

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Mathematics for Computer Science
MIT 6.042J/18.062J

Number Theory: GCD's & linear combinations



Albert R Meyer March 6, 2015

gcd-def.1

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Arithmetic Assumptions

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



Albert R Meyer March 6, 2015

gcd-def.2

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

The Division Theorem

For $b > 0$ and any a , have

$q = \text{quotient}(a,b)$

$r = \text{remainder}(a,b)$

\exists **unique** numbers q, r such that
 $a = qb + r$ and $0 \leq r < b$.

Take this for granted too!



Albert R Meyer March 6, 2015

gcd-def.3

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Divisibility

c **divides** a ($c|a$) iff

$a = k \cdot c$ for some k

$5|15$ because $15 = 3 \cdot 5$

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



Albert R Meyer March 6, 2015

gcd-def.4



Simple Divisibility Facts

- $c|a$ implies $c|(sa)$
- $[a=k'c$ implies $(sa)=\underbrace{(sk')}_k c]$

Albert R Meyer March 6, 2015 gcd-def.5



Simple Divisibility Facts

- $c|a$ implies $c|(sa)$
- if $c|a$ and $c|b$ then $c|(a+b)$
- $[if a=k_1c, b=k_2c$ then $a+b=(k_1+k_2)c]$

Albert R Meyer March 6, 2015 gcd-def.6



Simple Divisibility Facts

c a common divisor of a, b

- if $c|a$ and $c|b$ then $c|\underbrace{(sa+tb)}_{\text{integer linear combination of } a \text{ and } b}$

Albert R Meyer March 6, 2015 gcd-def.7



Common Divisors

Common divisors of a & b divide integer linear combinations of a & b .

Albert R Meyer March 6, 2015 gcd-def.9



GCD

$\text{gcd}(a,b) ::=$ the **greatest** common divisor of a and b

$\text{gcd}(10,12) = 2$

$\text{gcd}(13,12) = 1$

$\text{gcd}(17,17) = 17$

$\text{gcd}(0, n) = n$ for $n > 0$



Albert R Meyer March 6, 2015 gcd-def.10



GCD

$\text{gcd}(a,b) ::=$ the **greatest** common divisor of a and b

lemma: p prime implies $\text{gcd}(p,a) = 1$ or p

proof: The only divisors of p are ± 1 & $\pm p$.



Albert R Meyer March 6, 2015 gcd-def.11

MIT OpenCourseWare
<https://ocw.mit.edu>

6.042J / 18.062J Mathematics for Computer Science
Spring 2015

For information about citing these materials or our Terms of Use, visit: <https://ocw.mit.edu/terms>.