

# 디오판토스

10117 박재은, 20105 김대현, 30217 임은규



비전부 수학자 발표

# CONTENTS - 목차



## 생애

- 디오판토스의 생애

## 디오판토스 방정식

- 디오판토스 방정식의 정의와 그 종류

## 정수론과 합동식

- 디오판토스가 큰 기여를 한 정수론과 그것의 바탕인 합동방정식을 알아보자.

# 생애 - LIFE

일생에  $\frac{1}{6}$ 은 소년이였다.  
그리고  $\frac{1}{12}$ 년후에 수염을 길렀고  
다시  $\frac{1}{7}$ 년이 지나고 결혼을 하였다  
5년이 지나 아들을 낳았고  
아들은 아버지 나이의 반년을 살았다.  
그는 아들이 죽은후 4년 뒤에 죽었다



# 생애에 관한 방정식

디오판토스의 사망 당시 나이를 'x'라고 놓고 방정식을 세우면

$$\frac{1}{6}x + \frac{1}{12}x + \frac{1}{7}x + 5 + \frac{1}{2}x + 4 = x$$

$$14x + 7x + 12x + 420 + 42x + 336 = 84x$$

$$14x + 7x + 12x + 42x + 756 = 84x$$

$$9x = 756$$

$$x = 84 \text{ 이다.}$$



# 디오판토스 방정식

디오판토스 방정식이란 다항방정식의 정수해, 유리수해를 찾는 것이다.

종류(방정식처럼 분류 되었진 않으나, 몇몇 디오판토스 방정식에만 이름이 붙어있다)

- 일차 부정방정식
  - 피타고라스 세 쌍 문제
  - 합동수 문제
- 

# 부정(不定)방정식

부정방정식은 미지수의 개수보다 식의 개수가 적어 근이 무수히 많아 근을 정할 수 없는 방정식이다. ' $X + Y = 10$ '과 같은 간단해 보이는 문제도 특정한 조건이 없다면 부정방정식이 된다. 디오판토스 방정식의 일환을 부정방정식이라 소개했지만 엄밀히 따지자면 둘은 제한이 있음과 없음에 따라 나뉜다. 디오판토스 방정식은 주로 부정방정식이 많지만 디오판토스의 부정방정식은 해의 범위가 정수/유리수라는 점에서 다르다. 물론 평범한 부정방정식은 해에 제한없이 해의 범위가 복소수이다. 예를 들어 ' $X^2 + Y^2 + 1 = 0$ '와 같은 식은 복소수 해는 무한히 많으나 실수 해는 없다. 따라서 위의 식은 디오판토스 방정식은 아니다.

# 피타고라스 세 쌍 문제

피타고라스 세 쌍 문제는 직각삼각형의 빗변의 제곱이 밑변의 제곱과 높이의 제곱의 합과 같다는 것이다. 즉 밑변을  $a$ , 높이를  $b$ , 빗변을  $c$ 라고 놓으면 ' $a^2 + b^2 = c^2$ '라는 부정방정식이 된다.

## 해를 구하는 방법

- 실수 부분과 허수부분이 모두 정수인 ' $a + bi$ '를 정한다.
- 복소수 ' $z = x + yi = (a + bi)^2$ '에 대해 ' $z$ 의 절댓값'을 구한다. ( $x, y$ 는 실수이다.)
- $\{|x|, |y|, |z|\}$ 는 피타고라스 세 쌍이다.

# 피타고라스 세 쌍 문제

## 주의점

만약 ' $xyz = 0$ '이라면 앞서 소개한 세 조건을 만족하나 삼각형의 세 변의 길이가 될 수는 없다. ' $xyz = 0$ '이라면 삼각형의 세 변 중 한 변의 길이가 '0'으로 변이 존재할 수 없게된다.

# CONGRUENCE(합동식)

## 정의

“정수  $a, b, m$ 에 대하여,  $m \mid (a-b)$ 일 때  $a$ 는 법  $m$ 에 대하여  $b$ 와 합동이다”라고 한다.  
이때 기호로  $a$ 기호로는  $a \equiv b \pmod{m}$ 라고 쓴다.

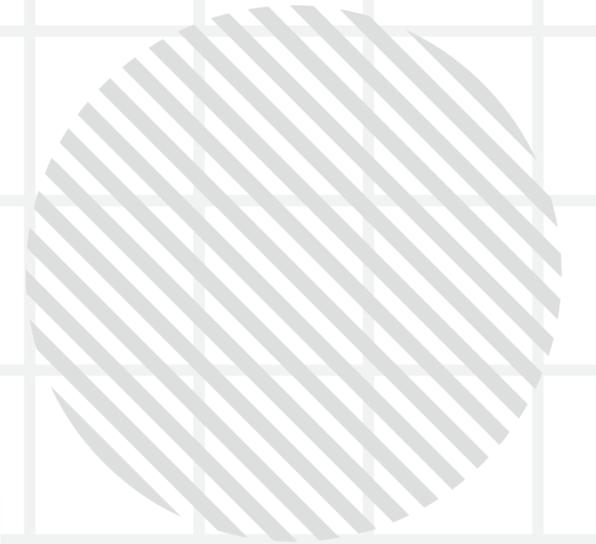
## 정수의 분류

모든 정수를 자연수  $n$ 으로 나누면 그 나머지가  $0, 1, 2, \dots, n-1$  중 하나가 된다.  
즉, 모든 정수는 다음 중 어느 하나로 표현이 가능하다.(단,  $k \in \mathbb{Z}$ )

# 합동식의 성질

1. **반사성** :  $a \equiv a \pmod{m}$ 의 꼴로 두 항 모두 같은 항이다.
2. **대칭성** (교환 법칙):  $a \equiv b \pmod{m}$ 이면  $b \equiv a \pmod{m}$ 의 꼴이다.
3. **추이성** :  $a \equiv b \pmod{m}, b \equiv c \pmod{m}$ 이면  $a \equiv c \pmod{m}$ 의 꼴이다.
4. **복부호동순**:  $a \equiv b \pmod{m}, c \equiv d \pmod{m}$ 이면,  $a \pm c \equiv b \pm d \pmod{m}$ 의 꼴이다.
5. **비례의 호환성**:  $a \equiv b \pmod{m}, c \equiv d \pmod{m}$ 이면,  $ac \equiv bd \pmod{m}$ 의 꼴이다.
6. **지수의 호환성** :  $a \equiv b \pmod{m}$ 이면,  $a^k \equiv b^k \pmod{m}$ 의 꼴이다.
7.  $ab \equiv ac \pmod{m}$ 이고,  $d = \text{최대공약수}(a, m)$ 이면,  $b \equiv c \pmod{dm}$ 의 꼴이다.
8.  $a \equiv b \pmod{m}$ 이고,  $n$ 이  $m$ 의 약수이면,  $a \equiv b \pmod{n}$ 의 꼴이다.
9.  $a \equiv b \pmod{m}$ 이고,  $d > 0$ 이  $a, b, m$ 의 공약수이면,  $d/a \equiv d/b \pmod{dm}$

# THANK YOU



10117 박재은, 20105 김대현, 30217 임은규

