

### 나눗셈 알고리즘과 Euclid 호제법

✓ Euclid 호제법을 이용하여 다음 최대공약수를 구하시오.

1. (9005, 3003)

$$\begin{array}{r|rr|l}
 2 & 9005 & 3003 & 1 \\
 & 6006 & 2999 & \\
 \hline
 749 & 2999 & 4 & 1 \\
 & 2996 & 3 & \\
 \hline
 & 3 & 1 & 
 \end{array}$$

이므로  $(9005, 3003) = 1$  이다.

2. (1508, 462)

$$\begin{array}{r|rr|l}
 3 & 1508 & 462 & 4 \\
 & 1386 & 488 & \\
 \hline
 -5 & 122 & -26 & 3 \\
 & 130 & -24 & \\
 \hline
 & -8 & -2 & 
 \end{array}$$

이므로  $(1508, 462) = 2$  이다.

3. (2793, 1953)

$$\begin{array}{r|rr|l}
 1 & 2793 & 1953 & 2 \\
 & 1953 & 1680 & \\
 \hline
 3 & 840 & 273 & 13 \\
 & 819 & 273 & \\
 \hline
 & 21 & 0 & 
 \end{array}$$

이므로  $(2793, 1953) = 21$  이다.

4. (18183, 6069)

$$\begin{array}{r|rr|l}
 3 & 18183 & 6069 & -253 \\
 & 18207 & 6072 & \\
 \hline
 & -24 & -3 & 
 \end{array}$$

이므로  $(18183, 6069) = 3$  이다.

✓ Euclid 호제법을 이용하여 최대공약수  $(a,b)$  를  $(a,b) = as + bt$  형태로 표현하시오.

1.  $(9005, 3003)$

$$\begin{array}{r|rr}
 1 & 9005 & 3003 & -751 \\
 0 & 9009 & 3004 & 1 \\
 \hline
 1 & -4 & -1 & -3 \\
 \hline
 751 & & & 1 - (-3) \cdot (-751) = -2252
 \end{array}$$

$9005 \cdot 751 + 3003 \cdot (-2252) = -1$  이므로  $9005 \cdot (-751) + 3003 \cdot 2252 = 1 = (9005, 3003)$  이다.

2.  $(1508, 462)$

$$\begin{array}{r|rr}
 3 & 1508 & 462 & 4 \\
 \hline
 & 1386 & 488 & \\
 -5 & 122 & -26 & 3 \\
 \hline
 & 130 & -24 & \\
 \hline
 & -8 & -2 & 
 \end{array}$$

$$\begin{aligned}
 &1, 0, 1, -4, 1 - (-4) \cdot (-5) = -19, -4 - (-19) \cdot 3 = 53 \\
 &0, 1, -3, 1 - (-3) \cdot 4 = 13, -3 - 13 \cdot (-5) = 62, 13 - 62 \cdot 3 = -173 \\
 &\Rightarrow -2 = 1508 \cdot 53 + 462 \cdot (-173) \\
 &(1508, 462) = 2 = 1508 \cdot (-53) + 462 \cdot 173
 \end{aligned}$$

3.  $(2793, 1953)$

$$\begin{array}{r|rr}
 1 & 2793 & 1953 & 2 \\
 \hline
 & 1953 & 1680 & \\
 3 & 840 & 273 & 13 \\
 \hline
 & 819 & 273 & \\
 \hline
 & 21 & 0 & 
 \end{array}$$

$$\begin{aligned}
 &1, 0, 1, -2, 1 - (-2) \cdot 3 = 7 \\
 &0, 1, -1, 1 - (-1) \cdot 2 = 3, -1 - 3 \cdot 3 = -10 \\
 &\Rightarrow (2793, 1953) = 21 = 2793 \cdot 7 + 1953 \cdot (-10)
 \end{aligned}$$

4.  $(18183, 6069)$

$$\begin{array}{r|rr}
 3 & 18183 & 6069 & -253 \\
 \hline
 & 18207 & 6072 & \\
 & -24 & -3 & 
 \end{array}$$

$$\begin{aligned}
 &1, 0, 1, 253 \\
 &0, 1, -3, 1 - (-3)(-253) = -758 \\
 &\Rightarrow (18183, 6069) = 3 = 18183 \cdot (-253) + 6069 \cdot 758
 \end{aligned}$$

**Note**

$a, b$ 가 크지 않은 수일 때에는 유클리드 호제법을 이용하지 않고  
 최대 공약수  $d = \gcd(a,b)$  를  $a$ 와  $b$ 의 일차결합  $d = ax + by$ 로 나타낼 수 있다.  
 이를 위해서는  $\mathbb{Z}_n$ 에서  $a^{-1}$ 을 빠르게 계산하는 방법을 익혀야 한다.  
 $\mathbb{Z}_n$ 의 계산법을 익히고 유클리드 호제법을 이용하지 않는 방법을 소개한다.