유클리드 호제법을 증명 해봅시다.

> $d, m, n,$이 어떤 정수일 때
> 1. d가 m과 n의 공약수일때, $m + n$도 d의 약수이다.
> 2. d가 m과 n의 공약수일때, $m - n$도 d의 약수이다.

이에 대한 증명은 간단합니다.

$m = dq_1, n = dq_2($ q_1, q_2는 어떤 정수)

$m + n = d(q_1 + q_2), m - n = d(q_1 - q_2)$

참고로 d가 n의 약수(인수)일 때 $d \mid n$으로 표시합니다.

m과 n의 최대공약수는 $gcd(m, n)$이라고 합니다.

r이 a를 b로 나눈 나머지라면 $r = a \, mod \, b$입니다.

이를써서 위 명제를 다시 적으면 $d \mid n, d \mid m \Rightarrow d \mid (m + n), d \mid (m - n)$

> 유클리드 호제법
> a가 음이 아닌 정수이고, b가 양의 정수이며, r이 a를 b로 나눈 나머지라면 a와 b의 최대공약수는 b와 r의 최대공약수와 같다.

위 명제를 위에 적었던 표기법을 사용하면

a가 음이 아닌 정수이고, b가 양의 정수이며 $r = a \, mod \, b$이면 $gcd(a, b) = gcd(b, r)$이다.

뭐 어쨋든, 증명을 하자면 $a = bq + r(0 \leq r < b, q$ 는 어떤 정수)인데, c를 a와 b의 공약수라 하면, c는 bq의 약수인 것은 자명합니다. a또한 c의 약수이므로 c는 $a - bq(= r)$의 약수입니다. 따라서 c는 b와 r의 공약수입니다. 반대로 c'가 b와 r의 공약수이면, c'는 $bq + r(= a)$의 약수가 되고 따라서 a와 b의 공약수가 됩니다. 따라서 a와 b의 공약수 집합이 b와 r의 공약수 집합과 같으므로 $gcd(a, b) = gcd(b, r)$이 성립합니다.

유클리드 호제법을 이용해 b, r를 새로운 a, b로서 보고 연속해서 사용하면, a 자리에는 최대공약수가 b는 0이 됩니다.