

SOME DEFINITIONS AND FACTS FROM NUMBER THEORY

Definition $a \mid b$ (a divides b) means there is a number d such that $b = a \cdot d$

Definition $\gcd(a, b)$, the greatest common divisor of a and b , is the largest number that divides both a and b .

Definition $\text{lcm}(a, b)$, the least common multiple of a and b , is the smallest number divisible by both a and b .

Exercise What is $\gcd(a, b) \cdot \text{lcm}(a, b)$ equal to (try some examples).

Definition a and b are relatively prime means $\gcd(a, b) = 1$; that is, the only number that divides both a and b is 1.

Definition p is prime means that the only numbers that divide p are 1 and p itself.

Definition A linear combination of a and b is any number that can be formed from a and b by computing $x \cdot a + y \cdot b$ for some integers (positive or negative) x and y .

Example Both 43 and 1 are linear combinations of 3 and 7 because we can write them as:

$$\begin{aligned}43 &= 3 \cdot 5 + 4 \cdot 7 \\1 &= 3 \cdot 5 + (-2) \cdot 7\end{aligned}$$

Theorem (Euclid) The greatest common divisor of a and b is always a linear combination of a and b .

Proposition if $\gcd(a, b) = 1$ and $a \mid bn$ then $a \mid n$.

Remark Note that when a and b are not relatively prime, then a may divide bn without a dividing either b or n . (Find a simple example of this.)

Proposition If p and q are different primes, then $\gcd(p, q) = 1$.

Proposition Let $d = \gcd(a, b)$; then a/d and b/d are relatively prime (i.e. $\gcd(a/d, b/d) = 1$).

Proposition If $\gcd(u, v) = 1$ then $\gcd(ud, vd) = d$.

Proposition c is a linear combination of a and b if and only if $\gcd(a, b) \mid c$.

Proposition Given a , there is a b such that $ab \equiv 1 \pmod{N}$ if and only if $\gcd(a, N) = 1$.