로 $f(a) \equiv k \equiv 0 \pmod p$ 를 얻는다.

따라서 $p \mid k$ 이고 $p-1=dk$ 이므로 $k \mid p-1$ 에서 $p \mid p-1$ 을 얻는데 이것은 p가 소수라는 조건에 모순이다. 그러므로 (4)에 있는 합동방정식은 공통해를 갖지 않는다. (5)

한편 라그랑주의 정리에 의하면 합동방정식 $x^d \equiv 1 \pmod p$ 은 법 p에서 d개 이하의 해를 갖고 합동방정식 $f(x) \equiv 0 \pmod p$ 은 법 p에서 $d(k-1)$개 이하의 해를 갖는다.

따라서 (5)에 의하면 합동방정식 $x^{p-1} \equiv 1 \pmod p$ 은 법 p에서 $d+d(k-1)=dk=p-1$개 이하의 해를 갖는데 $1,2,...,p-1$ 은 모두 합동방정식 $x^{p-1} \equiv 1 \pmod p$ 의 해 이므로 법 p에서 정확히 $p-1$개의 해를 갖는다.

그러므로 합동방정식 $x^d \equiv 1 \pmod p$ 은 법 p에서 정확히 d개의 해를 가져야 하고 합동방정식 $f(x) \equiv 0 \pmod p$ 은 법 p에서 정확히 $d(k-1)$개의 해를 가져야 한다.

만약 둘중 적어도 하나의 합동방정식이 해를 d개 또는 $d(k-1)$개보다 적게 가지면 합동방정식 $x^{p-1} \equiv 1 \pmod p$ 은 법 p에서 $p-2$개 이하의 해를 가져서 모순이다. ■

Lemma 3.2.2 자연수 n에 대하여 다음이 성립한다.

(a). 음이 아닌 n개의 실수 $a_1,a_2,...,a_n$ 에 대하여 $\sum_{k=1}^{n} a_k = 0$ 이면

$a_1 = a_2 = \cdots = a_n = 0$ 이다.

(b). $2n$개의 실수 $a_1,a_2,...,a_n,b_1,b_2,...,b_n$ 가 모든 $k = 1,2,...,n$ 에 대하여

$a_k \geq b_k$ 를 만족할 때 $\sum_{k=1}^{n} a_k = \sum_{k=1}^{n} b_k$ 이면 모든 $k = 1,2,...,n$ 에 대하여

$a_k = b_k$ 이다.

(증명)

(a). 결론을 부정해서 적당한 자연수 i에 대하여 $a_i \neq 0$ 이라고 가정하자.

그러면 $a_i > 0$ 이므로 $0 = \sum_{k=1}^{n} a_k \geq a_i > 0$ 인데 이것은 모순이다.

따라서 $a_1 = a_2 = \cdots = a_n = 0$ 이다. ■

(b). $c_n = a_n - b_n$ 라고 하자. 그러면 조건에 의해 모든 $k = 1,2,...,n$ 에 대하여

$c_k \geq 0$ 이고 $\sum_{k=1}^{n} c_k = 0$ 이므로 (a)에 의하면 모든 $k = 1,2,...,n$ 에 대하여 $c_k = 0$

이다. 따라서 모든 $k = 1,2,...,n$ 에 대하여 $a_k = b_k$ 이다. ■

Lemma 3.2.1, Lemma 3.2.2를 사용해서 다음 정리를 증명할수 있는데 다음 정리는 소수의 원시근이 항상 존재한다는 사실을 증명할 때 강력한 도구가 됩니다.

Theorem 3.2.1 p가 소수일 때 $d \mid p-1$ 을 만족하는 모든 자연수 d에 대하여 법 p에서 위수가 d인 정수는 항상 존재하고 $\mathbb{Z}_p^{\times}$에 $\phi(d)$개 있다.

(증명)

$\psi(d)$를 법 p에서 위수가 d인 정수들 중 $\mathbb{Z}_p^{\times} = \{1,2,...,p-1\}$에 있는 정수의 개수라고 정의하자. 그러면 $\mathbb{Z}_p^{\times}$에 있는 모든 정수는 $p-1$ 의 약수를 위수로 가지므로

$p-1 = \sum_{d \mid p-1} \psi(d)$ 가 성립한다. 그리고 가우스의 정리에 의하면 $p-1 = \sum_{d \mid p-1} \phi(d)$

이므로 정리하면 $\sum_{d \mid p-1} \psi(d) = \sum_{d \mid p-1} \phi(d)$ 를 얻는다.

이제 $p-1$ 의 모든 양의 약수 d에 대하여 $\psi(d) \leq \phi(d)$ 임을 보이자.

만약 $\psi(d) = 0$ 이면 $\psi(d) \leq \phi(d)$ 임은 명백하다. 따라서 $\psi(d) > 0$ 을 가정하자.

그러면 위수가 d인 정수가 존재한다. 그것을 $a \in \mathbb{Z}_p^{\times}$ 라고 하면 법 p에서 a의 위수가 d이므로 $a, a^2, a^3, ..., a^d$ 는 법 p에서 서로 합동이 아니다.

법 p에서 a의 위수가 d이므로 각각의 $k=1,2,...,d$ 에 대하여 $(a^k)^d \equiv (a^d)^k \equiv 1 \pmod p$ 를 만족한다. 따라서 d개의 정수 $a,a^2,a^3,...,a^d$ 는 합동방정식 $x^d \equiv 1 \pmod p$ 의 해가 된다.

Lemma 3.2.1에 의하면 합동방정식 $x^d \equiv 1 \pmod p$ 은 법 p에서 정확히 d개의 해를 가지므로 $a,a^2,a^3,...,a^d$ 가 법 p에서 합동방정식 $x^d \equiv 1 \pmod p$ 의 해를 모두 모은 것이 된다.

법 p에서 위수가 d인 모든 정수는 합동방정식 $x^d \equiv 1 \pmod p$ 을 만족한다. 따라서 위수가 d인 정수는 $a,a^2,a^3,...,a^d$ 중 하나와 합동이다.

각각의 $k=1,2,...,d$ 에 대하여 $\mathrm{ord}_p(a^k)=\dfrac{d}{\gcd(d,k)}$ 이므로 $a,a^2,a^3,...,a^d$ 중 위수가 d인 정수의 개수는 $\gcd(d,k)=1$ 을 만족하는 d 이하의 자연수의 개수와 같고 그 개수는 $\phi(d)$이다. 따라서 $\psi(d)=\phi(d)$ 가 성립한다.

그러므로 $p-1$ 의 모든 양의 약수 d에 대하여 $\psi(d) \le \phi(d)$ 이고 $\sum_{d \mid p-1} \psi(d)=\sum_{d \mid p-1} \phi(d)$ 이므로 Lemma 3.2.2에 의하면 $p-1$ 의 모든 양의 약수 d에 대하여 $\psi(d)=\phi(d)$ 가 성립한다. 따라서 위수가 d인 정수는 $\mathbb{Z}_p^{\times}$에 $\phi(d)$개 있다. ■

p가 소수일 때 법 p의 원시근은 위수가 $\phi(p)=p-1$ 인 정수입니다. 따라서 다음을 얻을수 있습니다. Theorem 3.2.1의 Corollary이긴 한데 3.2절에서 제일 중요한 정리입니다.

Corollary 3.2.1 p가 소수이면 법 p의 원시근은 항상 존재하고 $\mathbb{Z}_p^{\times}$에 $\phi(p-1)$개 있다.

(증명)
Theorem 3.2.1에서 $d=p-1$ 인 경우이다. ■

p가 소수이면 $\phi(\phi(p))=\phi(p-1)$ 이므로 Corollary 3.2.1과 Theorem 3.1.4는 뭐가 다른지 헷갈릴수 있는데 Theorem 3.1.4는 법 n의 원시근이 존재한다는 것을 가정했을 때 원시근이 $\mathbb{Z}_n^{\times}$에 $\phi(\phi(n))$개 있다는 정리이고 Corollary 3.2.1은 p가 소수일 때 법 p의 원시근의 존재성까지 보장해주는 정리입니다.

Theorem 3.2.1을 이용하면 소수 p가 $p \equiv 1 \pmod 4$ 를 만족할 때 합동방정식 $x^2 \equiv -1 \pmod p$ 의 해가 존재한다는 것을 보일수 있습니다. $4 \mid p-1$ 이므로 Theorem 3.2.1에 의하면 법 p에서 위수가 4인 정수 a가 존재합니다.

따라서 $a^4 \equiv 1 \pmod p$ 이고 p는 소수이므로 $a^2 \equiv \pm 1 \pmod p$ 인데 $\mathrm{ord}_p(a)=4$ 이므로 $a^2 \equiv -1 \pmod p$ 가 되어야 합니다. 그러므로 합동방정식 $x^2 \equiv -1 \pmod p$ 의 해가 존재합니다.

p가 소수이면 법 p의 원시근이 항상 존재하는데 법 p의 원시근을 실제로 구하는 것은 복잡하고 어려운 일입니다. Problem 3.1.6을 이용하면 계산량을 줄일 방법이 있는데 이 방법도 숫자가 커지면 불편한건 마찬가지입니다.

$p=2$ 이면 모든 홀수는 법 p의 원시근이므로 p가 홀수인 소수라고 가정하면 $p-1 \geq 2$ 입니다. 따라서 $p-1$ 을 소인수분해한 결과를 $p-1=p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ 라고 할 때 Theorem 3.2.1에 의하면 각각의 $i=1,2,...,r$ 에 대하여 $\mathrm{ord}_p(a_i)=p_i^{k_i}$ 를 만족하는 정수 a_i는 존재합니다.

이때 $a=a_1a_2\cdots a_r$ 라고 하면 Problem 3.1.6과 수학적 귀납법에 의해 $\mathrm{ord}_p(a)=p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}=p-1$ 을 만족합니다. 따라서 a는 법 p의 원시근입니다.

예를 들어 $p=23$ 이면 $p-1=22=2\times 11$ 인데 법 23에서 위수가 2인 정수는 -1이고 위수가 11인 정수는 2이므로 법 23의 한 원시근은 -2입니다.

200보다 작은 소수의 원시근 중 가장 작은 자연수 원시근을 나열하면 다음과 같다고 합니다.

소수	최소의 양의 원시근	소수	최소의 양의 원시근
2	1	89	3
3	2	97	5
5	2	101	2
7	3	103	5
11	2	107	2
13	2	109	6
17	3	113	3
19	2	127	3
23	5	131	2
29	2	137	3
31	3	139	2
37	2	149	2
41	6	151	6
43	3	157	5
47	5	163	2
53	2	167	5
59	2	173	2
61	2	179	2
67	2	181	2
71	7	191	19
73	5	193	5
79	3	197	2
83	2	199	3

1927년에 수학자 에밀 아틴(Emil Artin)이 a가 -1도 아니고 제곱수도 아닐 때 a를 원시근으로 갖는 소수의 개수는 무한하다는 추측을 제시했는데 아직 완벽하게 풀리지 않은 문제라고 합니다.

a가 제곱수이면 a를 원시근으로 갖는 홀수인 소수는 존재하지 않습니다. 적당한 정수 b에 대하여 $a=b^2$ 을 만족한다고 하고 $\gcd(a,p)=1$ 을 만족하는 홀수인 소수 p를 임의로 하나 택하면 $\gcd(b,p)=1$ 임은 명백합니다.

따라서 페르마의 작은 정리에 의하면 $a^{\frac{p-1}{2}} \equiv \left(b^2\right)^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \pmod p$ 이므로 $\mathrm{ord}_p(a) \leq \frac{p-1}{2} < p-1 = \phi(p)$ 입니다. 그러므로 a를 원시근으로 갖는 홀수인 소수 p는 존재하지 않습니다.

그리고 모든 소수 p에 대하여 $(-1)^2 \equiv 1 \pmod p$ 이므로 $\mathrm{ord}_p(-1) \leq 2$ 입니다. 따라서 $p \geq 5$ 이면 $\mathrm{ord}_p(-1) \leq 2 < p-1 = \phi(p)$ 이므로 -1을 원시근으로 갖는 소수의 후보는 $p=2,3$ 이고 실제로 $p=2,3$ 이면 -1은 법 p의 원시근이 됩니다.

마지막으로 2.2절에서 증명하지 않았던 Korselt의 판정법을 증명하겠습니다.
Korselt의 판정법을 증명하려면 소수 p가 원시근을 갖는다는 사실을 알고 있아야 해서 원시근을 소개하지 않았던 2.2절에서는 증명할수 없었습니다.

Theorem 3.2.2 Korselt의 판정법(Korselt's Criterion)
합성수 n이 카마이클 수가 될 필요충분조건은 다음을 만족하는 것이다.

(a). n은 제곱인수가 없는 정수이다.
(b). $p \mid n$ 을 만족하는 모든 소수 p에 대하여 $p-1 \mid n-1$ 이다.

(증명)
$(\Longrightarrow)$ 합성수 n이 카마이클 수라고 하자. 그러면 $\gcd(a,n)=1$ 을 만족하는 임의의 정수 a에 대하여 $a^n \equiv a \pmod n$ 을 만족하고 $\gcd(a,n)=1$ 이므로 양변에 법 n에서 a의 곱셈에 대한 역원을 곱하면 $a^{n-1} \equiv 1 \pmod n$ 을 얻는다.

먼저 (a)를 증명하자. n의 한 소인수를 p라고 하면 적당한 자연수 k와 $\gcd(m,p)=1$ 을 만족하는 적당한 자연수 m이 존재해서 $n=p^k m$ 을 만족하고 중국인의 나머지 정리에 의하면 다음을 만족하는 정수 a가 법 n에서 유일하게 존재한다.

$$a \equiv 1+p \pmod{p^k}$$
$$a \equiv 1 \pmod m$$

그러면 $a \equiv 1 \pmod p$, $a \equiv 1 \pmod m$ 이므로 $\gcd(a,p)=\gcd(a,m)=1$ 이고 따라서 $\gcd(a,p^k m)=1$ 이다. 즉, $\gcd(a,n)=1$ 이고 n은 카마이클 수 이므로 $a^{n-1} \equiv 1 \pmod n$ 을 만족한다.

이제 결론을 부정해서 $k \geq 2$ 라고 가정하자. 그러면 $p^2 \mid p^k$ 이므로 다음을 얻는다.

$$a^{n-1} \equiv (1+p)^{n-1} \equiv 1 \pmod{p^2}$$

따라서 이항정리에 의하면 다음을 얻을수 있다.

$$(1+p)^{n-1} \equiv 1+(n-1)p \equiv 1 \pmod{p^2}$$

그러므로 $(n-1)p \equiv 0 \pmod{p^2}$ 이고 $n = p^k m$ 이므로 $p \equiv 0 \pmod{p^2}$ 인데 이것은 모순이다. 따라서 $k=1$ 이어야 한다. 그러므로 n은 제곱인수가 없는 정수이다.

이제 (b)를 증명하자. $p \mid n$ 을 만족하는 소수 p를 임의로 하나 택하면 (a)가 성립함을 이미 증명했으므로 $p^2 \nmid n$ 을 만족해야 한다. 따라서 $\gcd\left(p, \frac{n}{p}\right)=1$ 이다. 그리고 p는 소수이므로 법 p의 원시근이 존재한다. 법 p의 원시근을 b라고 하자.

그러면 중국인의 나머지 정리에 의해 다음을 만족하는 정수 a가 법 n에서 유일하게 존재한다.

$$a \equiv b \pmod{p}$$
$$a \equiv 1 \pmod{\frac{n}{p}}$$

b는 법 p의 원시근이므로 $\gcd(b,p)=1$ 이고 $a \equiv b \pmod{p}$ 이므로 $\gcd(a,p)=1$ 이다. 그리고 $\gcd\left(a, \frac{n}{p}\right)=1$ 이므로 $\gcd(a,n)=1$ 을 만족하고 n은 카마이클 수 이므로 $a^{n-1} \equiv 1 \pmod{n}$ 을 만족한다.

따라서 $a^{n-1} \equiv b^{n-1} \equiv 1 \pmod{p}$ 인데 $\mathrm{ord}_p(b)=\phi(p)=p-1$ 이므로 $p-1 \mid n-1$ 을 만족해야 한다. 그러므로 (b)가 성립한다.

$(\Leftarrow)$ 조건에 의하면 n은 제곱인수가 없는 합성수이므로 소인수분해한 결과가 $n = p_1 p_2 \cdots p_r$ 형태로 나타난다. 이제 $\gcd(a,n)=1$ 을 만족하는 임의의 정수 a를 택하자. 그러면 각각의 $i=1,2,...,r$ 에 대하여 $\gcd(a,p_i)=1$ 을 만족한다.

따라서 페르마의 작은 정리에 의하면 $a^{p_i-1} \equiv 1 \pmod{p_i}$ 이고 (b)에 의하면 $p_i-1 \mid n-1$ 이므로 $a^{n-1} \equiv 1 \pmod{p_i}$ 를 만족한다. 그리고 $n = p_1 p_2 \cdots p_r$ 이므로 $a^{n-1} \equiv 1 \pmod{n}$ 을 만족한다.

양변에 a를 곱하면 $a^n \equiv a \pmod{n}$ 을 얻는다. 따라서 n은 카마이클 수이다. ■

Problem 3.2.1 p는 홀수인 소수이고 r은 법 p의 원시근일 때 다음을 증명하시오.

(a). $r^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ 이다.

(b). r'이 법 p에서 r과 다른 법 p의 원시근이면 rr'은 법 p의 원시근이 아니다.

(c). 정수 r'이 $rr' \equiv 1 \pmod{p}$ 를 만족하면 r'도 법 p의 원시근이다.

(증명)

(a). p가 홀수인 소수이므로 $\frac{p-1}{2}$ 는 자연수이고 $r^{p-1} \equiv 1 \pmod{p}$ 이므로

$\left(r^{\frac{p-1}{2}}\right)^2 \equiv 1 \pmod{p}$ 를 만족한다. 그리고 p가 소수이므로 $r^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$

인데 r은 법 p의 원시근이므로 $r^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ 가 되어야 한다. ■

(b). (a)에 의하면 $r^{\frac{p-1}{2}} \equiv (r')^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ 을 만족한다.

따라서 $(rr')^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ 이므로 $\mathrm{ord}_p(rr') \leq \frac{p-1}{2} < p-1 = \phi(p)$ 이다.

그러므로 rr'은 법 p의 원시근이 될수 없다. ■

(c). 조건에 의하면 $\mathrm{ord}_p(r') = \mathrm{ord}_p(r) = \phi(p) = p-1$ 이므로

r'은 법 p의 원시근이다. ■

Problem 3.2.2 다음 물음에 답하시오.

(a). p가 홀수인 소수일 때 법 p의 원시근이 존재한다는 사실을 이용해서

$(p-1)! \equiv -1 \pmod{p}$ 임을 증명하시오.

(b). p가 $p \equiv 1 \pmod{4}$ 를 만족하는 소수이면 법 p의 원시근을 r이라고 할 때

$r^{\frac{p-1}{4}}$ 는 합동방정식 $x^2 \equiv -1 \pmod{p}$ 의 해가 된다는 것을 증명하시오.

(증명)

(a). 법 p의 원시근을 r이라고 하자. 그러면 $\{r, r^2, r^3, \ldots, r^{p-1}\}$은 법 p에 대한 기약잉여계이고 기약잉여계의 원소를 모두 곱하면 다음을 얻는다.

$$r^{1+2+\cdots+(p-1)} = r^{\frac{p(p-1)}{2}}$$

p는 홀수인 소수이므로 Problem 3.2.1 (a)에 의하면 다음을 얻는다.

$$r^{\frac{p(p-1)}{2}} \equiv \left(r^{\frac{p-1}{2}}\right)^p \equiv (-1)^p \equiv -1 \pmod{p}$$

따라서 $(p-1)! \equiv r^{\frac{p(p-1)}{2}} \equiv -1 \pmod{p}$ 가 성립한다. ■

(b). 조건에 의하면 p는 홀수인 소수이고 $\frac{p-1}{4}$ 는 자연수이다. 따라서 Problem 3.2.1 (a)에 의하면 다음을 얻는다.

$$\left(r^{\frac{p-1}{4}}\right)^2 \equiv r^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

그러므로 $r^{\frac{p-1}{4}}$ 는 합동방정식 $x^2 \equiv -1 \pmod{p}$ 의 해가 된다. ■

Problem 3.2.3 p는 홀수인 소수이고 r은 법 p의 원시근일 때 다음을 증명하시오.
(a). $p \equiv 1 \pmod 4$ 이면 $\mathrm{ord}_p(-r) = p-1 = \phi(p)$ 이다.
즉, $-r$도 법 p의 원시근이다.
(b). $p \equiv 3 \pmod 4$ 이면 $\mathrm{ord}_p(-r) = \dfrac{p-1}{2}$ 이다.

(증명)
편의상 $k = \mathrm{ord}_p(-r)$ 라고 하자.

(a). $p-1$ 은 짝수이므로 $(-r)^{p-1} \equiv r^{p-1} \equiv 1 \pmod p$ 를 만족한다.
따라서 $k \mid p-1$ 이므로 $k \le p-1$ 가 성립한다.

그리고 $(-r)^k \equiv (-1)^k r^k \equiv 1 \pmod p$ 이므로 $(-r)^{2k} \equiv r^{2k} \equiv 1 \pmod p$
를 만족한다. 따라서 $p-1 \mid 2k$ 인데 조건에 의하면 $4 \mid p-1$ 이므로 $4 \mid 2k$ 이다.
즉, $2 \mid k$ 이므로 k는 짝수이다.

따라서 $(-r)^k \equiv (-1)^k r^k \equiv r^k \equiv 1 \pmod p$ 이므로 $p-1 \mid k$ 를 만족하고
$p-1 \le k$ 가 성립한다. 그러므로 $k = p-1$ 이다. 즉, $-r$은 법 p의 원시근이다. ■

(b). 조건에 의하면 $\dfrac{p-1}{2}$ 는 홀수이므로 Problem 3.2.1 (a)에 의하면 다음을 만족한다.

$$(-r)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} r^{\frac{p-1}{2}} \equiv 1 \pmod p$$

따라서 $k \mid \dfrac{p-1}{2}$ 이므로 $k \le \dfrac{p-1}{2}$ 가 성립한다.

그리고 $(-r)^k \equiv (-1)^k r^k \equiv 1 \pmod p$ 이므로 $(-r)^{2k} \equiv r^{2k} \equiv 1 \pmod p$
를 만족한다. 따라서 $p-1 \mid 2k$ 이고 $p-1$ 은 짝수이므로 $\dfrac{p-1}{2} \mid k$ 를 만족한다.
그러므로 $\dfrac{p-1}{2} \le k$ 가 성립하고 정리하면 $k = \dfrac{p-1}{2}$ 를 얻는다. ■

Problem 3.2.4 p가 홀수인 소수일 때 $\mathbb{Z}_p^{\times}$에 있는 $\phi(p-1)$개의 법 p의 원시근을 모두 곱한 것은 법 p에서 $(-1)^{\phi(p-1)}$과 합동임을 증명하시오.

(증명)
법 p의 원시근을 r이라고 하면 $\{r, r^2, r^3, \ldots, r^{p-1}\}$은 법 p에 대한 기약잉여계이다.
그리고 r^k가 법 p의 원시근이 될 필요충분조건은 $\gcd(k, p-1) = 1$ 을 만족하는 것이다.
따라서 1부터 $p-1$까지의 자연수 중 $p-1$과 서로소인 자연수를 각각 $k_1, k_2, \ldots, k_{\phi(p-1)}$
라고 하면 법 p의 원시근을 모두 모은 것은 $r^{k_1}, r^{k_2}, \ldots, r^{k_{\phi(p-1)}}$ 이다.

$p-1 \geq 2$ 이므로 Problem 2.1.9에 의해 다음을 얻는다.

$$k_1 + k_2 + \cdots + k_{\phi(p-1)} = \frac{(p-1)\phi(p-1)}{2}$$

그리고 r은 법 p의 원시근이므로 Problem 3.2.1 (a)에 의하면 $r^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ 이다. 따라서 다음을 얻을수 있다.

$$r^{k_1} r^{k_2} \cdots r^{k_{\phi(p-1)}} \equiv r^{k_1 + k_2 + \cdots + k_{\phi(p-1)}} \equiv r^{\frac{(p-1)\phi(p-1)}{2}} \equiv (-1)^{\phi(p-1)} \pmod{p}$$

■

Problem 3.2.5 p가 홀수인 소수일 때 모든 자연수 n에 대하여 다음이 성립함을 증명하시오.

$$1^n + 2^n + \cdots + (p-1)^n \equiv \begin{cases} 0 & (p-1 \nmid n) \\ -1 & (p-1 \mid n) \end{cases} \pmod{p}$$

(증명)

case1) $p-1 \mid n$

$a \in \mathbb{Z}_p^{\times}$ 이면 페르마의 작은 정리에 의해 $a^{p-1} \equiv 1 \pmod{p}$ 이고 $p-1 \mid n$ 이므로 $a^n \equiv 1 \pmod{p}$ 를 얻는다. 따라서 다음이 성립한다.

$$1^n + 2^n + \cdots + (p-1)^n \equiv p-1 \equiv -1 \pmod{p}$$

case2) $p-1 \nmid n$

법 p의 원시근을 r이라고 하자. 그러면 $r^{p-1} \equiv 1 \pmod{p}$ 이므로 $\{1, r, r^2, \ldots, r^{p-2}\}$ 는 법 p에 대한 기약잉여계가 된다. 따라서 다음이 성립한다.

$$1^n + 2^n + \cdots + (p-1)^n \equiv 1 + r^n + r^{2n} + \cdots + r^{(p-2)n} \pmod{p}$$

그리고 등비수열의 합 공식에 의하면 다음을 얻는다.

$$1 + r^n + r^{2n} + \cdots + r^{(p-2)n} = \frac{r^{(p-1)n} - 1}{r^n - 1}$$

한편 $r^{p-1} \equiv 1 \pmod{p}$ 이므로 $r^{(p-1)n} \equiv 1 \pmod{p}$ 이다. 그러므로 $r^{(p-1)n} - 1 \equiv 0 \pmod{p}$ 이다. 이제 $\gcd(r^n - 1, p) = 1$ 임을 보이자.

만약 $\gcd(r^n - 1, p) \neq 1$ 이면 p는 소수이므로 $r^n \equiv 1 \pmod{p}$ 를 만족하고 r은 법 p의 원시근이므로 $p-1 \mid n$ 을 만족하는데 이것은 $p-1 \nmid n$ 에 모순이다. 따라서 $\gcd(r^n - 1, p) = 1$ 이다.

그러므로 $r^{(p-1)n} - 1 \equiv 0 \pmod{p}$ 의 양변을 $r^n - 1$ 로 나눌수 있고 나누면 $1 + r^n + r^{2n} + \cdots + r^{(p-2)n} \equiv \frac{r^{(p-1)n} - 1}{r^n - 1} \equiv 0 \pmod{p}$ 를 얻는다.

따라서 $1^n + 2^n + \cdots + (p-1)^n \equiv 0 \pmod{p}$ 이다. ■

3.3 원시근을 갖는 자연수

작성자 : 네냐플(Nenyaffle)

3.2절에서 모든 소수는 원시근을 갖는다는 것을 증명했습니다. 그런데 소수가 아니어도 원시근을 가질수 있습니다. 예를 들어 $n=9$ 일 때 $\phi(9)=6$ 이고

$$2^1 \equiv 2 \pmod 9$$
$$2^2 \equiv 4 \pmod 9$$
$$2^3 \equiv 8 \pmod 9$$
$$2^6 \equiv 1 \pmod 9$$

이므로 2는 법 9의 원시근입니다. 9는 소수가 아니지만 원시근이 존재합니다.
3.3절에서는 원시근을 갖는 자연수가 어떤 자연수인지 소개하는게 목표입니다.

Theorem 3.3.1 $n \geq 3$ 을 만족하는 자연수 n이 임의로 주어져있다고 하자. 그러면 모든 홀수 a에 대하여 $a^{2^{n-2}} \equiv 1 \pmod{2^n}$ 을 만족한다. 따라서 $n \geq 3$ 이면 모든 홀수 a에 대하여 $\mathrm{ord}_{2^n}(a) \leq 2^{n-2} < 2^{n-1} = \phi(2^n)$ 이므로 2^n은 원시근을 가질수 없다.

(증명)

홀수 a를 임의로 하나 택하고 집합 S 를 $S=\{n \in \mathbb{N} : a^{2^n} \equiv 1 \pmod{2^{n+2}}\}$ 라고 하자. 만약 $S=\mathbb{N}$ 이면 모든 자연수 n에 대하여 $a^{2^n} \equiv 1 \pmod{2^{n+2}}$ 를 만족하므로 $n \geq 3$ 이면 $a^{2^{n-2}} \equiv 1 \pmod{2^n}$ 을 만족한다는 것이 증명된다.

먼저 a가 홀수일 때 $a^2 \equiv 1 \pmod 8$ 임을 보이자. a가 홀수이므로 적당한 정수 k에 대하여 $a=2k+1$ 을 만족하고 따라서 다음을 얻는다.

$$a^2-1=(2k+1)^2-1=4k(k+1)$$

$k, k+1$ 은 연속한 정수이므로 $k(k+1)$은 짝수이다. 따라서 $8 \mid 4k(k+1)=a^2-1$ 이므로 $a^2 \equiv 1 \pmod 8$ 이 성립한다. 그러므로 $1 \in S$ 이다.

이제 임의의 자연수 n에 대하여 $n \in S$ 라고 가정하자. 그러면 $a^{2^n} \equiv 1 \pmod{2^{n+2}}$ 이므로 적당한 정수 b가 존재해서 $a^{2^n}=1+2^{n+2}b$ 를 만족한다. 따라서 다음을 얻는다.

$$\begin{aligned} a^{2^{n+1}} &= \left(a^{2^n}\right)^2 \\ &= \left(1+2^{n+2}b\right)^2 \\ &= 1+2^{n+3}b+2^{2n+4}b^2 \end{aligned}$$

n은 자연수이므로 $2n+4 \geq n+3$ 이다. 따라서 $2^{n+3} \mid 2^{2n+4}$ 이므로 다음을 얻는다.

$$a^{2^{n+1}} \equiv 1 \pmod{2^{n+3}}$$

그러므로 $n+1 \in S$ 이고 수학적 귀납법에 의하면 $S=\mathbb{N}$ 이다. 따라서 모든 자연수 n에 대하여 $a^{2^n} \equiv 1 \pmod{2^{n+2}}$ 가 성립하므로 $n \geq 3$ 을 만족하는 모든 자연수 n에 대하여 $a^{2^{n-2}} \equiv 1 \pmod{2^n}$ 가 성립한다. ■

Theorem 3.3.2 자연수 m, n이 $m \geq 3, n \geq 3, \gcd(m,n)=1$ 을 만족하면 mn은 원시근을 가질수 없다.

(증명)

$d=\gcd(\phi(m),\phi(n))$ 라고 하자. 그러면 m, n은 3 이상의 자연수이므로 $\phi(m), \phi(n)$은 모두 짝수이다. 따라서 $d \geq 2$ 이다.

그러므로 $h=\frac{\phi(m)\phi(n)}{d}$ 라고 하면 $\gcd(m,n)=1$ 이고 $d \geq 2$ 이므로 $h=\frac{\phi(mn)}{d} \leq \frac{\phi(mn)}{2}$ 를 만족한다. 이제 $\gcd(a,mn)=1$ 을 만족하는 모든 정수 a에 대하여 $a^h \equiv 1 \pmod{mn}$ 임을 보이자.

$\gcd(a,mn)=1$ 과 $\gcd(a,m)=\gcd(a,n)=1$ 은 동치이다. 따라서 오일러의 정리에 의하면 다음 합동식이 성립한다.

$$a^{\phi(m)} \equiv 1 \pmod{m}$$
$$a^{\phi(n)} \equiv 1 \pmod{n}$$

그리고 $h=\frac{\phi(m)\phi(n)}{d}$ 이므로 다음을 얻을수 있고

$$a^h \equiv 1 \pmod{m}$$
$$a^h \equiv 1 \pmod{n}$$

$\gcd(m,n)=1$ 이므로 $a^h \equiv 1 \pmod{mn}$ 을 얻는다.

따라서 $\mathrm{ord}_{mn}(a) \leq h \leq \frac{\phi(mn)}{2} < \phi(mn)$ 이므로 mn은 원시근을 가질수 없다. ■

Theorem 3.3.1, Theorem 3.3.2에 의하면 원시근을 가질수 있는 자연수의 후보를 줄일수 있습니다. $n \geq 2$ 이면 n은 소수의 곱으로 표현되는데 만약 n이 홀수인 소인수를 2개 이상 가지면 $a \geq 3, b \geq 3, \gcd(a,b)=1$ 를 만족하는 적당한 자연수 a, b가 존재해서 $n=ab$ 를 만족하므로 Theorem 3.3.2에 의하면 n은 원시근을 가질수 없습니다.

그러므로 n이 원시근을 가지려면 홀수인 소인수의 개수는 1개 이하가 되어야 합니다. 따라서 가능한 경우는 자연수 m, k와 홀수인 소수 p에 대하여 $n=2^m$ 또는 $n=2^m p^k$ 인데 만약 $m \geq 3$ 이면 Theorem 3.3.1에 의해 $n=2^m$ 은 원시근을 가질수 없습니다.

$n=2^m p^k$ 인 경우 만약 $m \geq 2$ 이면 $2^m \geq 4$ 이고 $p^k \geq 3$ 인데 $\gcd(2^m,p^k)=1$ 이므로 Theorem 3.3.2에 의해 $n=2^m p^k$ 은 원시근을 가질수 없습니다.

그러므로 $n \geq 2$ 일 때 홀수인 소수 p와 자연수 k에 대하여 $n=2, 4, p^k, 2p^k$ 이런 형태로 표현되지 않는 자연수 n은 원시근을 가질수 없습니다. 이제 $n=2, 4, p^k, 2p^k$ 이런 형태로 표현되는 자연수는 원시근을 갖는다는 것을 증명하겠습니다.

$n=2,4$ 일 때 원시근이 존재함은 명백합니다. $n=2$ 일땐 1이 원시근이고 $n=4$ 일땐 3이 원시근입니다. 따라서 $n=p^k$ 또는 $n=2p^k$ 로 표현될 때 원시근을 갖는다는 것을 증명하면 충분합니다.

Lemma 3.3.1 p가 홀수인 소수이면 $r^{p-1}\not\equiv 1 \pmod{p^2}$ 을 만족하는 법 p의 원시근 r이 존재한다.

(증명)

p는 소수이므로 원시근을 갖는다. 한 원시근을 r이라고 하자. 만약 $r^{p-1}\not\equiv 1 \pmod{p^2}$ 을 만족하면 정리는 증명된다. 따라서 $r^{p-1}\equiv 1 \pmod{p^2}$ 을 만족한다고 가정하자.

이때 $r'=r+p$ 라고 하면 $r'\equiv r \pmod{p}$ 이므로 r'도 법 p의 원시근이고 이항정리에 의하면 $r^{p-1}\equiv 1 \pmod{p^2}$ 이므로 다음을 얻는다.

$$(r')^{p-1}\equiv r^{p-1}+(p-1)pr^{p-2}\equiv 1-pr^{p-2} \pmod{p^2}$$

r은 법 p의 원시근이므로 $\gcd(r,p)=1$ 이다. 따라서 $\gcd(r^{p-2},p)=1$ 이므로 $p\nmid r^{p-2}$ 에서 $p^2\nmid pr^{p-2}$ 를 얻는다. 그러므로 $(r')^{p-1}\not\equiv 1 \pmod{p^2}$ 이다.

따라서 r'은 정리를 만족하는 법 p의 원시근이다. ■

Theorem 3.3.3 p가 홀수인 소수이면 p^2은 원시근을 갖는다. 구체적으로는 r이 법 p의 원시근일 때 r과 $r+p$ 둘중 적어도 하나는 법 p^2의 원시근이다.

(증명)

$\mathrm{ord}_{p^2}(r)=n$ 라고 하자. 그러면 $n\mid\phi(p^2)=p(p-1)$ 이고 $r^n\equiv 1 \pmod{p^2}$ 에서 $r^n\equiv 1 \pmod{p}$ 를 만족한다. 그리고 $\mathrm{ord}_p(r)=p-1$ 이므로 $p-1\mid n$ 이다.

따라서 $p-1\mid n$ 이고 $n\mid p(p-1)$ 인데 p는 소수이므로 $n=p-1$ 또는 $n=p(p-1)$ 이다. $n=p(p-1)$ 이면 r은 법 p^2의 원시근이므로 정리가 증명되고 $n=p-1$ 이면 Lemma 3.3.1의 증명과정에 의해 $(r+p)^{p-1}\not\equiv 1 \pmod{p^2}$ 을 만족한다.

$r+p$도 법 p의 원시근이므로 같은 방법으로 $\mathrm{ord}_{p^2}(r+p)=p-1$ 또는 $\mathrm{ord}_{p^2}(r+p)=p(p-1)$ 임을 보일수 있는데 $(r+p)^{p-1}\not\equiv 1 \pmod{p^2}$ 이므로 $\mathrm{ord}_{p^2}(r+p)=p(p-1)=\phi(p^2)$ 이다. 따라서 $r+p$는 법 p^2의 원시근이다. ■

법 p^2의 원시근이 존재한다는 것은 Lemma 3.3.1을 가지고 Theorem 3.3.3을 증명하는 방식으로 증명됩니다. 일반적으로 $k\geq 2$ 일 때 법 p^k의 원시근이 존재한다는 것도 비슷하게 증명하는 편입니다. 이때는 수학적 귀납법을 사용하게 됩니다.

Lemma 3.3.2 p가 홀수인 소수이고 r은 $r^{p-1} \not\equiv 1 \pmod{p^2}$ 을 만족하는 법 p의 원시근이면 $k \geq 2$ 를 만족하는 모든 자연수 k에 대하여 다음을 만족한다.

$$r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$$

(증명)

수학적 귀납법을 사용하자. 조건에 의하면 $k=2$ 일 때 $r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$가 성립한다. 이제 $k \geq 2$ 를 만족하는 모든 자연수 k에 대하여 $r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$가 성립한다고 가정하자.

r은 법 p의 원시근이므로 $\gcd(r,p^{k-1})=1$ 을 만족한다. 따라서 오일러의 정리에 의하면 $r^{\phi(p^{k-1})} \equiv r^{p^{k-2}(p-1)} \equiv 1 \pmod{p^{k-1}}$ 가 성립한다. 그러므로 적당한 정수 a가 존재해서 $r^{p^{k-2}(p-1)} = 1 + ap^{k-1}$ 를 만족한다.

가정에 의하면 $r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$ 이므로 $ap^{k-1} \not\equiv 0 \pmod{p^k}$ 이다.
따라서 $\gcd(a,p)=1$ 이고 다음을 얻는다.

$$r^{p^{k-1}(p-1)} \equiv (1+ap^{k-1})^p \equiv 1 + ap^k \pmod{p^{k+1}}$$

$\gcd(a,p)=1$ 이므로 $ap^k \not\equiv 0 \pmod{p^{k+1}}$ 이다. 따라서 다음을 얻는다.

$$r^{p^{k-1}(p-1)} \not\equiv 1 \pmod{p^{k+1}}$$

그러므로 $k+1$ 일때도 주어진 정리가 참이다. 따라서 수학적 귀납법에 의하면 $k \geq 2$ 를 만족하는 모든 자연수 k에 대하여 주어진 정리가 참이다. ■

Theorem 3.3.4 p가 홀수인 소수이면 $k \geq 2$ 를 만족하는 자연수 k에 대하여 법 p^k의 원시근이 존재한다.

(증명)

Lemma 3.3.1에 의하면 $r^{p-1} \not\equiv 1 \pmod{p^2}$ 을 만족하는 법 p의 원시근 r이 존재하고 $k \geq 2$ 이므로 Lemma 3.3.2에 의하면 r은 $r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$ 도 만족한다.

$\mathrm{ord}_{p^k}(r)=n$ 라고 하자. 그러면 $n \mid \phi(p^k)=p^{k-1}(p-1)$ 이고 $r^n \equiv 1 \pmod{p^k}$ 에서 $r^n \equiv 1 \pmod{p}$ 를 만족한다. 그리고 $\mathrm{ord}_p(r)=p-1$ 이므로 $p-1 \mid n$ 이다.

따라서 $p-1 \mid n$ 이고 $n \mid p^{k-1}(p-1)$ 인데 p는 소수이므로 $0 \leq m \leq k-1$ 을 만족하는 정수 m에 대하여 $n = p^m(p-1)$ 을 만족한다.

이제 $m = k-1$ 임을 보이자. 결론을 부정해서 $m \leq k-2$ 라고 하면 $p^m \mid p^{k-2}$ 이므로 $n \mid p^{k-2}(p-1)$ 이고 $r^n \equiv 1 \pmod{p^k}$ 이므로 $r^{p^{k-2}(p-1)} \equiv 1 \pmod{p^k}$ 를 만족하는데 이것은 $r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$ 에 모순이다.

따라서 $m=k-1$ 이 되어야 하고 이때 $\mathrm{ord}_{p^k}(r)=n=p^{k-1}(p-1)=\phi(p^k)$ 를 만족한다. 그러므로 r은 법 p^k의 원시근이다. ■

Theorem 3.3.4에 의하면 p가 홀수인 소수이고 $k\geq 2$ 일 때 법 p^k의 원시근이 존재하고 3.2절에서 소수 p의 원시근이 존재한다는 것을 증명했으므로 정리하면 자연수 k에 대하여 법 p^k의 원시근이 존재한다는 것을 알수 있습니다.

Corollary 3.3.1 p가 홀수인 소수이면 자연수 k에 대하여 법 $2p^k$의 원시근이 존재한다.

(증명)
자연수 k에 대하여 법 p^k의 원시근이 존재한다. 그것을 r이라고 하자. 이때 r이 홀수라고 가정해도 무방하다. 만약 r이 짝수이면 $r'=r+p^k$ 라고 할 때 r'은 홀수이고 $r'\equiv r\pmod{p^k}$ 이므로 r'도 법 p^k의 원시근이다. 따라서 r이 홀수라고 가정해자.

$\gcd(r,p)=1$ 이고 r은 홀수이므로 $\gcd(r,2p^k)=1$ 을 만족한다. $\mathrm{ord}_{2p^k}(r)=n$ 라고 하면 p는 홀수인 소수이므로 $n\mid\phi(2p^k)=\phi(2)\phi(p^k)=\phi(p^k)$ 를 만족한다.
따라서 $n\leq\phi(p^k)$ 이다.

그리고 $r^n\equiv 1\pmod{2p^k}$ 이므로 $r^n\equiv 1\pmod{p^k}$ 이고 $\mathrm{ord}_{p^k}(r)=\phi(p^k)$ 이므로 $\phi(p^k)\mid n$ 을 만족한다. 따라서 $\phi(p^k)\leq n$ 이다.

그러므로 $n=\phi(p^k)=\phi(2p^k)$ 를 얻는다. 따라서 r은 법 $2p^k$의 원시근이다. ■

3.2절과 3.3절에서 소개한 모든 내용을 요약한 것이 다음 정리입니다.

Theorem 3.3.5 n이 $n\geq 2$ 를 만족하는 자연수일 때 법 n의 원시근이 존재할 필요충분조건은 n이 홀수인 소수 p와 자연수 k에 대하여 다음과 같이 표현되는 것이다.

$$n=2,4,p^k,2p^k$$

증명과정에 의하면 p가 홀수인 소수이고 k는 $k\geq 2$ 를 만족하는 자연수일 때 $r^{p-1}\not\equiv 1\pmod{p^2}$ 을 만족하는 법 p의 원시근은 법 p^k의 원시근이 됩니다.
그리고 법 p^k의 원시근 중에서 홀수인 원시근은 법 $2p^k$의 원시근이 됩니다.

그런데 정리를 증명한 방법으로 p^k의 원시근을 모두 찾을수 있는 것은 아닙니다. $n=5$ 이면 $\mathbb{Z}_5^{\times}$에 있는 법 5의 원시근은 $2,3$ 이고 $n=25$ 이면 $\mathbb{Z}_{25}^{\times}$에 있는 법 25의 원시근은 $2,3,8,12,13,17,22,23$ 입니다.

$2^{5-1}\not\equiv 1\pmod{25}$, $3^{5-1}\not\equiv 1\pmod{25}$ 이므로 증명과정에 의하면 $2,3$은 법 25의 원시근이 됩니다. 하지만 나머지 원시근은 증명과정을 이용해서 찾을수 없습니다.

Problem 3.3.1 m, n은 자연수이고 m이 홀수이면 $\gcd(2^m-1, 2^n+1)=1$ 임을 증명하시오.

(증명)

$d=\gcd(2^m-1, 2^n+1)$ 라고 하고 결론을 부정해서 $d \geq 2$ 라고 가정하자.

그러면 $2^m-1, 2^n+1$ 은 모두 홀수이므로 d는 3 이상의 홀수이다. 따라서 d의 약수들 중 홀수인 소수가 존재한다. 그것을 p라고 하면 다음을 얻는다.

$$2^m \equiv 1 \pmod{p}$$
$$2^n \equiv -1 \pmod{p}$$

따라서 $2^m \equiv 2^{2n} \equiv 1 \pmod{p}$ 이므로 $k=\mathrm{ord}_p(2)$라고 하면 $k \mid m,\ k \mid 2n$ 이므로 $k \mid \gcd(m,2n)$ 을 만족한다. 이제 $\gcd(m,2n)=\gcd(m,n)$ 이 성립함을 보이자.

$r=\gcd(m,2n)$ 라고 하면 $r \mid m,\ r \mid 2n$ 인데 m은 홀수이므로 r도 홀수이다. 따라서 $\gcd(r,2)=1$ 이므로 $r \mid n$ 을 만족한다.

이제 임의의 자연수 c에 대하여 $c \mid m,\ c \mid n$ 라고 가정하자. 그러면 $c \mid 2n$ 이고 $r=\gcd(m,2n)$ 이므로 최대공약수의 정의에 의하면 $c \leq r$ 이다. 따라서 최대공약수의 정의에 의하면 $r=\gcd(m,n)$ 이다. 그러므로 $\gcd(m,2n)=\gcd(m,n)$ 가 성립한다.

$k \mid \gcd(m,2n)=\gcd(m,n)$ 이므로 $k \mid m, k \mid n$ 을 만족한다.

그러므로 $2^n \equiv 1 \equiv -1 \pmod{p}$ 에서 $2 \mid p$ 를 얻는데 이것은 p가 홀수인 소수라는 것에 모순이다. 따라서 $d=1$ 이 되어야 한다. 즉, $\gcd(2^m-1, 2^n+1)=1$ 이다. ■

Problem 3.3.2 p는 홀수인 소수이고 n은 자연수일 때 다음을 증명하시오.

(a). $\gcd(a,p)=1$ 을 만족하는 정수 a에 대하여 $\mathrm{ord}_p(a)=k$ 라고 하자. 그러면 모든 자연수 m에 대하여 $a^{p^m k} \equiv 1 \pmod{p^{m+1}}$ 이다.

(b). 법 p^n의 임의의 원시근 r은 법 p의 원시근이다.

(c). $n \geq 2$ 이면 법 p^2의 임의의 원시근 r은 법 p^n의 원시근이다.

(증명)

(a). 집합 S 를 $S=\{m \in \mathbb{N} : a^{p^m k} \equiv 1 \pmod{p^{m+1}}\}$ 라고 하자. 조건에 의하면 $a^k \equiv 1 \pmod{p}$ 이므로 적당한 정수 b가 존재해서 $a^k = 1+pb$ 를 만족한다. 따라서 양변을 p제곱하면 이항정리에 의해 다음을 얻는다.

$$a^{pk} \equiv (1+pb)^p \equiv 1 \pmod{p^2}$$

그러므로 $1 \in S$ 이다. 이제 임의의 자연수 m에 대하여 $m \in S$ 라고 가정하자.

$a^{p^m k} \equiv 1 \pmod{p^{m+1}}$ 이므로 적당한 정수 c가 존재해서 $a^{p^m k} = 1+p^{m+1}c$ 를 만족한다. 따라서 양변을 p제곱하면 이항정리에 의해 다음을 얻는다.

$$a^{p^{m+1}k} \equiv (1+p^{m+1}c)^p \equiv 1 \pmod{p^{m+2}}$$

따라서 $m+1 \in S$ 이다. 그러므로 수학적 귀납법에 의하면 $S=\mathbb{N}$ 이고 모든 자연수 m에 대하여 $a^{p^m k} \equiv 1 \pmod{p^{m+1}}$ 가 성립한다. ■

(b). $\mathrm{ord}_p(a)=k$ 라고 하자. 그러면 (a)의 결과에 의해 $r^{p^{n-1}k} \equiv 1 \pmod{p^n}$ 이고 r은 법 p^n의 원시근이므로 $\phi(p^n) \mid p^{n-1}k$ 가 성립한다. 따라서 $p^{n-1}(p-1) \mid p^{n-1}k$ 에서 $p-1 \mid k$ 이므로 $p-1 \le k$ 가 성립한다.

그리고 $r^k \equiv 1 \pmod{p}$ 이므로 $k \mid \phi(p)=p-1$ 은 명백하다. 따라서 $k \le p-1$ 이므로 정리하면 $k=p-1=\phi(p)$ 를 얻는다. 그러므로 r은 법 p의 원시근이다. ■

(c). 조건에 의하면 $r^{p-1} \not\equiv 1 \pmod{p^2}$ 을 만족하고 $\gcd(r,p^2)=1$ 이므로 $\gcd(r,p)=1$ 을 만족하고 $n \ge 2$ 이므로 $\gcd(r,p^{n-1})=1$ 을 만족한다.

이 다음은 Lemma 3.3.2와 Theorem 3.3.4의 증명과정을 그대로 따르면 r은 법 p^n의 원시근이 된다는 것을 알수 있다. ■

Problem 3.3.3 자연수 n과 홀수인 소수 p에 대하여 다음을 증명하시오.
(a). 법 n의 원시근이 존재하면 $d \mid \phi(n)$ 을 만족하는 모든 자연수 d에 대하여 위수가 d인 정수는 $\mathbb{Z}_n^{\times}$에 $\phi(d)$개 있다.
(b). r이 법 p^2의 원시근이면 합동방정식 $x^{p-1} \equiv 1 \pmod{p^2}$ 을 만족하는 해는 법 p^2에서 $r^p, r^{2p}, \ldots, r^{(p-1)p}$ 뿐이다.

(증명)
(a). 법 n의 원시근을 r이라고 하자. 그러면 $\mathrm{ord}_n(r)=\phi(n)$ 이고 $\{r, r^2, r^3, \ldots, r^{\phi(n)}\}$은 법 n에 대한 기약잉여계이다. 따라서 $1 \le k \le \phi(n)$을 만족하는 자연수 k에 대하여 $\mathrm{ord}_n(r^k)=\dfrac{\phi(n)}{\gcd(\phi(n),k)}$ 이다.

따라서 위수가 d인 정수가 될 필요충분조건은 $\gcd(\phi(n),k)=\dfrac{\phi(n)}{d}$ 를 만족하는 것이고 $\gcd(\phi(n),k)=\dfrac{\phi(n)}{d}$ 를 만족하는 $\phi(n)$보다 작거나 같은 자연수 k의 개수는 2.1절에서 소개한 가우스의 정리의 증명과정에 의하면 $\phi\left(\dfrac{\phi(n)}{\frac{\phi(n)}{d}}\right)=\phi(d)$임을 알수 있다.

■

(b). 합동방정식 $x^{p-1} \equiv 1 \pmod{p^2}$ 의 해는 법 p^2에서 곱셈에 대한 역원을 가지므로 그 해는 $\mathbb{Z}_{p^2}^{\times}$에 모두 있다. 그리고 법 p^2의 원시근은 존재하므로 그것을 r이라고 하면 $\{r, r^2, r^3, ..., r^{p(p-1)}\}$은 법 p^2에 대한 기약잉여계이다.

$1 \le k \le p(p-1)$ 인 자연수 k에 대하여 r^k가 주어진 합동방정식의 해라고 하면 $r^{k(p-1)} \equiv 1 \pmod{p^2}$ 이므로 $\phi(p^2) \mid k(p-1)$ 을 만족한다.
즉, $p(p-1) \mid k(p-1)$ 이므로 $p \mid k$ 를 얻고 따라서 k는 p의 배수이다.

역으로 k가 p의 배수이면 r^k는 주어진 합동방정식의 해가 된다. 그리고 $p(p-1)$보다 작거나 같은 p의 배수는 $p, 2p, 3p, \ ..., p(p-1)$ 이다. 따라서 주어진 합동방정식의 해는 법 p^2에서 $r^p, r^{2p}, ..., r^{(p-1)p}$ 뿐이다. ■

Problem 3.3.4 p는 홀수인 소수이고 k는 자연수일 때 다음을 증명하시오.
(a). r이 법 p^k의 원시근일 때 r이 법 $2p^k$의 원시근이 될 필요충분조건은 r이 홀수인 것이다.
(b). r이 법 p의 원시근이고 t는 $(r+tp)^{p-1} \not\equiv 1 \pmod{p^2}$ 을 만족하는 정수이면 $r+tp$는 법 p^k의 원시근이다.

(증명)
(a). $(\Longrightarrow)$ r이 법 $2p^k$의 원시근이므로 $\gcd(r, 2p^k) = 1$ 을 만족해야 한다. 따라서 r은 홀수이다. 만약 r이 짝수이면 $\gcd(r, 2p^k) \ge 2$ 이므로 모순이다.

$(\Longleftarrow)$ 이것은 Corollary 3.3.1의 증명과정을 그대로 따르면 얻을수 있다. ■

(b). $r \equiv r + tp \pmod{p}$ 이므로 조건에 의하면 $r+tp$도 법 p의 원시근이다.
따라서 $k = 1$ 이면 명백하다. 그리고 $k \ge 2$ 인 경우는 Lemma 3.3.2와 Theorem 3.3.4의 증명과정을 그대로 따르면 $r+tp$가 법 p^k의 원시근임을 알수 있다. ■

3.4 이산로그

작성자 : 네냐플(Nenyaffle)

3.4절에서는 로그함수와 비슷한 역할을 하는 것을 소개하려고 합니다. 그것을 이산로그 또는 지수라고 부르는데 이 지수는 대학 입학 전부터 배운 지수와는 동음이의어 입니다. 영어로 쓰면 대학 입학 전에 배운 지수는 Exponent 이고 3.4절에서 소개하는 지수는 Index 입니다.

n이 원시근을 갖는 자연수일 때 r을 법 n의 원시근이라고 하면 $\{r, r^2, r^3, \ldots, r^{\phi(n)}\}$은 법 n에 대한 기약잉여계입니다. 따라서 $\gcd(a,n)=1$ 을 만족하는 임의의 정수 a에 대하여 집합 $S=\{k\in\mathbb{N} : r^k \equiv a \pmod n\}$는 공집합이 아닙니다.

정렬원리에 의하면 집합 S 는 가장 작은 원소를 갖고 최소원소를 다음과 같이 정의합니다.

Definition 3.4.1 이산로그(Discrete Logarithm)
n은 원시근을 갖는 자연수이고 r을 법 n의 원시근이라고 하자. $\gcd(a,n)=1$ 을 만족하는 정수 a에 대하여 $r^k \equiv a \pmod n$ 을 만족하는 가장 작은 자연수 k를 밑이 r인 a의 **이산로그(Discrete Logarithm)**라고 정의한다. 기호로는 $\mathrm{ind}_r a$ 로 나타낸다.

해석학에서는 자연로그를 주로 다루기 때문에 자연로그를 쓸땐 $\log_e x$ 대신 $\log x$ 라고 쓰는것처럼 이산로그도 혼돈의 우려가 없을땐 r을 생략해서 $\mathrm{ind}\, a$ 로 쓰기도 합니다.

이산로그의 정의에 의하면 $1 \le \mathrm{ind}_r a \le \phi(n)$ 과 $r^{\mathrm{ind}_r a} \equiv a \pmod n$ 는 명백합니다. 그리고 $a \equiv b \pmod n$ 이면 a, b의 이산로그는 같습니다. $a \equiv b \pmod n$ 이면 이산로그의 정의에 의해 $r^{\mathrm{ind}_r a} \equiv r^{\mathrm{ind}_r b} \pmod n$ 이고 r은 법 n의 원시근이므로

$$\mathrm{ind}_r a \equiv \mathrm{ind}_r b \pmod{\phi(n)}$$

를 만족합니다. 그리고 $1 \le \mathrm{ind}_r a \le \phi(n), 1 \le \mathrm{ind}_r b \le \phi(n)$ 이므로

$$\mathrm{ind}_r a = \mathrm{ind}_r b$$

가 성립합니다. 따라서 법 n에 대하여 합동인 정수는 같은 이산로그를 갖습니다.

이제 이산로그의 값을 실제로 구해보겠습니다. $n=13$ 이면 2는 법 n의 원시근입니다. 그러므로 2^{12}까지 계산해보면 법 13에 대하여 다음을 얻습니다.

$$2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^3 \equiv 8,\ 2^4 \equiv 3$$
$$2^5 \equiv 6,\ 2^6 \equiv 12,\ 2^7 \equiv 11,\ 2^8 \equiv 9$$
$$2^9 \equiv 5,\ 2^{10} \equiv 10,\ 2^{11} \equiv 7,\ 2^{12} \equiv 1$$

그러므로 법 13에서 밑이 2인 이산로그를 표로 정리하면 다음과 같습니다.

a	1	2	3	4	5	6	7	8	9	10	11	12
$\mathrm{ind}_2 a$	12	1	4	2	9	5	11	3	8	10	7	6

한편 6도 법 13의 원시근입니다. 그래서 밑이 6인 이산로그도 잘 정의되는데 같은 방법으로 계산해보면 다음을 얻습니다.

a	1	2	3	4	5	6	7	8	9	10	11	12
$\mathrm{ind}_6 a$	12	5	8	10	9	1	7	3	4	2	11	6

이제 이산로그의 기본성질을 소개하고 증명하겠습니다. 로그함수의 기본성질과 비슷합니다.

Theorem 3.4.1 n은 원시근을 갖는 자연수이고 r을 법 n의 원시근이라고 하자.
$\gcd(a,n)=1$ 일 때 $\mathrm{ind}\, a$를 밑이 r인 a의 이산로그라고 하면 다음이 성립한다.
(a). $\gcd(a,n)=\gcd(b,n)=1$ 이면 $\mathrm{ind}\, ab \equiv \mathrm{ind}\, a + \mathrm{ind}\, b \pmod{\phi(n)}$ 이다.
(b). 모든 자연수 k에 대하여 $\mathrm{ind}\, a^k \equiv k\mathrm{ind}\, a \pmod{\phi(n)}$ 이다.
(c). $\mathrm{ind}\, 1 \equiv 0 \pmod{\phi(n)}, \mathrm{ind}\, r \equiv 1 \pmod{\phi(n)}$ 이다.

(증명)
(a). 조건에 의하면 $\gcd(ab,n)=1$ 이므로 ab의 이산로그는 잘 정의되고
이산로그의 정의에 의하면 다음이 성립한다.

$$r^{\mathrm{ind}\, a} \equiv a \pmod{n}$$
$$r^{\mathrm{ind}\, b} \equiv b \pmod{n}$$
$$r^{\mathrm{ind}\, ab} \equiv ab \pmod{n}$$

따라서 $r^{\mathrm{ind}\, a + \mathrm{ind}\, b} \equiv r^{\mathrm{ind}\, ab} \pmod{n}$ 이므로 다음을 얻는다.

$$\mathrm{ind}\, ab \equiv \mathrm{ind}\, a + \mathrm{ind}\, b \pmod{\phi(n)}$$

■

(b). 조건에 의하면 $\gcd(a^k,n)=1$ 이므로 a^k의 이산로그는 잘 정의되고
이산로그의 정의에 의하면 다음이 성립한다.

$$r^{\mathrm{ind}\, a} \equiv a \pmod{n}$$
$$r^{\mathrm{ind}\, a^k} \equiv a^k \pmod{n}$$

따라서 $r^{\mathrm{ind}\, a^k} \equiv \left(r^{\mathrm{ind}\, a}\right)^k \equiv r^{k\mathrm{ind}\, a} \pmod{n}$ 이므로 다음을 얻는다.

$$\mathrm{ind}\, a^k \equiv k\mathrm{ind}\, a \pmod{\phi(n)}$$

■

(c). 이산로그의 정의에 의하면 다음이 성립한다.

$$r^{\mathrm{ind}\, 1} \equiv 1 \equiv r^0 \pmod{n}$$
$$r^{\mathrm{ind}\, r} \equiv r \equiv r^1 \pmod{n}$$

따라서 $\mathrm{ind}\, 1 \equiv 0 \pmod{\phi(n)}, \mathrm{ind}\, r \equiv 1 \pmod{\phi(n)}$ 이다. ■

Problem 3.4.1 n은 원시근을 갖는 자연수이다. 다음을 증명하시오.
문제에 있는 모든 기호는 잘 정의된다고 가정한다.

(a). 법 n에서 a의 곱셈에 대한 역원을 x라고 하면
$\mathrm{ind}_r x \equiv -\mathrm{ind}_r a \pmod{\phi(n)}$ 이다.

(b). 모든 정수 k에 대하여 $\mathrm{ind}_r a^k \equiv k\mathrm{ind}_r a \pmod{\phi(n)}$ 이다. k가 음의 정수이면
a^k는 법 n에서 a의 곱셈에 대한 역원을 $-k$번 거듭제곱한 값으로 정의한다.

(c). a, b가 법 n의 원시근이고 $\gcd(c,n)=1$ 이면
$(\mathrm{ind}_a b)(\mathrm{ind}_b c) \equiv \mathrm{ind}_a c \pmod{\phi(n)}$ 이다.
(d). r이 법 n의 원시근일 때 $\mathrm{ind}_r a \equiv \mathrm{ind}_r b \pmod{\phi(n)}$ 이면
$a \equiv b \pmod{n}$ 이다.
(e). $\gcd(a,n)=\gcd(c,n)=1$ 이고 b는 법 n의 원시근일 때
$a^{\mathrm{ind}_b c} \equiv c^{\mathrm{ind}_b a} \pmod{n}$ 이다.

(증명)
(a). 조건에 의하면 $ax \equiv 1 \pmod{n}$ 이므로 양변에 밑이 r인 이산로그를 취하면
$\mathrm{ind}_r a + \mathrm{ind}_r x \equiv 0 \pmod{\phi(n)}$ 을 얻는다.
따라서 $\mathrm{ind}_r x \equiv -\mathrm{ind}_r a \pmod{\phi(n)}$ 이다. ■

(b). k가 음이 아닌 정수이면 Theorem 3.4.1에 의해 명백하다. 따라서 k가 음의 정수라고 가정하자. 그러면 a^k는 법 n에서 곱셈에 대한 역원을 $-k$번 거듭제곱한 값 이므로
$ax \equiv 1 \pmod{n}$ 을 만족하는 정수 x에 대하여 $a^k = x^{-k}$ 라고 할수 있다.

그러므로 $a^{-k}x^{-k} \equiv 1 \pmod{n}$ 이고 (a)의 결과와 기본성질에 의하면 다음을 얻는다.

$$\mathrm{ind}_r a^k \equiv \mathrm{ind}_r x^{-k} \equiv -k\mathrm{ind}_r x \equiv k\mathrm{ind}_r a \pmod{\phi((n))}$$

따라서 k가 음의 정수일때도 $\mathrm{ind}_r a^k \equiv k\mathrm{ind}_r a \pmod{\phi(n)}$ 가 성립한다.
정리하면 모든 정수 k에 대하여 $\mathrm{ind}_r a^k \equiv k\mathrm{ind}_r a \pmod{\phi(n)}$ 이다. ■

(c). 이산로그의 정의에 의하면 $a^{\mathrm{ind}_a b} \equiv b \pmod{n}$ 이 성립한다.
따라서 양변을 $\mathrm{ind}_b c$ 만큼 거듭제곱하면 이산로그의 정의에 의해 다음을 얻는다.

$$\left(a^{\mathrm{ind}_a b}\right)^{\mathrm{ind}_b c} \equiv a^{(\mathrm{ind}_a b)(\mathrm{ind}_b c)} \equiv b^{\mathrm{ind}_b c} \equiv c \equiv a^{\mathrm{ind}_a c} \pmod{n}$$

그러므로 $(\mathrm{ind}_a b)(\mathrm{ind}_b c) \equiv \mathrm{ind}_a c \pmod{\phi(n)}$ 를 얻는다. ■

(d). 이산로그의 정의에 의하면 $1 \le \mathrm{ind}_r a \le \phi(n), 1 \le \mathrm{ind}_r b \le \phi(n)$ 이므로
조건을 만족할 경우 $\mathrm{ind}_r a = \mathrm{ind}_r b$ 가 성립한다. 그러므로 다음을 얻는다.

$$a \equiv r^{\mathrm{ind}_r a} \equiv r^{\mathrm{ind}_r b} \equiv b \pmod{n}$$

■

(e). $x = a^{\mathrm{ind}_b c}, y = c^{\mathrm{ind}_b a}$ 라고 하자. 그러면 다음을 얻는다.

$$\mathrm{ind}_b x \equiv (\mathrm{ind}_b c)(\mathrm{ind}_b a) \pmod{\phi(n)}$$
$$\mathrm{ind}_b y \equiv (\mathrm{ind}_b a)(\mathrm{ind}_b c) \pmod{\phi(n)}$$

따라서 $\mathrm{ind}_b x \equiv \mathrm{ind}_b y \pmod{\phi(n)}$ 이므로 (d)에 의하면 $x \equiv y \pmod{n}$ 이다.
그러므로 $a^{\mathrm{ind}_b c} \equiv c^{\mathrm{ind}_b a} \pmod{n}$ 가 성립한다. ■

n이 원시근을 갖는 자연수이고 a는 $\gcd(a,n)=1$ 을 만족하는 정수일 때 이산로그는 자연수 k에 대하여 $x^k \equiv a \pmod n$ 이런 형태의 합동방정식을 풀 때 유용합니다.

Theorem 3.4.2 n이 원시근을 가지는 자연수이고 a는 $\gcd(a,n)=1$ 을 만족하는 정수일 때 자연수 k에 대하여 합동방정식 $x^k \equiv a \pmod n$ 이 해를 가지기 위한 필요충분조건은 $a^{\frac{\phi(n)}{\gcd(k,\phi(n))}} \equiv 1 \pmod n$ 을 만족하는 것이다. (6)

$d=\gcd(k,\phi(n))$ 라고 하면 합동방정식 $x^k \equiv a \pmod n$ 이 해를 가질 경우 법 n에서 정확히 d개의 해를 갖는다.

(증명)

법 n의 원시근을 r이라고 하고 $d=\gcd(k,\phi(n))$ 라고 하자.

$(\Longrightarrow)$ 주어진 합동방정식의 하나의 해를 b라고 하자. 그러면 $b^k \equiv a \pmod n$ 이므로 양변에 밑이 r인 이산로그를 취하면 다음을 얻는다.

$$k\mathrm{ind}_r b \equiv \mathrm{ind}_r a \pmod{\phi(n)}$$

따라서 $d \mid \mathrm{ind}_r a$ 가 성립하므로 다음을 얻는다.

$$\frac{\phi(n)\mathrm{ind}_r a}{d} \equiv 0 \pmod{\phi(n)}$$

그러므로 $a^{\frac{\phi(n)}{d}} \equiv 1 \pmod n$ 가 성립한다.

$(\Longleftarrow)$ (6)의 양변에 밑이 r인 이산로그를 취하면 다음을 얻을수 있다.

$$\frac{\phi(n)\mathrm{ind}_r a}{d} \equiv 0 \pmod{\phi(n)} \quad (7)$$

$\mathrm{ind}_r a$를 d로 나눈 몫을 q, 나머지를 r이라고 하자. 그러면 $0 \le r < d$ 이고 $\mathrm{ind}_r a = dq + r$ 을 만족한다. 따라서 (7)에 의하면 다음을 얻는다.

$$\frac{\phi(n)r}{d} \equiv 0 \pmod{\phi(n)}$$

이제 $r=0$ 임을 보이자. 결론을 부정해서 $r \neq 0$ 이라고 가정하면 r은 자연수이고 $0 < \frac{r}{d} < 1$ 을 만족한다. 그리고 조건에 의하면 $\phi(n) \mid \frac{\phi(n)r}{d}$ 이므로 $\phi(n) \le \frac{\phi(n)r}{d}$ 에서 $\frac{r}{d} \ge 1$ 을 얻는데 이것은 모순이다.

따라서 $r=0$ 이 되어야 하고 이때 $d \mid \mathrm{ind}_r a$ 가 성립한다. 그리고 주어진 합동방정식 $x^k \equiv a \pmod n$ 의 양변에 밑이 r인 이산로그를 취하면 다음을 얻는다.

$$k\mathrm{ind}_r x \equiv \mathrm{ind}_r a \pmod{\phi(n)} \quad (8)$$

$d \mid \mathrm{ind}_r a$ 이므로 (8)을 만족하는 $\mathrm{ind}_r x$는 법 $\phi(n)$에서 정확히 d개 있고 Problem 3.4.1 (d)에 의하면 $\mathrm{ind}_r x$가 결정될 때 x는 법 n에서 유일하게 결정된다. 따라서 합동방정식 $x^k \equiv a \pmod n$ 은 법 n에서 정확히 d개의 해를 갖는다. ■

이산로그를 이용해서 합동방정식 $x^9 \equiv 5 \pmod{13}$ 의 해를 $\mathbb{Z}_{13}$에서 구해보겠습니다.

$\gcd(9, \phi(13)) = 3$ 이고 $5^{\frac{\phi(13)}{3}} \equiv 5^4 \equiv 1 \pmod{13}$ 이므로 Theorem 3.4.2에 의하면 주어진 합동방정식의 해는 $\mathbb{Z}_{13}$에서 3개 존재합니다.

2는 법 13의 원시근이므로 합동방정식의 양변에 밑이 2인 이산로그를 취하면 $9\mathrm{ind}_2 x \equiv \mathrm{ind}_2 5 \pmod{12}$ 를 얻을수 있습니다. 그리고 밑이 2인 이산로그표를 보면

a	1	2	3	4	5	6	7	8	9	10	11	12
$\mathrm{ind}_2 a$	12	1	4	2	9	5	11	3	8	10	7	6

$\mathrm{ind}_2 5 = 9$ 이므로 $9\mathrm{ind}_2 x \equiv 9 \pmod{12}$ 에서 $\mathrm{ind}_2 x \equiv 1 \pmod 4$ 을 얻고 $1 \le \mathrm{ind}_2 x \le 12$ 이므로 가능한 경우는 $\mathrm{ind}_2 x = 1, 5, 9$ 입니다.
따라서 주어진 합동방정식의 해를 $\mathbb{Z}_{13}$에서 찾으면 $x = 2, 5, 6$ 입니다.

6도 법 13의 원시근이므로 같은 방법으로 합동방정식에 밑이 6인 이산로그를 취해서 다음 이산로그 표를 이용하면 구할수 있습니다.

a	1	2	3	4	5	6	7	8	9	10	11	12
$\mathrm{ind}_6 a$	12	5	8	10	9	1	7	3	4	2	11	6

양변에 밑이 6인 이산로그를 취하면 $9\mathrm{ind}_6 x \equiv \mathrm{ind}_6 5 \pmod{12}$ 이고 표를 보면 $\mathrm{ind}_6 5 = 9$ 이므로 $9\mathrm{ind}_6 x \equiv 9 \pmod{12}$ 에서 $\mathrm{ind}_6 x \equiv 1 \pmod 4$ 을 얻을수 있습니다. 따라서 같은 방법으로 $x = 2, 5, 6$ 을 얻을수 있습니다.

그리고 이산로그를 이용하면 특정 조건 하에서 지수합동방정식도 풀수 있습니다.

Theorem 3.4.3 n은 원시근을 갖는 자연수이고 r은 법 n의 원시근이다. $\gcd(a,n) = \gcd(b,n) = 1$ 을 만족하는 정수 a, b에 대하여 $d = \gcd(\mathrm{ind}_r a, \phi(n))$ 라고 할 때 $a^x \equiv b \pmod n$ 이 해를 가질 필요충분조건은 $d \mid \mathrm{ind}_r b$ 이다.

만약 x가 음의 정수이면 a^x는 법 n에서 a의 곱셈에 대한 역원을 $-x$번 거듭제곱한 값으로 정의한다. 그리고 $a^x \equiv b \pmod n$ 의 해가 존재하면 법 $\phi(n)$에서 정확히 d개의 해를 갖는다.

(증명)

$(\Longrightarrow)$ 주어진 합동방정식의 하나의 해를 c라고 하자. 그러면 $a^c \equiv b \pmod n$ 이므로 양변에 밑이 r인 이산로그를 취하면 Problem 3.4.1 (b)에 의해 다음을 얻는다.

$$c\mathrm{ind}_r a \equiv \mathrm{ind}_r b \pmod{\phi(n)}$$

따라서 $d \mid \mathrm{ind}_r b$ 가 성립한다.

($\Leftarrow$) $d=\gcd(\mathrm{ind}_r a, \phi(n))$ 이고 $d \mid \mathrm{ind}_r b$ 이므로 적당한 정수 s, t가 존재해서 다음을 만족한다.

$$s\mathrm{ind}_r a + t\phi(n) = \mathrm{ind}_r b$$

따라서 $s\mathrm{ind}_r a \equiv \mathrm{ind}_r b \pmod{\phi(n)}$ 이므로 $a^s \equiv b \pmod{n}$ 을 만족한다.
그러므로 주어진 합동방정식의 해가 존재한다.

이제 $d=\gcd(\mathrm{ind}_r a, \phi(n))$ 일 때 합동방정식 $a^x \equiv b \pmod{n}$ 의 해가 존재할 경우 법 $\phi(n)$에서 정확히 d개 존재함을 보이자. 해가 존재하므로 $d \mid \mathrm{ind}_r b$ 이고 이때 합동방정식 $x\mathrm{ind}_r a \equiv \mathrm{ind}_r b \pmod{\phi(n)}$ 은 법 $\phi(n)$에서 d개의 해를 갖는다.

그리고 $x\mathrm{ind}_r a \equiv \mathrm{ind}_r b \pmod{\phi(n)}$ 를 만족하는 x가 결정되면 그 x는 $a^x \equiv b \pmod{n}$ 의 해가 된다. 역으로 $a^x \equiv b \pmod{n}$ 를 만족하는 x가 결정되면 그 x는 $x\mathrm{ind}_r a \equiv \mathrm{ind}_r b \pmod{\phi(n)}$ 의 해가 된다.

따라서 합동방정식 $a^x \equiv b \pmod{n}$ 의 해는 법 $\phi(n)$에서 정확히 d개 있다. ■

합동방정식 $5^x \equiv 4 \pmod{19}$ 의 해를 $\mathbb{Z}_{18}$에서 구해보겠습니다. 2는 법 19의 원시근이고 $\mathrm{ind}_2 4 = 2, \mathrm{ind}_2 5 = 16$ 입니다. $\gcd(16, \phi(19)) = 2$ 이고 $2 \mid \mathrm{ind}_2 4$ 이므로 Theorem 3.4.3에 의하면 $5^x \equiv 4 \pmod{19}$ 는 법 18에서 2개의 해를 갖습니다.

$5^x \equiv 4 \pmod{19}$ 의 양변에 밑이 2인 이산로그를 취하면 $16x \equiv 2 \pmod{18}$ 에서 $8x \equiv 1 \pmod{9}$ 이고 따라서 $x \equiv 8 \pmod{9}$ 을 얻습니다. 그러므로 $16x \equiv 2 \pmod{18}$ 의 해는 $\mathbb{Z}_{18}$에서 구하면 $x = 8, 17$ 입니다.

따라서 $5^x \equiv 4 \pmod{19}$ 의 해는 $\mathbb{Z}_{18}$에서 구하면 $x = 8, 17$ 입니다.

Problem 3.4.2 p가 홀수인 소수이고 r은 법 p의 원시근일 때 다음을 증명하시오.

$$\mathrm{ind}_r(-1) = \mathrm{ind}_r(p-1) = \frac{p-1}{2}$$

(증명)

$p-1 \equiv -1 \pmod{p}$ 이므로 $\mathrm{ind}_r(-1) = \frac{p-1}{2}$ 임을 증명하면 충분하다.

r이 법 p의 원시근이므로 $r^{p-1} \equiv 1 \pmod{p}$ 이고 p는 홀수인 소수이므로 $\frac{p-1}{2}$는 자연수이다. 따라서 $r^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$ 를 얻는데 r은 법 p의 원시근이므로 $r^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ 이다. 그러므로 $\mathrm{ind}_r(-1) = \frac{p-1}{2}$ 이다. ■

Problem 3.4.3 p는 홀수인 소수이고 r은 법 p의 원시근일 때 다음을 증명하시오.

$$\mathrm{ind}_r(p-a)\equiv \mathrm{ind}_r a+\frac{p-1}{2}\ (\mathrm{mod}\ p-1)$$

(증명)

$p-a\equiv -a\ (\mathrm{mod}\ p)$ 이므로 Problem 3.4.2와 이산로그의 성질에 의하면 다음을 얻는다.

$$\mathrm{ind}_r a+\frac{p-1}{2}\equiv \mathrm{ind}_r a+\mathrm{ind}_r(-1)\equiv \mathrm{ind}_r(-a)\equiv \mathrm{ind}_r(p-a)\ (\mathrm{mod}\ p-1)$$

■

Problem 3.4.4 p가 홀수인 소수이고 n은 자연수일 때 합동방정식 $x^{2^n}\equiv -1\ (\mathrm{mod}\ p)$ 의 해가 존재할 필요충분조건은 $p\equiv 1\ (\mathrm{mod}\ 2^{n+1})$ 임을 증명하시오.

(증명)

$d=\gcd(2^n,p-1)$ 라고 하자. 그러면 $d\mid 2^n$ 이므로 $k\le n$ 을 만족하는 적당한 음이 아닌 정수 k에 대하여 $d=2^k$ 를 만족한다.

$(\Rightarrow)$ Theorem 3.4.2에 의하면 $(-1)^{\frac{p-1}{2^k}}\equiv 1\ (\mathrm{mod}\ p)$ 를 만족한다.

만약 $\frac{p-1}{2^k}$ 가 홀수이면 $2\mid p$ 인데 이것은 p가 홀수인 것에 모순이다.

따라서 $\frac{p-1}{2^k}$ 는 짝수이다. 그러므로 적당한 자연수 m에 대하여 $p-1=2^{k+1}m$ 을 만족하고 $2^k=\gcd(2^n,2^{k+1}m)$ 을 얻는다.

m은 자연수이므로 적당한 음이 아닌 정수 s와 적당한 홀수 t에 대하여 $m=2^s t$ 로 표현 가능하다. 따라서 $2^k=\gcd(2^n,2^{k+s+1}t)$ 인데 t는 홀수이므로 다음을 만족한다.

$$\gcd(2^n,2^{k+s+1}t)=2^{\min(n,k+s+1)}$$

그러므로 $2^k=2^{\min(n,k+s+1)}$ 에서 $k=\min(n,k+s+1)$ 을 얻고 $k+s+1>k$ 이므로 $k=n$ 이 되어야 한다. 따라서 $p-1=2^{n+1}m$ 에서 $p\equiv 1\ (\mathrm{mod}\ 2^{n+1})$ 이다.

$(\Leftarrow)$ 이 경우 $(-1)^{\frac{p-1}{2^k}}\equiv 1\ (\mathrm{mod}\ p)$ 을 만족하므로 Theorem 3.4.2에 의하면 합동방정식 $x^{2^n}\equiv -1\ (\mathrm{mod}\ p)$ 의 해가 존재한다. ■

Problem 3.4.5 p는 $p\ge 5$ 를 만족하는 소수이고 a는 $\gcd(a,p)=1$ 을 만족하는 정수일 때 합동방정식 $x^3\equiv a\ (\mathrm{mod}\ p)$ 에 대하여 다음을 증명하시오.

(a). $p\equiv 1\ (\mathrm{mod}\ 6)$ 이면 해를 갖지 않거나 법 p에서 정확히 3개의 해를 갖는다.

(b). $p\equiv 5\ (\mathrm{mod}\ 6)$ 이면 법 p에서 유일한 해를 갖는다.

(증명)
$d=\gcd(3,p-1)$ 라고 하자.

(a). 조건에 의하면 적당한 자연수 k에 대하여 $p=6k+1$ 을 만족한다.
그리고 $3 \mid 6k$ 이므로 $d=\gcd(3,6k)=3$ 을 얻고 $\frac{p-1}{3}=2k$ 이다.

따라서 $a^{2k} \equiv 1 \pmod p$ 이면 주어진 합동방정식은 Theorem 3.4.2에 의해 법 p에서 정확히 3개의 해를 갖고 $a^{2k} \not\equiv 1 \pmod p$ 이면 해를 갖지 않는다. ■

(b). 조건에 의하면 적당한 음이 아닌 정수 k에 대하여 $p=6k+5$ 를 만족한다.
따라서 $p-1 \equiv 1 \pmod 3$ 이므로 $p-1$ 은 3의 배수가 아니다. 그러므로 $d=1$ 이다.

그리고 $\gcd(a,p)=1$ 이므로 페르마의 작은 정리에 의하면 $a^{p-1} \equiv 1 \pmod p$ 이다.
따라서 Theorem 3.4.2에 의하면 주어진 합동방정식은 법 p에서 유일한 해를 갖는다. ■

Problem 3.4.6 p는 소수이고 $\{r_1,r_2,...,r_{p-1}\}$은 법 p에 대한 기약잉여계이다.
이때 자연수 k에 대하여 $\{r_1^k,r_2^k,...,r_{p-1}^k\}$가 법 p에 대한 기약잉여계가 될 필요충분조건은 $\gcd(k,p-1)=1$ 을 만족하는 것임을 증명하시오.

(증명)
$(\Longrightarrow)$ $\gcd(a,p)=1$ 을 만족하는 임의의 정수 a를 택하자. 그러면 조건에 의해
적당한 $i=1,2,...,p-1$ 가 존재해서 $r_i^k \equiv a \pmod p$ 를 만족한다.

따라서 합동방정식 $x^k \equiv a \pmod p$ 은 해가 존재하고 그 해는 법 p에서 유일하므로
Theorem 3.4.2에 의하면 $\gcd(k,p-1)=1$ 을 만족해야 한다.

$(\Longleftarrow)$ 조건에 의하면 각각의 $i=1,2,...,p-1$ 에 대하여 $\gcd(r_i,p)=1$ 이므로
$\gcd(r_i^k,p)=1$ 이다. 따라서 $\{r_1^k,r_2^k,...,r_{p-1}^k\}$ 의 원소의 개수가 $p-1$ 임을 보이면 충분하다.

$\gcd(r_i^k,p)=1$ 이므로 합동방정식 $x^k \equiv r_i^k \pmod p$ 의 해는 p와 서로소이다.
따라서 합동방정식의 $x^k \equiv r_i^k \pmod p$ 의 해가 될수 있는 후보는 법 p에 대한
기약잉여계에 모두 있다. 이제 해가 법 p에서 유일함을 보이자.

$\gcd(k,p-1)=1$ 이고 페르마의 작은 정리에 의하면 $\left(r_i^k\right)^{p-1} \equiv 1 \pmod p$ 이므로
Theorem 3.4.2에 의하면 합동방정식 $x^k \equiv r_i^k \pmod p$ 의 해는 법 p에서 유일하고
그 유일한 해가 $x=r_i$ 임은 명백하다.

그러므로 $\left\{r_1^k, r_2^k, \ldots, r_{p-1}^k\right\}$ 에는 법 p에서 모두 다른 원소이다.

따라서 $\left\{r_1^k, r_2^k, \ldots, r_{p-1}^k\right\}$는 법 p에 대한 기약잉여계이다. ■

Problem 3.4.7 p는 홀수인 소수이고 r은 법 p의 원시근이라고 하자.
그러면 $S=\left\{r, r^2, r^3, \ldots, r^{p-1}\right\}$는 법 p에 대한 기약잉여계이다. $a \in S$ 이고 자연수 k에 대하여 $d=\gcd(k, p-1)$ 라고 할 때 합동방정식 $x^k \equiv a \pmod p$ 의 해가 존재할 필요충분조건은 a가 $r^d, r^{2d}, \ldots, r^{\left(\frac{p-1}{d}\right)d}$ 중 하나임을 증명하시오.

(증명)

Theorem 3.4.2에 의하면 합동방정식 $x^k \equiv a \pmod p$ 의 해가 존재할 필요충분조건은 $a^{\frac{p-1}{d}} \equiv 1 \pmod p$ 를 만족하는 것이다. 그리고 $\frac{p-1}{d} \mid p-1$ 이므로 Lemma 3.2.1에 의하면 합동방정식 $x^{\frac{p-1}{d}} \equiv 1 \pmod p$ 의 해는 법 p에서 정확히 $\frac{p-1}{d}$개 있다.

그리고 합동방정식 $x^{\frac{p-1}{d}} \equiv 1 \pmod p$ 의 해는 p와 서로소이므로 결국 집합 S 에 합동방정식의 해가 될수 있는 후보가 모두 들어있다.

한편 $\frac{p-1}{d}$개의 정수 $r^d, r^{2d}, \ldots, r^{\left(\frac{p-1}{d}\right)d}$ 는 모두 합동방정식 $x^{\frac{p-1}{d}} \equiv 1 \pmod p$ 을 만족한다. 그러므로 법 p에서 $r^d, r^{2d}, \ldots, r^{\left(\frac{p-1}{d}\right)d}$ 는 합동방정식 $x^{\frac{p-1}{d}} \equiv 1 \pmod p$ 의 해를 모두 모은 것이다.

정리하면 합동방정식 $x^k \equiv a \pmod p$ 의 해가 존재할 필요충분조건은 a가 $r^d, r^{2d}, \ldots, r^{\left(\frac{p-1}{d}\right)d}$ 중 하나인 것이다. ■

4. 이차잉여

4.1 르장드르 기호

작성자 : 네냐플(Nenyaffle)

2.4절에서 $f(x)$가 정수계수 다항식일 때 모든 소수 p에 대하여 합동방정식 $f(x)\equiv 0 \pmod p$ 을 풀수 있으면 Theorem 2.4.3과 중국인의 나머지 정리를 이용해서 모든 자연수 n에 대하여 합동방정식 $f(x)\equiv 0 \pmod n$ 을 풀수 있다고 이야기했습니다.

그런데 합동방정식 $f(x)\equiv 0 \pmod p$ 의 일반적인 해법은 아직까지 알려져있지 않습니다. 그나마 현재 알려져있는건 $f(x)$가 일차식인 경우와 이차식인 경우인데 일차식인 경우는 2.3절에서 이미 소개했으므로 4장에서는 $f(x)$가 이차식인 경우에 대해 소개하려고 합니다.

$f(x)=ax^2+bx+c$ 일 때 합동방정식 $ax^2+bx+c\equiv 0 \pmod p$ 을 보다 간단한 형태로 변형하려고 합니다. 우선 $p=2$ 이면 해가 될수 있는 후보는 $0,1$ 이므로 $x=0,1$ 만 대입해보면 됩니다. 따라서 p가 홀수인 소수라고 가정하겠습니다.

그리고 $a\equiv 0 \pmod p$ 이면 합동방정식은 $bx+c\equiv 0 \pmod p$ 가 되는데 이것은 일차합동방정식 이므로 해법을 이미 알고 있습니다. 따라서 $a\not\equiv 0 \pmod p$ 즉, $p\nmid a$ 를 가정하겠습니다.

p가 홀수인 소수이고 $p\nmid a$ 이므로 $\gcd(4a,p)=1$ 입니다. 따라서 $4a$는 법 p에서 곱셈에 대한 역원이 존재하므로 $ax^2+bx+c\equiv 0 \pmod p$ 은 다음과 동치입니다.

$$4a\left(ax^2+bx+c\right)\equiv 0 \pmod p$$

그리고 $4a\left(ax^2+bx+c\right)=(2ax+b)^2-\left(b^2-4ac\right)$ 이므로 다음을 얻습니다.

$$(2ax+b)^2\equiv b^2-4ac \pmod p$$

따라서 $y=2ax+b, d=b^2-4ac$ 라고 치환하면 합동방정식은 $y^2\equiv d \pmod p$ 와 같이 간단하게 변형됩니다. 그러므로 합동방정식 $ax^2+bx+c\equiv 0 \pmod p$ 의 한 해가 $x=x_0$ 이면 $y=2ax_0+b$ 는 $y^2\equiv d \pmod p$ 의 한 해가 됩니다.

역으로 $y^2\equiv d \pmod p$ 의 한 해가 $y=y_0$ 이면 $\gcd(2a,p)=1$ 이므로 $2ax+b\equiv y_0 \pmod p$ 를 만족하는 정수 x는 법 p에서 유일하게 존재합니다.

그것을 $x=x_0$ 라고 하면 $y_0^2\equiv\left(2ax_0+b\right)^2\equiv d\equiv b^2-4ac \pmod p$ 에서 $4a\left(ax_0^2+bx_0+c\right)\equiv 0 \pmod p$ 을 얻을수 있고 $\gcd(4a,p)=1$ 이므로 $ax_0^2+bx_0+c\equiv 0 \pmod p$ 를 얻을수 있습니다.

예를 들어 합동방정식 $5x^2-6x+2\equiv 0 \pmod{13}$ 은 $y=10x-6$ 이고 $d=-4$ 이므로 결국 $y^2\equiv -4\equiv 9 \pmod{13}$ 을 풀면 됩니다. 이 경우 $y=\pm 3$ 이 해가 됨은 명백하고 13은 소수이므로 합동방정식 $y^2\equiv 9 \pmod{13}$ 의 해는 다음과 같습니다.

$$y\equiv 3,10 \pmod{13}$$

따라서 $10x\equiv 9 \pmod{13}$ 또는 $10x\equiv 16\equiv 3 \pmod{13}$ 을 얻을수 있고 이것을 풀면 $x\equiv 10,12 \pmod{13}$ 을 얻을수 있습니다. 그러므로 합동방정식 $5x^2-6x+2\equiv 0 \pmod{13}$ 의 해를 $\mathbb{Z}_{13}$에서 찾으면 $x=10,12$ 입니다.

그러므로 $\gcd(a,p)=1$ 을 만족하는 정수 a에 대하여 $x^2\equiv a \pmod{p}$ 이런 형태의 합동방정식을 풀수 있으면 일반적인 이차합동방정식을 풀수 있게 됩니다. $\gcd(a,p)=1$ 을 가정하는 이유는 처음에 p를 홀수인 소수로 가정하는 이유와 비슷한데 만약 $\gcd(a,p)\neq 1$ 이면 $a\equiv 0 \pmod{p}$ 이므로 $x^2\equiv 0 \pmod{p}$ 이 되어서 해가 존재하기 때문입니다.

Definition 4.1.1 이차잉여(Quadratic Residue), 이차 비잉여(Quadratic Nonresidue)
p가 홀수인 소수이고 a는 $\gcd(a,p)=1$ 을 만족하는 정수일 때 합동방정식 $x^2\equiv a \pmod{p}$ 의 해가 존재하면 a를 법 p에 대한 **이차잉여(Quadratic Residue)** 라고 정의하고 해가 존재하지 않으면 a를 법 p에 대한 **이차 비잉여(Quadratic Nonresidue)**라고 정의한다.

$\gcd(a,p)=\gcd(b,p)=1$ 일 때 $a\equiv b \pmod{p}$ 이면 합동방정식 $x^2\equiv a \pmod{p}$ 의 해가 존재할 경우 합동방정식 $x^2\equiv b \pmod{p}$ 의 해도 존재합니다. 따라서 법 p에 대한 이차잉여는 $\mathbb{Z}_p^{\times}=\{1,2,...,p-1\}$ 에서만 고려해도 충분합니다.

우선 단순하게 생각해보면 $\gcd(a,p)=1$ 이므로 합동방정식 $x^2\equiv a \pmod{p}$ 의 해가 될수 있는 후보는 모두 $\mathbb{Z}_p^{\times}=\{1,2,...,p-1\}$에 있습니다. 따라서 $\mathbb{Z}_p^{\times}$의 원소를 합동방정식에 모두 대입했을 때 합동식이 성립하려면 a가 x에 대입한 원소를 제곱한것과 합동이 되면 됩니다.

예를 들어 $p=13$ 일 때 $x^2\equiv a \pmod{13}$ 의 해가 존재하도록 하는 13과 서로소인 정수 a를 구한다고 하면 1부터 12까지의 자연수를 모두 제곱했을 때 법 13에서 다음이 성립합니다.

$$\begin{aligned} 1^2&\equiv 12^2\equiv 1\\ 2^2&\equiv 11^2\equiv 4\\ 3^2&\equiv 10^2\equiv 9\\ 4^2&\equiv 9^2\equiv 3\\ 5^2&\equiv 8^2\equiv 12\\ 6^2&\equiv 7^2\equiv 10 \end{aligned} \tag{1}$$

따라서 a를 $a=1,3,4,9,10,12$ 중 하나로 택하면 $x^2\equiv a \pmod{p}$ 의 해가 존재하고 $1,3,4,9,10,12$ 가 법 13에 대한 이차잉여가 됩니다.

(1)을 잘 보면 합이 13이 되는 자연수는 제곱했을 때 법 13에 대해 합동이 됩니다.
실제로 합이 p인 정수는 법 p에 대해 합동이 되는데 정수 x에 대하여 $y=p-x$ 라고 하면 $y^2 \equiv (p-x)^2 \equiv p^2-2px+x^2 \equiv x^2 \pmod{p}$ 를 만족합니다.

그러므로 $\mathbb{Z}_p^{\times}$의 원소들 중 법 p에 대한 이차잉여는 다음 자연수들 중 하나와 합동입니다.

$$1^2, 2^2, 3^2, \ ..., \left(\frac{p-1}{2}\right)^2 \tag{2}$$

이것은 (1)을 보면 쉽게 알수 있습니다. 그리고 (2)에 있는 자연수는 법 p에서 서로 합동이 아닌 자연수입니다. 만약 $1 \le k < m \le \frac{p-1}{2}$ 를 만족하는 자연수 k, m에 대하여 $k^2 \equiv m^2 \pmod{p}$ 라고 가정하면 합동방정식 $x^2 \equiv k^2 \pmod{p}$ 은 법 p에서 서로 다른 해를 $k, -k, m, -m$ 이렇게 4개 갖고 이것은 라그랑주의 정리에 모순입니다.

따라서 법 p에 대한 이차잉여는 $\mathbb{Z}_p^{\times}$에 $\frac{p-1}{2}$개 있다는 것을 알수 있습니다. 그러므로 이차 비잉여도 $\mathbb{Z}_p^{\times}$에 $(p-1)-\frac{p-1}{2}=\frac{p-1}{2}$개 있습니다. 즉, 개수가 같습니다.

한편 이차잉여의 표현을 간단하게 하기 위해 고안된 기호가 있습니다.
그것을 다음과 같이 정의합니다.

Definition 4.1.2 르장드르 기호(Legendre Symbol)
p는 홀수인 소수이고 a는 $\gcd(a,p)=1$ 을 만족하는 정수라고 하자.
그러면 **르장드르 기호(Legendre Symbol)** (a/p)를 다음과 같이 정의한다.

$$(a/p)=\begin{cases}1 & (a\text{가 법 } p\text{에 대한 이차잉여}) \\ -1 & (a\text{가 법 } p\text{에 대한 이차 비잉여})\end{cases}$$

책에 따라서는 르장드르 기호를 $\left(\frac{a}{p}\right)$로 쓰기도 하는데 저는 분수와 헷갈려서 (a/p)로 쓰는 것을 선호합니다.

르장드르 기호를 사용하면 표현이 간단해진다는 장점이 있습니다. 예를 들어 3이 법 13에 대한 이차잉여라는 것을 설명하려면 $x^2 \equiv 3 \pmod{13}$ 의 해가 존재한다는 길고 지루한 이야기를 해야합니다. 그런데 $(3/13)=1$ 이 등식만 쓰면 3은 법 13에 대한 이차잉여라는 것을 바로 알수 있습니다.

같은 이유로 르장드르 기호를 사용하면 정리의 서술도 간편해집니다.

Theorem 4.1.1 오일러의 판정법(Euler's Criterion)
p가 홀수인 소수이고 a는 $\gcd(a,p)=1$ 을 만족하는 정수일 때 다음이 성립한다.

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

(증명)

페르마의 작은 정리에 의하면 $a^{p-1} \equiv 1 \pmod{p}$ 를 만족하고 p는 홀수인 소수이므로 $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$ 를 만족한다.

마찬가지로 p는 홀수인 소수이므로 $\gcd(2, p-1) = 2$ 이다. 따라서 Theorem 3.4.2에 의하면 a가 법 p에 대한 이차잉여가 될 필요충분조건은 $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ 이고 a가 법 p에 대한 이차 비잉여가 될 필요충분조건은 $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ 이다.

그러므로 르장드르 기호의 정의에 의하면 $(a/p) \equiv a^{\frac{p-1}{2}} \pmod{p}$ 를 얻는다. ■

오일러의 판정법은 르장드르 기호가 갖는 성질을 증명할 때 유용합니다. 그리고 르장드르 기호가 없으면 오일러 판정법을 서술할 때 a가 법 p에 대한 이차잉여가 될 필요충분조건이 $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ 이고 이차 비잉여가 될 필요충분조건이 $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ 이라고 길게 써야 합니다. 르장드르 기호는 길고 지루한 문장을

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

이렇게 간단하게 표현할수 있게 해줍니다.

르장드르 기호가 갖는 성질을 증명하기 전에 간단한 성질을 소개하겠습니다. a, b가 $a^2 = b^2 = 1$ 을 만족하는 정수이고 p는 홀수인 소수일 때 $a \equiv b \pmod{p}$ 이면 $a = b$ 가 성립합니다. (3)

만약 $a \neq b$ 이면 $|a-b| = 2$ 이므로 조건에 의해 $2 \mid p$ 를 얻는데 이것은 p가 홀수인 것에 모순입니다. 따라서 $a = b$ 가 되어야 합니다. 르장드르 기호는 제곱하면 1이 되는 정수이므로 기본성질을 증명할 때 (3)을 이용하는 경우가 많습니다.

Theorem 4.1.2 p가 홀수인 소수이고 a, b는 $\gcd(a,p) = \gcd(b,p) = 1$ 을 만족하는 정수일 때 다음 등식이 성립한다.

(a). $a \equiv b \pmod{p}$ 이면 $(a/p) = (b/p)$ 이다.
(b). $(a^2/p) = 1$ 이다.
(c). $(ab/p) = (a/p)(b/p)$ 이다.
(d). $(1/p) = 1$ 이고 $(-1/p) = (-1)^{\frac{p-1}{2}}$ 이다.

(증명)

(a). $a \equiv b \pmod{p}$ 이므로 $x^2 \equiv a \pmod{p}$ 의 해가 존재하는 것과 $x^2 \equiv b \pmod{p}$ 의 해가 존재하는 것은 동치이다. 따라서 $(a/p) = (b/p)$ 이다. ■

(b). $x^2 \equiv a^2 \pmod{p}$ 의 해는 $x = a$ 로 존재하므로 명백하다. ■

(c). 오일러의 판정법에 의하면 다음을 얻는다.

$$(ab/p) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv (a/p)(b/p) \pmod{p}$$

따라서 (3)에 의하면 $(ab/p) = (a/p)(b/p)$ 가 성립한다. ■

(d). (b)에 의하면 $(1/p) = 1$ 은 명백하다. 그리고 오일러의 판정법에 의하면 $(-1/p) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$ 이므로 (3)에 의하면 $(-1/p) = (-1)^{\frac{p-1}{2}}$ 이다. ■

(d)의 등식은 $(-1/p) = \begin{cases} 1 & (p \equiv 1 \pmod 4) \\ -1 & (p \equiv 3 \pmod 4) \end{cases}$ 라고 표현할수도 있습니다.

Theorem 4.1.2를 이용하면 르장드르 기호를 쉽게 계산할수 있습니다.

$$\begin{aligned} (-38/11) &= (-1/11)(38/11) \\ &= (-1)^{\frac{11-1}{2}} (5/11) \ (\because 38 \equiv 5 \pmod{11}) \\ &= -(5/11) \end{aligned}$$

이고 $(5/11) \equiv 5^{\frac{11-1}{2}} \equiv 1 \pmod{11}$ 이므로 (3)에 의하면 $(5/11) = 1$ 입니다.
따라서 $(-38/11) = -1$ 입니다. 즉, -38은 법 11에 대한 이차 비잉여이고
합동방정식 $x^2 \equiv -38 \pmod{11}$ 의 해가 존재하지 않는다는 것을 알수 있습니다.

일반적으로 p가 홀수인 소수이고 a는 $\gcd(a,p) = 1$ 를 만족하는 정수일 때 a가 $a = \pm p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ 로 소인수분해 된다면 $\gcd(a,p) = 1$ 이므로 각각의 $i = 1,2,...,r$ 에 대하여 $\gcd(p_i,p) = 1$ 입니다. 따라서 Theorem 4.1.2에 의하면 다음을 얻습니다.

$$(a/p) = (\pm 1/p)(p_1/p)^{k_1}(p_2/p)^{k_2} \cdots (p_r/p)^{k_r}$$

$(\pm 1/p)$의 값은 Theorem 4.1.2를 이용해서 계산할수 있으므로 결국 (a/p)를 계산하기 위해 서로 다른 소수 p, q에 대하여 (p/q)를 계산하는 방법만 알면 됩니다. 따라서 4장 전체의 목적은 서로 다른 소수 p, q에 대하여 (p/q)를 계산하는 방법을 소개하는겁니다.

오일러의 판정법에 의하면 $(p/q) \equiv p^{\frac{q-1}{2}} \pmod{q}$ 이므로 오일러의 판정법만 알면 계산할수 있다고 생각할수 있는데 일반적으로 $p^{\frac{q-1}{2}}$ 를 계산하는게 쉽지 않습니다.
p, q가 조금만 커져도 매우 큰 자연수가 되기 때문입니다.

계산기가 발달된 현대에는 계산하기 쉬울수도 있지만 계산기가 없었던 시대에는 힘들었기 때문에 새로운 방법이 필요했습니다. 수학자 가우스가 (p/q)를 계산할 때 큰 도움이 되는 등식을 발견했는데 그것은 나중에 소개하겠습니다.

Problem 4.1.1 p는 홀수인 소수이고 a는 $\gcd(a,p)=1$ 을 만족하는 정수일 때 합동방정식 $x^2 \equiv -a^2 \pmod{p}$ 의 해가 존재할 필요충분조건은 $p \equiv 1 \pmod{4}$ 임을 증명하시오.

(증명)

$(-a^2/p)=(-1/p)(a^2/p)=(-1)^{\frac{p-1}{2}}$ 이므로 합동방정식의 해가 존재할 필요충분조건은 $\frac{p-1}{2}$가 짝수인 것이고 이것은 $p \equiv 1 \pmod{4}$ 와 동치이다. ■

Problem 4.1.2 p는 홀수인 소수이고 a는 법 p에 대한 이차잉여일 때 다음을 증명하시오.
(a). a는 법 p의 원시근이 될수 없다.
(b). $p \equiv 1 \pmod{4}$ 이면 $p-a$ 는 법 p에 대한 이차잉여이고 $p \equiv 3 \pmod{4}$ 이면 $p-a$ 는 법 p에 대한 이차 비잉여이다.
(c). $p \equiv 3 \pmod{4}$ 이면 $x \equiv \pm a^{\frac{p+1}{4}} \pmod{p}$ 는 합동방정식 $x^2 \equiv a \pmod{p}$ 의 해가 된다.

(증명)

(a). 오일러의 판정법에 의하면 $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ 이므로 법 p에서 a의 위수는 $\phi(p)=p-1$ 보다 작다. 따라서 a는 법 p의 원시근이 될수 없다. ■

(b). $p-a \equiv -a \pmod{p}$ 이므로 $(-a/p)=(-1/p)(a/p)=(-1/p)$ 이다. 따라서 $p \equiv 1 \pmod{4}$ 이면 $(-1/p)=1$ 이고 $p \equiv 3 \pmod{4}$ 이면 $(-1/p)=-1$ 이므로 주어진 명제는 참이다. ■

(c). 오일러의 판정법에 의하면 $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ 이므로 $a^{\frac{p+1}{2}} \equiv a \pmod{p}$ 를 얻고 $p \equiv 3 \pmod{4}$ 이므로 $\frac{p+1}{4}$은 자연수이다. 따라서 다음을 얻는다.

$$\left(\pm a^{\frac{p+1}{4}}\right)^2 \equiv a^{\frac{p+1}{2}} \equiv a \pmod{p}$$

그러므로 $x \equiv \pm a^{\frac{p+1}{4}} \pmod{p}$ 는 주어진 합동방정식의 해가 된다. ■

Problem 4.1.3 음이 아닌 정수 n에 대하여 $F_n = 2^{2^n}+1$ 이 소수이면 법 F_n에 대한 모든 이차 비잉여는 법 F_n의 원시근임을 증명하시오.

(증명)

법 F_n에 대한 이차 비잉여를 a라고 하자. 그러면 F_n은 소수이므로 오일러의 판정법에 의해 다음을 얻을수 있다.

$$a^{\frac{F_n-1}{2}} \equiv a^{2^{2^n}-1} \equiv -1 \pmod{F_n} \tag{4}$$

따라서 $a^{2^{2^n}} \equiv 1 \pmod{F_n}$ 이고 자연수 k에 대하여 2^k의 양의 약수는 $0 \le m \le k$ 를 만족하는 정수 m에 대하여 2^m 형태로 나타난다.

그러므로 2^{2^n}의 양의 약수는 $0 \le m \le 2^n$을 만족하는 정수 m에 대하여 2^m 형태로 나타난다. 이제 $a^{2^m} \equiv 1 \pmod{F_n}$ 을 만족할 경우 $m = 2^n$ 임을 보이자.

만약 $m \neq 2^n$ 이면 $m \le 2^n - 1$ 이므로 $2^m \mid 2^{2^n-1}$ 이다.
따라서 $a^{2^{2^n-1}} \equiv 1 \pmod{F_n}$ 을 얻는데 F_n은 홀수이므로 이것은 (4)에 모순이다.
그러므로 $m = 2^n$ 이고 따라서 법 F_n에서 a의 위수는 $\phi(F_n) = 2^{2^n}$ 이다.
즉, a는 법 F_n의 원시근이다. ■

Problem 4.1.4 p가 소수일 때 법 p의 원시근 r에 대하여 법 p의 기약잉여계를 $S = \{r, r^2, r^3, \ldots, r^{p-1}\}$로 나타냈다고 하자. 다음을 증명하시오.
(a). $p \ge 3$ 일 때 $1 \le k \le p-1$ 을 만족하는 자연수 k에 대하여 r^k가 법 p의 이차잉여가 될 필요충분조건은 k가 짝수인 것이다.
(b). $p \ge 5$ 이면 S 의 원소들 중 법 p의 모든 이차잉여의 합은 p의 배수이다.
(c). $p \ge 7$ 이면 S 의 원소들 중 법 p의 모든 이차잉여의 제곱의 합은 p의 배수이다.

(증명)
(a). r은 법 p의 원시근이므로 $r^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ 를 만족한다.
따라서 $\left(r^k\right)^{\frac{p-1}{2}} \equiv (-1)^k \pmod{p}$ 이므로 오일러의 판정법에 의하면 r^k가 법 p의 이차잉여가 될 필요충분조건은 $(-1)^k \equiv 1 \pmod{p}$ 을 만족하는 것이고 (3)에 의하면 $(-1)^k = 1$ 이다. 그러므로 조건을 만족할 필요충분조건은 k가 짝수인 것이다. ■

(b). (a)에 의하면 법 p의 모든 이차잉여는 $r^2, r^4, \ldots, r^{p-1}$ 이라고 해도 충분하다.
그리고 등비수열의 합 공식에 의하면 다음을 얻는다.

$$r^2 + r^4 + \cdots + r^{p-1} = \frac{r^2\left(r^{p-1}-1\right)}{r^2-1} \tag{5}$$

이제 $\gcd(r^2-1, p) = 1$ 임을 보이자. 결론을 부정해서 $\gcd(r^2-1, p) \neq 1$ 이라고 가정하면 p는 소수이므로 $r^2 \equiv 1 \pmod{p}$ 이다. 따라서 $p-1 \mid 2$ 를 만족하므로 $p-1 \le 2$ 에서 $p \le 3$ 인데 이것은 조건에 모순이다.

그러므로 $\gcd(r^2-1,p)=1$ 이고 법 p에서 r^2-1 의 곱셈에 대한 역원이 존재한다.
따라서 다음을 얻는다.

$$\frac{r^2(r^{p-1}-1)}{r^2-1} \equiv \frac{r^2(1-1)}{r^2-1} \equiv 0 \pmod{p}$$

그러므로 (5)는 p의 배수이다. ■

(c). (a)에 의하면 법 p의 모든 이차잉여는 $r^2, r^4, \ldots, r^{p-1}$ 이라고 해도 충분하다.
그리고 등비수열의 합 공식에 의하면 다음을 얻는다.

$$r^4 + r^8 + \cdots + r^{2(p-1)} = \frac{r^4(r^{2(p-1)}-1)}{r^4-1} \tag{6}$$

이제 $\gcd(r^4-1,p)=1$ 임을 보이자. 결론을 부정해서 $\gcd(r^4-1,p)\neq 1$ 이라고 가정하면 p는 소수이므로 $r^4 \equiv 1 \pmod{p}$ 이다. 따라서 $p-1 \mid 4$ 를 만족하므로 $p-1 \leq 4$ 에서 $p \leq 5$ 인데 이것은 조건에 모순이다.

그러므로 $\gcd(r^4-1,p)=1$ 이고 법 p에서 r^4-1 의 곱셈에 대한 역원이 존재한다.
따라서 다음을 얻는다.

$$\frac{r^4(r^{2(p-1)}-1)}{r^4-1} \equiv \frac{r^4(1-1)}{r^4-1} \equiv 0 \pmod{p}$$

그러므로 (6)은 p의 배수이다. ■

Problem 4.1.5 p가 홀수인 소수일 때 법 p의 원시근 r에 대하여 법 p의 기약잉여계를 $S=\{r, r^2, r^3, \ldots, r^{p-1}\}$로 나타냈다고 하자. 다음을 증명하시오.

(a). S 의 원소들 중 법 p의 모든 이차잉여의 곱은 법 p에 대하여 $r^{\frac{p^2-1}{4}}$ 과 합동이다.

(b). S 의 원소들 중 법 p의 모든 이차 비잉여의 곱은 법 p에 대하여 $r^{\frac{(p-1)^2}{4}}$ 과 합동이다.

(증명)

Problem 4.1.4에 의하면 r^k가 법 p의 이차잉여가 될 필요충분조건은 k가 짝수이다. (7)

(a). (7)에 의하면 이차잉여의 곱은 다음과 같다.

$$r^{2+4+6+\cdots+(p-1)} \equiv r^{\left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right)} \equiv r^{\frac{p^2-1}{4}} \pmod{p}$$

■

(b). 이차 비잉여의 곱은 다음과 같다.

$$r^{1+3+5+\cdots+(p-2)} \equiv r^{\frac{\left(\frac{p-1}{2}\right)(1+(p-2))}{2}} \equiv r^{\frac{(p-1)^2}{4}} \pmod{p}$$

■

Problem 4.1.6 p가 홀수인 소수일 때 다음을 증명하시오.
(a). r이 법 p의 원시근이면 r은 법 p에 대한 이차 비잉여이다.
(b). 법 p의 원시근이 아니면서 법 p에 대한 이차 비잉여의 개수는
$\frac{p-1}{2}-\phi(p-1)$ 이다.

(증명)

(a). p가 홀수인 소수이고 r이 법 p의 원시근이므로 $r^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ 이다.
따라서 오일러의 판정법에 의하면 r은 법 p에 대한 이차 비잉여이다. ■

(b). (a)에 의하면 법 p에 대한 이차 비잉여는 법 p의 원시근을 모두 포함한다.
따라서 조건을 만족하는 것의 개수는 법 p의 이차 비잉여의 개수 $\frac{p-1}{2}$ 에서
법 p의 원시근의 개수 $\phi(p-1)$ 를 뺀 $\frac{p-1}{2}-\phi(p-1)$ 이다. ■

Problem 4.1.7 홀수인 소수 q에 대하여 $p=2q+1$ 도 소수라고 하자.
다음 물음에 답하시오.
(a). $\mathbb{Z}_p^{\times}$에서 법 p의 이차 비잉여의 개수와 법 p의 원시근의 개수를 구하시오.
(b). $2q$는 법 p에 대한 이차 비잉여이면서 법 p의 원시근이 아님을 증명하시오.

(풀이)

(a). 조건에 의하면 $\mathbb{Z}_p^{\times}$에서 법 p에 대한 이차 비잉여의 개수는 $\frac{p-1}{2}=q$ 이고
법 p의 원시근의 개수는 $\phi(\phi(p))=\phi(2q)=\phi(q)=q-1$ 이다. ■

(b). q가 홀수인 소수이므로 $q=2k+1$ 라고 하면 $p=4k+3$ 이다.
따라서 $p \equiv 3 \pmod{4}$ 이므로 $(2q/p)=(-1/p)=-1$ 을 얻고
그러므로 $2q$는 법 p에 대한 이차 비잉여이다.

그리고 $2q \equiv -1 \pmod{p}$ 이고 $(-1)^2 \equiv 1 \pmod{p}$ 이므로 $2q$는 법 p의
원시근이 될수 없다. 만약 법 p의 원시근이면 $\phi(p)=p-1 \mid 2$ 에서 $p-1 \leq 2$ 이므로
$p \leq 3$ 을 얻는데 q는 홀수인 소수이므로 $p \geq 7$ 이다. 따라서 모순이다. ■

Problem 4.1.7 (a)의 조건을 만족할 경우 $\mathbb{Z}_p^{\times}$에서 법 p에 대한 이차 비잉여의 개수는 법 p의 원시근보다 하나 더 많고 Problem 4.1.6 (a)에 의하면 법 p에 대한 이차 비잉여는 법 p의 원시근을 모두 포함하고 있습니다.

그리고 Problem 4.1.7 (b)에 의하면 $\mathbb{Z}_p^{\times}$에서 법 p에 대한 이차 비잉여인데 원시근은 아닌 유일한 원소가 $2q$입니다.

Problem 4.1.8 p는 $p \equiv 1 \pmod 8$ 을 만족하는 소수이고 r은 법 p의 원시근이다. 그러면 $x \equiv \pm\left(r^{\frac{p-1}{8}} + r^{\frac{7(p-1)}{8}}\right) \pmod p$ 는 합동방정식 $x^2 \equiv 2 \pmod p$ 의 해가 됨을 증명하시오.

(증명)

$a = r^{\frac{p-1}{8}}$ 라고 하자. 그러면 $a + a^7$ 가 주어진 합동방정식을 만족함을 보이면 충분하다.

r은 법 p의 원시근이므로 $a^8 \equiv 1 \pmod p$ 이고 $a^4 \equiv r^{\frac{p-1}{2}} \equiv -1 \pmod p$ 이므로 $a^{12} \equiv (a^4)^3 \equiv (-1)^3 \equiv -1 \pmod p$ 이다. 따라서 다음을 얻는다.

$$(a + a^7)^2 \equiv a^2 + a^{14} + 2 \equiv a^2(1 + a^{12}) + 2 \equiv 2 \pmod p$$

그러므로 $x \equiv \pm\left(r^{\frac{p-1}{8}} + r^{\frac{7(p-1)}{8}}\right) \pmod p$ 는 합동방정식 $x^2 \equiv 2 \pmod p$ 의 해가 된다. ■

Problem 4.1.9 p가 홀수인 소수이고 r은 법 p의 원시근, a는 $\gcd(a,p)=1$ 을 만족하는 정수일 때 다음을 증명하시오.

(a). $(a/p) = (-1)^{\mathrm{ind}_r a}$ 이다.

(b). $\sum_{a=1}^{p-1} (a/p) = 0$ 이다.

(증명)

(a). 조건에 의하면 $r^{\frac{p-1}{2}} \equiv -1 \pmod p$ 이므로 이산로그의 정의에 의하면

$$(a/p) \equiv r^{\frac{(\mathrm{ind}_r a)(p-1)}{2}} \equiv (-1)^{\mathrm{ind}_r a} \pmod p$$

가 성립한다. 따라서 (3)에 의하면 $(a/p) = (-1)^{\mathrm{ind}_r a}$ 이다. ■

(b). 1부터 $p-1$ 까지의 자연수들 중엔 짝수와 홀수 모두 $\frac{p-1}{2}$개 있다.

즉, 개수가 같으므로 (a)에 의하면 (b)의 합은 $\frac{p-1}{2}$개의 1과 $\frac{p-1}{2}$개의 -1을 더하는 것과 같다. 따라서 $\sum_{a=1}^{p-1} (a/p) = 0$ 이다. ■

Problem 4.1.10 p가 홀수인 소수일 때 다음 물음에 답하시오.

(a). $\sum_{a=1}^{p-2} (a(a+1)/p) = -1$ 임을 증명하시오.

(b). $(a/p)=(a+1/p)=1$ 를 만족하는 $1 \le a \le p-2$ 인 정수 a의 개수를 $N(p)$라고 하자. 그러면 $f_p(a)=\frac{1}{4}(1+(a/p))(1+(a+1/p))$ 에 대하여 $N(p)=\sum_{a=1}^{p-2} f_p(a)$ 임을 증명하고 이것을 이용해서 $N(p)=\frac{1}{4}\left(p-4-(-1)^{\frac{p-1}{2}}\right)$ 임을 증명하시오.

(c). $p \ge 7$ 이면 (8)을 만족하는 $1 \le a, b \le p-2$ 인 정수 a, b가 존재함을 증명하시오.

$$\begin{matrix}(a/p)=(a+1/p)=1\\(b/p)=(b+1/p)=-1\end{matrix} \tag{8}$$

(증명)

(a). $1 \le a \le p-2$ 이면 a는 법 p에서 곱셈에 대한 역원을 갖는다. 그것을 x라고 하면 $ax \equiv 1 \pmod p$ 이므로 $(ax/p)=(a/p)(x/p)=1$ 을 얻는다.
따라서 $(a/p)=(x/p)$ 가 성립한다.

그러므로 $(a(a+1)/p)=(a/p)(a+1/p)=(x/p)(a+1/p)=(1+x/p)$ 이고 $(p-1)^2 \equiv 1 \pmod p$ 이므로 a가 $1 \le a \le p-2$ 에서 움직이면 x도 $1 \le x \le p-2$ 에서만 움직인다.

그리고 $1 \le a \le p-2$ 를 만족하는 자연수 a는 법 p에서 곱셈에 대한 역원을 갖는다.
따라서 Problem 4.1.9 (b)에 의하면 다음을 얻는다.

$$\begin{aligned}\sum_{a=1}^{p-2}(a(a+1)/p) &= \sum_{x=1}^{p-2}(1+x/p)\\ &= -(1/p)+\sum_{x=1}^{p-1}(x/p)\\ &= -1\end{aligned}$$

■

(b). 르장드르 기호의 정의에 의하면 $f_p(a)=1$ 을 만족할 필요충분조건은 $(a/p)=(a+1/p)=1$ 임을 쉽게 알수 있다. 마찬가지로 르장드르 기호의 정의에 의하면 $f_p(a)$가 가질수 있는 값은 $0,1$ 뿐이므로 $N(p)=\sum_{a=1}^{p-2} f_p(a)$ 임은 명백하다.

따라서 (a)와 Problem 4.1.9 (b), Theorem 4.1.2에 의하면 다음을 얻는다.

$$
\begin{aligned}
N(p) &= \sum_{a=1}^{p-2} f_p(a) \\
&= \frac{1}{4}\sum_{a=1}^{p-2}(1+(a/p)+(a+1/p)+(a/p)(a+1/p)) \\
&= \frac{1}{4}\left(p-2+\sum_{a=1}^{p-2}(a/p)+\sum_{a=1}^{p-2}(a+1/p)+\sum_{a=1}^{p-2}(a(a+1)/p)\right) \\
&= \frac{1}{4}(p-2-(p-1/p)-(1/p)-1) \\
&= \frac{1}{4}(p-2-(-1/p)-(1/p)-1) \\
&= \frac{1}{4}\left(p-4-(-1)^{\frac{p-1}{2}}\right)
\end{aligned}
$$

■

(c). $1 \le a, b \le p-2$ 이면서 (8)을 만족하는 정수 a의 개수를 $N_1(p)$, 정수 b의 개수를 $N_2(p)$라고 하자. 그러면 (b)에 의해 $N_1(p)=\frac{1}{4}\left(p-4-(-1)^{\frac{p-1}{2}}\right)$ 이고 (b)와 비슷한 방법으로 $g_p(a)=\frac{1}{4}(1-(a/p))(1-(a+1/p))$ 라고 하면 $N_2(p)=\sum_{a=1}^{p-2} g_p(a)$ 임을 쉽게 알수 있다. 따라서 다음을 얻을수 있다.

$$
\begin{aligned}
N_2(p) &= \sum_{a=1}^{p-2} g_p(a) \\
&= \frac{1}{4}\sum_{a=1}^{p-2}(1-(a/p)-(a+1/p)+(a/p)(a+1/p)) \\
&= \frac{1}{4}\left(p-2-\sum_{a=1}^{p-2}(a/p)-\sum_{a=1}^{p-2}(a+1/p)+\sum_{a=1}^{p-2}(a(a+1)/p)\right) \\
&= \frac{1}{4}(p-2+(p-1/p)+(1/p)-1) \\
&= \frac{1}{4}(p-2+(-1/p)+(1/p)-1) \\
&= \frac{1}{4}\left(p-2+(-1)^{\frac{p-1}{2}}\right)
\end{aligned}
$$

그러므로 정리하면 다음과 같다.

$$
\begin{aligned}
N_1(p) &= \frac{1}{4}\left(p-4-(-1)^{\frac{p-1}{2}}\right) \\
N_2(p) &= \frac{1}{4}\left(p-2+(-1)^{\frac{p-1}{2}}\right)
\end{aligned}
$$

$p \ge 7$ 이면 $N_1(p), N_2(p)$는 모두 자연수임을 쉽게 알수 있다.

따라서 $p \ge 7$ 이면 $1 \le a, b \le p-2$ 이면서 (8)을 만족하는 정수 a, b가 존재한다. ■

Problem 4.1.11 다음을 증명하시오.
(a). p가 홀수인 소수이고 a,k는 $\gcd(a,p)=\gcd(k,p)=1$ 을 만족하는 정수이다.
이때 방정식 $x^2-ay^2=kp$ 을 만족하는 정수 x,y가 존재하면 $(a/p)=1$ 이다.
(b). $x^2+5y^2=7$ 을 만족하는 정수 x,y는 존재하지 않는다. 따라서 (a)의 역은 거짓이다.

(증명)
(a). 적당한 정수 x_0,y_0 가 존재해서 $x_0^2-ay_0^2=kp$ 를 만족한다고 가정했을 때 $\gcd(x_0,p)=\gcd(y_0,p)=1$ 임을 보이자. 결론을 부정해서 x_0,y_0 둘중 적어도 하나가 p의 배수라고 가정하면 $x_0^2-ay_0^2=kp$ 이고 $\gcd(a,p)=1$ 이므로 나머지 하나도 p의 배수가 되어야 한다.

따라서 $p^2 \mid kp$ 이므로 $p \mid k$ 를 얻는데 이것은 $\gcd(k,p)=1$ 에 모순이다.
그러므로 $\gcd(x_0,p)=\gcd(y_0,p)=1$ 이다. 즉, y_0는 법 p에서 곱셈에 대한 역원을 갖고 그것을 z_0라고 하면 다음을 얻는다.

$$x_0^2 \equiv ay_0^2 \pmod{p} \Rightarrow (x_0z_0)^2 \equiv a \pmod{p}$$

그러므로 $(a/p)=1$ 이다. ■

(b). 오일러의 판정법에 의하면 $(-5/7)=1$ 임을 쉽게 알수 있다.
따라서 $x^2+5y^2=7$ 을 만족하는 정수 x,y가 존재하지 않음을 보이자.
그러면 이것은 (a)의 역이 거짓임을 설명할수 있는 반례가 된다.

모든 정수 a에 대하여 $a^2 \equiv 0,1,4 \pmod{5}$ 임을 쉽게 알수 있다.
그러므로 $x^2+5y^2=7$ 을 만족하는 정수 x,y가 존재한다면 $x^2 \equiv 2 \pmod{5}$ 인데 이것은 $a^2 \equiv 0,1,4 \pmod{5}$ 에 모순이다.

따라서 $x^2+5y^2=7$ 을 만족하는 정수 x,y는 존재하지 않는다. ■

4.2 가우스의 보조정리

작성자 : 네냐플(Nenyaffle)

4.2절에서는 4장에서 가장 중요한 정리인 이차 상호 법칙을 증명할 때 도움이 되는 가우스의 보조정리를 소개하려고 합니다. 여기서 소개할 가우스의 보조정리는 르장드르 기호를 직접 계산할 때 크게 도움이 되는 정리는 아닙니다.

Theorem 4.2.1 가우스의 보조정리(Gauss's Lemma)

p는 홀수인 소수이고 a는 $\gcd(a,p)=1$ 을 만족하는 정수이다. 그리고 집합 S 를 $S=\left\{a,2a,3a,...,\left(\frac{p-1}{2}\right)a\right\}$라고 할 때 S 의 원소들 중 p로 나눈 나머지가 $\frac{p}{2}$보다 큰 원소의 개수를 n이라고 하자. 그러면 다음 등식이 성립한다.

$$(a/p)=(-1)^n$$

(증명)

$\gcd(a,p)=1$ 이므로 S 의 원소 $a,2a,3a,...,\left(\frac{p-1}{2}\right)a$는 법 p에서 모두 0이 아니고 서로 다른 원소이다. 따라서 S 는 법 p에서 0이 아닌 원소를 $\frac{p-1}{2}$개 가지고 있고 S 의 원소를 p로 나눈 나머지는 모두 양수이다.

S 의 원소를 p로 나눈 나머지는 각각의 $i=1,2,...,m$ 에 대하여 $0<r_i<\frac{p}{2}$ 인 $r_1,r_2,...,r_m$ 과 각각의 $j=1,2,...,n$ 에 대하여 $\frac{p}{2}<s_j<p$ 인 $s_1,s_2,...,s_n$ 에 대해 $r_1,r_2,...,r_m,s_1,s_2,...,s_n$ 으로 배열할수 있고 이때 $m+n=\frac{p-1}{2}$ 이다.

예를 들어 $a=5,p=13$ 이면 $S=\{5,10,15,20,25,30\}$ 이고 S 의 원소를 13으로 나눈 나머지를 배열하면 $5,10,2,7,12,4$ 이다. 그리고 $\frac{p}{2}=6.5$ 이므로 이때 $r_1=5,r_2=2,r_3=4$ 이고 $s_1=10,s_2=7,s_3=12$ 이다.

각각의 $j=1,2,...,n$ 에 대하여 $0<p-s_j<\frac{p}{2}$ 이므로 다음 $m+n=\frac{p-1}{2}$개의 자연수는 모두 $\frac{p}{2}$보다 작다.

$$r_1,r_2,...,r_m,p-s_1,p-s_2,\ ...,p-s_n \tag{9}$$

이제 (9)는 서로 다른 자연수임을 보이자. 결론을 부정해서 적당한 i,j가 존재해서 $p-s_i=r_j$ 라고 가정하면 s_i,r_j는 S 의 어떤 원소를 p로 나눈 나머지이다.

따라서 $1 \le u, v \le \frac{p-1}{2}$ 를 만족하는 자연수 u, v가 존재해서

$s_i \equiv ua \pmod p$, $r_j \equiv va \pmod p$ 를 만족한다. 그러므로 다음을 얻는다.

$$(u+v)a \equiv s_i + r_j \equiv 0 \pmod p$$

$\gcd(a,p)=1$ 이므로 $u+v \equiv 0 \pmod p$ 에서 $p \mid u+v$ 인데 $2 \le u+v \le p-1$ 이므로 이것은 모순이다. 따라서 (9)는 서로 다른 자연수이다.

(9)는 서로 다른 $\frac{p-1}{2}$개의 자연수이고 모두 $\frac{p}{2}$보다 작으므로 (9)는 1부터 $\frac{p-1}{2}$까지의 자연수를 배열한 것에 불과하다. 그러므로 다음이 성립한다.

$$\begin{aligned}\left(\frac{p-1}{2}\right)! &\equiv r_1 r_2 \cdots r_m (p-s_1)(p-s_2)\cdots(p-s_n) \\ &\equiv (-1)^n r_1 r_2 \cdots r_m s_1 s_2 \cdots s_n \pmod p\end{aligned}$$

그리고 $r_1, r_2, ..., r_m, s_1, s_2, ..., s_n$ 은 S 의 원소를 p로 나눈 나머지를 배열한 것이므로 이들의 곱은 S 의 원소를 모두 곱한것과 법 p에서 합동이다. 따라서 다음을 얻는다.

$$\begin{aligned}\left(\frac{p-1}{2}\right)! &\equiv (-1)^n r_1 r_2 \cdots r_m s_1 s_2 \cdots s_n \\ &\equiv (-1)^n a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod p\end{aligned}$$

$\gcd\left(\left(\frac{p-1}{2}\right)!, p\right)=1$ 이므로 $(-1)^n a^{\frac{p-1}{2}} \equiv 1 \pmod p$ 이고 양변에 $(-1)^n$을 곱하면 오일러의 판정법에 의해 다음을 얻는다.

$$(a/p) \equiv a^{\frac{p-1}{2}} \equiv (-1)^n \pmod p$$

p는 홀수인 소수이므로 $(a/p)=(-1)^n$ 가 성립한다. ■

예를 들어 $a=5, p=13$ 이면 $S=\{5,10,15,20,25,30\}$ 이고 S 의 원소를 13으로 나눈 나머지를 배열하면 $5,10,2,7,12,4$ 입니다. 그리고 $\frac{p}{2}=6.5$ 이므로 S 의 원소들 중 13으로 나눈 나머지가 6.5를 넘는 것은 $10, 7, 12$ 이렇게 3개입니다.

따라서 가우스의 보조정리에 의하면 $(5/13)=(-1)^3=-1$ 입니다. 오일러의 판정법을 사용해서 계산해봐도 $(5/13) \equiv 5^{\frac{13-1}{2}} \equiv 5^6 \equiv -1 \pmod{13}$ 이므로 $(5/13)=-1$ 을 얻을수 있습니다.

가우스의 보조정리를 사용하면 p가 홀수인 소수일 때 $(2/p)$를 쉽게 계산할수 있습니다. 나중에 이차 상호 법칙을 배우면 $(2/p)$를 쉽게 계산할수 있다는 것이 중요하다는 것을 알게 될겁니다.

Corollary 4.2.1 p가 홀수인 소수이면 다음이 성립한다.

(a). $(2/p)=\begin{cases}1 & (p\equiv\pm 1\,(\mathrm{mod}\,8))\\ -1 & (p\equiv\pm 3\,(\mathrm{mod}\,8))\end{cases}$ 이다.

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

(증명)

(a). 집합 S 를 다음과 같이 정의하자.

$$S=\left\{1\times 2, 2\times 2, 3\times 2, \ ..., \left(\frac{p-1}{2}\right)\times 2\right\}=\{2,4,6,...,p-1\}$$

그러면 S 의 원소는 모두 p보다 작으므로 S 의 원소들 중 p로 나누었을 때 나머지가 $\frac{p}{2}$보다 큰 자연수의 개수는 S 의 원소들 중 $\frac{p}{2}$보다 큰 자연수의 개수와 같다.

S 의 원소는 $1\le k\le\frac{p-1}{2}$ 를 만족하는 자연수 k에 대하여 $2k$로 표현되고

$2k<\frac{p}{2}$ 를 만족할 필요충분조건은 $k<\frac{p}{4}$ 이다. 따라서 바닥함수 $\lfloor x\rfloor$ 의 정의에 의하면 $k<\frac{p}{4}$ 를 만족하는 자연수 k의 개수는 $\left\lfloor\frac{p}{4}\right\rfloor$ 이므로 S 의 원소들 중 $\frac{p}{2}$보다 큰 자연수의 개수는 $\frac{p-1}{2}-\left\lfloor\frac{p}{4}\right\rfloor$ 라고 할수 있다.

한편 p는 홀수인 소수이므로 적당한 정수 k에 대하여
$p=8k-3, 8k-1, 8k+1, 8k+3$ 형태로만 나타나고 가우스의 보조정리에 의하면

$p=8k-3$ 일 때 $n=4k-2-\left\lfloor 2k-\frac{3}{4}\right\rfloor=2k-1$ 이므로 $(2/p)=-1$

$p=8k-1$ 일 때 $n=4k-1-\left\lfloor 2k-\frac{1}{4}\right\rfloor=2k$ 이므로 $(2/p)=1$

$p=8k+1$ 일 때 $n=4k-\left\lfloor 2k+\frac{1}{4}\right\rfloor=2k$ 이므로 $(2/p)=1$

$p=8k+3$ 일 때 $n=4k+1-\left\lfloor 2k+\frac{3}{4}\right\rfloor=2k+1$ 이므로 $(2/p)=-1$

이다. 따라서 정리하면 $(2/p)=\begin{cases}1 & (p\equiv\pm 1\,(\mathrm{mod}\,8))\\ -1 & (p\equiv\pm 3\,(\mathrm{mod}\,8))\end{cases}$ 를 얻을수 있다. ■

(b). 정수 k에 대하여 $p=8k\pm1$ 이면 $\frac{p^2-1}{8}=8k^2\pm2k$ 이므로 짝수이고

$p=8k\pm3$ 이면 $\frac{p^2-1}{8}=8k^2\pm6k+1$ 이므로 홀수이다.

따라서 (a)에 의하면 $(2/p)=(-1)^{\frac{p^2-1}{8}}$ 이다. ■

이제 Corollary 4.2.1을 이용해서 쉽게 증명할수 있는 2가지 정리를 소개하겠습니다.

Theorem 4.2.2 p와 $2p+1$이 모두 홀수인 소수이면 $2\times(-1)^{\frac{p-1}{2}}$ 는 법 $2p+1$의 하나의 원시근이다.

(증명)

$q=2p+1$ 라고 하자. p는 홀수인 소수이므로 $p\equiv1\pmod4$ 또는 $p\equiv3\pmod4$ 를 만족한다.

case1) $p\equiv1\pmod4$

이 경우 $\frac{p-1}{2}$는 짝수이므로 $2\times(-1)^{\frac{p-1}{2}}=2$ 이다. 그리고 p,q가 홀수인 소수이므로 $\phi(q)=2p$ 의 양의 약수는 $1,2,p,2p$ 뿐이다.

p가 홀수인 소수이므로 $q\geq7$ 이다. 따라서 다음은 명백하다.

$$2^1\not\equiv1\pmod q$$
$$2^2\not\equiv1\pmod q$$

한편 오일러의 판정법에 의하면 $(2/q)\equiv2^p\pmod q$ 이고 $p\equiv1\pmod4$ 이면 $q\equiv3\pmod8$ 이므로 Corollary 4.2.1에 의하면 $(2/q)=-1$ 이다. 따라서 $2^p\equiv-1\not\equiv1\pmod q$ 이다.

그러므로 법 q에서 2의 위수는 $2p=\phi(q)$ 이다. 따라서 2는 법 q의 원시근이다.

case2) $p\equiv3\pmod4$

이 경우 $\frac{p-1}{2}$는 홀수이므로 $2\times(-1)^{\frac{p-1}{2}}=-2$ 이고 $\phi(q)=2p$ 이므로 $2p$의 양의 약수는 $1,2,p,2p$ 뿐이다. 그리고 $q\geq7$ 이므로 다음은 명백하다.

$$(-2)^1\not\equiv1\pmod q$$
$$(-2)^2\not\equiv1\pmod q$$

마찬가지로 오일러의 판정법에 의하면 $(-2/q)\equiv(-2)^p\pmod q$ 이고 $p\equiv3\pmod4$ 이면 $q\equiv7\equiv-1\pmod8$ 이다. 따라서 $q\equiv-1\equiv3\pmod4$ 이므로 $(-2/q)=(-1/q)(2/q)=-1$ 을 얻는다.

그러므로 $(-2)^p \equiv -1 \neq 1 \pmod{q}$ 에서 법 q에서 -2의 위수는 $2p = \phi(q)$ 임을 알수 있다. 따라서 -2는 법 q의 원시근이다.

정리하면 $2 \times (-1)^{\frac{p-1}{2}}$ 는 법 $q = 2p+1$ 의 하나의 원시근이다. ■

Theorem 4.2.2에서 p와 $2p+1$이 모두 홀수인 소수가 되도록 하는 소수 p를 수학에서는 **소피 제르맹 소수(Sophie Germain Prime)**라고 부릅니다. 소피 제르맹은 1776년에 프랑스 파리에서 태어났고 페르마의 마지막 정리의 증명에 큰 기여를 한 여성 수학자입니다.

조금 구체적으로 이야기하자면 수학자 오일러가 페르마 본인이 $n = 4$ 일 때 증명한 것을 발견했고 오일러가 이것을 이용해서 $n = 3$ 일때의 증명을 했습니다. 그런데 $n = 5$ 일때의 증명은 발견하지 못했습니다.

이렇게 수학자들이 개별적인 n에 대해 페르마의 마지막 정리를 증명하려고 하던 시대에 소피 제르맹은 소피 제르맹 소수를 이용해서 현대에 **소피 제르맹의 정리(Sophie Germain's Theorem)**라고 부르는 정리를 발표했습니다.

소피 제르맹은 소피 제르맹의 정리를 이용해서 보다 많은 자연수 n에 대해 페르마의 마지막 정리가 성립한다는 것을 한번에 증명한 업적을 남긴 수학자입니다. 물론 소피 제르맹도 모든 자연수 n에 대해 성립한다는 것을 증명하지는 못했습니다.

소피 제르맹 소수의 개수가 무한한지는 아직 알려지지 않았습니다. 현재까지 발견된 가장 큰 소피 제르맹 소수는 $2618163402417 \times 2^{1290000} - 1$ 이고 388342자리 자연수입니다.

한편 Corollary 4.2.1을 이용하면 $8k-1$ 형태를 갖는 소수의 개수가 무한하다는 것도 쉽게 증명할수 있습니다.

Theorem 4.2.3 $k \in \mathbb{Z}$ 일 때 $8k-1$ 형태를 갖는 소수의 개수는 무한하다.

(증명)

정수 m, n에 대하여 $a = 8m+1, b = 8n+1$ 이면 다음이 성립한다.

$$ab = 8(8mn+m+n)+1$$

따라서 a, b가 $8k+1$ 형태를 갖는 정수이면 ab도 $8k+1$ 형태를 갖는 정수이다. (10)

이제 결론을 부정해서 $8k-1$ 형태를 갖는 소수의 개수가 유한하다고 가정하고 그것을 $p_1, p_2, \ldots, p_n$ 이라고 하자. 그리고 자연수 N 을 $N = (4p_1p_2 \cdots p_n)^2 - 2$ 라고 하자.

그러면 N은 3 이상의 홀수이므로 홀수인 소수만 소인수로 갖고 그것을 p라고 하면

$$(4p_1p_2 \cdots p_n)^2 \equiv 2 \pmod{p}$$

이다. 따라서 $(2/p) = 1$ 이므로 Corollary 4.2.1에 의하면 $p \equiv \pm 1 \pmod{8}$ 이다.
그러므로 N의 소인수는 모두 $8k \pm 1$ 형태이다.

이제 N이 $8k-1$ 형태의 소수를 약수로 갖는다는 것을 증명하자. 결론을 부정해서 N이 $8k+1$ 형태의 소수만 약수로 갖는다고 가정하면 (10)에 의해 N은 $8k+1$ 형태의 정수가 되어야 하는데 N은 $16k-2$ 형태의 정수이다. 이것은 모순이다.

따라서 N은 $8k-1$ 형태의 소수를 약수로 갖는다. 그러므로 적당한 $i=1,2,...,n$ 에 대하여 $p=p_i$ 를 만족하고 $p_i \mid N$ 인데 $p_i \mid (4p_1p_2\cdots p_n)^2$ 이므로 $p_i \mid 2$ 를 얻는다.

즉, $p_i=2$ 인데 이것은 p_i가 홀수인 소수라는 것에 모순이다. 따라서 $8k-1$ 형태를 갖는 소수의 개수는 무한하다. ■

Problem 4.2.1 자연수 n에 대하여 $p=3\times 2^n+1$ 이 소수일 때 $p\neq 13$ 이면 2는 법 p의 원시근이 될수 없음을 증명하시오.

$n=1$ 이면 $p=7$ 이고 이때 $2^3\equiv 1 \pmod p$ 이므로 2는 법 p의 원시근이 될수 없다. 그리고 $n=2$ 이면 $p=13$ 이고 이때 다음 식에 의하면 2는 법 p의 원시근이다.

$$2^1\equiv 2 \pmod{13}$$
$$2^2\equiv 4 \pmod{13}$$
$$2^3\equiv 8 \pmod{13}$$
$$2^4\equiv 3 \pmod{13}$$
$$2^6\equiv 12 \pmod{13}$$
$$2^{12}\equiv 1 \pmod{13}$$

따라서 $n\geq 3$ 일 때 2가 법 p의 원시근이 될수 없음을 증명하면 충분하다.

조건에 의하면 $\phi(p)=3\times 2^n$ 이고 오일러의 판정법에 의하면 다음을 얻는다.

$$(2/p)\equiv 2^{3\times 2^{n-1}} \pmod p$$

$n\geq 3$ 이므로 $p\equiv 1 \pmod 8$ 이고 따라서 Corollary 4.2.1에 의하면 $(2/p)=1$ 이다. 그러므로 $2^{3\times 2^{n-1}}\equiv 1 \pmod p$ 이고 $3\times 2^{n-1}<3\times 2^n=\phi(p)$이므로 2는 법 p의 원시근이 될수 없다. ■

Problem 4.2.2 다음을 증명하시오.

(a). p와 $q=2p+1$가 모두 홀수인 소수이면 -4는 법 q의 원시근이다.

(b). p가 $p\equiv 1 \pmod 4$ 를 만족하는 소수이면 -4와 $\dfrac{p-1}{4}$는 모두 법 p에 대한 이차잉여이다.

(증명)

(a). q는 소수이므로 $\phi(q)=2p$ 이고 조건에 의하면 다음은 명백하다.

$$(-4)^1\not\equiv 1 \pmod q$$
$$(-4)^2\not\equiv 1 \pmod q$$

그리고 오일러의 판정법에 의하면 $(-4/q)\equiv (-4)^p \pmod q$ 를 얻는다.

p가 홀수인 소수이므로 $q \equiv 3 \pmod 4$ 이다. 따라서 $(-4/q) = (-1/q)(2/q)^2 = -1$ 이므로 $(-4)^p \equiv -1 \not\equiv 1 \pmod q$ 이다. 그러므로 -4는 법 q의 원시근이다. ■

(b). $p \equiv 1 \pmod 4$ 이므로 $(-4/p) = (-1/p)(2/p)^2 = 1$ 이다.
따라서 -4는 법 p에 대한 이차잉여이다.

그리고 조건에 의하면 $\frac{p-1}{4}$는 자연수이고 $(p-1/p) = (-1/p) = 1$ 이다.
따라서 $(p-1/p) = (4/p)\left(\frac{p-1}{4}/p\right) = 1$ 이고 $(4/p) = (2/p)^2 = 1$ 이므로
$\left(\frac{p-1}{4}/p\right) = 1$ 이다. 그러므로 $\frac{p-1}{4}$는 법 p에 대한 이차잉여이다. ■

Problem 4.2.3 p와 $q = 4p+1$가 모두 홀수인 소수일 때 다음을 증명하시오.
(a). 법 q에 대한 임의의 이차 비잉여 a는 법 q의 원시근이거나 $\mathrm{ord}_q(a) = 4$ 이다.
(b). 2는 법 q의 원시근이다.

(증명)
(a). 오일러의 판정법에 의하면 $(a/q) \equiv a^{2p} \equiv -1 \pmod q$ 이다.
따라서 $a^{4p} \equiv 1 \pmod q$ 이고 $\phi(q) = 4p$ 이다. 이제 편의상 $\mathrm{ord}_q(a) = k$ 라고 하면 $k \mid 4p$ 이고 p는 홀수인 소수이므로 k가 가질수 있는 값은 $1, 2, 4, p, 2p, 4p$ 이다.

a는 법 q에 대한 이차 비잉여이므로 $a \not\equiv 1 \pmod q$ 이다. 그리고 $a^2 \equiv 1 \pmod q$ 이면 q는 소수이고 $a \not\equiv 1 \pmod q$ 이므로 $a \equiv -1 \pmod q$ 인데 $q \equiv 1 \pmod 4$ 이므로 $(a/q) = (-1/q) = 1$ 이다. 그러므로 $a \not\equiv -1 \pmod q$ 이다.

따라서 $a^2 \not\equiv 1 \pmod q$ 이다. 그리고 $a^{2p} \equiv -1 \pmod q$ 이므로 $a^p \not\equiv 1 \pmod q$ 임은 명백하다. 정리하면 가능한 경우는 $a^4 \equiv 1 \pmod q$ 또는 $a^{4p} \equiv 1 \pmod q$ 인데 $a^4 \equiv 1 \pmod q$ 이면 $\mathrm{ord}_q(a) = 4$ 이고 $a^{4p} \equiv 1 \pmod q$ 이면 a는 법 q의 원시근이 된다. ■

(b). p가 홀수인 소수이므로 $q \equiv 5 \equiv -3 \pmod 8$ 을 만족한다. 따라서 Corollary 4.2.1 에 의하면 $(2/q) = -1$ 이므로 2는 법 q에 대한 이차 비잉여이다. 그러므로 (a)에 의하면 $\mathrm{ord}_q(2) = 4$ 또는 2가 법 q의 원시근이다.

그런데 $2^4 \equiv 1 \pmod q$ 이면 $q \mid 15$ 인데 p는 홀수인 소수이므로 $q \geq 13$ 이다.
따라서 이것은 모순이다. 그러므로 2는 법 q의 원시근이다. ■

Problem 4.2.4 p가 $p \equiv 1 \pmod 4$ 를 만족하는 소수이면 $\mathbb{Z}_p^{\times}$에서 법 p에 대한 이차잉여의 총합은 $\frac{p(p-1)}{4}$ 임을 증명하시오.

(증명)
조건에 의하면 $(-1/p)=1$ 이므로 $(a/p)=1$ 이면 다음을 만족한다.

$$(p-a/p)=(-a/p)=(-1/p)(a/p)=1$$

따라서 $a \in \mathbb{Z}_p^{\times}$가 법 p에 대한 이차잉여이면 $p-a \in \mathbb{Z}_p^{\times}$ 이고 $p-a$ 도 법 p에 대한 이차잉여이다. 그리고 조건에 의하면 $\frac{p-1}{4}$은 자연수이고 $\mathbb{Z}_p^{\times}$에서 법 p에 대한 이차잉여는 $\frac{p-1}{2}$개 있다.

$\mathbb{Z}_p^{\times}$에서 법 p에 대한 이차잉여를 모두 모은 것을 $a_1, a_2, \ldots, a_{\frac{p-1}{2}}$ 라고 하면

$$a_1 + a_2 + \cdots + a_{\frac{p-1}{2}} = (p-a_1) + (p-a_2) + \cdots + \left(p - a_{\frac{p-1}{2}}\right)$$

이므로 $a_1 + a_2 + \cdots + a_{\frac{p-1}{2}} = \frac{1}{2} \times \frac{p(p-1)}{2} = \frac{p(p-1)}{4}$ 가 성립한다. ■

$\mathbb{Z}_p^{\times}$에서 모든 원소의 합은 $\frac{p(p-1)}{2}$ 이므로 Problem 4.2.4에 의하면 $p \equiv 1 \pmod 4$ 일 때 $\mathbb{Z}_p^{\times}$에서 법 p에 대한 이차 비잉여의 총합도 $\frac{p(p-1)}{4}$ 임을 쉽게 알수 있습니다.

4.3 이차 상호 법칙

작성자 : 네냐플(Nenyaffle)

4.3절에서는 이차 상호 법칙을 소개할건데 이것은 4장 전체에서 가장 중요한 정리입니다. 이차 상호 법칙은 가우스가 증명한 정리인데 르장드르 기호를 계산할 때 큰 도움이 되는 정리입니다.

이 정리는 서로 다른 홀수인 소수 p, q가 주어져있는데 q가 p에 비해 매우 큰 소수일 때 (p/q)를 계산하기 쉽게 만들어줍니다. 한 예로 $(5/227)$를 지금까지 배운 지식만 가지고 계산하려면 오일러의 판정법을 사용할수밖에 없습니다.

그런데 오일러의 판정법을 사용해서 계산하려면 5^{113}이 법 227에서 얼마인지 계산해야 하는데 이것을 계산하는게 쉽지 않습니다. 현대에는 계산기가 발달되어있으니 $5^{113} \equiv -1 \pmod{227}$ 임을 쉽게 알수 있고 따라서 $(5/227)=-1$ 인데 과거에는 계산기가 없었으므로 쉽게 계산할수 있는 방법이 필요했습니다.

아직 이차 상호 법칙을 소개하지 않았는데 결론부터 말하자면 이차 상호 법칙에 의해 $(5/227)=(227/5)$ 가 성립합니다. 그리고 $227 \equiv 2 \pmod{5}$ 이므로 $(227/5)=(2/5)$ 이고 따라서 오일러의 판정법에 의하면 $(2/5) \equiv 2^2 \equiv -1 \pmod{5}$ 에서 $(2/5)=-1$ 을 얻을수 있습니다.

그러므로 $(5/227)=-1$ 입니다. 이차 상호 법칙을 사용하면 $(5/227)$를 쉽게 계산할수 있다는 것을 알수 있습니다. 4.3절에서는 이차 상호 법칙을 소개하는게 목표입니다.

이차 상호 법칙을 증명하기 위해 필요한 보조정리가 있습니다. 가우스의 보조정리를 특정 조건 하에서 좀 더 깔끔하게 서술한 정리입니다.

Lemma 4.3.1 p는 홀수인 소수이고 a는 $\gcd(a,p)=1$ 을 만족하는 홀수일 때 다음 등식이 성립한다.

$$(a/p)=(-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor}$$

여기서 $\lfloor x \rfloor$ 는 x를 넘지 않는 최대의 정수이다.

(증명)

집합 S 를 $S=\left\{a,2a,3a,...,\left(\frac{p-1}{2}\right)a\right\}$라고 하자. 그리고 $1 \le k \le \frac{p-1}{2}$ 를 만족하는 자연수 k에 대하여 ka를 p로 나눈 몫을 q_k, 나머지를 t_k라고 하면 $q_k = \left\lfloor \frac{ka}{p} \right\rfloor$ 이고 $ka = p\left\lfloor \frac{ka}{p} \right\rfloor + t_k$ 가 성립한다. 그리고 $0 < t_k < p$ 이다.

$\frac{p-1}{2}$개의 t_k중 $0 < t_k < \frac{p}{2}$를 만족하는 것을 $r_1, r_2, ..., r_m$ 라고 하고

$\frac{p}{2} < t_k < p$ 를 만족하는 것을 $s_1, s_2, ..., s_n$ 라고 하자. 그러면 다음 등식을 얻는다.

$$\sum_{k=1}^{\frac{p-1}{2}} ka = p\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor + \sum_{k=1}^{m} r_k + \sum_{k=1}^{n} s_k \tag{11}$$

그리고 다음 $m+n = \frac{p-1}{2}$개의 자연수는 모두 0과 $\frac{p}{2}$ 사이에 있다.

$$r_1, r_2, ..., r_m, p-s_1, p-s_2, \ ..., p-s_n \tag{12}$$

따라서 가우스의 보조정리의 증명과정에 의하면 (12)는 1부터 $\frac{p-1}{2}$까지의 자연수를 배열한것에 불과하므로 다음 등식을 얻는다.

$$\sum_{k=1}^{\frac{p-1}{2}} k = \sum_{k=1}^{m} r_k + \sum_{k=1}^{n} (p-s_k) = pn + \sum_{k=1}^{m} r_k - \sum_{k=1}^{n} s_k \tag{13}$$

(11)에서 (13)을 빼면 다음 등식을 얻는다.

$$(a-1)\sum_{k=1}^{\frac{p-1}{2}} k = p\left(\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor - n\right) + 2\sum_{k=1}^{n} s_k \tag{14}$$

그리고 조건에 의하면 $a \equiv p \equiv 1 \pmod 2$ 이므로 (14)에서 다음을 얻을수 있다.

$$0 \equiv \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor - n \pmod 2$$

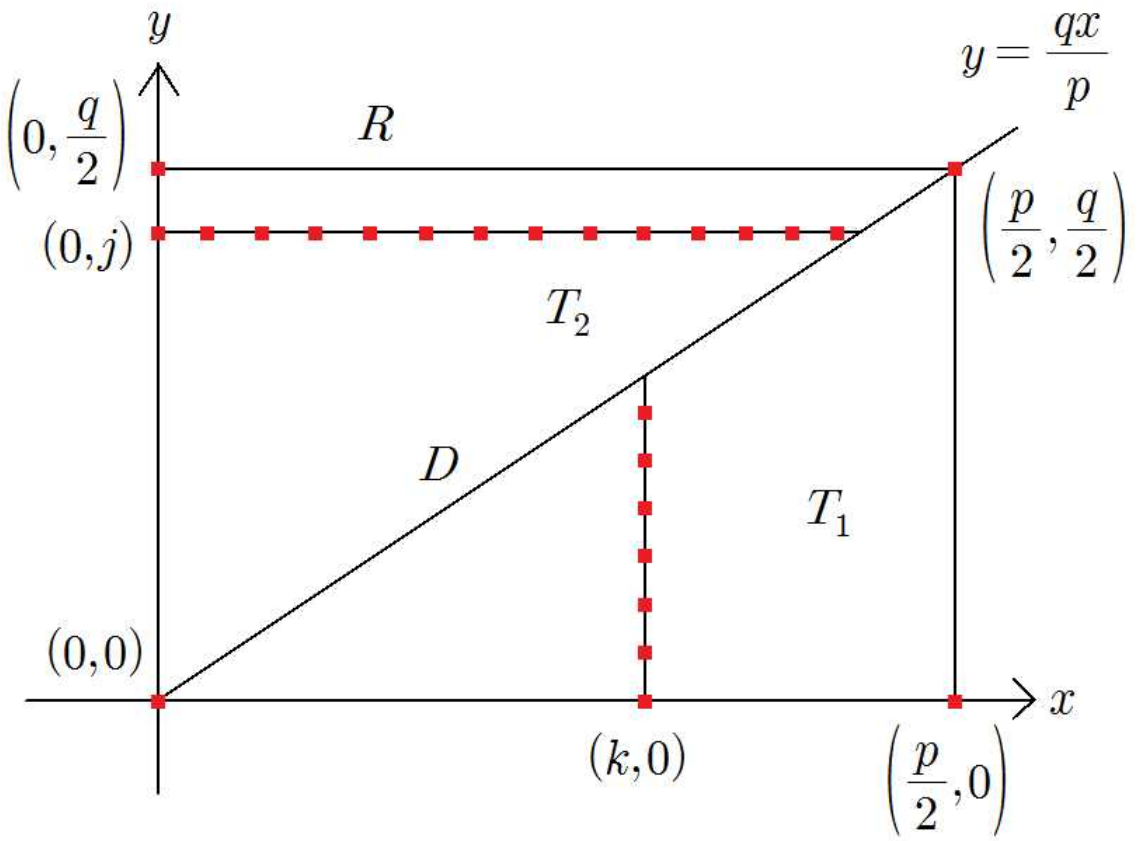
따라서 $n \equiv \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor \pmod 2$ 이므로 n과 $\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor$ 는 둘다 짝수이거나 둘다 홀수이다. 그러므로 $(-1)^n = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor}$ 이고 가우스의 보조정리에 의하면 $(a/p) = (-1)^n = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor}$ 가 성립한다. ■

Theorem 4.3.1 이차 상호 법칙(Quadratic Reciprocity Law)

p, q가 서로 다른 홀수인 소수이면 $(p/q)(q/p) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$ 이다.

(증명)

좌표평면에서 각 성분이 모두 정수인 점을 격자점이라고 부르는데 이차 상호 법칙은 4개의 점 $(0,0), \left(\frac{p}{2}, 0\right), \left(0, \frac{q}{2}\right), \left(\frac{p}{2}, \frac{q}{2}\right)$을 꼭짓점으로 갖는 직사각형 내부에 있는 격자점의 개수를 세는 방법을 이용해서 증명할 것이다.



위 그림처럼 4개의 점 $(0,0),\left(\frac{p}{2},0\right),\left(0,\frac{q}{2}\right),\left(\frac{p}{2},\frac{q}{2}\right)$을 꼭짓점으로 갖는 직사각형을 R이라 하고 두 점 $(0,0),\left(\frac{p}{2},\frac{p}{2}\right)$을 이은 선분을 D,

세 점 $(0,0),\left(\frac{p}{2},0\right),\left(\frac{p}{2},\frac{q}{2}\right)$을 꼭짓점으로 갖는 삼각형을 T_1,

세 점 $(0,0),\left(0,\frac{q}{2}\right),\left(\frac{p}{2},\frac{q}{2}\right)$을 꼭짓점으로 갖는 삼각형을 T_2라고 하자.

그러면 직사각형 R 내부에 있는 격자점의 개수는 4개의 점 $(1,1),\left(\frac{p-1}{2},1\right),\left(1,\frac{q-1}{2}\right),\left(\frac{p-1}{2},\frac{q-1}{2}\right)$을 꼭짓점으로 갖는 직사각형의 넓이인 $\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$ 과 같다.

이제 삼각형 T_1, T_2 내부에 있는 격자점의 개수를 구하자. 그 개수를 구하기 위해 먼저 선분 D 위에 있는 격자점은 $(0,0)$이 유일함을 보이자. 선분 D 를 포함하는 직선의 방정식은 $y=\frac{qx}{p}$ 이다. 따라서 D 위에 $(0,0)$이 아닌 격자점이 존재한다면 $px=qy$ 를 만족하는 $1\le x\le\frac{p-1}{2}, 1\le y\le\frac{q-1}{2}$ 인 자연수 x, y가 존재한다.

$px = qy$ 이면 $p \mid qy$ 이고 p, q는 서로 다른 소수이므로 $p \mid y$ 를 얻는다. 그리고 y는 자연수이므로 $p \leq y$ 를 만족하는데 이것은 모순이다. 따라서 D 위에 있는 격자점은 $(0,0)$이 유일하다.

그러므로 T_1, T_2 내부에 있는 격자점의 개수를 모두 더한 것은 직사각형 R 내부에 있는 격자점의 개수 $\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$와 같다. 따라서 T_1, T_2 내부에 있는 격자점의 개수를 구해보자. (15)

1) T_1의 내부에 있는 격자점의 개수

$1 \leq k \leq \frac{p-1}{2}$ 를 만족하는 자연수 k를 임의로 하나 택하자. 그러면 직선 $x = k$ 위에 있으면서 $y \leq \frac{qx}{p}$ 를 만족하는 자연수 y의 개수가 직선 $x = k$ 위에 있으면서 T_1의 내부에 있는 격자점의 개수이다.

즉, $y \leq \frac{kq}{p}$를 만족하는 자연수 y의 개수가 T_1의 내부에 있는 격자점의 개수이고 그 개수는 바닥함수의 정의에 의하면 $\left\lfloor \frac{kq}{p} \right\rfloor$ 이다. 따라서 T_1의 내부에 있는 격자점의 개수는 $\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor$ 이다.

2) T_2의 내부에 있는 격자점의 개수

$1 \leq j \leq \frac{p-1}{2}$ 를 만족하는 자연수 j를 임의로 하나 택하자. 그러면 직선 $y = j$ 위에 있으면서 $x \leq \frac{py}{q}$ 를 만족하는 자연수 x의 개수가 직선 $y = j$ 위에 있으면서 T_2의 내부에 있는 격자점의 개수이다.

즉, $x \leq \frac{jp}{q}$를 만족하는 자연수 x의 개수가 T_2의 내부에 있는 격자점의 개수이고 그 개수는 바닥함수의 정의에 의하면 $\left\lfloor \frac{jp}{q} \right\rfloor$ 이다. 따라서 T_2의 내부에 있는 격자점의 개수는 $\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{jp}{q} \right\rfloor$ 이다.

따라서 1), 2), (15)에 의하면 $\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor + \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{jp}{q} \right\rfloor = \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$ 가 성립한다. 그러므로 Lemma 4.3.1에 의하면 다음 등식을 얻는다.

$$(p/q)(q/p) = (-1)^{\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{jp}{q} \right\rfloor + \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor} = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$$

■

이차 상호 법칙은 가우스가 증명한 정리입니다. 이차 상호 법칙을 증명하기 위해 필요한 것이 4.2절에서 소개한 가우스의 보조정리인데 가우스의 보조정리나 이차 상호 법칙이나 정리와 증명과정을 보면 이런 생각을 어떻게 했는지 신기할 뿐입니다.

이차 상호 법칙은 다음과 같이 기억하는게 좀 더 편합니다.

Corollary 4.3.1 p, q가 서로 다른 홀수인 소수이면 다음이 성립한다.

$$(p/q) = \begin{cases} (q/p) & (p \equiv 1 \pmod 4 \text{ 또는 } q \equiv 1 \pmod 4) \\ -(q/p) & (p \equiv q \equiv 3 \pmod 4) \end{cases}$$

(증명)

먼저 두 정수 a, b에 대하여 ab가 홀수일 필요충분조건은 a, b가 모두 홀수인 것이다.

따라서 p, q가 서로 다른 홀수인 소수일 때 $\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$가 홀수일 필요충분조건은 $\frac{p-1}{2}, \frac{q-1}{2}$가 모두 홀수인 것이고 이것은 $p \equiv q \equiv 3 \pmod 4$ 와 동치이다.

$p \equiv q \equiv 3 \pmod 4$ 이면 이차 상호 법칙에 의해 $(p/q)(q/p) = -1$ 이고 양변에 (q/p)를 곱하면 $(q/p)^2 = 1$ 이므로 $(p/q) = -(q/p)$ 가 성립한다.

그리고 $\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$ 가 짝수인 것은 $p \equiv 1 \pmod 4$ 또는 $q \equiv 1 \pmod 4$ 가 성립하는 것과 동치이다. 따라서 이 경우에는 이차 상호 법칙에 의해 $(p/q)(q/p) = 1$ 이고 양변에 (q/p)를 곱하면 $(q/p)^2 = 1$ 이므로 $(p/q) = (q/p)$ 가 성립한다. ■

4.3절을 시작할 때 보여준 $(5/227) = (227/5)$ 는 $5 \equiv 1 \pmod 4$ 이므로 Corollary 4.3.1에 의해 성립하는 등식입니다.

4.2절에서 이차 상호 법칙을 배우면 p가 홀수인 소수일 때 $(2/p)$를 쉽게 계산할수 있다는 것이 중요하다는 것을 알게 될거라고 이야기했는데 그 이유는 다음과 같습니다.

p, q가 서로 다른 소수일 때 이차 상호 법칙을 이용해서 (p/q)를 계산할수 있는데 그 과정에서 홀수인 소수 r에 대해 $(2/r)$가 나오면 2는 짝수인 소수이므로 이것은 더 이상 이차 상호 법칙을 이용해서 계산할수 없습니다.

따라서 $(2/r)$은 Corollary 4.2.1을 이용해서 계산해야 합니다. 즉, Corollary 4.2.1이 없었으면 이차 상호 법칙이 있다고 해도 $(2/r)$을 계산하기 위해 많은 고민을 해야할수도 있습니다.

p가 소수일 때 다항합동방정식 $f(x)\equiv 0 \pmod p$ 의 해법이 알려져있지 않아서 일반적인 다항합동방정식 $f(x)\equiv 0 \pmod n$ 의 해법이 알려져있지 않다는 것을 생각해보면 이해하기 쉬울겁니다.

이차 상호 법칙을 사용해서 르장드르 기호 $(21084/1999)$를 계산해보겠습니다.
우선 $21084 \equiv 1094 \pmod{1999}$ 이고 $1094 = 2\times 547$, 그리고 1999는 소수이고 $1999 \equiv -1 \pmod 8$ 이므로 다음을 얻습니다.

$$(21084/1999)=(1094/1999)=(2/1999)(547/1999)=(547/1999)$$

547도 소수이고 $547 \equiv 1999 \equiv 3 \pmod 4$ 이므로 이차 상호 법칙에 의하면 $(547/1999)=-(1999/547)$ 입니다. 그리고 $1999 \equiv 358 \pmod{547}$ 이고 $358 = 2\times 179$, 그리고 $547 \equiv 3 \pmod 8$ 이므로 다음을 얻습니다.

$$-(1999/547)=-(358/547)=-(2/547)(179/547)=(179/547)$$

179도 소수이고 $179 \equiv 547 \equiv 3 \pmod 4$ 이므로 $(179/547)=-(547/179)$ 이고 $547 \equiv 10 \pmod{179}$, $179 \equiv 3 \pmod 8$ 에서 다음을 얻습니다.

$$-(547/179)=-(10/179)=-(2/179)(5/179)=(5/179)$$

$5 \equiv 1 \pmod 4$ 이고 $179 \equiv 4 \pmod 5$ 이므로 다음을 얻습니다.

$$(5/179)=(179/5)=(4/5)=(2/5)^2=1$$

따라서 $(21084/1999)=1$ 입니다. 그러므로 합동방정식 $x^2 \equiv 21084 \pmod{1999}$ 은 법 1999에서 해가 존재합니다.

이차 상호 법칙을 이용하면 홀수인 소수 p가 무엇인지 알고 있을 때 $q>p$ 인 홀수 소수 q에 대하여 (p/q)를 결정할수 있는 경우가 많습니다.

Theorem 4.3.2 p가 $p\neq 3$ 을 만족하는 홀수인 소수이면 다음이 성립한다.

$$(3/p)=\begin{cases}1 & (p\equiv \pm 1 \pmod{12})\\ -1 & (p\equiv \pm 5 \pmod{12})\end{cases}$$

(증명)

이차 상호 법칙에 의하면 $(3/p)=\begin{cases}(p/3) & (p\equiv 1 \pmod 4)\\ -(p/3) & (p\equiv 3 \pmod 4)\end{cases}$ 을 얻을수 있고

p가 $p\neq 3$ 을 만족하는 홀수인 소수이므로 다음을 얻을수 있다.

$$(p/3)=\begin{cases}(1/3) & (p\equiv 1 \pmod 3)\\ (2/3) & (p\equiv 2 \pmod 3)\end{cases}=\begin{cases}1 & (p\equiv 1 \pmod 3)\\ -1 & (p\equiv 2 \pmod 3)\end{cases}$$

따라서 $(3/p)=1$ 은 $p\equiv 1 \pmod 4, p\equiv 1 \pmod 3$ 또는 $p\equiv 3 \pmod 4, p\equiv 2 \pmod 3$ 을 만족하는 것과 동치이다.

$\gcd(4,3)=1$ 이므로 $p\equiv 1\pmod 4$, $p\equiv 1\pmod 3$ 이면 $p\equiv 1\pmod{12}$ 이고 $p\equiv 3\pmod 4$, $p\equiv 2\pmod 3$ 는 중국인의 나머지 정리를 이용해서 풀면 $M_1=3, M_2=4, x_1=3, x_2=1$ 에서 다음을 얻을수 있다.

$$p\equiv 3M_1x_1+2M_2x_2\equiv 35\equiv -1\pmod{12}$$

그러므로 $(3/p)=1$ 을 만족할 필요충분조건은 $p\equiv\pm 1\pmod{12}$ 이다.
마찬가지로 $(3/p)=-1$ 을 만족할 필요충분조건은 다음 둘중 하나를 만족하는 것이고

$$p\equiv 1\pmod 4,\ p\equiv 2\pmod 3$$
$$p\equiv 3\pmod 4,\ p\equiv 1\pmod 3$$

이것도 중국인의 나머지 정리를 이용해서 풀면 $p\equiv\pm 5\pmod{12}$ 를 얻을수 있다.
정리하면 다음 등식을 얻는다.

$$(3/p)=\begin{cases}1 & (p\equiv\pm 1\pmod{12})\\ -1 & (p\equiv\pm 5\pmod{12})\end{cases}$$

■

한편 홀수인 소수 p가 무엇인지 알고 있을 때 $(p/q)=1$ 또는 $(p/q)=-1$ 을 만족하는 $q>p$ 인 홀수 소수 q가 무엇인지 관심을 갖는것도 자연스러운 일이고 그런 홀수 소수 q를 구할 때 계산을 줄일수 있는 정리가 있습니다. 그 전에 보조정리를 소개하겠습니다.

Lemma 4.3.2 p는 소수이고 q는 $q>p$ 를 만족하는 홀수인 소수이면 다음을 만족하는 자연수 r은 유일하게 존재한다.

(a). 적당한 정수 k가 존재해서 $q=4kp\pm r\ (0<r<4p)$ 이다.
(b). $r\equiv 1\pmod 4$ 이다.

(증명)
q를 $4p$로 나눈 나머지를 r_0라고 하자. 그러면 적당한 정수 k가 존재해서 $q=4kp+r_0$ 와 $0<r_0<4p$ 를 만족하고 나머지는 유일하다. 그리고 $4p$는 짝수이고 q는 홀수이므로 r_0는 홀수이다. 따라서 $r_0\equiv 1\pmod 4$ 또는 $r_0\equiv 3\pmod 4$ 를 만족해야 한다.

$r_0\equiv 1\pmod 4$ 이면 $r=r_0$ 가 조건을 만족하는 유일한 자연수이다.
$r_0\equiv 3\pmod 4$ 이면 $r=4p-r_0$ 라고 할 때 $q=4p(k+1)-r$ 이고
$r\equiv -r_0\equiv 1\pmod 4$ 이므로 조건을 만족하는 유일한 자연수이다. ■

Theorem 4.3.3 p는 홀수인 소수이고 q는 $q>p$ 인 홀수 소수라고 할 때 자연수 r은 다음과 같이 정의된다.

(a). $p\equiv 1\pmod 4$ 이면 r은 q를 p로 나눈 나머지이다.
(b). $p\equiv 3\pmod 4$ 이면 r은 Lemma 4.3.2를 만족하는 유일한 자연수이다.

그러면 $(p/q)=(r/p)$ 이다.

(증명)
$p \equiv 1 \pmod 4$ 이면 $q \equiv r \pmod p$ 이므로 이차 상호 법칙에 의하면 다음을 만족한다.

$$(p/q) = (q/p) = (r/p)$$

$p \equiv 3 \pmod 4$ 이면 Lemma 4.3.2의 증명과정에서 q를 $4p$로 나눈 나머지를 r_0라고 할 때 $r_0 \equiv 1 \pmod 4$ 이면 $r = r_0$ 이고 $r_0 \equiv 3 \pmod 4$ 이면 $r = 4p - r_0$ 이다.

$r = r_0$ 이면 $q \equiv r \equiv 1 \pmod 4$ 이므로 이차 상호법칙에 의하면 다음을 얻는다.

$$(p/q) = (q/p) = (r/p)$$

$r = 4p - r_0$ 이면 $q \equiv -r \equiv 3 \pmod 4$ 이므로 이차 상호법칙에 의하면 다음을 얻는다.

$$(p/q) = -(q/p) = -(-r/p) = -(-1/p)(r/p) = (r/p)$$

따라서 $(p/q) = (r/p)$ 이다. ■

Theorem 4.3.3을 이용해서 $(7/p) = 1$ 을 만족하는 $p > 7$ 인 홀수 소수 p가 무엇인지 구할수 있습니다. $7 \equiv 3 \pmod 4$ 이므로 $p = 28k \pm r$ 과 $0 < r < 28$, 그리고 $r \equiv 1 \pmod 4$ 를 만족하는 자연수 r이 유일하게 존재하고 $(7/p) = (r/7)$ 입니다.

따라서 $(r/7) = 1$ 이고 $0 < r < 28$ 과 $r \equiv 1 \pmod 4$ 을 만족하는 자연수 r중 $(r/7) = 1$ 을 만족하는 것을 모두 구하면 됩니다.

$$1^2 \equiv 6^2 \equiv 1 \pmod 7$$
$$2^2 \equiv 5^2 \equiv 4 \pmod 7$$
$$3^2 \equiv 4^2 \equiv 2 \pmod 7$$

이므로 $\mathbb{Z}_7^{\times}$에서 법 7에 대한 이차잉여는 $1, 2, 4$ 입니다. 따라서 이것을 28을 넘지 않을때까지 7씩 더해보면 다음을 얻습니다.

$$1, 8, 15, 22$$
$$2, 9, 16, 23$$
$$4, 11, 18, 25$$

이들중 $r \equiv 1 \pmod 4$ 을 만족하는 것은 $1, 9, 25$ 입니다. 따라서 조건을 만족하는 소수 p는 $p = 28k \pm 1,\ 28k \pm 9,\ 28k \pm 25$ 이런 형태로만 나옵니다.

$p \equiv 3 \pmod 4$ 일 때 $q = 4kp \pm r$ 형태로 나오는 이유는 이차 상호 법칙과 중국인의 나머지 정리 때문인데 그 과정을 자세히 설명하자면 다음과 같습니다.

$p \equiv 3 \pmod 4$ 이면 이차 상호 법칙에 의해 다음을 만족합니다.

$$(p/q) = \begin{cases} (q/p) & (q \equiv 1 \pmod 4) \\ -(q/p) & (q \equiv 3 \pmod 4) \end{cases}$$

그리고 q를 p로 나눈 나머지를 r이라고 하면 $q \equiv r \pmod p$ 이므로 다음을 얻습니다.

$$(p/q) = \begin{cases} (r/p) & (q \equiv 1 \pmod 4) \\ -(r/p) & (q \equiv 3 \pmod 4) \end{cases}$$

q를 p로 나눈 나머지들 중엔 법 p에서 이차잉여가 되는것도 있고 이차 비잉여가 되는것도 있습니다. 그러므로 다음 두가지 경우가 발생합니다.

case1) $q \equiv r \pmod{p}$ 이고 $(r/p)=1$
이 경우 $(p/q)=1$ 을 만족하려면 $q \equiv 1 \pmod{4}$ 가 되어야 합니다.
따라서 다음 연립합동방정식을 얻을수 있습니다.

$$q \equiv 1 \pmod{4}$$
$$q \equiv r \pmod{p}$$

그리고 $\gcd(4,p)=1$ 이므로 중국인의 나머지 정리에 의하면 연립합동방정식의 해가 $q \equiv a \pmod{4p}$ 형태로 나옵니다.

$(p/q)=-1$ 을 만족하려면 $q \equiv 3 \pmod{4}$ 가 되어야 하고 이때도 중국인의 나머지 정리에 의해 $q \equiv a \pmod{4p}$ 형태로 나온다는 것을 알수 있습니다.

case2) $q \equiv r \pmod{p}$ 이고 $(r/p)=-1$
이 경우 $(p/q)=1$ 을 만족하려면 $q \equiv 3 \pmod{4}$ 가 되어야 합니다.
따라서 다음 연립합동방정식을 얻을수 있습니다.

$$q \equiv 3 \pmod{4}$$
$$q \equiv r \pmod{p}$$

그리고 $\gcd(4,p)=1$ 이므로 중국인의 나머지 정리에 의하면 연립합동방정식의 해가 $q \equiv b \pmod{4p}$ 형태로 나옵니다.

$(p/q)=-1$ 을 만족하려면 $q \equiv 1 \pmod{4}$ 가 되어야 하고 이때도 중국인의 나머지 정리에 의해 $q \equiv b \pmod{4p}$ 형태로 나온다는 것을 알수 있습니다.

그러므로 어느 경우든 $q=4kp+m$ 형태로 나옵니다. $p \equiv 1 \pmod{4}$ 이면 q에 관계없이 $q \equiv r \pmod{p}$ 이면 $(p/q)=(q/p)=(r/p)$ 가 성립하므로 이 경우에는 $q=pk+m$ 형태로 나오는겁니다.

이 과정을 깔끔하게 정리해놓은게 Theorem 4.3.3입니다. 따라서 Theorem 4.3.3을 굳이 기억할 필요는 없습니다. case를 하나하나 나누는 것으로 풀수 있기 때문입니다.

Problem 4.3.1 다음 물음에 답하시오.
(a). $(5/p)=-1$ 을 만족하는 모든 홀수 소수 p를 합동식으로 나타내시오.
(b). $(10/p)=1$ 을 만족하는 모든 홀수 소수 p를 합동식으로 나타내시오.

(증명)
(a). $p=3$ 이면 $(5/3)=(2/3)=-1$ 이다. 따라서 $p>5$ 인 경우를 가정하자.
그러면 $5 \equiv 1 \pmod{4}$ 이므로 $p=5k+r\ (0<r<5)$ 라고 하면 이차 상호 법칙에 의해 $(5/p)=(r/5)$ 이다. 따라서 $(r/5)=-1$ 을 만족하는 자연수 r을 구하면 충분하다.

$$1^2 \equiv 4^2 \equiv 1 \pmod 5$$
$$2^2 \equiv 3^2 \equiv 4 \pmod 5$$

이므로 $\mathbb{Z}_5^{\times}$에서 법 5에 대한 이차 비잉여는 $2, 3$ 이다. 따라서 $r = 2, 3$ 으로 택하면 충분하고 이때 $p = 5k+2, 5k+3$ 형태를 갖는다. 그리고 $p = 3$ 은 $5k+3$ 형태이므로 정리하면 $p \equiv 2 \pmod 5$ 또는 $p \equiv 3 \pmod 5$ 를 얻는다. ■

(b). 조건에 의하면 $(2/p) = (5/p) = 1$ 또는 $(2/p) = (5/p) = -1$ 이다.

case1) $(2/p) = (5/p) = 1$
$(2/p) = 1$ 을 만족할 필요충분조건은 $p \equiv \pm 1 \pmod 8$ 이고 $(5/p) = 1$ 을 만족할 필요충분조건은 (a)의 풀이과정에서 $p \equiv 1 \pmod 5$ 또는 $p \equiv 4 \pmod 5$ 임을 쉽게 알수 있다. 따라서 다음 연립합동방정식을 얻을수 있다.

$$\begin{cases} p \equiv 1 \pmod 8 \\ p \equiv 1 \pmod 5 \end{cases}, \quad \begin{cases} p \equiv 1 \pmod 8 \\ p \equiv 4 \pmod 5 \end{cases}$$

$$\begin{cases} p \equiv -1 \pmod 8 \\ p \equiv 1 \pmod 5 \end{cases}, \quad \begin{cases} p \equiv -1 \pmod 8 \\ p \equiv 4 \pmod 5 \end{cases}$$

중국인의 나머지 정리를 사용해서 풀면 $p \equiv \pm 1, \pm 9 \pmod{40}$ 을 얻는다.

case2) $(2/p) = (5/p) = -1$
$(2/p) = -1$ 을 만족할 필요충분조건은 $p \equiv \pm 3 \pmod 8$ 이고 $(5/p) = -1$ 을 만족할 필요충분조건은 (a)의 풀이과정에 의하면 $p \equiv 2 \pmod 5$ 또는 $p \equiv 3 \pmod 5$ 이다. 따라서 다음 연립합동방정식을 얻을수 있다.

$$\begin{cases} p \equiv 3 \pmod 8 \\ p \equiv 2 \pmod 5 \end{cases}, \quad \begin{cases} p \equiv 3 \pmod 8 \\ p \equiv 3 \pmod 5 \end{cases}$$

$$\begin{cases} p \equiv -3 \pmod 8 \\ p \equiv 2 \pmod 5 \end{cases}, \quad \begin{cases} p \equiv -3 \pmod 8 \\ p \equiv 3 \pmod 5 \end{cases}$$

중국인의 나머지 정리를 사용해서 풀면 $p \equiv \pm 3, \pm 13 \pmod{40}$ 을 얻는다.
따라서 정리하면 $p \equiv \pm 1, \pm 3, \pm 9, \pm 13 \pmod{40}$ 을 얻는다. ■

Problem 4.3.2 p가 홀수인 소수이면 다음이 성립한다.

$$(-2/p) = \begin{cases} 1 & (p \equiv 1 \pmod 8 \text{ 또는 } p \equiv 3 \pmod 8) \\ -1 & (p \equiv 5 \pmod 8 \text{ 또는 } p \equiv 7 \pmod 8) \end{cases} \tag{16}$$

(16)을 이용해서 $8k+3$ 형태를 갖는 소수의 개수가 무한함을 증명하시오.

(증명)
결론을 부정해서 $8k+3$ 형태를 갖는 소수의 개수가 유한하다고 가정하고 그것을 $p_1,p_2,...,p_n$ 라고 하자. 그리고 $N=(p_1p_2\cdots p_n)^2+2$ 라고 정의하자.

그러면 N은 $N\geq 3$ 을 만족하는 홀수이므로 홀수인 소수를 약수로 갖는다. 그것을 p라고 하면 $(p_1p_2\cdots p_n)^2\equiv -2\pmod p$ 이므로 $(-2/p)=1$ 이다. 따라서 (16)에 의하면 p는 $8k+1$ 또는 $8k+3$ 형태이다.

만약 N의 모든 소인수가 $8k+1$ 형태이면 N도 $8k+1$ 형태가 되어야 하는데 $N\equiv 3^{2n}+2\equiv 9^n+2\equiv 3\pmod 8$ 이므로 N은 $8k+3$ 형태이다. 따라서 이것은 모순이므로 N은 $8k+3$ 형태의 소인수를 갖는다.

그러므로 적당한 $i=1,2,...,n$ 에 대하여 $p_i\mid N$ 을 만족하므로 $p_i\mid 2$ 인데 이것은 p_i가 $8k+3$ 형태를 갖는 소수라는 것에 모순이다. 따라서 $8k+3$ 형태를 갖는 소수의 개수는 무한하다. ■

Problem 4.3.3 Problem 4.3.1의 풀이과정에 의하면 p가 $p\neq 5$ 인 홀수 소수일 때 다음이 성립한다.

$$(5/p)=\begin{cases}1 & (p\equiv 1\pmod 5 \text{ 또는 } p\equiv 4\pmod 5)\\ -1 & (p\equiv 2\pmod 5 \text{ 또는 } p\equiv 3\pmod 5)\end{cases} \tag{17}$$

(17)을 이용해서 $5k+4$ 형태를 갖는 소수의 개수가 무한함을 증명하시오.

(증명)
결론을 부정해서 $5k+4$ 형태를 갖는 소수의 개수가 유한하다고 가정하고 그것을 $p_1,p_2,...,p_n$ 라고 하자. 그리고 $N=(2p_1p_2\cdots p_n)^2-5$ 라고 정의하자.

그러면 N은 $N\geq 3$ 을 만족하는 홀수이므로 홀수인 소수를 약수로 갖는다. 그것을 p라고 하면 $(2p_1p_2\cdots p_n)^2\equiv 5\pmod p$ 이므로 $(5/p)=1$ 이다. 따라서 (16)에 의하면 p는 $5k+1$ 또는 $5k+4$ 형태이다.

만약 N의 모든 소인수가 $5k+1$ 형태이면 N도 $5k+1$ 형태가 되어야 하는데 $N\equiv 4^{2n+1}-5\equiv -6\equiv 4\pmod 5$ 이므로 N은 $5k+4$ 형태이다. 따라서 이것은 모순이므로 N은 $5k+4$ 형태의 소인수를 갖는다.

그러므로 적당한 $i=1,2,...,n$ 에 대하여 $p_i\mid N$ 을 만족하므로 $p_i\mid 5$ 인데 이것은 p_i가 $5k+4$ 형태를 갖는 소수라는 것에 모순이다. 따라서 $5k+4$ 형태를 갖는 소수의 개수는 무한하다. ■

Problem 4.3.4 p는 홀수인 소수이고 a는 $\gcd(a,p)=1$ 을 만족하는 자연수일 때 다음을 증명하시오.
(a). $p \equiv 2a-1 \pmod{4a}$ 이고 $a \equiv 1 \pmod 4$ 이면 $(a/p)=1$ 이다.
(b). $p \equiv \pm 1 \pmod{4a}$ 이면 $(a/p)=1$ 이다.

(증명)
(a). $a=1$ 이면 명백하다. 따라서 $a \geq 2$ 인 경우를 가정하자. 그러면 $a \equiv 1 \pmod 4$ 이므로 a의 소인수중 $4k+3$ 형태를 갖는 소인수는 하나도 없거나 짝수개만 존재한다.

따라서 a의 소인수분해가 $4k+1$ 형태를 갖는 소수 $p_1,p_2,...,p_m$ 과 $4k+3$ 형태를 갖는 소수 $q_1,q_2,...,q_{2n}$ 에 대하여 $a=p_1p_2\cdots p_mq_1q_2\cdots q_{2n}$ 형태로 나온다고 하자. $p_1,p_2,...,p_m$ 과 $q_1,q_2,...,q_{2n}$ 들 중에는 같은 소수가 있을수도 있고 m,n 둘중 하나는 0일수도 있다.

$a \equiv 1 \pmod 4$ 이고 $p \equiv 2a-1 \pmod{4a}$ 이므로 $p \equiv 2a-1 \equiv 1 \pmod 4$ 를 만족한다. 먼저 각각의 $i=1,2,...,m$ 에 대하여 (p_i/p)를 계산하자.

$p \equiv 1 \pmod 4$ 이고 $p_i \mid a$ 이므로 $p \equiv 2a-1 \equiv -1 \pmod{p_i}$ 을 얻는다.
그러면 $p_i \equiv 1 \pmod 4$ 이므로 다음이 성립한다.

$$(p_i/p)=(p/p_i)=(-1/p_i)=1$$

이제 각각의 $j=1,2,...,2n$ 에 대하여 (q_j/p)를 계산하자. $p \equiv 1 \pmod 4$ 이고 $q_j \mid a$ 이므로 $p \equiv 2a-1 \equiv -1 \pmod{q_j}$ 을 얻는다. 그러면 $q_j \equiv 3 \pmod 4$ 이므로 다음이 성립한다.

$$(q_j/p)=(p/q_j)=(-1/q_j)=-1$$

따라서 정리하면 $(a/p)=(-1)^{2n}=1$ 을 얻을수 있다. ■

(b). $a=1$ 이면 명백하다. 따라서 $a \geq 2$ 를 가정하자. 그러면 a는 $a=2^{k_0}p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ 로 소인수분해된다. 여기서 $p_1,p_2,...,p_r$ 은 p와 다른 홀수인 소수이고 $k_0,k_1,...,k_r$ 은 음이 아닌 정수이다.

만약 k_0가 자연수이면 a는 짝수이므로 $8 \mid 4a$ 이고 조건에 의하면 $p \equiv \pm 1 \pmod 8$ 이다. 따라서 $(2/p)=1$ 이므로 $(2^{k_0}/p)=(2/p)^{k_0}=1$ 이다. 그러므로 각각의 $i=1,2,...,r$ 에 대하여 (p_i/p)만 계산하면 충분하다.

case1) $p \equiv 1 \pmod{4a}$
$p_i \mid a$ 이므로 이 경우 $p \equiv 1 \pmod{p_i}$ 를 만족하고 이차 상호 법칙에 의하면
$(p_i/p) = (p/p_i) = (1/p_i) = 1$ 을 얻는다. 따라서 $(a/p) = 1$ 이다.

case2) $p \equiv -1 \pmod{4a}$
조건에 의하면 $p \equiv -1 \equiv 3 \pmod 4$ 이고 $p_i \mid a$ 이므로 $p \equiv -1 \pmod{p_i}$ 를
만족한다. 그리고 p_i는 홀수인 소수이므로 $p_i \equiv 1 \pmod 4$ 또는 $p_i \equiv 3 \pmod 4$ 이다.

만약 $p_i \equiv 1 \pmod 4$ 이면 이차 상호 법칙에 의해 다음을 얻는다.

$$(p_i/p) = (p/p_i) = (-1/p_i) = 1$$

만약 $p_i \equiv 3 \pmod 4$ 이면 $p \equiv 3 \pmod 4$ 이므로 이차 상호 법칙에 의해

$$(p_i/p) = -(p/p_i) = -(-1/p_i) = 1$$

가 성립한다. 따라서 어느 경우든 $(p_i/p) = 1$ 이므로 $(a/p) = 1$ 이다.

정리하면 $(a/p) = 1$ 을 얻는다. ■

Problem 4.3.5 홀수인 소수 p, q는 $\gcd(k,p) = \gcd(k,q) = 1$ 을 만족하는 적당한 정수 k에 대하여 $p = q + 4k$ 를 만족한다. 그러면 $(k/p) = (k/q)$ 임을 증명하시오.

(증명)
조건에 의하면 $p \neq q$ 이다. 그리고 $(4/p) = 1$ 이고 $4k \equiv -q \pmod p$ 이므로

$$(k/p) = (4k/p) = (-q/p) = (-1/p)(q/p)$$

이다. 마찬가지로 조건에 의하면 $p \equiv q \pmod 4$ 이다. 따라서 2가지 경우가 발생한다.

case1) $p \equiv q \equiv 1 \pmod 4$
이 경우 $(-1/p) = 1$ 이고 이차 상호 법칙에 의하면 $(q/p) = (p/q)$ 이다.
그리고 $p \equiv 4k \pmod q$ 이므로 $(p/q) = (4k/q) = (k/q)$ 를 얻는다.
따라서 $(k/p) = (-1/p)(q/p) = (k/q)$ 이다.

case2) $p \equiv q \equiv 3 \pmod 4$
이 경우 $(-1/p) = -1$ 이고 이차 상호 법칙에 의하면 $(q/p) = -(p/q)$ 이다.
그리고 $p \equiv 4k \pmod q$ 이므로 $(p/q) = (4k/q) = (k/q)$ 를 얻는다.
따라서 $(k/p) = (-1/p)(q/p) = (k/q)$ 이다.

그러므로 어느 경우든 $(k/p) = (k/q)$ 이다. ■

Problem 4.3.6 정수 a, b에 대하여 $5a^2 \equiv b^2 \pmod 7$ 이면 $5a^2 \equiv b^2 \pmod{49}$
임을 증명하시오.

(증명)
$\gcd(a,7)=1$ 라고 가정하자. 그러면 a는 법 7에서 곱셈에 대한 역원이 존재하고 따라서 합동방정식 $x^2 \equiv 5 \pmod 7$ 의 해가 존재한다는 것을 쉽게 알수 있다.

그런데 $(5/7)=(7/5)=(2/5)=-1$ 이므로 합동방정식 $x^2 \equiv 5 \pmod 7$ 의 해는 존재하지 않는다. 이것은 모순이므로 $\gcd(a,7)=7$ 이 되어야 한다.

따라서 $a \equiv 0 \pmod 7$ 이므로 조건에 의하면 $b^2 \equiv 0 \pmod 7$ 에서 7은 소수이므로 $b \equiv 0 \pmod 7$ 을 얻을수 있다. 즉, a, b는 모두 7의 배수이므로 $49 \mid 5a^2 - b^2$ 을 만족한다.

그러므로 $5a^2 \equiv b^2 \pmod{49}$ 가 성립한다. ■

Problem 4.3.7 정수 k에 대하여 q는 $q=13k+1$ 형태의 소수이고 p는 $p=4q+1$ 형태의 소수일 때 13은 법 p의 원시근임을 보이시오.

(증명)
p가 소수이므로 $\phi(p)=4q$ 이고 q도 소수이므로 $\phi(p)$의 양의 약수가 될수 있는 자연수는 $1,2,4,q,2q,4q$ 가 전부이다. 그리고 조건에 의하면 $p \geq 317$ 이므로 다음은 명백하다.

$$13 \not\equiv 1 \pmod p$$
$$13^2 \not\equiv 1 \pmod p$$

그리고 $13^4 - 1 = 2^4 \times 3 \times 5 \times 7 \times 17$ 이므로 $13^4 \not\equiv 1 \pmod p$ 도 명백하다.

오일러의 판정법에 의하면 $(13/p) \equiv 13^{2q} \pmod p$ 가 성립하고 $13 \equiv 1 \pmod 4$ 이므로 이차 상호 법칙과 $p \equiv 5 \pmod{13}$ 임을 이용하면 다음을 얻을수 있다.

$$(13/p)=(p/13)=(5/13)=(13/5)=(3/5)=-1$$

그러므로 $13^{2q} \equiv -1 \pmod p$ 가 성립한다.

즉, $13^q \not\equiv 1 \pmod p$ 는 명백하므로 법 p에서 13의 위수는 $4q$가 되어야 한다.
따라서 13은 법 p의 원시근이다. ■

4.4 야코비 기호

작성자 : 네냐플(Nenyaffle)

야코비 기호는 르장드르 기호를 일반화한 기호입니다. 정의는 다음과 같습니다.

Definition 4.4.1 야코비 기호(Jacobi Symbol)
n이 $n \geq 3$ 을 만족하는 홀수일 때 홀수인 소수 $p_1, p_2, ..., p_r$ 에 대하여
$n = p_1 p_2 \cdots p_r$ 을 만족한다고 하자. $p_1, p_2, ..., p_r$ 중에는 같은 소수가 있을수도 있다.
그러면 $\gcd(a,n) = 1$ 을 만족하는 정수 a에 대하여 다음과 같이 정의한다.

$$(a/n) = (a/p_1)(a/p_2)\cdots(a/p_r)$$

이때 (a/n)을 **야코비 기호(Jacobi Symbol)**라고 정의한다.

야코비 기호는 르장드르 기호를 일반화한 기호이기 때문에 르장드르 기호와 똑같은 기호를 사용합니다. n이 홀수인 소수이면 (a/n)은 르장드르 기호와 같은 역할을 하기 때문입니다.

그런데 야코비 기호는 르장드르 기호와 달리 합동방정식에서 좋은 결과를 주지 않습니다.
$x^2 \equiv a \pmod{n}$ 의 해가 존재하면 야코비 기호와 르장드르 기호의 정의,
그리고 합동식의 성질에 의해 $(a/n) = 1$ 을 만족하지만 역은 성립하지 않습니다.

$(2/15) = (2/3)(2/5) = (-1)^2 = 1$ 인데 합동방정식 $x^2 \equiv 2 \pmod{15}$ 의 해는 존재하지 않습니다. 따라서 역은 일반적으로 성립하지 않습니다.

야코비 기호도 르장드르 기호와 비슷한 성질을 가지고 있습니다.

Theorem 4.4.1 m, n은 3 이상의 홀수인 자연수이고 a, b는 정수일 때 다음이 성립한다.
(a). $\gcd(a,n) = \gcd(b,n) = 1$ 일 때 $a \equiv b \pmod{n}$ 이면 $(a/n) = (b/n)$ 이다.
(b). $\gcd(a,n) = \gcd(b,n) = 1$ 이면 $(ab/n) = (a/n)(b/n)$ 이다.
(c). $\gcd(a,m) = \gcd(a,n) = 1$ 이면 $(a/mn) = (a/m)(a/n)$ 이다.
(d). $\gcd(a,n) = 1$ 이면 $(a^2/n) = (a/n^2) = 1$ 이다.
(e). $\gcd(ab,mn) = 1$ 이면 $(ab/mn) = (a/m)(a/n)(b/m)(b/n)$ 이다.
(f). $(1/n) = 1$ 이다.
(g). $(-1/n) = (-1)^{\frac{n-1}{2}}$ 이다.
(h). $(2/n) = (-1)^{\frac{n^2-1}{8}}$ 이다.
(i). $\gcd(m,n) = 1$ 이면 $(m/n)(n/m) = (-1)^{\left(\frac{m-1}{2}\right)\left(\frac{n-1}{2}\right)}$ 이다.

(증명)
(a). $a \equiv b \pmod{n}$ 이면 n의 임의의 소인수 p에 대하여 $a \equiv b \pmod{p}$ 를 만족한다. 따라서 $(a/p) = (b/p)$ 이다. 그러므로 야코비 기호의 정의에 의하면 $(a/n) = (b/n)$ 가 성립한다. ■

(b), (c). 야코비 기호의 정의에 의하면 명백하다. ■

(d). (b), (c)에 의하면 다음 등식이 성립한다.

$$(a^2/n)=(a/n)^2=1$$
$$(a/n^2)=(a/n)^2=1$$

■

(e). (b), (c)에 의하면 다음 등식이 성립한다.

$$(ab/mn)=(a/mn)(b/mn)=(a/m)(a/n)(b/m)(b/n)$$

■

(f). (d)에서 $a=1$ 인 경우이므로 $(1/n)=1$ 이다. ■

(g). 먼저 a,b가 홀수이면 $\frac{ab-1}{2}\equiv\frac{a-1}{2}+\frac{b-1}{2}\pmod 2$ 임을 보이자.

$\frac{ab-1}{2}-\left(\frac{a-1}{2}-\frac{b-1}{2}\right)=\frac{(a-1)(b-1)}{2}$ 이고 a,b가 홀수이므로 우변은 짝수이다. 따라서 $\frac{ab-1}{2}\equiv\frac{a-1}{2}+\frac{b-1}{2}\pmod 2$ 이다. (18)

그러므로 홀수인 소수 $p_1,p_2,...,p_r$ 에 대하여 $n=p_1p_2\cdots p_r$ 라고 하면
(18)과 수학적 귀납법에 의해 다음을 얻을수 있다.

$$(-1/n)=(-1/p_1)\cdots(-1/p_r)=(-1)^{\sum_{k=1}^{r}\frac{p_k-1}{2}}=(-1)^{\frac{p_1p_2\cdots p_r-1}{2}}=(-1)^{\frac{n-1}{2}}$$

■

(h). $\frac{a^2b^2-1}{8}-\left(\frac{a^2-1}{8}+\frac{b^2-1}{8}\right)=\frac{(a^2-1)(b^2-1)}{8}$ 이므로 a,b가 홀수이면 우변은 짝수이다. 따라서 $\frac{a^2b^2-1}{8}\equiv\frac{a^2-1}{8}+\frac{b^2-1}{8}\pmod 2$ 이다. (19)

그러므로 홀수인 소수 $p_1,p_2,...,p_r$ 에 대하여 $n=p_1p_2\cdots p_r$ 라고 하면
수학적 귀납법에 의해 다음을 얻을수 있다.

$$(2/n)=(2/p_1)\cdots(2/p_r)=(-1)^{\sum_{k=1}^{r}\frac{p_k^2-1}{8}}=(-1)^{\frac{p_1^2p_2^2\cdots p_r^2-1}{8}}=(-1)^{\frac{n^2-1}{8}}$$

■

(i). $\gcd(m,n)=1$ 이므로 m,n을 소수의 곱으로 나타낸 결과가 다음과 같다고 할 때

$$m=p_1p_2\cdots p_r$$
$$n=q_1q_2\cdots q_s$$

모든 i,j에 대하여 $\gcd(p_i,q_j)=1$ 을 만족한다. 따라서 이차 상호 법칙과 (18)에 의하면 다음 등식이 성립한다.

$$
\begin{aligned}
(m/n) &= (m/q_1)(m/q_2)\cdots(m/q_s) \\
&= \prod_{\substack{1 \le i \le r \\ 1 \le j \le s}} (p_i/q_j) \\
&= \prod_{\substack{1 \le i \le r \\ 1 \le j \le s}} (q_j/p_i)(-1)^{\left(\frac{p_i-1}{2}\right)\left(\frac{q_j-1}{2}\right)} \\
&= (n/m)(-1)^{\sum\limits_{\substack{1 \le i \le r \\ 1 \le j \le s}} \left(\frac{p_i-1}{2}\right)\left(\frac{q_j-1}{2}\right)} \\
&= (n/m)(-1)^{\left(\sum\limits_{i=1}^{r} \frac{p_i-1}{2}\right)\left(\sum\limits_{j=1}^{s} \frac{q_j-1}{2}\right)} \\
&= (n/m)(-1)^{\left(\frac{p_1p_2\cdots p_r-1}{2}\right)\left(\frac{q_1q_2\cdots q_s-1}{2}\right)} \\
&= (n/m)(-1)^{\left(\frac{m-1}{2}\right)\left(\frac{n-1}{2}\right)}
\end{aligned}
$$

따라서 $(m/n)(n/m) = (-1)^{\left(\frac{m-1}{2}\right)\left(\frac{n-1}{2}\right)}$ 이다. ■

Problem 4.4.1 n이 3 이상의 홀수이면서 제곱인수가 없는 자연수일 때 다음을 증명하시오.
(a). $\gcd(a,n)=1$ 과 $(a/n)=-1$ 을 만족하는 정수 a가 존재한다.
(b). $S=\{a_1,a_2,...,a_{\phi(n)}\}$가 법 n에 대한 기약잉여계일 때 $\sum\limits_{k=1}^{\phi(n)}(a_k/n)=0$ 이다.

(증명)
(a). n이 소수이면 이차 비잉여가 항상 존재하므로 명백하다.
따라서 n이 합성수인 경우를 가정하자.

조건에 의하면 n을 소인수분해한 결과는 서로 다른 소수 $p_1,p_2,...,p_r\,(r \ge 2)$ 에 대하여 $n = p_1p_2\cdots p_r$ 이다. 그리고 $(b/p_1)=-1$ 을 만족하는 정수 $b \in \mathbb{Z}_{p_1}^{\times}$ 는 항상 존재하고 중국인의 나머지 정리에 의하면 다음을 만족하는 정수 a도 항상 존재한다.

$$
\begin{aligned}
a &\equiv b \pmod{p_1} \\
a &\equiv 1 \pmod{p_2} \\
a &\equiv 1 \pmod{p_3} \\
&\vdots \\
a &\equiv 1 \pmod{p_r}
\end{aligned}
$$

이때 $\gcd(a,n)=1$ 이고 $(a/p_1)=-1$ 와 $(a/p_2)=(a/p_3)=\cdots=(a/p_r)=1$ 을 만족한다. 따라서 $(a/n)=-1$ 이므로 조건을 만족하는 정수 a가 존재한다. ■

(b). (a)에 의하면 $\gcd(a,n)=1$ 과 $(a/n)=-1$ 을 만족하는 정수 a가 존재한다.
이때 $aS=\{aa_1,aa_2,...,aa_{\phi(n)}\}$ 라고 정의하면 aS 도 법 n에 대한 기약잉여계이다.

따라서 $x=\sum_{k=1}^{\phi(n)}(a_k/n)$ 라고 하면 S 와 aS 의 원소는 법 n에서 일대일로 대응되므로

야코비 기호의 성질에 의하면 $x=\sum_{k=1}^{\phi(n)}(aa_k/n)$ 가 성립하고 다음을 얻는다.

$$\begin{aligned} x &= \sum_{k=1}^{\phi(n)}(aa_k/n) \\ &= \sum_{k=1}^{\phi(n)}(a/n)(a_k/n) \\ &= -\sum_{k=1}^{\phi(n)}(a_k/n) \\ &= -x \end{aligned}$$

그러므로 $x=\sum_{k=1}^{\phi(n)}(a_k/n)=0$ 이다. ■

야코비 기호를 일반화한 기호도 있는데 수학에서는 **크로네커 기호(Kronecker Symbol)**라고 부릅니다. 크로네커 기호는 야코비 기호 (a/n) 에서 n이 임의의 정수인 경우로 확장시킨 기호입니다. 확장시키는 과정은 다음과 같습니다.

1) $n=0$
$\gcd(a,0)=|a|$ 이므로 $|a|=1$ 즉, $a=\pm 1$ 일때만 정의하고
$(a/0)=1$ 라고 정의합니다.

2) $n=1$
$\gcd(a,1)=1$ 이고 이때는 $(a/1)=1$ 라고 정의합니다.

3) $n=-1$
$\gcd(a,-1)=1$ 이고 이때는 $(a/-1)=\begin{cases}-1 & (a<0)\\ 1 & (a\geq 0)\end{cases}$ 라고 정의합니다.

4) $n=2$
a가 홀수일때만 정의하고 $(a/2)=\begin{cases}1 & (a\equiv\pm 1 \pmod 8)\\ -1 & (a\equiv\pm 3 \pmod 8)\end{cases}$ 라고 정의합니다.

5) 나머지 경우
$u=\pm 1$ 일 때 적당한 소수 $p_1,p_2,...,p_r$ 에 대하여 $n=up_1p_2\cdots p_r$ 로 표현되면
$\gcd(a,n)=1$ 일 때 $(a/n)=(a/u)(a/p_1)(a/p_2)\cdots(a/p_r)$ 라고 정의합니다.
$p_1,p_2,...,p_r$ 중에는 같은 소수가 있을수도 있습니다.

이렇게 정의한 크로네커 기호도 야코비 기호와 비슷한 성질을 가지고 있습니다.
그 성질을 여기서 소개하진 않겠습니다.

5. 산술 함수

5.1 여러 가지 산술 함수

작성자 : 네냐플(Nenyaffle)

5장에서는 산술 함수에 대해 소개하려고 합니다. 정수론에서 **산술 함수(Arithmetic Function)**의 정의는 자연수 전체의 집합 $\mathbb{N}$을 정의역으로 갖는 함수입니다. 책에 따라서는 이런 함수를 Number Theoretic Function 이라고 부르기도 합니다.

한 예로 오일러의 ϕ함수 $\phi(n)$은 산술 함수입니다. 정의역이 $\mathbb{N}$인 함수이기 때문입니다. 그리고 자연수 n에 대하여 $\tau(n)$을 n의 양의 약수의 개수, $\sigma(n)$을 양의 약수의 총합으로 정의하면 $\tau(n), \sigma(n)$도 산술 함수입니다.

앞으로 $\tau(n), \sigma(n)$은 각각 자연수 n의 양의 약수의 개수와 총합을 나타내는 기호로 사용하겠습니다.

산술 함수를 소개하기 전에 5장에서 자주 사용하게 될 보조정리를 먼저 소개하겠습니다. 대학 입학 전에 이미 배운 내용입니다.

Lemma 5.1.1 $n \geq 2$ 를 만족하는 자연수 n을 소인수분해한 결과가 $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ 이라고 하자. 이때 각각의 $i = 1,2,...,r$ 에 대하여 a_i를 $0 \leq a_i \leq k_i$ 를 만족하는 정수라고 하면 n의 양의 약수 d는 $d = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ 이런 형태로 표현된다.

(증명)

$d = 1$ 이면 $a_1 = a_2 = \cdots = a_r = 0$ 일 때 $d = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ 를 만족한다.

따라서 $d \geq 2$ 라고 가정하자. 그러면 $q \mid d$ 를 만족하는 소수 q가 존재하고 $d \mid n$ 이므로 $q \mid p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ 을 얻는다. 따라서 적당한 $i = 1,2,...,r$ 에 대하여 $q = p_i$ 를 만족하고 그러므로 d는 $p_1, p_2, ..., p_r$ 이외의 소인수를 갖지 않는다.

따라서 d를 소인수분해한 결과는 $d = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ 이런 형태로만 나온다.

이제 각각의 $i = 1,2,...,r$ 에 대하여 $0 \leq a_i \leq k_i$ 임을 보이자.

결론을 부정해서 적당한 $i = 1,2,...,r$ 에 대해 $a_i > k_i$ 라고 가정하면 $a_i \geq 1 + k_i$ 이고 따라서 $p_i^{1+k_i} \mid d$ 이다. 그리고 $d \mid n$ 이므로 $p_i^{1+k_i} \mid p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ 이고 $p_1, p_2, ..., p_r$ 은 서로 다른 소수이므로 $p_i^{1+k_i} \mid p_i^{k_i}$ 에서 $p \mid 1$ 을 얻는데 이것은 모순이다.

그러므로 $d = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ 로 소인수분해 되면 각각의 $i = 1,2,...,r$ 에 대하여 $0 \leq a_i \leq k_i$ 를 만족한다. ■

이제 이것을 이용해서 대학 입학 전에 배운 공식을 증명할수 있습니다.
사실 증명방법도 대학 입학 전에 배운 방법과 똑같습니다.

Theorem 5.1.1 $n \geq 2$ 를 만족하는 자연수 n을 소인수분해한 결과가
$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ 라고 하면 다음이 성립한다.
(a). $\tau(n) = (k_1+1)(k_2+1)\cdots(k_r+1)$ 이다.
(b). $\sigma(n) = \left(\frac{p_1^{k_1+1}-1}{p_1-1}\right)\left(\frac{p_2^{k_2+1}-1}{p_2-1}\right)\cdots\left(\frac{p_r^{k_r+1}-1}{p_r-1}\right)$ 이다.

(증명)

Lemma 5.1.1에 의하면 n의 양의 약수는 $d = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ 이런 형태이고
이때 각각의 $i = 1,2,...,r$ 에 대하여 $0 \leq a_i \leq k_i$ 를 만족한다.

(a). $0 \leq a_i \leq k_i$ 를 만족하는 정수 a_i의 개수는 k_i+1 이므로 각각의 $i = 1,2,...,r$ 에 대하여 소인수 p_i를 뽑는 경우의 수는 k_i+1 이다. 그리고 $p_i^{a_i}$가 결정되면 양의 약수가 결정되므로 n의 양의 약수의 개수는 다음과 같다.

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

■

(b). 다항식의 전개식과 Lemma 5.1.1을 생각해보면 다음 식은 양의 약수의 총합과 같다.

$$\left(1+p_1+p_1^2+\cdots+p_1^{k_1}\right)\left(1+p_2+p_2^2+\cdots+p_2^{k_2}\right)\cdots\left(1+p_r+p_r^2+\cdots+p_r^{k_r}\right)$$

따라서 등비수열의 합 공식에 의하면 다음을 얻는다.

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

■

$n = 1$ 이면 $\tau(1) = \sigma(1) = 1$ 은 명백하므로 $n \geq 2$ 일 때만 조사해도 충분합니다.
그리고 $\tau(n)$을 이용해서 n의 양의 약수의 곱을 나타낼수 있는데 방법은 다음과 같습니다.

n의 양의 약수를 크기 순서대로 나열한 것을 $d_1, d_2, ..., d_{\tau(n)}$ 라고 하면
이것을 다음과 같이 나열해서 같은 열에 있는 약수들끼리 곱하는겁니다. 이것은 등차수열의 합 공식을 유도하는 방법과 비슷한 방법입니다.

$$d_1 \quad d_2 \quad \cdots \quad d_{\tau(n)}$$

$$d_{\tau(n)} \quad d_{\tau(n)-1} \quad \cdots \quad d_1$$

위처럼 나열해서 같은 열에 있는 약수들끼리 곱하면 $\tau(n)$개의 n이 나옵니다.
6의 양의 약수를 다음과 같이 나열해서

1 2 3 6
6 3 2 1

같은 열끼리 곱하면 모두 $\tau(6) = 4$개의 6이 나오는 것을 생각해보면 쉽습니다.

따라서 $\left(d_1 d_2 \cdots d_{\tau(n)}\right)^2 = n^{\tau(n)}$ 이므로 $d_1 d_2 \cdots d_{\tau(n)} = n^{\frac{\tau(n)}{2}}$ 가 성립합니다.

좀 더 깔끔하게 표현하면 $\prod_{d \mid n} d = n^{\frac{\tau(n)}{2}}$ 입니다.

우변을 보면 $\frac{\tau(n)}{2}$ 가 있어서 $\tau(n)$이 홀수일 때 $n^{\frac{\tau(n)}{2}}$ 가 자연수가 될수 없다고 생각할수도 있는데 실제로 $n^{\frac{\tau(n)}{2}}$ 가 양의 약수의 곱이 된다는 것을 모른다고 해도 자연수가 된다는 것을 보일수 있습니다.

Theorem 5.1.1 (a)에 의하면 $\tau(n)$이 홀수가 될 필요충분조건은 모든 $i = 1,2,...,r$ 에 대하여 $k_i + 1$ 이 홀수가 되는 것입니다. 즉, 모든 $i = 1,2,...,r$ 에 대하여 k_i가 짝수가 되는 것이고 n을 소인수분해 했을 때 소인수의 지수가 모두 짝수이면 n은 어떤 자연수의 제곱으로 표현됩니다.

자연수 m에 대하여 $n = m^2$ 이면 $n^{\frac{\tau(n)}{2}} = m^{\tau(m^2)}$ 이므로 $\tau(n)$이 홀수일때도 $n^{\frac{\tau(n)}{2}}$ 은 자연수가 된다는 것을 쉽게 알수 있습니다.

이제 특수한 조건을 만족하는 산술함수를 소개하겠습니다. 오일러의 ϕ함수를 소개할때도 나온건데 m, n이 $\gcd(m,n) = 1$ 을 만족하는 자연수이면 $\phi(mn) = \phi(m)\phi(n)$ 가 성립합니다. 이런 성질을 만족하는 산술 함수를 다음과 같이 정의합니다.

Definition 5.1.1 승법 함수(Multiplicative Function)
산술 함수 f가 $\gcd(m,n) = 1$ 을 만족하는 모든 자연수 m, n에 대하여 $f(mn) = f(m)f(n)$ 가 성립하면 f를 **승법 함수(Multiplicative Function)**라고 정의한다.

오일러의 ϕ함수를 소개할때도 설명했지만 승법 함수의 장점은 소수 p에 대하여 $f(p^k)$의 값만 구할수 있으면 모든 자연수 n에 대하여 $f(n)$의 값을 구할수 있다는 것입니다.

그리고 모든 자연수 n에 대하여 $\gcd(n,1) = 1$ 이므로 f가 승법 함수이면 $f(n) = f(1)f(n)$ 가 성립합니다. 따라서 $f(n) \neq 0$ 을 만족하는 자연수 n이 존재한다면 $f(1) = 1$ 가 성립합니다.

오일러의 ϕ함수는 승법 함수임을 2장에서 증명했습니다. 여기서는 $\tau(n)$과 $\sigma(n)$도 승법 함수임을 보이겠습니다.

Theorem 5.1.2 $\tau(n), \sigma(n)$은 모두 승법 함수이다.

(증명)
$\gcd(m,n) = 1$ 을 만족하는 임의의 자연수 m, n에 대하여 다음을 증명하자.

$$\tau(mn) = \tau(m)\tau(n), \sigma(mn) = \sigma(m)\sigma(n) \quad (1)$$

m, n 둘중 적어도 하나가 1이면 (1)은 명백하다. 따라서 $m \geq 2, n \geq 2$ 를 가정하자.
그러면 m, n을 소인수분해한 결과가 다음과 같이 나온다고 할 때

$$m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$
$$n = q_1^{j_1} q_2^{j_2} \cdots q_s^{j_s}$$

$\gcd(m,n)=1$ 이므로 $p_1, p_2, ..., p_r, q_1, q_2, ..., q_s$ 는 모두 서로 다른 소수가 되어야 한다.
그리고 이때 $mn = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} q_1^{j_1} q_2^{j_2} \cdots q_s^{j_s}$ 이므로 Theorem 5.1.1에 의하면

$$\tau(mn) = (k_1+1)\cdots(k_r+1)(j_1+1)\cdots(j_s+1) = \tau(m)\tau(n)$$
$$\sigma(mn) = \left(\frac{p_1^{k_1+1}-1}{p_1-1}\right)\cdots\left(\frac{p_r^{k_r+1}-1}{p_r-1}\right)\left(\frac{q_1^{j_1+1}-1}{q_1-1}\right)\cdots\left(\frac{q_s^{j_s+1}-1}{q_s-1}\right) = \sigma(m)\sigma(n)$$

가 성립한다. 따라서 $\tau(n), \sigma(n)$은 모두 승법 함수이다. ■

이제 좀 더 일반적인 승법 함수의 성질을 소개하겠습니다. 그것을 소개하기 위해서는
다음 보조정리가 필요합니다.

Lemma 5.1.2 m, n이 $\gcd(m,n)=1$ 을 만족하는 자연수이면 두 집합 S, T 를
$S = \{d \in \mathbb{N} : d \mid mn\}$
$T = \{d_1 d_2 \in \mathbb{N} : d_1, d_2$는 $d_1 \mid m,\ d_2 \mid n,\ \gcd(d_1,d_2)=1$을 만족하는 자연수$\}$
라고 정의할 때 $S = T$ 이다.

(증명)
m, n 둘중 적어도 하나가 1이면 $S = T$ 는 명백하다. 따라서 $m \geq 2, n \geq 2$ 를
가정하자. 그러면 m, n을 소인수분해한 결과가 다음과 같이 나온다고 할 때

$$m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$
$$n = q_1^{j_1} q_2^{j_2} \cdots q_s^{j_s}$$

$\gcd(m,n)=1$ 이므로 $p_1, p_2, ..., p_r, q_1, q_2, ..., q_s$ 는 모두 서로 다른 소수가 되어야 하고
이때 $mn = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} q_1^{j_1} q_2^{j_2} \cdots q_s^{j_s}$ 이다. 이제 $S = T$ 임을 보이자.

$(\subset)$ 임의의 $x \in S$ 를 택하자. 그러면 Lemma 5.1.1에 의해 x는 다음과 같이 나타난다.

$$x = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$$

이때 $d_1 = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, $d_2 = q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$ 라고 하면 $x = d_1 d_2$ 이고 d_1, d_2는 자연수,
$d_1 \mid m,\ d_2 \mid n,\ \gcd(d_1,d_2)=1$ 이므로 $x \in T$ 이다.

$(\supset)$ 임의의 $x \in T$ 를 택하자. 그러면 $d_1 \mid m,\ d_2 \mid n,\ \gcd(d_1,d_2)=1$ 를 만족하는
자연수 d_1, d_2에 대하여 $x = d_1 d_2$ 이고 이때 $x \mid mn$ 은 명백하다. 따라서 $x \in S$ 이다.

정리하면 $S = T$ 를 얻는다. ■

Lemma 5.1.2는 $\gcd(m,n)=1$ 일 때 mn의 모든 양의 약수는 m의 양의 약수와 n의 양의 약수를 곱한 형태로만 표현된다는 정리입니다.

Lemma 5.1.3 두 수열 $\{a_n\}, \{b_n\}$에 대하여 다음 등식이 성립한다.

$$\sum_{\substack{1 \le i \le m \\ 1 \le j \le n}} a_i b_j = \left(\sum_{i=1}^{m} a_i\right)\left(\sum_{j=1}^{n} b_j\right) \tag{2}$$

(2)에서 좌변은 $a_i b_j$에 $1 \le i \le m, 1 \le j \le n$ 을 만족하는 자연수 i, j를 모두 대입한 것을 더했다는 기호이다. 예를 들어 $m=2, n=3$ 이면 (2)의 좌변은 다음과 같다.

$$\sum_{\substack{1 \le i \le 2 \\ 1 \le j \le 3}} a_i b_j = a_1b_1 + a_1b_2 + a_1b_3 + a_2b_1 + a_2b_2 + a_2b_3$$

(증명)

기호의 정의에 의하면 다음 등식을 얻을수 있다.

$$\begin{aligned}\sum_{\substack{1 \le i \le m \\ 1 \le j \le n}} a_i b_j &= a_1\sum_{j=1}^{n} b_j + a_2\sum_{j=1}^{n} b_j + \cdots + a_m\sum_{j=1}^{n} b_j \\ &= (a_1 + a_2 + \cdots + a_m)\sum_{j=1}^{n} b_j \\ &= \left(\sum_{i=1}^{m} a_i\right)\left(\sum_{j=1}^{n} b_j\right)\end{aligned}$$

■

2개의 보조정리를 이용해서 다음을 증명할수 있습니다.

Theorem 5.1.3 f가 승법 함수일 때 산술 함수 F를 다음과 같이 정의하자.

$$F(n) = \sum_{d \mid n} f(d)$$

그러면 F는 승법 함수이다.

(증명)

$\gcd(m,n)=1$ 을 만족하는 자연수 m, n을 임의로 택하고 $F(mn)=F(m)F(n)$ 임을 보이자. Lemma 5.1.2와 Lemma 5.1.3에 의하면 다음 등식이 성립한다.

$$\begin{aligned}F(mn) &= \sum_{d \mid mn} f(d) \\ &= \sum_{d_1 \mid m,\, d_2 \mid n} f(d_1 d_2) \\ &= \sum_{d_1 \mid m,\, d_2 \mid n} f(d_1) f(d_2) \\ &= \left(\sum_{d_1 \mid m} f(d_1)\right)\left(\sum_{d_2 \mid n} f(d_2)\right) \\ &= F(m)F(n)\end{aligned}$$

따라서 F는 승법 함수이다. ■

$\tau(n)=\sum_{d\mid n}1,\ \sigma(n)=\sum_{d\mid n}d$ 인데 $f(n)=1,\ g(n)=n$ 이 승법 함수임은 명백하므로 Theorem 5.1.3에 의하면 $\tau(n)=\sum_{d\mid n}1,\ \sigma(n)=\sum_{d\mid n}d$ 는 모두 승법 함수임을 쉽게 알수 있습니다.

비슷하게 f,g가 승법 함수일 때 $F(n)=f(n)g(n)$ 이면 F가 승법 함수임은 명백하고 모든 자연수 n에 대하여 $g(n)\neq 0$ 일 때 $G(n)=\frac{f(n)}{g(n)}$ 이면 G가 승법 함수임은 명백합니다.

Theorem 5.1.4 f가 산술 함수일 때 산술 함수 F를 $F(n)=\sum_{d\mid n}f(d)$ 라고 정의하자.
그러면 모든 자연수 N에 대하여 $\sum_{n=1}^{N}F(n)=\sum_{k=1}^{N}f(k)\left\lfloor\frac{N}{k}\right\rfloor$ 이다.
여기서 $\lfloor x\rfloor$ 는 바닥함수이다.

(증명)

$\sum_{n=1}^{N}F(n)$을 다음과 같은 방법으로 구해보자. 1부터 N까지의 자연수의 양의 약수를 다음과 같이 모두 모았다고 하자.

$$\begin{aligned}&1\text{의 양의 약수 : } 1\\&2\text{의 양의 약수 : } 1,2\\&3\text{의 양의 약수 : } 1,3\\&\vdots\\&N\text{의 양의 약수 : } d_1,d_2,\ldots,d_{\tau(N)}\end{aligned}\tag{3}$$

그러면 $k\le N$ 을 만족하는 자연수 k에 대하여 k가 (3)에 총 몇 번 등장하는지 조사하면 충분하다. (3)은 1부터 N까지의 자연수의 양의 약수를 모두 모은 것이므로 k가 (3)에 등장하면 그것은 k의 배수에서만 등장한다. 어떤 자연수가 k를 양의 약수로 가질 필요충분조건은 그 자연수가 k의 배수인 것이기 때문이다.

1부터 N까지의 자연수들 중 k의 배수의 개수는 $\left\lfloor\frac{N}{k}\right\rfloor$ 이고 따라서 $\sum_{n=1}^{N}F(n)$ 에서 $f(k)$는 총 $\left\lfloor\frac{N}{k}\right\rfloor$ 개 나온다. 그러므로 각각의 $k=1,2,\ldots,N$ 에 대하여 모두 더하면 $\sum_{n=1}^{N}F(n)=\sum_{k=1}^{N}f(k)\left\lfloor\frac{N}{k}\right\rfloor$ 가 성립한다. ■

Theorem 5.1.4에서 $\sum_{n=1}^{N}F(n)=\sum_{n=1}^{N}f(n)\left\lfloor\frac{N}{n}\right\rfloor$ 이렇게 k 대신 n을 써도 됩니다.

$\tau(n)=\sum_{d\mid n}1,\ \sigma(n)=\sum_{d\mid n}d$ 이므로 Theorem 5.1.4에 의하면 다음 등식이 성립합니다.

$$\sum_{n=1}^{N}\tau(n)=\sum_{n=1}^{N}\left\lfloor\frac{N}{n}\right\rfloor$$

$$\sum_{n=1}^{N}\sigma(n)=\sum_{n=1}^{N}n\left\lfloor\frac{N}{n}\right\rfloor$$

그리고 $n=\sum_{d\mid n}\phi(d)$ 이므로 $\sum_{n=1}^{N}n=\sum_{n=1}^{N}\phi(n)\left\lfloor\frac{N}{n}\right\rfloor$ 가 성립하고 좌변은

$\sum_{n=1}^{N}n=\frac{N(N+1)}{2}$ 이므로 $\sum_{n=1}^{N}\phi(n)\left\lfloor\frac{N}{n}\right\rfloor=\frac{N(N+1)}{2}$ 도 성립합니다.

Problem 5.1.1 다음을 증명하시오.

(a). 모든 자연수 n에 대하여 $\tau(n)<2\sqrt{n}$ 이다.

(b). $\sigma(n)$이 홀수가 될 필요충분조건은 n이 완전제곱수 또는 완전제곱수의 2배인 것이다.

(증명)

(a). $n=1$ 이면 $\tau(n)=1$, n이 소수이면 $n\geq 2$ 이고 $\tau(n)=2$ 이므로 주어진 부등식이 성립함은 명백하다. 따라서 n이 합성수인 경우를 가정하자.

case1) n이 완전제곱수인 합성수

n이 완전제곱수인 합성수이므로 $m\geq 2$ 인 적당한 자연수 m이 존재해서 $n=m^2$ 을 만족하고 이 경우 $\sqrt{n}=m$ 은 n의 양의 약수이다.

그리고 완전제곱수의 양의 약수를 크기 순서대로 나열하면 $\sqrt{n}=m$ 을 기준으로 좌우로 같은 개수만큼 있게 된다. 따라서 $\sqrt{n}=m$ 이하의 양의 약수의 개수는 $1+\frac{\tau(n)-1}{2}=\frac{\tau(n)+1}{2}$ 이다.

그리고 $\lfloor x\rfloor$ 를 바닥함수라고 할 때 $\lfloor\sqrt{n}\rfloor$ 은 $\sqrt{n}$ 보다 작은 자연수의 개수이다.

따라서 $\frac{\tau(n)+1}{2}\leq\lfloor\sqrt{n}\rfloor$ 이고 $\sqrt{n}=m$ 이므로 다음 부등식이 성립한다.

$$\tau(n)\leq 2\lfloor\sqrt{n}\rfloor-1<2\lfloor\sqrt{n}\rfloor=2\sqrt{n}$$

case2) n이 완전제곱수가 아닌 합성수

이 경우 $\sqrt{n}$ 은 자연수가 아니다. 그리고 n이 합성수이므로 n은 $\sqrt{n}$ 보다 작은 양의 약수를 갖고 n의 양의 약수를 크기 순서대로 나열하면 $\sqrt{n}$ 보다 작은 약수의 개수와 $\sqrt{n}$ 보다 큰 약수의 개수는 같다는 것을 쉽게 알수 있다.

따라서 $\frac{\tau(n)}{2} \leq \lfloor \sqrt{n} \rfloor$ 이므로 $\tau(n) \leq 2 \lfloor \sqrt{n} \rfloor < 2\sqrt{n}$ 을 얻는다.

그러므로 어느 경우든 $\tau(n) < 2\sqrt{n}$ 가 성립한다. ■

(b). Theorem 5.1.1의 증명과정에 의하면 $n \geq 2$ 일 때 $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ 으로 소인수분해 되었을 경우 $\sigma(n)$이 홀수일 필요충분조건은 모든 $i = 1,2,...,r$ 에 대하여 $1 + p_i + p_i^2 + \cdots + p_i^{k_i}$ 가 홀수인 것이다. (4)

$(\Longrightarrow)$ $n = 1$ 이면 명백하다. 따라서 $n \geq 2$ 를 가정하자. 만약 n이 홀수이면 $p_1, p_2, ..., p_r$ 은 모두 홀수이므로 (4)를 만족하려면 k_i가 짝수가 되어야 한다.
따라서 이 경우 n의 모든 소인수의 지수는 짝수이므로 완전제곱수이다.

n이 짝수이면 2를 소인수로 갖는데 $p_i = 2$ 일 때 k_i가 자연수이면 $1 + 2 + 2^2 + \cdots + 2^{k_i}$ 는 홀수이다. 그리고 홀수인 소인수에 대해서는 n이 홀수인 경우의 풀이를 그대로 따르면 소인수의 지수가 모두 짝수라는 사실을 얻을수 있다.

이 경우 n은 완전제곱수 또는 완전제곱수의 2배가 된다. 구체적으로 2의 지수가 짝수이면 완전제곱수가 되고 2의 지수가 홀수이면 완전제곱수의 2배가 된다.

$(\Longleftarrow)$ 이 경우에는 직접 계산해보면 명백하므로 생략한다. ■

Problem 5.1.2 자연수 n에 대하여 다음을 증명하시오.

(a). $\sum_{d \mid n} \frac{1}{d} = \frac{\sigma(n)}{n}$ 이다.

(b). $n \geq 2$ 일 때 n이 $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ 로 소인수분해 되면 다음 부등식이 성립한다.

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

(c). $\frac{\sigma(n!)}{n!} \geq 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$ 이다.

(d). n이 합성수이면 $\sigma(n) > n + \sqrt{n}$ 이다.

(e). $k \geq 2$ 인 임의의 자연수 k에 대하여 $\tau(n) = k$ 를 만족하는 자연수 n의 개수는 무한하고 $\sigma(n) = k$ 를 만족하는 자연수 n의 개수는 유한하다.

(증명)

(a). d가 n의 약수이면 $\frac{n}{d}$도 n의 약수이므로 $\sigma(n) = \sum_{d \mid n} \frac{n}{d}$ 가 성립한다.

따라서 $\sum_{d \mid n} \frac{1}{d} = \frac{\sigma(n)}{n}$ 를 얻을수 있다. ■

(b). 조건에 의하면 $\sigma(n)=\left(\frac{p_1^{k_1+1}-1}{p_1-1}\right)\left(\frac{p_2^{k_2+1}-1}{p_2-1}\right)\cdots\left(\frac{p_r^{k_r+1}-1}{p_r-1}\right)$ 이고

모든 $i=1,2,...,r$ 에 대하여 다음 부등식을 얻을수 있다.

$$p_i^{k_i}\times\frac{p_i-1}{p_i^{k_i+1}-1}=\frac{p_i-1}{p_i-\frac{1}{p_i^{k_i}}}>\frac{p_i-1}{p_i}=1-\frac{1}{p_i}$$

따라서 $\frac{n}{\sigma(n)}>\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)$ 가 성립한다.

그리고 $n\geq 2$ 이면 $\tau(n)\geq 2$ 이므로 (a)에 의하면 $\frac{\sigma(n)}{n}>1$ 이다.

그러므로 다음 부등식을 얻을수 있다.

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

■

(c). $1,2,...,n$ 은 모두 $n!$의 양의 약수이다. 따라서 (a)에 의하면 다음 부등식을 얻는다.

$$\frac{\sigma(n!)}{n!}=\sum_{d\mid n!}\frac{1}{d}\geq 1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}$$

■

(d). n이 합성수이므로 n은 $\sqrt{n}$ 보다 작은 양의 약수를 갖는다. 그것을 d라고 하면

$d\leq\sqrt{n}$ 이므로 $\frac{1}{d}\geq\frac{1}{\sqrt{n}}$ 이고 $\tau(n)\geq 3$ 이므로 (a)에 의하면 다음을 얻을수 있다.

$$\frac{\sigma(n)}{n}=\sum_{d\mid n}\frac{1}{d}>1+\frac{1}{\sqrt{n}}$$

따라서 $\sigma(n)>n+\sqrt{n}$ 가 성립한다. ■

(e). $k\geq 2$ 이므로 모든 소수 p에 대하여 $n=p^{k-1}$ 은 자연수이고 이때 $\tau(n)=k$ 이다.
그리고 소수의 개수는 무한하므로 결국 $\tau(n)=k$ 을 만족하는 자연수 n의 개수는 무한하다.

$\sigma(n)=k$ 이면 $n\geq 2$ 이므로 (b)에서 $n<k$ 를 얻는다. 그러므로 $\sigma(n)=k$ 를
만족하는 자연수 n은 $n<k$ 를 만족하고 k는 고정된 자연수이므로 $\sigma(n)=k$ 를
만족하는 자연수 n의 개수는 유한하다. ■

Problem 5.1.3 두 자연수 m, n에 대하여 다음을 증명하시오.
(a). $m \geq 2, n \geq 2$ 일 때 $p \mid n$ 을 만족하는 모든 소수 p가 $p \mid m$ 도 만족하면 $\phi(nm) = n\phi(m)$ 이다.
(b). $n \geq 2$ 이면 $\phi(n^2) + \phi((n+1)^2) \leq 2n^2$ 이다.
(c). 자연수 d가 $d \mid n$ 를 만족하면 $\phi(d) \mid \phi(n)$ 이다.
(d). $d = \gcd(m,n)$ 이면 $\phi(m)\phi(n) = \dfrac{\phi(mn)\phi(d)}{d}$ 이다.
(e). $\phi(m)\phi(n) = \phi(\gcd(m,n))\phi(\mathrm{lcm}(m,n))$ 이다.

(증명)
(a). 조건에 의하면 n의 소인수는 모두 m의 소인수이다. 따라서 n의 소인수분해가 $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ 일 때 m의 소인수분해는 다음과 같이 표현할수 있다.

$$m = p_1^{j_1} p_2^{j_2} \cdots p_r^{j_r} p_{r+1}^{j_{r+1}} \cdots p_s^{j_s}$$

따라서 다음 등식이 성립한다.

$$\phi(nm) = nm\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)\left(1-\frac{1}{p_{r+1}}\right)\cdots\left(1-\frac{1}{p_s}\right) = n\phi(m)$$

■

(b). (a)를 이용하면 모든 자연수 n에 대하여 $\phi(n^2) = n\phi(n)$ 가 성립한다는 것을 쉽게 알수 있다. 그리고 $n \geq 2$ 이므로 $\phi(n) \leq n-1$ 에서 다음 부등식을 얻는다.

$$\phi(n^2) + \phi((n+1)^2) = n\phi(n) + (n+1)\phi(n+1) \leq n(n-1) + n(n+1) = 2n^2$$

■

(c). $n = 1$ 이면 명백하다. 따라서 $n \geq 2$ 를 가정하자. $\phi(n)$은 승법 함수이므로 Lemma 5.1.1에 의하면 a, b가 $a \leq b$ 를 만족하는 자연수일 때 $\phi(p^a) \mid \phi(p^b)$ 가 성립함을 보이면 충분하다.

$\phi(p^a) = p^{a-1}(p-1)$, $\phi(p^b) = p^{b-1}(p-1)$ 이고 $a \leq b$ 이므로 $\phi(p^a) \mid \phi(p^b)$ 는 명백하다. 그리고 $\phi(n)$이 승법 함수이므로 $\phi(d) \mid \phi(n)$ 가 성립한다. ■

(d). $d = 1$ 이면 $\phi(n)$이 승법 함수라는 사실에 의해 참이다. 따라서 $d \geq 2$ 를 가정하자. 그러면 m, n은 공통 소인수가 존재하므로 소인수분해한 결과가 다음과 같다고 할수 있다.

$$m = p_1^{a_1} p_2^{a_2} \cdots p_u^{a_u} q_1^{b_1} q_2^{b_2} \cdots q_v^{b_v}$$
$$n = p_1^{c_1} p_2^{c_2} \cdots p_u^{c_u} r_1^{d_1} r_2^{d_2} \cdots r_w^{d_w}$$

여기서 $q_1, q_2, \ldots, q_v, r_1, r_2, \ldots, r_w$ 는 $p_1, p_2, \ldots, p_r$ 과 다른 소수이고 각 소인수의 지수는 모두 자연수이다. 그리고 각각의 $i = 1, 2, \ldots, u$ 에 대하여 $k_i = \min(a_i, c_i)$ 라고 하면 $d = p_1^{k_1} p_2^{k_2} \cdots p_u^{k_u}$ 임을 Lemma 5.1.1의 증명과 유사한 방법을 사용해서 보일수 있다. 따라서 각각 계산하면 다음을 얻는다.

$$\phi(m)=m\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_u}\right)\left(1-\frac{1}{q_1}\right)\cdots\left(1-\frac{1}{q_v}\right)$$
$$\phi(n)=n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_u}\right)\left(1-\frac{1}{r_1}\right)\cdots\left(1-\frac{1}{r_w}\right)$$

$$\phi(mn)=mn\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_u}\right)\left(1-\frac{1}{q_1}\right)\cdots\left(1-\frac{1}{q_v}\right)\left(1-\frac{1}{r_1}\right)\cdots\left(1-\frac{1}{r_w}\right)$$

$$\phi(d)=d\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_u}\right)$$

그러므로 $\phi(m)\phi(n)=\dfrac{\phi(mn)\phi(d)}{d}$ 임을 쉽게 알수 있다. ■

(e). $d=\gcd(m,n), l=\mathrm{lcm}(m,n)$ 라고 하자. $d=1$ 이면 $\phi(n)$이 승법 함수라는 사실과 $l=mn$ 이라는 사실에 의해 참이다. 따라서 $d\geq 2$ 를 가정하자. 그러면 m,n은 공통 소인수가 존재하므로 소인수분해한 결과가 다음과 같다고 할수 있다.

$$m=p_1^{a_1}p_2^{a_2}\cdots p_u^{a_u}q_1^{b_1}q_2^{b_2}\cdots q_v^{b_v}$$
$$n=p_1^{c_1}p_2^{c_2}\cdots p_u^{c_u}r_1^{d_1}r_2^{d_2}\cdots r_w^{d_w}$$

여기서 $q_1,q_2,...,q_v,r_1,r_2,...,r_w$ 는 $p_1,p_2,...,p_r$ 과 다른 소수이고 각 소인수의 지수는 모두 자연수이다. 그리고 각각의 $i=1,2,...,u$ 에 대하여 $k_i=\min(a_i,c_i)$ 라고 하면 $d=p_1^{k_1}p_2^{k_2}\cdots p_u^{k_u}$ 임을 Lemma 5.1.1의 증명과 유사한 방법을 사용해서 보일수 있다.

마찬가지로 각각의 $i=1,2,...,u$ 에 대하여 $j_i=\max(a_i,c_i)$ 라고 하면
$l=p_1^{j_1}p_2^{j_2}\cdots p_u^{j_u}q_1^{b_1}q_2^{b_2}\cdots q_v^{b_v}r_1^{d_1}r_2^{d_2}\cdots r_w^{d_w}$ 임을 같은 방법으로 보일수 있다.
따라서 각각 계산하면 다음을 얻는다.

$$\phi(m)=m\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_u}\right)\left(1-\frac{1}{q_1}\right)\cdots\left(1-\frac{1}{q_v}\right)$$
$$\phi(n)=n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_u}\right)\left(1-\frac{1}{r_1}\right)\cdots\left(1-\frac{1}{r_w}\right)$$
$$\phi(d)=d\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_u}\right)$$
$$\phi(l)=l\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_u}\right)\left(1-\frac{1}{q_1}\right)\cdots\left(1-\frac{1}{q_v}\right)\left(1-\frac{1}{r_1}\right)\cdots\left(1-\frac{1}{r_w}\right)$$

그리고 $mn=dl$ 이므로 $\phi(m)\phi(n)=\phi(d)\phi(l)$ 임을 쉽게 알수 있다.
즉, $\phi(m)\phi(n)=\phi(\gcd(m,n))\phi(\mathrm{lcm}(m,n))$ 이다. ■

Problem 5.1.4 자연수 n에 대하여 산술 함수 $\omega(n)$을 다음과 같이 정의하자.

$$\omega(n)=\begin{cases}0 & (n=1)\\ n\text{의 서로 다른 소인수의 개수} & (n\geq 2)\end{cases}$$

예를 들면 $360=2^3\times 3^2\times 5$ 이므로 $\omega(360)=3$ 이다. 다음 물음에 답하시오.

(a). m,n이 $\gcd(m,n)=1$ 을 만족하는 자연수이면 $\omega(mn)=\omega(m)+\omega(n)$ 임을 증명하시오. 따라서 모든 자연수 a에 대하여 $a^{\omega(n)}$은 승법 함수이다.
(b). 임의의 자연수 a,n에 대하여 $\tau(n^a)=\sum_{d\mid n}a^{\omega(d)}$ 임을 증명하시오.

(증명)
(a). m,n 둘중 적어도 하나가 1이면 명백하다. 따라서 $m\geq 2, n\geq 2$ 를 가정하자.
그러면 m,n을 소인수분해한 결과가 다음과 같이 나온다고 할 때

$$m=p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$$
$$n=q_1^{j_1}q_2^{j_2}\cdots q_s^{j_s}$$

$\gcd(m,n)=1$ 이므로 $p_1,p_2,...,p_r,q_1,q_2,...,q_s$ 는 모두 서로 다른 소수가 되어야 한다.
그리고 이때 $mn=p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}q_1^{j_1}q_2^{j_2}\cdots q_s^{j_s}$ 이므로 다음을 얻는다.

$$\omega(m)=r$$
$$\omega(n)=s$$
$$\omega(mn)=r+s$$

따라서 $\omega(mn)=\omega(m)+\omega(n)$ 가 성립한다. 그러므로 $a^{\omega(mn)}=a^{\omega(m)}a^{\omega(n)}$ 에서
$a^{\omega(n)}$이 승법 함수임을 쉽게 알수 있다. ■

(b). $\gcd(m,n)=1$ 이면 $\gcd(m^a,n^a)=1$ 이므로 $\tau(n^a)$는 승법 함수이다.
그리고 (a)와 Theorem 5.1.3에 의하면 $\sum_{d\mid n}a^{\omega(n)}$은 승법 함수이다.

따라서 소수 p와 자연수 k에 대하여 $n=p^k$ 일 때 등식이 성립하는지 확인하면 충분하다.

$n=p^k$ 이면 $\tau(n^a)=\tau(p^{ak})=ak+1$ 이고 p^k의 양의 약수는 $1,p,p^2,...,p^k$ 이므로
$\sum_{d\mid p^k}a^{\omega(d)}=a^{\omega(1)}+a^{\omega(p)}+a^{\omega(p^2)}+\cdots+a^{\omega(p^k)}=1+ak$ 이다. 즉, $n=p^k$ 일 때
등식이 성립하므로 모든 자연수 n에 대하여 $\tau(n^a)=\sum_{d\mid n}a^{\omega(d)}$ 이다. ■

Problem 5.1.5 임의의 자연수 s에 대하여 $\sigma_s(n)$을 n의 양의 약수의 s제곱합으로 정의하자. 즉, $\sigma_s(n)=\sum_{d\mid n} d^s$ 이다. $n \geq 2$ 일 때 n을 소인수분해한 결과가 $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ 이면 다음 등식이 성립함을 증명하시오.

$$\sigma_s(n)=\left(\frac{p_1^{s(k_1+1)}-1}{p_1^s-1}\right)\left(\frac{p_2^{s(k_2+1)}-1}{p_2^s-1}\right)\cdots\left(\frac{p_r^{s(k_r+1)}-1}{p_r^s-1}\right)$$

(증명)

자연수 s에 대하여 $f(n)=n^s$ 가 승법 함수임은 명백하므로 Theorem 5.1.3에 의하면 $\sigma_s(n)$은 승법 함수이다. 따라서 소수 p와 자연수 k에 대하여 $n=p^k$ 일때의 값만 구하면 충분하고

$$\sigma_s(p^k)=1+p^s+p^{2s}+\cdots+p^{ks}=\frac{p^{s(k+1)}-1}{p^s-1}$$

이므로 $\sigma_s(n)=\left(\frac{p_1^{s(k+1)}-1}{p_1^s-1}\right)\left(\frac{p_2^{s(k+1)}-1}{p_2^s-1}\right)\cdots\left(\frac{p_r^{s(k+1)}-1}{p_r^s-1}\right)$ 임을 쉽게 알수 있다.

■

Problem 5.1.6 리우빌 함수(Liouville Function)는 다음과 같이 정의되는 함수이다.

$$\lambda(n)=\begin{cases}1 & (n=1)\\ (-1)^{k_1+k_2+\cdots+k_r} & \left(n\text{의 소인수분해가 } n=p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r} \text{ 일 때}\right)\end{cases}$$

$360=2^3\times 3^2\times 5$ 이므로 $\lambda(360)=(-1)^{3+2+1}=1$ 이다. 다음 물음에 답하시오.

(a). λ는 승법 함수임을 증명하시오.

(b). 자연수 n에 대하여 $\sum_{d\mid n}\lambda(d)=\begin{cases}1 & (n\text{은 완전제곱수})\\ 0 & (\text{otherwise})\end{cases}$ 임을 증명하시오.

(증명)

(a). m,n 둘중 적어도 하나가 1이면 명백하다. 따라서 $m\geq 2, n\geq 2$ 를 가정하자. 그러면 m,n을 소인수분해한 결과가 다음과 같이 나온다고 할 때

$$m=p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$$
$$n=q_1^{j_1}q_2^{j_2}\cdots q_s^{j_s}$$

$\gcd(m,n)=1$ 이므로 $p_1,p_2,\ldots,p_r,q_1,q_2,\ldots,q_s$ 는 모두 서로 다른 소수가 되어야 한다. 그리고 이때 $mn=p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}q_1^{j_1}q_2^{j_2}\cdots q_s^{j_s}$ 이므로 다음을 얻는다.

$$\lambda(m)=(-1)^{k_1+k_2+\cdots+k_r}$$
$$\lambda(n)=(-1)^{j_1+j_2+\cdots+j_s}$$
$$\lambda(mn)=(-1)^{(k_1+k_2+\cdots+k_r)+(j_1+j_2+\cdots+j_s)}$$

따라서 $\lambda(mn)=\lambda(m)\lambda(n)$ 이 성립한다. 그러므로 λ는 승법 함수이다. ■

(b). (a)의 결과와 Theorem 5.1.3에 의하면 소수 p와 자연수 k에 대하여 $n=p^k$ 일때만 조사하면 충분하다. $n=p^k$ 이면 다음을 얻을수 있다.

$$\begin{aligned}\sum_{d\mid p^k}\lambda(d) &= \lambda(1)+\lambda(p)+\lambda(p^2)+\cdots+\lambda(p^k)\\ &= 1+(-1)+(-1)^2+\cdots+(-1)^k\\ &= \frac{1-(-1)^{k+1}}{1-(-1)}\\ &= \frac{1+(-1)^k}{2}\end{aligned}$$

따라서 k가 짝수이면 $\sum_{d\mid p^k}\lambda(d)=1$ 이고 k가 홀수이면 $\sum_{d\mid p^k}\lambda(d)=0$ 이다.

그러므로 $\sum_{d\mid n}\lambda(d)=\begin{cases}1 & (n\text{은 완전제곱수})\\ 0 & (\text{otherwise})\end{cases}$ 임을 쉽게 알수 있다. ■

Problem 5.1.7 산술 함수 f,g가 임의로 주어져있다고 할 때 다음을 증명하시오.

(a). 모든 자연수 n에 대하여 $\sum_{d\mid n}f(d)=\sum_{d\mid n}g(d)$ 이면 $f(n)=g(n)$ 이다.

(b). 모든 자연수 n에 대하여 $\prod_{d\mid n}f(d)=\prod_{d\mid n}g(d)\neq 0$ 이면 $f(n)=g(n)$ 이다.

(증명)

강한 귀납법을 사용하면 쉽게 증명할수 있다. 집합 S 를 $S=\{n\in\mathbb{N}:f(n)=g(n)\}$ 라고 정의하자.

(a). 조건에 의하면 $\sum_{d\mid 1}f(d)=\sum_{d\mid 1}g(d)$ 이므로 $f(1)=g(1)$ 이다. 따라서 $1\in S$ 이다.

임의의 자연수 n에 대하여 $1,2,\ldots,n\in S$ 라고 가정하자. 그러면 조건에 의해 $\sum_{d\mid n+1}f(d)=\sum_{d\mid n+1}g(d)$ 이고 $n+1$의 양의 약수들 중 $n+1$이 아닌 것은 모두 n 이하이므로 가정에 의하면 $f(n+1)=g(n+1)$ 이 성립해야 한다.

따라서 $n+1\in S$ 이다. 그러므로 강한 귀납법에 의하면 $S=\mathbb{N}$ 이고 이것은 모든 자연수 n에 대하여 $f(n)=g(n)$ 임을 의미한다. ■

(b). 조건에 의하면 모든 자연수 n에 대하여 $f(n)\neq 0, g(n)\neq 0$ 임을 쉽게 알수 있다. $\prod_{d\mid 1}f(d)=\prod_{d\mid 1}g(d)$ 이므로 $f(1)=g(1)$ 이다. 따라서 $1\in S$ 이다.

임의의 자연수 n에 대하여 $1,2,\ldots,n\in S$ 라고 가정하자. 그러면 조건에 의해 $\prod_{d\mid n+1}f(d)=\prod_{d\mid n+1}g(d)$ 이고 $n+1$의 양의 약수들 중 $n+1$이 아닌 것은 모두 n 이하이다. 그리고 f,g는 0이 아니므로 가정에 의하면 $f(n+1)=g(n+1)$ 이다.

따라서 $n+1 \in S$ 이다. 그러므로 강한 귀납법에 의하면 $S=\mathbb{N}$ 이고 이것은 모든 자연수 n에 대하여 $f(n)=g(n)$ 임을 의미한다. ■

Problem 5.1.8 f가 승법 함수일 때 산술 함수 F를 다음과 같이 정의하자.

$$F(n)=\prod_{d \mid n} f(d)$$

그러면 $\gcd(m,n)=1$ 을 만족하는 모든 자연수 m, n에 대하여
다음 등식이 성립함을 증명하시오.

$$F(mn)=(F(m))^{\tau(n)}(F(n))^{\tau(m)}$$

(증명)
Lemma 5.1.2에 의하면 다음 등식이 성립한다.

$$\begin{aligned} F(mn) &= \prod_{d \mid mn} f(d) \\ &= \prod_{d_1 \mid m,\, d_2 \mid n} f(d_1 d_2) \\ &= \prod_{d_1 \mid m,\, d_2 \mid n} f(d_1) f(d_2) \end{aligned}$$

이제 간단한 등식을 살펴보자. 수열 $\{a_n\}, \{b_n\}$에 대하여

$$\prod_{\substack{1 \le i \le m \\ 1 \le j \le n}} a_i b_j = a_1^n \left(\prod_{j=1}^{n} b_j\right) a_2^n \left(\prod_{j=1}^{n} b_j\right) \cdots a_m^n \left(\prod_{j=1}^{n} b_j\right) = \left(\prod_{i=1}^{m} a_i\right)^n \left(\prod_{j=1}^{n} b_j\right)^m$$

가 성립한다는 것을 쉽게 알수 있고 이것을 이용하면 다음을 얻을수 있다.

$$\begin{aligned} F(mn) &= \prod_{d_1 \mid m,\, d_2 \mid n} f(d_1) f(d_2) \\ &= \left(\prod_{d_1 \mid m} f(d_1)\right)^{\tau(n)} \left(\prod_{d_2 \mid n} f(d_2)\right)^{\tau(m)} \\ &= (F(m))^{\tau(n)} (F(n))^{\tau(m)} \end{aligned}$$

■

Problem 5.1.8을 일반화하면 다음 명제를 얻습니다. $m_1, m_2, \ldots, m_n$이 $i \neq j$ 일 때 $\gcd(m_i, m_j)=1$ 을 만족하는 자연수이면

$$\begin{aligned} &F(m_1 m_2 \cdots m_n) \\ &= (F(m_1))^{\tau(m_2)\tau(m_3)\cdots\tau(m_n)} (F(m_2))^{\tau(m_1)\tau(m_3)\cdots\tau(m_n)} \cdots (F(m_n))^{\tau(m_1)\tau(m_2)\cdots\tau(m_{n-1})} \end{aligned}$$

가 성립합니다. 이것은 수학적 귀납법을 사용해서 증명할수 있습니다.

Problem 5.1.9 f, g가 승법 함수일 때 산술 함수 F를 다음과 같이 정의하자.

$$F(n)=\sum_{d \mid n} f(d) g\left(\frac{n}{d}\right)=\sum_{d \mid n} f\left(\frac{n}{d}\right) g(d)$$

그러면 F도 승법 함수임을 증명하시오.

(증명)

$\gcd(m,n)=1$ 을 만족하는 자연수 m,n을 임의로 택하고 $F(mn)=F(m)F(n)$ 임을 보이자. $d_1 \mid m, d_2 \mid n, \gcd(d_1,d_2)=1$ 이면 $\gcd\left(\frac{m}{d_1},\frac{n}{d_2}\right)=1$ 임을 최대공약수의 정의와 $\gcd(m,n)=1$ 조건을 이용해서 쉽게 보일수 있다. 따라서 Lemma 5.1.2와 Lemma 5.1.3에 의하면 다음 등식이 성립한다.

$$\begin{aligned}
F(mn) &= \sum_{d \mid mn} f(d)g\left(\frac{mn}{d}\right) \\
&= \sum_{d_1 \mid m,\, d_2 \mid n} f(d_1d_2)g\left(\frac{mn}{d_1d_2}\right) \\
&= \sum_{d_1 \mid m,\, d_2 \mid n} f(d_1)f(d_2)g\left(\frac{m}{d_1}\right)g\left(\frac{n}{d_2}\right) \\
&= \left(\sum_{d_1 \mid m} f(d_1)g\left(\frac{m}{d_1}\right)\right)\left(\sum_{d_2 \mid n} f(d_2)g\left(\frac{n}{d_2}\right)\right) \\
&= F(m)F(n)
\end{aligned}$$

그러므로 F는 승법 함수이다. ■

Problem 5.1.10 두 자연수 n, N에 대하여 다음을 증명하시오.

(a). $\sum_{d \mid n}(\tau(d))^3 = \left(\sum_{d \mid n}\tau(d)\right)^2$ 이다.

(b). $\sum_{d \mid n}\sigma(d)=\sum_{d \mid n}\frac{n}{d}\tau(d)$ 이다.

(c). $\sum_{d \mid n}\frac{n}{d}\sigma(d)=\sum_{d \mid n}d\tau(d)$ 이다.

(d). $\sum_{d \mid n}(-1)^{\frac{n}{d}}\phi(d)=\begin{cases}0 & (n\text{은 짝수}) \\ -n & (n\text{은 홀수})\end{cases}$ 이다.

(e). $\sum_{d \mid n}\sigma(d)\phi\left(\frac{n}{d}\right)=n\tau(n)$ 이다.

(f). $\sum_{d \mid n}\tau(d)\phi\left(\frac{n}{d}\right)=\sigma(n)$ 이다.

(g). $\lambda(n)$은 리우빌 함수일 때 $\sum_{n=1}^{N}\lambda(n)\left\lfloor\frac{N}{n}\right\rfloor = \lfloor\sqrt{N}\rfloor$ 이다.

(h). $\sum_{n=1}^{2N}\tau(n)-\sum_{n=1}^{N}\left\lfloor\frac{2N}{n}\right\rfloor = N$ 이다.

(증명)

(a),(b),(c),(e),(f)에 있는 함수는 Theorem 5.1.3과 Problem 5.1.9에 의해 모두 승법 함수임을 알수 있고 $n=1$ 일 때 등식이 성립함은 명백하다. 따라서 (a),(b),(c),(e),(f) 5개의 문제를 풀땐 소수 p와 자연수 k에 대하여 $n=p^k$ 일 때 등식이 성립함을 보이면 충분하다.

(a). $n=p^k$ 이면 좌변과 우변은 다음과 같이 계산된다.

$$\sum_{d\,|\,p^k}(\tau(n))^3=1^3+2^3+3^3+\cdots+(k+1)^3=\frac{(k+1)^2(k+2)^2}{4}$$

$$\left(\sum_{d\,|\,p^k}\tau(n)\right)^2=(1+2+3+\cdots+(k+1))^2=\frac{(k+1)^2(k+2)^2}{4}$$

따라서 $n=p^k$ 일 때 등식이 성립하므로 $\sum_{d\,|\,n}(\tau(d))^3=\left(\sum_{d\,|\,n}\tau(d)\right)^2$ 이다. ■

(b). $n=p^k$ 이면 좌변과 우변은 다음과 같이 계산된다.

$$\sum_{d\,|\,p^k}\sigma(d)=1+(1+p)+\left(1+p+p^2\right)+\cdots+\left(1+p+p^2+\cdots+p^k\right)$$
$$=p^k+2p^{k-1}+3p^{k-2}+\cdots+kp+(k+1)$$

$$\sum_{d\,|\,p^k}\frac{p^k}{d}\tau(d)=p^k+2p^{k-1}+3p^{k-2}+\cdots+kp+(k+1)$$

따라서 $n=p^k$ 일 때 등식이 성립하므로 $\sum_{d\,|\,n}\sigma(d)=\sum_{d\,|\,n}\frac{n}{d}\tau(d)$ 이다. ■

(c). $n=p^k$ 이면 좌변과 우변은 다음과 같이 계산된다.

$$\sum_{d\,|\,p^k}\frac{p^k}{d}\sigma(d)=p^k+p^{k-1}(1+p)+p^{k-2}\left(1+p+p^2\right)+\cdots+\left(1+p+p^2+\cdots+p^k\right)$$
$$=kp^k+(k-1)p^{k-1}+\cdots+p+1$$

$$\sum_{d\,|\,p^k}d\tau(d)=1+p+2p^2+\cdots+(k-1)p^{k-1}+kp^k$$

따라서 $n=p^k$ 일 때 등식이 성립하므로 $\sum_{d\,|\,n}\frac{n}{d}\sigma(d)=\sum_{d\,|\,n}d\tau(d)$ 이다. ■

(d). case1) n은 홀수

이 경우 n의 양의 약수는 모두 홀수이므로 $\frac{n}{d}$은 홀수이다.

따라서 $\sum_{d\,|\,n}(-1)^{\frac{n}{d}}\phi(d)=-\sum_{d\,|\,n}\phi(d)=-n$ 이다.

case2) n은 짝수

이 경우 자연수 k와 홀수 N에 대하여 $n=2^kN$ 형태로 나타낼수 있다.

따라서 $\frac{n}{d}$가 짝수인 경우는 d의 소인수 2의 지수가 k 미만인 경우이고

$\frac{n}{d}$가 홀수인 경우는 d의 소인수 2의 지수가 k인 경우이다.

그러므로 다음 등식을 얻을수 있다.

$$\sum_{d\,|\,n}(-1)^{\frac{n}{d}}\phi(d)=\sum_{d\,|\,2^{k-1}N}\phi(d)-\sum_{d\,|\,2^kN,\,2^k\,|\,d}\phi(d)$$

여기서 $\sum_{d\,|\,2^{k-1}N}\phi(d)=2^{k-1}N$ 이다. 그리고 다음 등식도 성립한다.

$$\begin{aligned}\sum_{d\,|\,2^kN,\,2^k\,|\,d}\phi(d)&=\sum_{d\,|\,N}\phi\big(2^kd\big)\\&=\sum_{d\,|\,N}\phi\big(2^k\big)\phi(d)\ (\because\ d\,|\,N\text{ 이면 }d\text{는 홀수})\\&=2^{k-1}\sum_{d\,|\,N}\phi(d)\\&=2^{k-1}N\end{aligned}$$

따라서 $\sum_{d\,|\,n}(-1)^{\frac{n}{d}}\phi(d)=\sum_{d\,|\,2^{k-1}N}\phi(d)-\sum_{d\,|\,2^kN,\,2^k\,|\,d}\phi(d)=0$ 이다.

그러므로 $\sum_{d\,|\,n}(-1)^{\frac{n}{d}}\phi(d)=\begin{cases}0 & (n\text{은 짝수})\\ -n & (n\text{은 홀수})\end{cases}$ 이다. ■

(e). $n=p^k$ 이면 좌변은 다음과 같이 계산된다.

$$\begin{aligned}&\sum_{d\,|\,p^k}\sigma(d)\phi\left(\frac{p^k}{d}\right)\\&=p^{k-1}(p-1)+(1+p)p^{k-2}(p-1)+\big(1+p+p^2\big)p^{k-3}(p-1)+\cdots\\&+\big(1+p+p^2+\cdots+p^{k-1}\big)(p-1)+\big(1+p+p^2+\cdots+p^k\big)\\&=p^{k-1}(p-1)+p^{k-2}\big(p^2-1\big)+p^{k-3}\big(p^3-1\big)+\cdots+\big(p^k-1\big)\\&+\big(1+p+p^2+\cdots+p^k\big)\\&=kp^k-\big(p^{k-1}+p^{k-2}+p^{k-3}+\cdots+1\big)+\big(1+p+p^2+\cdots+p^k\big)\\&=(k+1)p^k\\&=p^k\tau\big(p^k\big)\end{aligned}$$

따라서 $n=p^k$ 일 때 등식이 성립하므로 $\sum_{d\,|\,n}\sigma(d)\phi\left(\frac{n}{d}\right)=n\tau(n)$ 이다. ■

(f). $n=p^k$ 이면 좌변은 다음과 같이 계산된다.

$$\begin{aligned}&\sum_{d\,|\,p^k}\tau(d)\phi\left(\frac{p^k}{d}\right)\\&=p^{k-1}(p-1)+2p^{k-2}(p-1)+3p^{k-3}(p-1)+\cdots+k(p-1)+(k+1)\\&=p^k+p^{k-1}+p^{k-2}+\cdots+p+1\\&=\sigma\big(p^k\big)\end{aligned}$$

따라서 $n=p^k$ 일 때 등식이 성립하므로 $\sum_{d\,|\,n}\tau(d)\phi\left(\frac{n}{d}\right)=\sigma(n)$ 이다. ■

(g). Problem 5.1.6 (b)에 의하면 $\sum_{d\mid n}\lambda(d)=\begin{cases}1 & (n\text{은 완전제곱수})\\ 0 & (\text{otherwise})\end{cases}$ 이다.

따라서 Theorem 5.1.4에 의하면 $\sum_{n=1}^{N}\lambda(n)\left\lfloor \frac{N}{n}\right\rfloor$ 은 N보다 작거나 같은 완전제곱수의 개수이다.

자연수 x가 $x^2\le N$ 을 만족하면 $1\le x\le\sqrt{N}$ 이고 이것을 만족하는 자연수 x의 개수는 $\lfloor\sqrt{N}\rfloor$ 이다. 따라서 $\sum_{n=1}^{N}\lambda(n)\left\lfloor \frac{N}{n}\right\rfloor=\lfloor\sqrt{N}\rfloor$ 가 성립한다. ■

(h). Theorem 5.1.4에서 다음 등식을 얻을수 있다.

$$\begin{aligned}\sum_{n=1}^{2N}\tau(n)&=\sum_{n=1}^{2N}\left\lfloor\frac{2N}{n}\right\rfloor\\&=\sum_{n=1}^{N}\left\lfloor\frac{2N}{n}\right\rfloor+\sum_{n=N+1}^{2N}\left\lfloor\frac{2N}{n}\right\rfloor\\&=\sum_{n=1}^{N}\left\lfloor\frac{2N}{n}\right\rfloor+\sum_{n=1}^{N}\left\lfloor\frac{2N}{N+n}\right\rfloor\end{aligned}$$

$1\le n\le N$ 이면 $1\le\frac{2N}{N+n}\le\frac{2N}{N+1}=1+\frac{N-1}{N+1}$ 이고 N이 자연수이므로 $0\le\frac{N-1}{N+1}<1$ 이다. 따라서 $\left\lfloor\frac{2N}{N+1}\right\rfloor=1$ 이므로 $\left\lfloor\frac{2N}{N+n}\right\rfloor=1$ 이다.

그러므로 $\sum_{n=1}^{2N}\tau(n)=\sum_{n=1}^{N}\left\lfloor\frac{2N}{n}\right\rfloor+\sum_{n=1}^{N}1=\sum_{n=1}^{N}\left\lfloor\frac{2N}{n}\right\rfloor+N$ 에서

$\sum_{n=1}^{2N}\tau(n)-\sum_{n=1}^{N}\left\lfloor\frac{2N}{n}\right\rfloor=N$ 을 얻을수 있다. ■

Problem 5.1.11 자연수 n에 대하여 다음을 증명하시오.

(a). $\tau(n^2)=n$ 이 성립할 필요충분조건은 $n=1,3$ 이다.

(b). $3\mid\sigma(3n+2)$ 이다.

(c). $4\mid\sigma(4n+3)$ 이다.

(증명)

(a). 수학적 귀납법을 이용하면 모든 자연수 n에 대하여 $3^n\ge 2n+1$ 가 성립하고 등호는 $n=1$ 일때만 성립한다는 것을 쉽게 증명할수 있다. 이것을 이용하자. (5)

$(\Rightarrow)$ 조건에 의하면 n은 홀수이다. $n=1$ 이면 명백하므로 $n\ge 3$ 을 가정하자.

그러면 n을 소인수분해한 결과가 $n=p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ 라고 했을 때 $p_1,p_2,...,p_r$ 은 서로 다른 홀수인 소수이므로 (5)에 의하면 모든 $i=1,2,...,r$ 에 대해 $p_i^{k_i}\ge 2k_i+1$ 이다.

$\tau(n^2)=(2k_1+1)(2k_2+1)\cdots(2k_r+1)$ 이므로 조건에 의하면 다음 등식이 성립한다.

$$(2k_1+1)(2k_2+1)\cdots(2k_r+1)=p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r} \tag{6}$$

만약 $r\geq 2$ 이면 $p_1,p_2,...,p_r$ 중에는 3보다 큰 소수가 존재하고 그런 소수를 p_j라고 하면 (5)에 의해 $p_j^{k_j}>2k_j+1$ 이다. 이것은 (6)에 모순이므로 $r=1$ 이어야 한다.

따라서 홀수인 소수 p와 자연수 k에 대하여 $2k+1=p^k$ 를 만족해야 하는데 (5)에 의하면 $p=3, k=1$ 이 되어야 한다. 그러므로 $n=3$ 이다.

$(\Leftarrow)$ 이 경우에는 직접 계산해보면 명백하므로 생략한다. ■

(b). n은 자연수이므로 $3n+2\geq 5$ 이다. 따라서 $3n+2$ 는 소인수분해가 가능하고 3의 배수가 아닌 $3k+r$ 형태의 소수는 $3k+1$ 또는 $3k+2$ 형태밖에 없으므로 $3n+2$ 형태를 갖는 자연수는 $3k+2$ 형태의 소인수를 홀수개 가져야 한다.

즉, $3n+2$ 의 소인수들 중에서 $p_1,p_2,...,p_r$ 을 $3k+1$ 형태의 소인수라고 하고 $q_1,q_2,...,q_s$ 를 $3k+2$ 형태의 소인수라고 할 때 $3n+2=p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}q_1^{j_1}q_2^{j_2}\cdots q_s^{j_s}$ 이면 $j_1+j_2+\cdots+j_s$ 는 홀수가 되어야 한다.

따라서 적당한 $i=1,2,...,s$ 에 대하여 j_i는 홀수이고 이때 다음 등식을 얻는다.

$$\sigma\left(q_i^{j_i}\right)=1+q_i+q_i^2+\cdots+q_i^{j_i}$$

그리고 $q_i\equiv -1 \pmod 3$ 이므로 다음을 얻을수 있다.

$$\begin{aligned}\sigma\left(q_i^{j_i}\right) &\equiv 1+(-1)+(-1)^2+\cdots+(-1)^{j_i}\\ &\equiv \frac{1-(-1)^{j_i+1}}{1-(-1)}\\ &\equiv 0 \pmod 3\end{aligned}$$

그러므로 $3\mid\sigma\left(q_i^{j_i}\right)$ 이고 σ는 승법 함수이므로 $3\mid\sigma(3n+2)$ 을 얻을수 있다. ■

(c). n은 자연수이므로 $4n+3\geq 7$ 이다. 따라서 $4n+3$ 은 소인수분해가 가능하고 $4k+r$ 형태의 홀수 소수는 $4k+1$ 또는 $4k+3$ 형태밖에 없으므로 $4n+3$ 형태를 갖는 자연수는 $4k+3$ 형태의 소인수를 홀수개 가져야 한다.

즉, $4n+3$ 의 소인수들 중에서 $p_1,p_2,...,p_r$ 을 $4k+1$ 형태의 소인수라고 하고 $q_1,q_2,...,q_s$ 를 $4k+3$ 형태의 소인수라고 할 때 $4n+3=p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}q_1^{j_1}q_2^{j_2}\cdots q_s^{j_s}$ 이면 $j_1+j_2+\cdots+j_s$ 는 홀수가 되어야 한다.

따라서 적당한 $i=1,2,...,s$ 에 대하여 j_i는 홀수이고 이때 다음 등식을 얻는다.

$$\sigma\left(q_i^{j_i}\right)=1+q_i+q_i^2+\cdots+q_i^{j_i}$$

그리고 $q_i \equiv -1 \pmod 4$ 이므로 다음을 얻을수 있다.

$$\begin{aligned}\sigma\left(q_i^{j_i}\right) &\equiv 1+(-1)+(-1)^2+\cdots+(-1)^{j_i} \\ &\equiv \frac{1-(-1)^{j_i+1}}{1-(-1)} \\ &\equiv 0 \pmod 4\end{aligned}$$

그러므로 $4 \mid \sigma\left(q_i^{j_i}\right)$ 이고 σ는 승법 함수이므로 $4 \mid \sigma(4n+3)$ 을 얻을수 있다. ■

5.2 뫼비우스 반전 공식

작성자 : 네냐플(Nenyaffle)

5.2절에서는 산술 함수 F, G가 주어져있을 때

$$F(n)=\sum_{d\mid n} f(d)$$
$$G(n)=\prod_{d\mid n} g(d)$$

를 만족하는 산술 함수 f, g가 특정 조건 하에서 유일하게 존재한다는 것을 소개하려고 합니다. 5.1절의 Problem 5.1.7에 의하면 $F(n)=\sum_{d\mid n} f(d)$를 만족하는 산술 함수 f가 존재할 경우 그것은 유일하고 $G(n)=\prod_{d\mid n} g(d)$를 만족하는 산술 함수 g가 존재할 경우 $G(n)\neq 0$ 이면 그것은 유일합니다. 따라서 존재성만 증명하면 충분합니다.

수열 $\{S_n\}$이 주어져있을 때 $S_n=\sum_{k=1}^{n} a_k$ 을 만족하는 수열 $\{a_n\}$은

$a_n=\begin{cases} S_n-S_{n-1} & (n\geq 2) \\ S_1 & (n=1) \end{cases}$ 으로 유일하게 존재한다는 것을 대학 입학 전에 배웠을테고

비슷한 방법으로 $S_n=\prod_{k=1}^{n} a_k$ 를 만족하는 수열 $\{a_n\}$은 $S_n\neq 0$ 일 때

$a_n=\begin{cases} \dfrac{S_n}{S_{n-1}} & (n\geq 2) \\ S_1 & (n=1) \end{cases}$ 으로 유일하게 존재한다는 것을 쉽게 증명할수 있습니다.

5.2절에서 소개하는 내용도 위와 비슷한겁니다.

Definition 5.2.1 뫼비우스 함수(Mobius Function)

자연수 n에 대하여 $\mu(n)$을 다음과 같이 정의하자.

$$\mu(n)=\begin{cases} 1 & (n=1) \\ 0 & (\text{적당한 소수 } p\text{가 존재해서 } p^2\mid n) \\ (-1)^r & (\text{서로 다른 소수 } p_1,p_2,\ldots,p_r \text{ 에 대하여 } n=p_1p_2\cdots p_r) \end{cases}$$

이때 산술 함수 μ를 **뫼비우스 함수(Mobius Function)**라고 정의한다.

예를 들면 $\mu(30)=\mu(2\times 3\times 5)=(-1)^3=-1$ 이고 $\mu(4)=\mu(2^2)=0$ 입니다. 그리고 n이 4의 배수이면 $2^2\mid n$ 이므로 $\mu(n)=0$ 을 만족합니다.

정의에 의하면 뫼비우스 함수는 n이 제곱인수가 없는 자연수일때만 0이 아닌 값을 갖습니다. 따라서 n의 양의 약수들 중 제곱인수가 없는 자연수의 개수는 $\sum_{d\mid n}|\mu(d)|$ 라고 나타낼수 있습니다.

Theorem 5.2.1 뫼비우스 함수 μ는 승법 함수이다.

(증명)

$\gcd(m,n)=1$ 을 만족하는 자연수 m,n을 임의로 택하고 $\mu(mn)=\mu(m)\mu(n)$ 임을 보이자. m,n 둘중 적어도 하나가 1이면 $\mu(mn)=\mu(m)\mu(n)$ 는 명백하다.
따라서 $m \geq 2, n \geq 2$ 를 가정하자.

만약 적당한 소수 p가 존재해서 $p^2 \mid m$ 또는 $p^2 \mid n$ 을 만족하면 $p^2 \mid mn$ 이므로 이 경우 $\mu(mn)=\mu(m)\mu(n)=0$ 이다. 그러므로 m,n이 제곱인수가 없는 합성수인 경우만 고려하면 충분하다.

제곱인수가 없는 서로소인 합성수 m,n을 소인수분해한 결과가 다음과 같이 나온다고 할 때

$$m = p_1 p_2 \cdots p_r$$
$$n = q_1 q_2 \cdots q_s$$

$\gcd(m,n)=1$ 이므로 $p_1,p_2,...,p_r,q_1,q_2,...,q_s$ 는 모두 서로 다른 소수가 되어야 하고 이때 $mn = p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s$ 이므로 다음을 얻는다.

$$\mu(m)=(-1)^r$$
$$\mu(n)=(-1)^s$$
$$\mu(mn)=(-1)^{r+s}$$

따라서 $\mu(mn)=\mu(m)\mu(n)$ 가 성립한다. 그러므로 μ는 승법 함수이다. ■

이제 5.2절의 목표인 뫼비우스 반전 공식을 소개하기 위해 필요한 보조정리 2개를 먼저 소개하겠습니다.

Lemma 5.2.1 자연수 n에 대하여 $\sum_{d \mid n} \mu(d) = \begin{cases} 1 & (n=1) \\ 0 & (n \geq 2) \end{cases}$ 이다.

(증명)

Theorem 5.2.1에 의하면 μ는 승법 함수이다. 따라서 $F(n)=\sum_{d \mid n} \mu(d)$ 라고 하면 F도 승법 함수이다. 그러므로 소수 p와 자연수 k에 대하여 $n=p^k$ 일때의 값을 구해보자.

$$F(p^k)=\sum_{d \mid p^k} \mu(d)=\mu(1)+\mu(p)+\mu(p^2)+\cdots+\mu(p^k)=0$$

이므로 $n \geq 2$ 이면 $F(n)=0$ 이다. 그리고 $F(1)=1$ 은 명백하므로 정리가 증명된다.
■

Lemma 5.2.2 자연수 n에 대하여 두 집합 S, T 를 다음과 같이 정의하자.

$$S=\left\{(c,d) \in \mathbb{N} \times \mathbb{N} : d \mid n \text{ 이고 } c \mid \frac{n}{d}\right\}$$
$$T=\left\{(c,d) \in \mathbb{N} \times \mathbb{N} : c \mid n \text{ 이고 } d \mid \frac{n}{c}\right\}$$

그러면 $S=T$ 이다.

(증명)

$(\subset)$ 임의의 $(c,d)\in S$ 를 택하자. 그러면 $d\mid n$ 이고 $c\mid \frac{n}{d}$ 이므로 적당한 자연수 u,v 가 존재해서 $n=du,\ \frac{n}{d}=cv$ 를 만족한다. 따라서 $n=du=dcv$ 에서 $cdv=n$ 이므로 $c\mid n$ 이고 $dv=\frac{n}{c}$ 이므로 $d\mid \frac{n}{c}$ 이다. 그러므로 $(c,d)\in T$ 이다.

$(\supset)$ 임의의 $(c,d)\in T$ 를 택하자. 그러면 $c\mid n$ 이고 $d\mid \frac{n}{c}$ 이므로 적당한 자연수 u,v 가 존재해서 $n=cu,\ \frac{n}{c}=dv$ 를 만족한다. 따라서 $n=cu=cdv$ 에서 $dcv=n$ 이므로 $d\mid n$ 이고 $cv=\frac{n}{d}$ 이므로 $c\mid \frac{n}{d}$ 이다. 그러므로 $(c,d)\in S$ 이다.

정리하면 $S=T$ 를 얻는다. ■

Theorem 5.2.2 뫼비우스 반전 공식(Mobius Inversion Formula)

산술 함수 f,g,F,G 에 대하여 다음이 성립한다.

(a). $F(n)=\sum_{d\mid n}f(d)$ 이면 $f(n)=\sum_{d\mid n}\mu(d)F\left(\frac{n}{d}\right)=\sum_{d\mid n}\mu\left(\frac{n}{d}\right)F(d)$ 이다.

(b). $G(n)=\prod_{d\mid n}g(d)\neq 0$ 이면 $g(n)=\prod_{d\mid n}\left(G\left(\frac{n}{d}\right)\right)^{\mu(d)}=\prod_{d\mid n}(G(d))^{\mu\left(\frac{n}{d}\right)}$ 이다.

(증명)

5.1절 Problem 5.1.7에 의하면 $F(n)=\sum_{d\mid n}f(d)$ 과 $G(n)=\prod_{d\mid n}g(d)\neq 0$ 을 만족하는 $f(n),g(n)$이 존재할 경우 그것은 유일하게 존재한다. 따라서 (a), (b)에서 주어진 $F(n),G(n)$의 식을 각각 $\sum_{d\mid n}\mu(d)F\left(\frac{n}{d}\right),\ \prod_{d\mid n}\left(g\left(\frac{n}{d}\right)\right)^{\mu(d)}$ 에 대입했을 때 $f(n),g(n)$ 이 나오는지 확인하면 충분하다.

(a). Lemma 5.2.1, Lemma 5.2.2에 의하면 다음을 얻는다.

$$\begin{aligned}\sum_{d\mid n}\mu(d)F\left(\frac{n}{d}\right)&=\sum_{d\mid n}\mu(d)\left(\sum_{c\mid \frac{n}{d}}f(c)\right)\\&=\sum_{d\mid n}\left(\sum_{c\mid \frac{n}{d}}\mu(d)f(c)\right)\\&=\sum_{c\mid n}\left(\sum_{d\mid \frac{n}{c}}\mu(d)f(c)\right)\\&=\sum_{c\mid n}f(c)\left(\sum_{d\mid \frac{n}{c}}\mu(d)\right)\\&=f(n)\end{aligned}$$

■

(b). 지수법칙과 Lemma 5.2.1, Lemma 5.2.2에 의하면 다음을 얻는다.

$$\begin{aligned}\prod_{d\,|\,n}\left(G\left(\frac{n}{d}\right)\right)^{\mu(d)} &= \prod_{d\,|\,n}\left(\prod_{c\,|\,\frac{n}{d}} g(c)\right)^{\mu(d)} \\ &= \prod_{d\,|\,n}\left(\prod_{c\,|\,\frac{n}{d}} (g(c))^{\mu(d)}\right) \\ &= \prod_{c\,|\,n}\left(\prod_{d\,|\,\frac{n}{c}} (g(c))^{\mu(d)}\right) \\ &= \prod_{c\,|\,n} (g(c))^{\sum_{d\,|\,\frac{n}{c}}\mu(d)} \\ &= g(n)\end{aligned}$$

■

$\tau(n)=\sum_{d\,|\,n}1$, $\sigma(n)=\sum_{d\,|\,n}d$ 이므로 뫼비우스 반전 공식에 의하면 다음을 얻습니다.

$$1=\sum_{d\,|\,n}\mu(d)\tau\left(\frac{n}{d}\right)=\sum_{d\,|\,n}\mu\left(\frac{n}{d}\right)\tau(d)$$
$$n=\sum_{d\,|\,n}\mu(d)\sigma\left(\frac{n}{d}\right)=\sum_{d\,|\,n}\mu\left(\frac{n}{d}\right)\sigma(d)$$

그리고 $\prod_{d\,|\,n}d=n^{\frac{\tau(n)}{2}}\neq 0$ 이므로 뫼비우스 반전 공식에 의하면 다음을 얻습니다.

$$n=\prod_{d\,|\,n}\left(\frac{n}{d}\right)^{\frac{\tau\left(\frac{n}{d}\right)\mu(d)}{2}}=\prod_{d\,|\,n}d^{\frac{\tau(d)\mu\left(\frac{n}{d}\right)}{2}}$$

$n=6$ 일 때 직접 계산해보면 실제로 성립한다는 것을 알수 있습니다.

$$\begin{aligned}\sum_{d\,|\,6}\mu(d)\tau\left(\frac{6}{d}\right) &= \mu(1)\tau(6)+\mu(2)\tau(3)+\mu(3)\tau(2)+\mu(6)\tau(1) \\ &= 4-2-2+1 \\ &= 1\end{aligned}$$

$$\begin{aligned}\sum_{d\,|\,6}\mu(d)\sigma\left(\frac{6}{d}\right) &= \mu(1)\sigma(6)+\mu(2)\sigma(3)+\mu(3)\sigma(2)+\mu(6)\sigma(1) \\ &= 12-4-3+1 \\ &= 6\end{aligned}$$

$$\begin{aligned}\prod_{d\,|\,6}\left(\frac{6}{d}\right)^{\frac{\tau\left(\frac{6}{d}\right)\mu(d)}{2}} &= 6^{\frac{\tau(6)\mu(1)}{2}}\times 3^{\frac{\tau(3)\mu(2)}{2}}\times 2^{\frac{\tau(2)\mu(3)}{2}}\times 1^{\frac{\tau(1)\mu(6)}{2}} \\ &= 6^2\times 3^{-1}\times 2^{-1}\times 1 \\ &= 6\end{aligned}$$

뫼비우스 반전 공식에 의하면 $F(n)=\sum_{d\mid n} f(d)$ 일 때 다음을 얻을수 있습니다.

$$f(n)=\sum_{d\mid n}\mu(d)F\left(\frac{n}{d}\right)=\sum_{d\mid n}\mu\left(\frac{n}{d}\right)F(d)$$

뫼비우스 함수는 승법 함수이므로 F가 승법 함수이면 5.1절의 Problem 5.1.9에 의해 f도 승법 함수가 됩니다.

수학자 프란츠 메르텐스(Franz Mertens)가 1897년에 뫼비우스 함수를 가지고 추측을 하나 제시했습니다. $M(n)=\sum_{k=1}^{n}\mu(k)$라고 할 때 모든 자연수 n에 대하여 $|M(n)|<\sqrt{n}$ 이 성립한다는 추측인데 이것은 1985년에 거짓임이 밝혀졌습니다.

반례를 직접 찾은 것은 아니고 $m(n)=\frac{M(n)}{\sqrt{n}}$ 이라고 할 때 다음을 보인겁니다.

$$\begin{aligned}\overline{\lim}\, m(n)&>1.06\\ \underline{\lim}\, m(n)&<-1.009\end{aligned}\tag{7}$$

여기서 $\overline{\lim}, \underline{\lim}$ 는 각각 해석학에 나오는 **상극한(Limit Superior)**과 **하극한(Limit Inferior)**을 나타내는 기호인데 상극한과 하극한이 무엇인지 설명하려면 해야할 말이 많기 때문에 자세한 설명은 생략하겠습니다. 상극한과 하극한에 대해 자세히 알고 싶으면 해석학 책을 찾아보길 바랍니다. 어떤 책을 봐도 나와있을겁니다.

결론만 말하자면 메르텐스 추측은 모든 자연수 n에 대하여 $|m(n)|<1$ 이 성립하는 것과 동치인데 $|m(n)|<1$ 이면 (7)에 모순입니다. 따라서 메르텐스 추측은 거짓입니다.

2016년에는 (7)의 부등식이 다음과 같이 발전되었습니다.

$$\begin{aligned}\overline{\lim}\, m(n)&>1.826054\\ \underline{\lim}\, m(n)&<-1.837625\end{aligned}$$

Problem 5.2.1 다음 물음에 답하시오.

(a). $\mu(n)+\mu(n+1)+\mu(n+2)=3$ 을 만족하는 자연수 n을 하나만 구하시오.

(b). 모든 자연수 n에 대하여 $\mu(n)\mu(n+1)\mu(n+2)\mu(n+3)=0$ 임을 증명하시오.

(c). $n\geq 3$ 이면 $\sum_{k=1}^{n}\mu(k!)=1$ 임을 증명하시오.

(d). 임의의 자연수 k에 대하여 다음을 만족하는 자연수 n이 존재함을 증명하시오.

$$\mu(n+1)=\mu(n+2)=\cdots=\mu(n+k)=0$$

(풀이)

(a). $n=33=3\times 11$ 이면 $n+1=34=2\times 17, n+2=35=5\times 7$ 이므로 $\mu(n)=\mu(n+1)=\mu(n+2)=1$ 을 만족한다. 따라서 $n=33$ 은 $\mu(n)+\mu(n+1)+\mu(n+2)=3$ 을 만족하는 하나의 자연수이다. ■

(b). 모든 자연수를 4로 나눈 나머지는 $0,1,2,3$ 이므로 $n, n+1, n+2, n+3$ 4개의 자연수 중 하나는 반드시 4의 배수가 되어야 한다. 그리고 4의 배수의 뫼비우스 함숫값은 0이므로 $\mu(n), \mu(n+1), \mu(n+2), \mu(n+3)$ 넷중 하나는 반드시 0이다.

그러므로 $\mu(n)\mu(n+1)\mu(n+2)\mu(n+3)=0$ 이 성립한다. ■

(c). $n=3$ 이면 $\sum_{k=1}^{3}\mu(k!)=\mu(1)+\mu(2)+\mu(6)=1$ 이다. 그리고 $k \geq 4$ 이면 $2^2 \mid k!$ 이므로 $n \geq 3$ 이면 $\sum_{k=1}^{n}\mu(k!)=1$ 임을 쉽게 알수 있다. ■

(d). 소수의 개수는 무한하므로 서로 다른 k개의 소수 $p_1, p_2, ..., p_k$ 는 항상 존재한다. 그리고 중국인의 나머지 정리에 의하면 다음 합동방정식의 해도 존재한다.

$$\begin{aligned} x &\equiv -1 \pmod{p_1^2} \\ x &\equiv -2 \pmod{p_2^2} \\ &\vdots \\ x &\equiv -k \pmod{p_k^2} \end{aligned} \tag{8}$$

따라서 (8)을 만족하는 자연수 n을 하나 택하면 각각의 $i=1,2,...,k$ 에 대하여 $p_i^2 \mid n+i$ 이므로 $\mu(n+1)=\mu(n+2)=\cdots=\mu(n+k)=0$ 을 만족한다.

그러므로 $\mu(n+1)=\mu(n+2)=\cdots=\mu(n+k)=0$ 을 만족하는 자연수 n은 항상 존재한다. ■

Problem 5.2.2 망골트 함수(Mangoldt Function)는 다음과 같이 정의되는 함수이다.

$$\Lambda(n)=\begin{cases}\ln p & (\text{소수 } p\text{와 자연수 } k\text{에 대하여 } n=p^k) \\ 0 & (\text{otherwise})\end{cases}$$

모든 자연수 n에 대하여 $\Lambda(n)=\sum_{d \mid n}\mu\left(\frac{n}{d}\right)\ln d=-\sum_{d \mid n}\mu(d)\ln d$ 임을 증명하시오.

(증명)

뫼비우스 반전 공식을 이용하기 위해 $\sum_{d \mid n}\Lambda(d)=\ln n$ 임을 보이자. $n=1$ 이면 명백하다.

$n \geq 2$ 일 때 n을 소인수분해한 결과가 $n=p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ 라고 하자. 망골트 함수는 소인수가 하나만 있는 자연수에서만 0이 아닌 값을 가지므로 다음 등식을 얻는다.

$$\begin{aligned} \sum_{d \mid n}\Lambda(n) &= \Lambda(p_1)+\cdots+\Lambda\left(p_1^{k_1}\right)+\Lambda(p_2)+\cdots+\Lambda\left(p_2^{k_2}\right)+\cdots+\Lambda(p_r)+\cdots+\Lambda\left(p_r^{k_r}\right) \\ &= k_1\ln p_1+k_2\ln p_2+\cdots+k_r\ln p_r \\ &= \ln\left(p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}\right) \\ &= \ln n \end{aligned}$$

따라서 뫼비우스 반전 공식과 Lemma 5.2.1에 의하면 주어진 등식이 성립한다. ■

Problem 5.2.3 다음을 주어진 식과 다른 형태로 표현하시오.

(a). $\sum_{d\mid n}\frac{(\mu(d))^2}{\tau(d)}$

(b). $\sum_{d\mid n}\frac{(\mu(d))^2}{\sigma(d)}$

(c). $\sum_{d\mid n}\frac{(\mu(d))^2}{\phi(d)}$

(d). f가 $f(1)=1$ 을 만족하는 승법 함수일 때 $\sum_{d\mid n}\mu(d)f(d)$

(e). $\sum_{d\mid n}\frac{\mu(d)}{d}$

(풀이)

문제에 주어진 함수는 모두 승법 함수이고 $n=1$ 일 때 1임은 명백하다. 따라서 소수 p와 자연수 k에 대하여 $n=p^k$ 일 때 어떤 값을 갖는지 조사하면 충분하다. 우선 $n\geq 2$ 라고 가정하고 n을 소인수분해한 결과를 $n=p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ 라고 하자.

(a). $\sum_{d\mid p^k}\frac{(\mu(d))^2}{\tau(d)}=\frac{(\mu(1))^2}{\tau(1)}+\frac{(\mu(p))^2}{\tau(p)}+\frac{(\mu(p^2))^2}{\tau(p^2)}+\cdots+\frac{(\mu(p^k))^2}{\tau(p^k)}=\frac{3}{2}$ 이므로

$n=p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ 이면 $\sum_{d\mid n}\frac{(\mu(d))^2}{\tau(d)}=\left(\frac{3}{2}\right)^r$ 이다. ■

(b). $\sum_{d\mid p^k}\frac{(\mu(d))^2}{\sigma(d)}=\frac{(\mu(1))^2}{\sigma(1)}+\frac{(\mu(p))^2}{\sigma(p)}+\frac{(\mu(p^2))^2}{\sigma(p^2)}+\cdots+\frac{(\mu(p^k))^2}{\sigma(p^k)}=\frac{p+2}{p+1}$

이므로 $\sum_{d\mid n}\frac{(\mu(d))^2}{\sigma(d)}=\left(\frac{p_1+2}{p_1+1}\right)\left(\frac{p_2+2}{p_2+1}\right)\cdots\left(\frac{p_r+2}{p_r+1}\right)$ 이다. ■

(c). $\sum_{d\mid p^k}\frac{(\mu(d))^2}{\phi(d)}=\frac{(\mu(1))^2}{\phi(1)}+\frac{(\mu(p))^2}{\phi(p)}+\frac{(\mu(p^2))^2}{\phi(p^2)}+\cdots+\frac{(\mu(p^k))^2}{\phi(p^k)}=\frac{p}{p-1}$

이므로 $\sum_{d\mid n}\frac{(\mu(d))^2}{\phi(d)}=\left(\frac{p_1}{p_1-1}\right)\left(\frac{p_2}{p_2-1}\right)\cdots\left(\frac{p_r}{p_r-1}\right)$ 이다. ■

(d). $n=p^k$ 이면 다음이 성립한다.

$$\sum_{d\mid p^k}\mu(d)f(d)=\mu(1)f(1)+\mu(p)f(p)+\mu(p^2)f(p^2)+\cdots+\mu(p^k)f(p^k)=1-f(p)$$

따라서 $\sum_{d\mid p^k}\mu(d)f(d)=(1-f(p_1))(1-f(p_2))\cdots(1-f(p_r))$ 이다. ■

(e). $\sum_{d\mid n}\phi(d)=n$ 이므로 뫼비우스 반전 공식에 의하면 $\sum_{d\mid n}\frac{n\mu(d)}{d}=\phi(n)$ 을 얻는다.

따라서 $\sum_{d\mid n}\frac{\mu(d)}{d}=\frac{\phi(n)}{n}$ 이다. ■

Problem 5.2.4 자연수 n에 대하여 다음을 증명하시오. 여기서 λ는 5.1절 Problem 5.1.6에서 정의한 리우빌 함수이고 ω는 5.1절 Problem 5.1.4에서 정의한 함수이다.

(a). $\sum_{d\mid n}\mu(d)\lambda(d)=2^{\omega(n)}$ 이다.

(b). $\sum_{d\mid n}\lambda\left(\frac{n}{d}\right)2^{\omega(d)}=1$ 이다.

(c). $\sum_{d\mid n}|\mu(d)|=2^{\omega(n)}$ 이다.

(증명)

문제에 주어진 함수는 모두 승법 함수이고 $n=1$ 일 때 등식이 성립함은 명백하다. 따라서 소수 p와 자연수 k에 대하여 $n=p^k$ 일 때 어떤 값을 갖는지 조사하면 충분하다.

(a). $\sum_{d\mid p^k}\mu(d)\lambda(d)=1-\lambda(p)=2$ 이므로 $\omega(n)$의 정의에 의하면

$\sum_{d\mid n}\mu(d)\lambda(d)=2^{\omega(n)}$ 가 성립한다. ■

(b). $n=p^k$ 이면 다음을 얻는다.

$$\begin{aligned}\sum_{d\mid p^k}\lambda\left(\frac{p^k}{d}\right)2^{\omega(d)}&=\lambda(p^k)2^{\omega(1)}+\lambda(p^{k-1})2^{\omega(p)}+\cdots+\lambda(1)2^{\omega(p^k)}\\&=(-1)^k+2\times\left((-1)^{k-1}+(-1)^{k-2}+\cdots+1\right)\\&=(-1)^k+2\times\frac{1-(-1)^k}{1-(-1)}\\&=1\end{aligned}$$

따라서 $\sum_{d\mid n}\lambda\left(\frac{n}{d}\right)2^{\omega(d)}=1$ 이다. ■

(c). $\sum_{d\mid p^k}|\mu(d)|=|\mu(1)|+|\mu(p)|=2$ 이므로 $\omega(n)$의 정의에 의하면

$\sum_{d\mid n}|\mu(d)|=2^{\omega(n)}$ 가 성립한다. ■

Problem 5.2.5 자연수 N에 대하여 다음을 증명하시오.

(a). $\sum_{n=1}^{N}\mu(n)\left\lfloor \frac{N}{n}\right\rfloor =1$ 이다.

(b). $\left|\sum_{n=1}^{N}\frac{\mu(n)}{n}\right|\le 1$ 이다.

(증명)

(a). $F(n)=\begin{cases}1 & (n=1)\\ 0 & (n\ge 2)\end{cases}$ 라고 하면 $\sum_{d\mid n}\mu(d)=F(n)$ 이므로 다음을 얻는다.

$$1=\sum_{n=1}^{N}F(n)=\sum_{n=1}^{N}\mu(n)\left\lfloor \frac{N}{n}\right\rfloor$$

■

(b). 우선 다음 등식이 성립함은 명백하다.

$$\sum_{n=1}^{N}\frac{\mu(n)}{n}=\sum_{\mu(n)>0}\frac{\mu(n)}{n}+\sum_{\mu(n)<0}\frac{\mu(n)}{n} \tag{9}$$

(9)에서 $\sum_{\mu(n)>0}\frac{\mu(n)}{n}$은 $1\le n\le N$ 을 만족하는 자연수 n 중에서 $\mu(n)>0$ 을 만족하는 자연수 n을 대입한 값을 모두 더했다는 기호이고 $\sum_{\mu(n)<0}\frac{\mu(n)}{n}$ 은 $\mu(n)<0$ 을 만족하는 자연수 n을 대입한 값을 모두 더했다는 기호이다. $\mu(n)>0$ 또는 $\mu(n)<0$ 을 만족하는 n이 존재하지 않으면 (9)의 우변에 있는 둘중 하나의 기호는 0으로 정의한다.

모든 실수 x에 대하여 $\lfloor x\rfloor \le x<1+\lfloor x\rfloor$ 가 성립하므로 다음을 얻을수 있다.

$$\begin{aligned}\sum_{\mu(n)>0}\frac{\mu(n)}{n}&=\frac{1}{N}\sum_{\mu(n)>0}\frac{N\mu(n)}{n}<\frac{1}{N}\sum_{\mu(n)>0}\mu(n)\left(1+\left\lfloor \frac{N}{n}\right\rfloor\right)\\ \sum_{\mu(n)>0}\frac{\mu(n)}{n}&=\frac{1}{N}\sum_{\mu(n)>0}\frac{N\mu(n)}{n}\ge\frac{1}{N}\sum_{\mu(n)>0}\mu(n)\left\lfloor \frac{N}{n}\right\rfloor\end{aligned} \tag{10}$$

$$\therefore\ \frac{1}{N}\sum_{\mu(n)>0}\mu(n)\left\lfloor \frac{N}{n}\right\rfloor\le\sum_{\mu(n)>0}\frac{\mu(n)}{n}<\frac{1}{N}\sum_{\mu(n)>0}\mu(n)\left(1+\left\lfloor \frac{N}{n}\right\rfloor\right)$$

$$\begin{aligned}\sum_{\mu(n)<0}\frac{\mu(n)}{n}&=\frac{1}{N}\sum_{\mu(n)<0}\frac{N\mu(n)}{n}\le\frac{1}{N}\sum_{\mu(n)<0}\mu(n)\left\lfloor \frac{N}{n}\right\rfloor\\ \sum_{\mu(n)<0}\frac{\mu(n)}{n}&=\frac{1}{N}\sum_{\mu(n)<0}\frac{N\mu(n)}{n}>\frac{1}{N}\sum_{\mu(n)<0}\mu(n)\left(1+\left\lfloor \frac{N}{n}\right\rfloor\right)\end{aligned} \tag{11}$$

$$\therefore\ \frac{1}{N}\sum_{\mu(n)<0}\mu(n)\left(1+\left\lfloor \frac{N}{n}\right\rfloor\right)<\sum_{\mu(n)<0}\frac{\mu(n)}{n}\le\frac{1}{N}\sum_{\mu(n)<0}\mu(n)\left\lfloor \frac{N}{n}\right\rfloor$$

따라서 (10), (11)의 부등식의 양변을 모두 더하면 (a)에 의해 다음을 얻을수 있다.

$$\begin{aligned}
\text{좌변} &= \frac{1}{N}\left(\sum_{\mu(n)<0}\mu(n)+\sum_{\mu(n)>0}\mu(n)\left\lfloor\frac{N}{n}\right\rfloor+\sum_{\mu(n)<0}\mu(n)\left\lfloor\frac{N}{n}\right\rfloor\right)\\
&= \frac{1}{N}\left(\sum_{\mu(n)<0}\mu(n)+\sum_{n=1}^{N}\mu(n)\left\lfloor\frac{N}{n}\right\rfloor\right)\\
&= \frac{1}{N}\left(1+\sum_{\mu(n)<0}\mu(n)\right)\\
&= \frac{1}{N}\left(1-\sum_{\mu(n)<0}1\right)
\end{aligned}$$

$$\begin{aligned}
\text{우변} &= \frac{1}{N}\left(\sum_{\mu(n)>0}\mu(n)+\sum_{\mu(n)>0}\mu(n)\left\lfloor\frac{N}{n}\right\rfloor+\sum_{\mu(n)<0}\mu(n)\left\lfloor\frac{N}{n}\right\rfloor\right)\\
&= \frac{1}{N}\left(\sum_{\mu(n)>0}\mu(n)+\sum_{n=1}^{N}\mu(n)\left\lfloor\frac{N}{n}\right\rfloor\right)\\
&= \frac{1}{N}\left(1+\sum_{\mu(n)>0}\mu(n)\right)\\
&= \frac{1}{N}\left(1+\sum_{\mu(n)>0}1\right)
\end{aligned}$$

$$\therefore\ \frac{1}{N}\left(1-\sum_{\mu(n)<0}1\right)<\sum_{n=1}^{N}\frac{\mu(n)}{n}<\frac{1}{N}\left(1+\sum_{\mu(n)>0}1\right)$$

이제 $\left|\sum_{n=1}^{N}\frac{\mu(n)}{n}\right|\le 1$ 임을 보이자. $-1\le\sum_{n=1}^{N}\frac{\mu(n)}{n}\le 1$ 임을 보이면 충분하다.

$N=1,2$ 이면 명백하므로 $N\ge 3$ 을 가정하자. 그러면 $\mu(2)=\mu(3)=-1$ 이므로 1부터 N까지의 자연수 중에서 $\mu(n)>0$ 을 만족하는 자연수 n은 $N-2$개 이하이다. 따라서 $\sum_{\mu(n)>0}1\le N-2$ 이므로 $\frac{1}{N}\left(1+\sum_{\mu(n)>0}1\right)\le\frac{N-1}{N}<1$ 을 얻는다.

마찬가지로 $\mu(1)=1$ 이므로 1부터 N까지의 자연수 중에서 $\mu(n)<0$ 을 만족하는 자연수 n은 $N-1$개 이하이다. 따라서 $\sum_{\mu(n)<0}1\le N-1$ 이므로

$\frac{1}{N}\left(1-\sum_{\mu(n)<0}1\right)\ge\frac{2-N}{N}>-1$ 을 얻는다.

그러므로 $N\ge 3$ 이면 $-1<\sum_{n=1}^{N}\frac{\mu(n)}{n}<1$ 이다. 따라서 모든 자연수 N에 대하여 $-1\le\sum_{n=1}^{N}\frac{\mu(n)}{n}\le 1$ 이므로 $\left|\sum_{n=1}^{N}\frac{\mu(n)}{n}\right|\le 1$ 을 얻는다. ■

다음 문제는 복소수를 어느정도 알고 있어야 풀수 있습니다. 따라서 복소수를 잘 모르면 다음 문제는 풀지 않아도 무방합니다.

Problem 5.2.6 실수 x와 $i=\sqrt{-1}$ 에 대하여 다음 등식이 성립한다는 것이 알려져 있다.

$$e^{ix}=\cos x+i\sin x \tag{12}$$

이때 (12)를 **오일러의 공식(Euler's Formula)**이라고 부른다. 오일러의 공식을 이용하면 자연수 n에 대하여 방정식 $x^n=1$ 의 해집합 S 를 다음과 같이 나타낼수 있다.

$$S=\left\{e^{\frac{2k\pi i}{n}}\in\mathbb{C}:k=1,2,...,n\right\}$$

그러면 모든 $\omega\in S$ 는 $\omega^n=1$ 을 만족하므로 정렬원리에 의하면 $\omega^m=1$ 을 만족하는 가장 작은 자연수 m이 존재하고 그것을 ω의 **위수(Order)**라고 정의한다. 그리고 위수가 n인 $\omega\in S$ 를 방정식 $x^n=1$ 의 **원시근(Primitive Root)**이라고 정의한다.

다음 물음에 답하시오.

(a). 집합 S 는 곱셈에 대해 닫혀있음을 증명하시오.

집합 S 는 곱셈에 대해 닫혀있고 $1\in S$ 이므로 S 는 곱셈에 대한 항등원이 존재한다. 그리고 모든 $\omega\in S$ 에 대하여 $\omega\times\omega^{n-1}=1$ 이므로 ω의 곱셈에 대한 역원이 $\omega^{-1}=\omega^{n-1}$ 로 존재한다. 그러므로 S 는 **곱셈군(Multiplicative Group)**이 된다.

(b). $\omega\in S$ 의 위수는 n의 양의 약수임을 증명하시오.

(c). $\omega\in S$ 의 위수가 m이면 ω^k의 위수는 $\dfrac{m}{\gcd(m,k)}$ 임을 증명하시오.

(d). 방정식 $x^n=1$ 의 원시근은 항상 존재하고 그 개수는 $\phi(n)$임을 증명하시오.

(e). 방정식 $x^n=1$ 의 원시근을 근으로 갖는 최고차항의 계수가 1인 $\phi(n)$차 다항식을 기호로 $\Phi_n(x)$라고 나타내고 이것을 **원분다항식(Cyclotomic Polynomial)**이라고 정의한다. 다음 등식이 성립함을 증명하시오.

$$\Phi_n(x)=\prod_{d\mid n}\left(x^{\frac{n}{d}}-1\right)^{\mu(d)}=\prod_{d\mid n}\left(x^d-1\right)^{\mu\left(\frac{n}{d}\right)}$$

(증명)

(a). 임의의 $a,b\in S$ 를 택하자. 그러면 $a^n=b^n=1$ 이므로 지수법칙에 의하면 $(ab)^n=a^nb^n=1$ 이다. 따라서 $ab\in S$ 이므로 S 는 곱셈에 대해 닫혀있다. ■

(b). $\omega \in S$ 의 위수를 m이라고 하자. 그리고 n을 m으로 나눈 몫을 q, 나머지를 r이라고 하면 $n = mq + r\ (0 \le r < m)$ 을 만족하고 이때 $1 = \omega^n = (\omega^m)^q \omega^r = \omega^r$ 을 얻는다.

만약 $r \neq 0$ 이면 $0 < r < m$ 이고 $\omega^r = 1$ 이므로 이것은 ω의 위수가 m이라는 조건에 모순이다. 따라서 $r = 0$ 이고 $n = mq$ 이므로 $m \mid n$ 이다. 즉, m은 n의 양의 약수이다. ■

(c). $d = \gcd(m,k)$ 라고 하고 ω^k의 위수를 r이라고 하자. 그러면 $\omega^{kr} = 1$ 이므로 (a)에 의하면 $m \mid kr$ 를 얻는다. 따라서 $\frac{m}{d} \mid \frac{k}{d} \times r$ 이고 $\gcd\left(\frac{m}{d}, \frac{k}{d}\right) = 1$ 이므로 $\frac{m}{d} \mid r$ 에서 $\frac{m}{d} \le r$ 을 얻는다.

그리고 ω의 위수는 m이고 $\frac{k}{d}$는 자연수이므로 $(\omega^k)^{\frac{m}{d}} = 1$ 이고 ω^k의 위수는 r이므로 $r \mid \frac{m}{d}$ 에서 $r \le \frac{m}{d}$ 을 얻을수 있다. 그러므로 $r = \frac{m}{d}$ 이다. 즉, ω^k의 위수는 $\frac{m}{d} = \frac{m}{\gcd(m,k)}$ 이다. ■

(d). $\xi_n = e^{\frac{2\pi i}{n}} = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)$ 라고 하고 ξ_n의 위수가 n임을 보이자.

자연수 m에 대하여 ξ_n의 위수를 m이라고 하자. 그러면 $\xi_n^m = 1$ 이고 (a)에 의하면 $m \mid n$ 이므로 $m \le n$ 이다.

$\xi_n^m = \cos\left(\frac{2m\pi}{n}\right) + i\sin\left(\frac{2m\pi}{n}\right) = 1$ 에서 $\cos\left(\frac{2m\pi}{n}\right) = 1,\ \sin\left(\frac{2m\pi}{n}\right) = 0$ 을 얻는다. 따라서 적당한 정수 k가 존재해서 $\frac{2m\pi}{n} = 2k\pi$ 를 만족하므로 $m = nk$ 에서 $n \mid m$ 을 얻는다. 즉, $n \le m$ 이다.

따라서 $m = n$ 이므로 ξ_n은 $x^n = 1$ 의 원시근이고 이때 집합 S 는 $S = \{\xi_n, \xi_n^2, \xi_n^3, ..., \xi_n^n\}$ 로 나타낼수 있음은 명백하다. 그러므로 $1 \le r \le n$ 을 만족하는 자연수 r에 대하여 ξ_n^r의 위수가 n이 되도록 하는 r만 찾으면 원시근을 모두 찾을수 있다.

ξ_n^r의 위수는 (c)에 의하면 $\frac{n}{\gcd(n,r)}$ 이므로 ξ_n^r가 방정식 $x^n = 1$ 의 원시근이 될 필요충분조건은 $\gcd(n,r) = 1$ 인 것이다. $\gcd(n,r) = 1$ 을 만족하는 $1 \le r \le n$ 인 자연수 r의 개수는 $\phi(n)$이므로 원시근은 $\phi(n)$개 있다. ■

(e). 뫼비우스 반전 공식을 이용하기 위해 $x^n-1=\prod_{d\mid n}\Phi_d(x)$임을 증명하면 충분하다.

$f(x)=\prod_{d\mid n}\Phi_d(x)$라고 하자. 그러면 $\deg(f(x))=\sum_{d\mid n}\phi(d)=n$ 이므로 $f(x)$는 최고차항의 계수가 1인 n차 다항식이다. 따라서 $T=\{x\in\mathbb{C}:f(x)=0\}$ 라고 할 때 $S=T$ 이면 대수학의 기본정리에 의해 $f(x)=x^n-1$ 가 증명된다. $S=T$ 임을 보이자.

$(\subset)$ ξ_n은 $x^n=1$ 의 원시근이므로 집합 S 의 임의의 원소는 $1\le r\le n$ 을 만족하는 자연수 r에 대하여 ξ_n^r로 나타낼수 있다. 그리고 ξ_n^r의 위수는 $\frac{n}{\gcd(n,r)}$ 이다.

$d=\frac{n}{\gcd(n,r)}$ 라고 하면 $d\mid n$ 이고 ξ_n^r의 위수는 d이므로 ξ_n^r은 $x^d=1$ 의 원시근이다. 그러므로 원분다항식의 정의에 의하면 $\Phi_d\left(\xi_n^r\right)=0$ 이므로 $f\left(\xi_n^r\right)=0$ 이다. 따라서 $\xi_n^r\in T$ 이므로 $S\subset T$ 이다.

$(\supset)$ 임의의 $a\in T$ 를 택하자. 그러면 $f(a)=0$ 이므로 $d\mid n$ 을 만족하는 적당한 자연수 d가 존재해서 $\Phi_d(a)=0$ 을 만족한다. 따라서 원분다항식의 정의에 의하면 a는 $x^d=1$ 의 원시근이므로 $a^d=1$ 을 만족하고 $d\mid n$ 이므로 $a^n=1$ 을 만족한다.

그러므로 $a\in S$ 이고 $T\subset S$ 이다. 정리하면 $S=T$ 를 얻을수 있고 $x^n-1=\prod_{d\mid n}\Phi_d(x)$이 증명된다. 따라서 뫼비우스 반전 공식에 의하면

$\Phi_n(x)=\prod_{d\mid n}\left(x^{\frac{n}{d}}-1\right)^{\mu(d)}=\prod_{d\mid n}\left(x^d-1\right)^{\mu\left(\frac{n}{d}\right)}$ 가 성립한다. ■

원분다항식을 10개만 구해보면 다음과 같습니다.

$$\Phi_1(x)=x-1$$
$$\Phi_2(x)=x+1$$
$$\Phi_3(x)=x^2+x+1$$
$$\Phi_4(x)=x^2+1$$
$$\Phi_5(x)=x^4+x^3+x^2+x+1$$
$$\Phi_6(x)=x^2-x+1$$
$$\Phi_7(x)=x^6+x^5+x^4+x^3+x^2+x+1$$
$$\Phi_8(x)=x^4+1$$
$$\Phi_9(x)=x^6+x^3+1$$
$$\Phi_{10}(x)=x^4-x^3+x^2-x+1$$

모든 원분다항식은 정수 범위에서 인수분해할수 없다는 사실이 알려져 있습니다. 이것을 수학에서는 **기약다항식(Irreducible Polynomial)**이라고 부르는데 나중에 대수학을 공부하면 보게 될겁니다.

$\Phi_1(x)$부터 $\Phi_{10}(x)$까지의 원분다항식을 보면 원분다항식의 계수와 상수항은 모두 0 아니면 ± 1 이라고 생각할수 있는데 실제로는 그렇지 않습니다. $\Phi_{105}(x)$는 다음과 같다고 합니다.

$$\Phi_{105}(x) = x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - 2x^{41} - x^{40} - x^{39} + x^{36} + x^{35} + x^{34} + x^{33} + x^{32} + x^{31} - x^{28} - x^{26} - x^{24} - x^{22} - x^{20} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} - x^{9} - x^{8} - 2x^{7} - x^{6} - x^{5} + x^{2} + x + 1$$

찾아보기

작성자 : 네냐플(Nenyaffle)

숫자와 외국어를 먼저 배열했고 한글은 ㄱ,ㄴ,ㄷ 순으로 배열했습니다.

참고서적

작성자 : 네냐플(Nenyaffle)

1. 오정환 & 이준복, 기초 정수론, 경문사, 2012

2. D. M. Burton, Elementary Number Theory 7ed, McGraw-Hill, 2010