유클리드 호제법

두 자연수 A, B에 대하여 $A > B$일 때,

A를 B로 나눈 몫과 나머지를 각각 q, R이라고 하면 다음과 같이 나타낼 수 있다.

$A = Bq + R$

이때 A와 B의 최대공약수를 G라고 하면 B와 R의 최대공약수도 G이다.

두 자연수 A, B의 최대공약수를 유클리드 호제법을 이용하여 구하는 과정은 다음과 같다.

1. 큰 수를 작은 수로 나눈다. (이때 편의상 큰 수를 A, 작은 수를 B라 하자.)
2. A가 B로 나누어떨어지면 B가 A, B의 최대공약수이다.

   (42와 21의 최대공약수는 21을 생각해보면 쉬움)
3. 나누어떨어지지 않는다면 $A = Bq + R$에서 B와 R의 최대공약수를 구하면 된다.

   즉, 큰 수를 B, 작은 수를 R로 두고 1~2의 과정을 반복한다.

예를 들어, 42와 24의 최대공약수는 다음과 같이 구할 수 있다.

1. 42를 24로 나눈 몫은 1, 나머지는 18이다.
2. 나누어 떨어지지 않으므로 24를 큰 수, 18을 작은 수로 두고 24를 18로 나눈다.
3. 24를 18로 나눈 몫은 1, 나머지는 6이다.
4. 나누어 떨어지지 않으므로 18을 큰 수, 6을 작은 수로 두고 18을 6으로 나눈다.
5. 나누어 떨어지므로 6이 42와 24의 최대공약수이다.

유클리드 호제법

두 자연수 A, B에 대하여 $A > B$일 때,

A를 B로 나눈 몫과 나머지를 각각 q, R이라고 하면 다음과 같이 나타낼 수 있다.

$A = Bq + R$

이때 A와 B의 최대공약수를 G라고 하면 B와 R의 최대공약수도 G이다.

증명)

A와 B의 최대공약수를 G라고 하면

$A = Ga$, $B = Gb$ (a, b는 서로소인 자연수)

로 나타낼 수 있다.

$A = Bq + R$에서 $Ga = Gbq + R$

위 식을 R에 대해 정리하면

$R = Ga - Gbq = G(a - bq)$

이때 B와 R의 최대공약수도 G임을 보이자.

즉, $B = Gb$, $R = G(a - bq)$에서 b와 $a - bq$가 서로소임을 보이자.

(귀류법)

b와 $a - bq$가 서로소가 아니라고 가정하면 공약수 t (t는 2보다 크거나 같은 자연수)가 존재하므로

$b = tm$, $a - bq = tn$ (m, n은 자연수)

으로 둘 수 있다.

$a - bq = tn$에서 $a = bq + tn$이고 이 식에 $b = tm$을 대입하면

$a = tmq + tn = t(mq + n)$

그런데, a, b는 2보다 크거나 같은 공약수 t를 가지게 되므로, a, b가 서로소인 자연수라는 사실에 모순이다.

즉, b와 $a - bq$는 서로소이다.

따라서 $A = Bq + R$일 때, A와 B의 최대공약수를 G라고 하면 B와 R의 최대공약수도 G이다.