정수론 기초

1.

피보나치 수열 $\{f_n\}$은 다음과 같이 정의된다.

$$f_1 = f_2 = 1, \qquad f_n = f_{n-1} + f_{n-2} \, (n \geq 3)$$

피보나치 수열의 유래를 간단히 쓰고 다음 등식이 성립함을 보이시오. [1998]

$$f_{n+1} f_{n-1} = f_n^2 + (-1)^n \; (n \geq 2)$$

Math induction ?

n에 대하여 수학적 귀납법을 적용하면 다음과 같다.

(i) $n = 2$인 경우

$f_3 \cdot f_1 = 2 \cdot 1 = 2, \qquad f_2^2 + (-1)^2 = 1 + 1 = 2$

따라서 $f_3 \cdot f_1 = f_2^2 + (-1)^2$ 가 성립.

(ii) $f_{n+1} f_{n-1} = f_n^2 + (-1)^n$이 성립한다 가정

$\Rightarrow f_{n+2} \cdot f_n = (f_{n+1} + f_n) \cdot f_n$

$= f_{n+1} \cdot f_n + f_n^2$

$= f_{n+1} \cdot f_n + (f_{n+1} \cdot f_{n-1} - (-1)^n)$

$= f_{n+1} (f_n + f_{n-1}) + (-1)^{n+1}$

$= f_{n+1}^2 + (-1)^{n+1}$ 이 성립.

2.

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

True

(귀류법) $q \leq p$ 이고 $q \mid p!+1$ 을 만족하는 소수 q가 존재한다 가정하자.

$q \leq p$ 이므로 $q \mid p!$ 이다. ?

그러면 $q \mid p!$ 이고 $q \mid p!+1$ 이므로 $q \mid (p!+1) - p! = 1$ 이다.

소수는 1의 약수일 수 없으므로 모순.

3.

〈보기〉에서 옳은 것을 모두 고른 것은? [2009]

〈보기〉

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

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

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

① ㄱ ② ㄴ ③ ㄱ, ㄴ
④ ㄱ, ㄷ ⑤ ㄴ, ㄷ

ㄱ. True

ㄴ. ~~False~~ (메르센 소수) 필충X 역성립X True → 나눗셈 알고리즘을 연속적으로 적용하여 다음을 얻을 수 있다:

$m = nq_1 + r_1, \quad 0 \le r_1 < n$ -(1)

$n = r_1 q_2 + r_2, \quad 0 \le r_2 < r_1$ -(2)

$r_1 = r_2 q_3 + r_3, \quad 0 \le r_3 < r_2$ -(3)

$\vdots$

$r_{t-2} = r_{t-1} \cdot q_t + r_t, \quad 0 \le r_{t-1} < r_{t-2}$ -(t)

$r_{t-1} = r_t \cdot q_{t+1}$ -(t+1)

따라서 $\gcd(m,n) = \gcd(n, r_1) = \cdots = \gcd(r_{t-1}, r_t) = \gcd(r_t, 0) = r_t$

(1)을 사용하여. $2^m - 1 = 2^{nq_1+r_1} - 1$

$= 2^{nq_1+r_1} - 2^{r_1} + 2^{r_1} - 1$

$= ((2^n)^{q_1} - 1) \cdot 2^{r_1} + (2^{r_1} - 1)$

$= (2^n - 1)((2^n)^{q_1-1} + \cdots + 2^n + 1) \cdot 2^{r_1} + (2^{r_1} - 1)$

ㄷ. 25진법 3자리

~~True~~ False

$A\,B\,C$

$25^3 \; 25^2 \; 25$

$25^3 A + 25^2 B + 25 C$

$= 5^6 A + \cdots$

(반례) $651 = 1 \cdot 25^2 + 1 \cdot 25 + 1 \cdot 25^0$

$= 1101_{(5)}$

$25 \underline{| 651}$
$25 \underline{) 26} \cdots 1$
$1 \cdots 1$

$5 \underline{| 651}$
$5 \underline{| 130} \cdots 1$
$5 \underline{| 26} \cdots 0$
$5 \underline{| 5} \cdots 1$
1

위와 비슷하게 (2) ~ (t+1)을 이용하여

$2^m - 1 = (2^n - 1)((2^n)^{q_1-1} + \cdots + 2^n + 1) 2^{r_1} + (2^{r_1} - 1)$

$2^n - 1 = (2^{r_1} - 1)((2^{r_1})^{q_2-1} + \cdots + 2^{r_1} + 1) 2^{r_2} + (2^{r_2} - 1)$

$2^{r_1} - 1 = (2^{r_2} - 1)((2^{r_2})^{q_3-1} + \cdots + 2^{r_2} + 1) \cdot 2^{r_3} + (2^{r_3} - 1)$

$\vdots$

$2^{r_{t-2}} - 1 = (2^{r_{t-1}} - 1)((2^{r_{t-1}})^{q_t-1} + \cdots + 2^{r_{t-1}} + 1) \cdot 2^{r_t} + (2^{r_t} - 1)$

$2^{r_{t-1}} - 1 = (2^{r_t} - 1)((2^{r_t})^{q_{t+1}-1} + \cdots + 2^{r_t} + 1)$

따라서 $\gcd(2^m - 1, 2^n - 1) = \gcd(2^n - 1, 2^{r_1} - 1)$

$\vdots$

$= \gcd(2^{r_t} - 1, 0) = 2^{r_t} - 1 = 2^{\gcd(m,n)} - 1$

$\gcd(m,n) =$ 1 이어야!

디오판투스 방정식

4.

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

True

$\gcd(7,31)=1$ $1 \mid 2$ 이므로 해 존재

5.

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

~~$2x+3y=55$ 55개~~

~~$\gcd(2,3)=1$ 1×55~~

(sol) $2x+3y=1$

$\gcd(2,3)=1$

$3=2\times1+1 \Rightarrow 1=3-2\times1$

$2=1\times2$ $\quad =2\times(-1)+3\times1$

$x=-1\times55,\ y=1\times55$

특수해가 $x_0=-55,\ y_0=55$

그럼 일반해는 $X=-55+\frac{3}{1}t$

$Y=55-\frac{2}{1}t,\ t\in\mathbb{Z}$

양수해를 구하려면 $-55+3t>0,\ 3t>55$

$55-2t>0,\ 55>2t$

$$\Rightarrow \begin{cases} t>\frac{55}{3}\fallingdotseq 18.xx & t=19 \\ t<\frac{55}{2}\fallingdotseq 27.xx & t=27 \end{cases} \quad 27-19+1 = 9개.$$

6.

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

10

$gcd(32, 14) = gcd(2^5 \times 7^0, 2^1 \times 7^1) = 2^1 \times 7^0 = 2$

$32 = 2^5 \quad 14 = 2 \times 7$

$32x + 14y = 2$

$gcd(32, 14) = 2$

$\Rightarrow 16x + 7y = 1$

$gcd(16, 7) = 1$

$16 = 7 \times 2 + 2$

$7 = 2 \times 3 + 1$

$\Rightarrow 1 = 7 - 2 \times 3$

$= 7 - 3(16 - 7 \times 2)$

$= 16 \times (-3) + 7 \times 7$

$\boxed{x = -3,\ y = 7}$

여기서 이것은 특수해이다.

$\Rightarrow |x| + |y|$

$= 3 + 7 = 10$ ■

(+ 일반해 구하기)

$x_0 = -3, \quad y_0 = 7$ 이므로,

$$\begin{cases} X = -3 + \frac{14}{2} t = -3 + 7t \\ Y = 7 - \frac{32}{2} t = 7 - 16t \end{cases}$$

$$\Rightarrow \begin{cases} |-3+7t| \le 10 \\ |7 - 16t| \le 10 \end{cases}$$

$-10 \le -3 + 7t \le 10 \Rightarrow -7 \le 7t \le 13 \Rightarrow -1 \le t \le \frac{13}{7}$ $t = 0, 1$

$-10 \le 7 - 16t \le 10 \quad -17 \le -16t \le 3 \quad -\frac{3}{16} \le t \le \frac{17}{16}$ $t = 0, 1$

$\Rightarrow t = 0, 1$

$t = 0 \Rightarrow X = -3,\ Y = 7$ 10

$t = 1 \Rightarrow X = 4,\ Y = 9$ 13

10 or 13. ■

7.

정수 x, y, z에 관한 다음 방정식의 일반해를 구하시오. [2008]

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

~~$3x + 4y$~~

~~$gcd(3, 4) = 1$ 이므로~~

~~$3x + 4y = t$ 라 두고 $t + 5z = 2$~~

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

$4 = 3 \times 1 + 1$

$3 = 1 \times 3$

$\Rightarrow 1 = 4 - 3 \times 1$

$= (-1) \times 3 + 4 \times 1$

$$\Rightarrow \begin{cases} x_0 = -1 \times (2 - 5t) = 5t - 2 \\ y_0 = 1 \times (2 - 5t) = 2 - 5t \end{cases}$$ 의 특수해

따라서 일반해는 $X = 5t - 2 + \frac{4}{1} s$, $z = t$, $(s, t \in \mathbb{Z})$

$Y = 2 - 5t - \frac{3}{1} s$

$\Rightarrow X = 5t - 2 + 4s,\ y = 2 - 5t - 3s.$ ■

선형합동식 관련

8.

정수 x, y, z에 관한 합동식 $x^2+y^2 \equiv 3z^2 \pmod 4$의 해집합은
$$\{(x, y, z) \mid x \equiv y \equiv z \equiv 0 \pmod 2\}$$
임을 보이시오. [2007]

(sol) $\forall a \in \mathbb{Z}$, $a^2 \equiv \begin{cases} 0 \pmod 4, & a \text{ 짝수} \\ 1 \pmod 4, & a \text{ 홀수} \end{cases}$ − (*)

(⇒)

x_0, y_0, z_0가 준식의 해라 하면 $x_0^2+y_0^2 \equiv 3z_0^2 \pmod 4$ 이다.

(*)에 의하여 $x_0^2+y_0^2$은 법 4에 대하여 0, 1, 2 중 하나와 합동이고 $3z_0^2$는 법 4에 대하여 0, 3 중 하나와 합동이다.

$x_0^2+y_0^2 \equiv 3z_0^2 \pmod 4$ 이므로 $x_0^2+y_0^2$와 $3z_0^2$ 모두 법 4에 대하여 0과 합동이 됨을 알 수 있다.

$x_0^2+y_0^2 \equiv 0 \pmod 4$ 이면 $x_0^2 \equiv y_0^2 \equiv 0 \pmod 4$ 이다. 또한 $3z_0^2 \equiv 0 \pmod 4$ 이면 $z_0^2 \equiv 0 \pmod 4$ 이므로

즉, x_0, y_0, z_0는 모두 짝수 ⇒ $x_0 \equiv y_0 \equiv z_0 \pmod 2$

(⇐) Supp/ $x \equiv y \equiv z \equiv 0 \pmod 2$ 라 가정하면

$x = 2a$, $y = 2b$, $c = 2c$ 를 만족하는 정수 a, b, c가 존재.

그러면 $x^2+y^2 = 4(a^2+b^2) \equiv 0 \equiv 4(3c^2) \equiv 3(4c^2) \equiv 3z^2 \pmod 4$ ■

9.

(참, 거짓 판정문제) 합동식 $6x \equiv 22 \pmod{32}$의 정수해는 법 32에 대하여 1개 뿐이다. [2010]

(sol) $\gcd(6, 32) = 2$ 는 22의 약수

⇒ 법 32에 대한 $6x \equiv 22 \pmod{32}$ 의 해는 2개 존재.

※ Thm) $ax \equiv b \pmod n$에 대하여 $d \mid b$ 이면 법 n에 대하여 합동이 아닌 d개의 해 존재 ($\gcd(a, n) = d$?)

중국인의 나머지 정리

10.

K고등학교의 전체 학생을 같은 인원수의 9팀으로 나누면 1명이 남고, 같은 인원수의 10팀으로 나누면 2명이 남으며, 같은 인원수의 11팀으로 나누면 10명이 남는다. K고등학교 전체 학생수 x가 $x \equiv a \pmod{990}$을 만족할 때, 정수 a의 값을 구하시오. (단, $0 \le a < 990$) [2006]

$\begin{cases} x\equiv 1 \pmod 9 \\ x\equiv 2 \pmod{10} \\ x\equiv 10 \pmod{11} \end{cases}$	$99x\equiv 1 \pmod{10}$	$90x_3\equiv 1 \pmod{11}$	$\Rightarrow x\equiv 5\cdot 110+9\cdot 99\cdot 2+6\cdot 90\cdot 10$
	$99x-10y=1$	$90x-11y=1$	$=550+1782+5400$
	$\gcd(99,10)=1$	$\gcd(90,11)=1$	$=7732 \pmod{990}$
$x\equiv x_1N_1a_1+x_2N_2a_2+x_3N_3a_3 \pmod{990}$	$99=10\times 9+9$	$90=11\times 8+2$	$990\times 7=6930$ $\quad 7732-6930=802$
$x_1=5,\ N_1=110,\ a_1=1$; $x_2=9,\ N_2=99,\ a_2=2$; $x_3=6,\ N_3=90,\ a_3=10$	$10=9\times 1+1$	$11=2\times 5+1$	$\Rightarrow x\equiv 802 \pmod{990}$
$110x\equiv 1 \pmod 9$	$\Downarrow$	$2=1\times 2$	$\therefore a=802$
$110x-9y=1$	$1=10-9$	$1=11-2\times 5$	
$\gcd(110,9)=1 \quad \Rightarrow 1=9-2\times 4$	$=10-(99-10\times 9)$	$=11-5(90-11\times 8)$	
$110=9\times 12+2 \quad =9-4(110-9\times 12)$	$=99\times(-1)+10\times 10$	$=90\times(-5)+11\times 9$	
$9=2\times 4+1 \quad =110\times(-4)+9\times(\ )$	$x\equiv -1\equiv 9 \pmod{10}$	$x\equiv -5\equiv 6 \pmod{11}$	
$2=1\times 2 \quad x\equiv -4\equiv 5 \pmod 9$			

11.

다음 연립일차합동식의 해를 구하시오. [2003]

$$\begin{cases} 8x \equiv 4 \pmod{22} \\ 3x \equiv 5 \pmod{25} \end{cases}$$

① 중국인의 나머지 정리 쓰기 위해 식정리

$8x\equiv 4 \pmod{22}$	ii) $3x\equiv 5 \pmod{25} \Rightarrow x\equiv 5\times 17 \pmod{25}$	① $25x\equiv 1 \pmod{11}$ ② $11x\equiv 1 \pmod{25}$
$\Rightarrow 4x\equiv 2 \pmod{11}$	$3x\equiv 1 \pmod{25}$ $\quad =85\equiv 10 \pmod{25}$	$25x-11y=1$, $\gcd(25,11)=1$
② 식 정리 위해 역원 구하기	$3x-25y=1$ $\quad x\equiv 10 \pmod{25}$	$25=11\times 2+3 \quad \Rightarrow 1=3-2$
i) $4x\equiv 1 \pmod{11} \Rightarrow x\equiv 3 \pmod{11}$	$\gcd(3,25)=1$	$11=3\times 3+2 \quad =3-(11-3\times 3)$
$4x-11y=1$	$25=3\times 8+1$	$3=2\times 1+1 \quad =11\times(-1)+3\times 4$
$\gcd(4,11)=1$	$3=1\times 3$	$=11\times(-1)+4(25-11\times 2)$
$11=4\times 2+3$	$\Downarrow$ $1=25-3\times 8$	$=11\times(-9)+25\times 4$
$4=3\times 1+1$	$x=-8\equiv 17 \pmod{25}$	$x_1=4$, $x_2=-9\equiv 16 \pmod{25}$
$\Downarrow$ $1=4-3$	$\Rightarrow \begin{cases} x\equiv 3 \pmod{11} \\ x\equiv 10 \pmod{25} \end{cases}$	$\Rightarrow x\equiv 4\times 25\times 3\ (6)+16\times 11\times 10 \pmod{275}$
$=4-(11-4\times 2)$		$=\cancel{300+1760=2060}$
$=11\times(-1)+4\times 3$ $x=3$ (법 11에 관한 4의 역원)	$x\equiv x_1N_1a_1+x_2N_2a_2 \pmod{11\times 25}$ $4 \quad 25 \quad 3 \qquad 16 \quad 11 \quad 10$	$\cancel{275\times 7=1925,\ 2060-1925=135}$ $\therefore x\equiv \cancel{135}\ 160 \pmod{275}$

12.

〈보기〉의 진위를 판정하고 이유를 설명하시오. [2012]

〈보기〉

연립합동식 $\begin{cases} x \equiv 4 \pmod{28} \\ x \equiv 6 \pmod{36} \end{cases}$의 정수해가 존재한다.

mod 28 → $2^2 \times 7$ 존재 X

mod 36 → $2^2 \times 3^2$ 모름

Fermat 정리

13.

다음 합동식을 만족하는 정수 x, y는 어느 것인가? [1995]

$$9^x \equiv y \pmod{19}$$

① $x = 35, y = 1$ ② $x = 36, y = -1$

③ $x = 36, y = 1$ ④ $x = 35, y = -1$

$9^{35} \equiv 1 \pmod{19}$

$(3^2)^{35} \equiv 1 \pmod{19}$??

$3^2 = 1$

$9 = 1 \pmod{19}$

14.

정수 $2^{15}14^{10}+2$를 11로 나누었을 때의 나머지는? [1992]

페르마 정리

$a^{p-1} \equiv 1 \pmod p$ 사용

$11 \nmid 2$, $11 \nmid 14$ 이므로 $2^{11-1} = 2^{10} \equiv 1 \pmod{11}$

$14^{11-1} = 14^{10} \equiv 1 \pmod{11}$

$\Rightarrow 2^{10} \cdot 14^{10} \equiv 1 \pmod{11}$

$2^{15} \cdot 14^{10} \equiv 32 \pmod{11}$

$2^{15} \cdot 14^{10} + 2 \equiv 34 \pmod{11}$

$\equiv 1 \pmod{11}$

따라서 나머지는 1이다.

15.

(참, 거짓 판정문제) 홀수인 소수 p $(p \neq 3)$은 합동식 $3^{p-1} \equiv 1 \pmod{2p}$를 만족시킨다. [2011]

홀수인 소수 p는 $\gcd(3, p) = 1$ 이므로 $3^{p-1} \equiv 1 \pmod p$

2p 되면

$\begin{cases} 3^{p-1} \equiv 1 \pmod 2 \\ 3^{p-1} \equiv 1 \pmod p \end{cases}$?

16.

오늘부터 n^7째 되는 날이 금요일이면 오늘부터 $(n+2)^7$째 되는 날은 무슨 요일인가? [1995]

$n^7 \equiv 5 \pmod 7$ 금

$(n+2)^7 \equiv x \pmod 7$??

17.

합동방정식 $x \equiv 25^{99} \pmod{19 \cdot 13}$과 연립합동방정식 $\begin{cases} x \equiv a \pmod{19} \\ x \equiv b \pmod{13} \end{cases}$이 동치가 되도록 하는 정수 a, b의 값을 각각 구하시오. 또한 합동방정식의 정수해 x의 값을 풀이 과정과 함께 쓰시오.
(단, $0 \le a < 19$, $0 \le b < 13$, $0 \le x < 247$) [2020]

$\begin{cases} x \equiv a \pmod{19} \\ x \equiv b \pmod{13} \end{cases}$

$x \equiv x_1 N_1 a_1 + x_2 N_2 a_2 \pmod{19 \cdot 13}$

$13 \cdot a$ $\quad$ $19 \cdot b$

$13x \equiv 1 \pmod{19}$ $\quad$ $19x \equiv 1 \pmod{13}$

$13x - 19y = 1$

$\gcd(13, 19) = 1$

$19 = 13 \times 1 + 7$ $\Rightarrow$ $1 = 7 - 6$

$13 = 7 \times 1 + 6$ $\quad = 7 - (13 - 7)$

$7 = 6 \times 1 + 1$ $\quad = 13 \times (-1) + 7 \times 2$

$= 13 \times (-1) + 2(19 - 13)$

$= 13 \times (-3) + 2 \times 19$

$x = -3,\ y = 2$

$x \equiv 16 \cdot 13 \cdot a + 2 \cdot 19 \cdot b \pmod{19 \cdot 13}$

$\equiv 25^{99}$