

Contents

0.1	Euclid's lemma	1
0.1.1	Statement	1
0.1.2	Proof	1

0.1 Euclid's lemma

0.1.1 Statement

If a prime number p divides product $a.b$ then p must divide at least of one of a or b .

0.1.2 Proof

From Bezout's identity we know that:

$$d = px + by$$

Where p and b are natural numbers and d is their greatest common denominator.

Let's choose a prime number for p . There are no common divisors, other than one. As a result there are exist values for x and y such that:

$$1 = px + by$$

Now, we are trying to prove that if p divides $a.b$ then p must divide at least one of a and b , so let's multiply this by a .

$$a = pax + aby$$

We know that p divides pax , and p divides ab by definition. As a result p can divide a .