

Euclid's Proof

Recall that we know that every integer can be written as a product of prime numbers. In particular, every integer greater than 1 has a prime divisor.

Proposition: There are infinitely many primes.

Euclid's Proof cont'd

Proof: Suppose that there are only finitely many prime numbers.

- ▶ Multiply them together and let P be their product.
- ▶ Consider the integer $P + 1$.
- ▶ This integer must have a prime divisor p , which must be greater than one, so we can write $P + 1 = pA$.
- ▶ Since P is the product of all the primes, we know that p is a divisor of P , so we can write $P = pB$.
- ▶ Therefore $1 = pA - P = pA - pB = p(A - B)$.
- ▶ This implies that p is a divisor of 1, so $p = 1$.
- ▶ We've proved that $p > 1$ and $p = 1$, which is a contradiction. Thus there cannot be finitely many primes.