

산술의 기본정리

산술의 기본 정리에 대한 내용은 다음과 같다.

2이상의 모든 양의 정수는 소수들의 곱으로 표현가능하고 그 형태는 순서를 무시하면 유일하다.

이 때 증명을 해야할 점은 총 두가지이다.

1. 모든 양의 정수는 소수들의 곱으로 표현이 가능하다.
2. 소수들의 곱의 형태가 순서를 무시하면 유일하다.

우선 소수의 정의는 본인을 제외한 나눌 수 있는 값은 존재하지 않는다는 의미이다.

이는 1을 제외한 가장 작은 약수라는 것을 의미한다.

의미를 이해하기 위해 예시를 들자면, 12를 기준으로 약수를 차례대로 작성하면, 1 2 3 4 6 12이다.

이 때 1을 제외한 가장 작은 약수는 2이다. 이 때 이 2는 소수이므로, 양의 정수 중 1을 제외한 가장 작은 약수가 소수라는 것이다.

이를 증명하는 방법은 가장 작은 약수가 소수가 아니라는 가정 즉, 귀류법을 활용하면 증명이 가능하다.

이제 1을 증명하기 위해 recursive한 방법을 활용해보도록 하겠다.

n 을 소수라고 가정하면, 약수는 1, n 이기 때문에 1이 자명하다.

n 을 합성수라고 가정해본다.

n 의 약수를 차례대로 나열하면, $1, a_1, a_2, a_3, \dots, n$

이 때 a_1 은 소수가 된다. n 을 a_1 으로 나눴을 때 몫을 p 라고 하면,

$n = a_1 * p$ 가 되고, p 가 소수이면 소수의 곱으로 표현되기 때문에 참이된다.

따라서 p 가 합성수일 때를 생각해본다.

p 가 합성수이면 마찬가지로 1을 제외한 가장 작은 약수가 존재할 것이다. 이는 a_1 과 동일하게 소수를 가지고 있다.

즉, 위 상황과 반복적으로 알고리즘이 진행되기 때문에, p 를 또 소수로 나누는 과정을 계속 진행하다보면 결국은 정수는 소수의 곱으로 표현가능하다는 것을 확인할 수 있다.