정수론 HW. 1

20011759 박수민

1. $x^2 - 5y^2 = 12$를 만족하는 정수근 x, y가 존재하지 않음을 보이시오.

정수근 x, y가 존재한다 가정하자, 그렇다면 양변의 값은 당연히 각각 정수이다. 이때 $mod\ 5$를 취해주면 다음과 같다.

$$x^2 - 5y^2 \equiv 12\ (mod\ 5)$$
$$x^2 - 5y^2 \equiv 2\ (mod\ 5)$$

이때, y는 정수이므로 $5y^2$ 또한 정수이고 $5|5y^2$이다. 그러므로

$$x^2 \equiv 2\ (mod\ 5)$$

이다. 그런데 x^2은 $mod\ 5$에서 1또는 4만 합동이다. 즉 $x^2 \not\equiv 2\ (mod\ 5)$이므로 모순,

그러므로 정수근이 존재하지 않는다.

2. $x^2 - y^2 = 1$의 유리근 x, y를 모두 구하시오

(-1,0)을 지나는 기울기가 $m \in \mathbb{Q}$인 직선을 가정하자,
이 직선의 방정식은 $m(x+1) = y$이다. 이 직선과 쌍곡선 $x^2 - y^2 = 1$의 교점을 생각해보면 쌍곡선 $x^2 - y^2 = 1$에 직선 $m(x+1) = y$를 대입하여 얻을 수 있는데 이때 나오는 식은 모든 계수가 유리수이기에 한 근이 유리수라면 다른 근은 유리수가 나와야 한다. 근과 계수의 관계에서 유리수집합은 사칙연산에 대해 닫혀 있기 때문이다. 이때 한 근은 무조건$x = -1$이므로 나머지 한 근은 유리수이다.
반대로, (-1,0)를 제외한 쌍곡선 위의 임의의 한 유리수 점과 (-1,0)를 잇는 직선의 울기는 마찬가지로 유리수가 나와야만 한다. 그러므로 쌍곡선 위의 모든 유리근은 기울기가 유리수이고 유리근을 지나는 직선과의 교점으로 표현할 수 있다.

$$x^2 - \left(m(x+1)\right)^2 = 1$$

$$x^2 - m^2(x^2 + 2x + 1) = 1$$
$$x^2 - m^2x^2 - 2m^2x - m^2 = 1$$
$$(1 - m^2)x^2 - 2m^2x - m^2 - 1 = 0$$

(-1,0)을 무조건 지나는 직선이므로 $(x + 1)$로 묶어서 정리하면 다음과 같다.

$$(1 - m^2)(x + 1)(x - \frac{m^2 + 1}{1 - m^2}) = 0$$

즉 $x = \frac{m^2+1}{1-m^2}$이며, 이를 직선의 방정식에 대입하면 $y = m\left(\frac{m^2+1}{1-m^2} + 1\right) = \frac{2m}{1-m^2}$

$m \neq \pm 1$인 모든 유리수 m에 대해 방정식 $x^2 - y^2 = 1$은 $(\frac{m^2+1}{1-m^2}, \frac{2m}{1-m^2})$ 유리수 해를 얻는다.

$$\therefore \left(\frac{m^2 + 1}{1 - m^2}, \frac{2m}{1 - m^2}\right), (단, m \neq \pm 1)$$

3. $\boldsymbol{y^2 = x^3 + 8, (1, -3), (-\frac{7}{4}, \frac{13}{8})}$유리근, 이를 이용하여 유리근 하나 더 구하시오

$(1, -3), (-\frac{7}{4}, \frac{13}{8})$을 지나는 직선의 방정식을 계산하면 다음과 같다.

$$y = \frac{-3 - \frac{13}{8}}{1 + \frac{7}{4}}(x - 1) - 3 = \frac{-\frac{37}{8}}{\frac{11}{4}}(x - 1) - 3 = -\frac{37}{22}(x - 1) - 3 = -\frac{37}{22}x - \frac{29}{22}$$

$$y = -\frac{37}{22}x - \frac{29}{22}$$

이 직선과 방정식 $y^2 = x^3 + 8$의 교점을 생각해보면 모든 계수가 유리수인 3차 방정식이 나오는데 근과 계수의 관계와, 유리수 집합에서의 사칙연산은 닫혀 있다는 점을 생각해보면 이미 $x = 1, -\frac{7}{4}$일 때 교점을 가지므로 나머지 한 근은 유리수여야 한다. 즉, 직선 $y = -\frac{37}{22}x - \frac{29}{22}$와 방정식 $y^2 = x^3 + 8$의 교점 중 $(1, -3), (-\frac{7}{4}, \frac{13}{8})$를 제외한 나머지 하나는 유리수가 되므로 이를 구하면 된다. 방정식에 직선을 대입하면 다음과 같다.

$$\left(-\frac{37}{22}x - \frac{29}{22}\right)^2 = x^3 + 8$$

$$\frac{1369}{484}x^2 + \frac{1073}{242}x + \frac{841}{484} = x^3 + 8$$

$$484x^3 - 1369x^2 - 2146x + 3031 = 0$$

$(1, -3), (-\frac{7}{4}, \frac{13}{8})$은 직선과 방정식 $y^2 = x^3 + 8$위의 점이기도 하기에 교점이다. 즉 위 방정식은 $x = 1, -\frac{7}{4}$를 해로 가지므로 $(x-1), (x+\frac{7}{4})$로 인수분해가 가능하다. 조립제법으로 풀어서 정리하면 다음과 같다.

$$484(x-1)(x+\frac{7}{4})(x-\frac{433}{121}) = 0$$

즉, 방정식 $y^2 = x^3 + 8$은 $(\frac{433}{121}, -\frac{9765}{1331})$을 유리근으로 가진다.

$$\therefore (\frac{433}{121}, -\frac{9765}{1331})$$

4. $\boldsymbol{(252, 198) = 252x + 198y}$**를 만족하는 정수** $\boldsymbol{x, y}$**를 구하시오**

우선 유클리드 호제법을 이용하면 $252 = 198 \times 1 + 54$ 이므로

$(252,198) = (198,54)$이다. 이때, $252 = a, 198 = b$라 하자 그럼 $252 = 198 \times 1 + 54$은 $a = b \times 1 + 54$이 되고, 이는 $54 = a - b$가 된다. 이를 위에 다시 대입하면

$$\begin{aligned} &(252,198) = (a, b) \\ &= (198,54) = (b, a-b) \end{aligned}$$

$198 = 54 \times 3 + 36$이므로 $b = (a-b) \times 3 + 36$에서 $36 = 4b - 3a$이 된다.

$$\begin{aligned} &(198,54) = (b, a-b) \\ &= (54,36) = (a-b, 4b-3a) \end{aligned}$$

위와 같은 방식으로 유클리드 호제법를 응용하여 정리하면 다음과 같다.

$$\begin{aligned} &(252,198) = (a, b) \\ &= (198,54) = (b, a-b) \\ &= (54,36) = (a-b, 4b-3a) \\ &= (36,18) = (4b-3a, 4a-5b) \\ &= (18,0) = (4a-5b, 0) \end{aligned}$$

즉 $(252,198) = 18 = 4a - 5b$이고 $a = 252, b = 198$이므로

$$(252,198) = 252 \cdot 4 + 198 \cdot (-5)$$

즉, $252x + 198y$의 정수근은 $x = 4, y = -5$이다.

$$\therefore x = 4, y = -5$$

추가로 이는 수 없이 많은 정수근 중 하나이다. 다른 "모든" 정수근을 구하기 위

해서는 $252x + 198y = 18$에서 252와 198의 최소 공배수 2,772를 생각해보면 x가 11(=2772/252)가 증가할 때, y가 14(=2772/198)가 감소한다면 여전히 방정식은 성립한다.

그러므로 임의의 정수 k에 대해 $(252,198) = 252(x_0 + 11k) + 198(y_0 - 14k)$이다.

이때 앞에서 적당한 근 $x = 4, y = -5$을 미리 구해 두었으므로 대입하여 모든 정수근을 구할 수 있다.

$$\therefore x = 4 + 11k, y = -5 - 14k, (k \in \mathbb{Z})$$

5. 합동방정식 $9x \equiv 12\ mod\ 15$의 해를 모두 구하시오.

$(9,15) = 3$ 이고 $3|12$ 이므로 위 합동 방정식에서 3으로 나누면 modular도 $(3,15) = 3$으로 나눠진다.

$$9x \equiv 12\ mod\ 15$$
$$3x \equiv 4\ mod\ 5$$

$3 \times 2 = 6 \equiv 1\ mod\ 5$이므로 곱셈 군 $\mathbb{Z}^*{}_5$에서 3의 곱셈 역원은 2이다.

그러므로 양변에 2를 곱해서 정리하면 다음과 같다.

$$2 \times 3x \equiv 2 \times 4\ mod\ 5$$
$$6x \equiv 8\ mod\ 5$$
$$x \equiv 3\ mod\ 5$$

즉 $x \equiv 3\ mod\ 5$이므로 $x = 3 + 5k\ (k \in \mathbb{Z})$이다.

$$\therefore\ x = 3 + 5k, (k \in \mathbb{Z})$$