

Mathematics for Computer Science MIT 6.042J/18.062J

Number Theory: GCD's & linear combinations



March 6, 2015

gcd-def.1



Arithmetic Assumptions

assume usual rules for +, ·, -: a(b+c) = ab + ac, ab = ba, (ab)c = a (bc), a - a = 0,a + 0 = a, a+1 > a,

 $\bigcirc 0 \bigcirc$

Albert R Meve

gcd-def.2

The Division Theorem

For b > 0 and any a, have

q = quotient(a,b)

r = remainder(a,b)

 \exists unique numbers q, r such that

a = qb + r and $0 \le r \le b$.

Take this for granted too!



Albert R Meyer



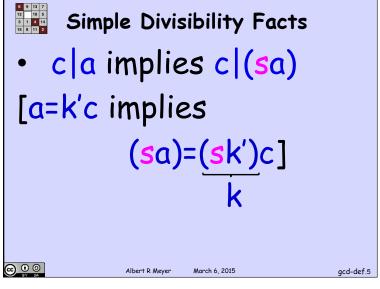
Divisibility

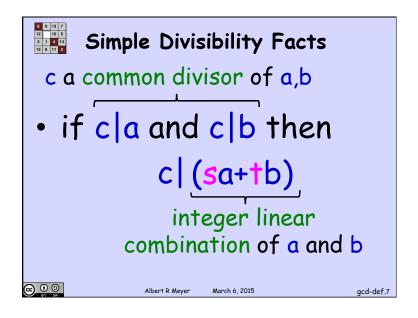
c divides a (c|a) iff a = k·c for some k

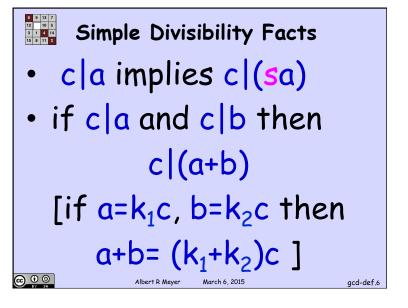
5|15 because 15 = 3.5

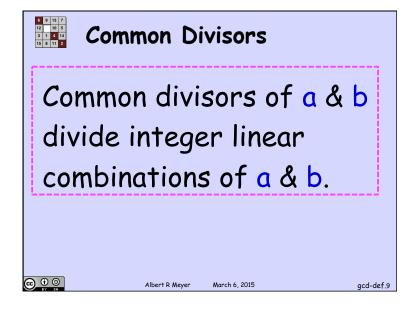
n|0 because $0 = 0 \cdot n$

Simple Divisibility Facts ca implies c (sa) [a=k'c implies (sa)=(sk')c@ <u>0</u> @ gcd-def.5









GCD gcd(a,b) ::= the greatest common divisor of a and b gcd(10,12) = 2 gcd(13,12) = 1 gcd(17,17) = 17 gcd(0, n) = n for n>0 CCD Albert R Meyer March 6, 2015

