

Some things about greatest common divisors that you should know and know how to prove:

Theorem GCD 1 If $a, b \neq 0$ then $1 \leq (a, b) \leq |b|$

proof: 1 divides evenly into every integer, so $1|a$ and $1|b$ and 1 is a common divisor of a and b , hence the greatest common divisor (a, b) must be at least as large as 1: $1 \leq (a, b)$

The greatest common divisor (a, b) must be a divisor of b , so $(a, b) | b$ and hence $(a, b) \leq |b|$. Thus $1 \leq (a, b) \leq |b|$

Theorem GCD 2 If $a \neq 0$ and p is prime, then $(a, p) = 1$ or p

proof: The greatest common divisor (a, p) must be a divisor of p , so (by definition of prime) $(a, p) = \pm 1, \pm p$ and 1 divides evenly into every integer so $1 \leq (a, p)$. Thus, $(a, p) = 1$ or p

Theorem GCD 3 If $a \neq 0$, p is prime and $p \nmid a$ then $(a, p) = 1$

proof: The greatest common divisor (a, p) must be a divisor of p , so (by definition of prime) $(a, p) = \pm 1, \pm p$ and 1 divides evenly into every integer so $1 \leq (a, p)$. Thus, $(a, p) = 1$ or p .

Also, (a, p) must be a divisor of a , so $(a, p) | a$. We are given $p \nmid a$, so $(a, p) = 1$.