

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

Mathematics for Computer Science  
MIT 6.042J/18.062J

# Computing GCD's The Euclidean Algorithm



Albert R Meyer March 6, 2015

gcdeuclid.1

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

## GCD Remainder Lemma

Lemma:

$$\gcd(a,b) = \gcd(b, \text{rem}(a,b))$$

for  $b \neq 0$

Proof:  $a = qb + r$

any divisor of 2 of these  
terms must divide all 3.



Albert R Meyer March 6, 2015

gcdeuclid.2

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

## GCD Remainder Lemma

Lemma:

$$\gcd(a,b) = \gcd(b, \text{rem}(a,b))$$

for  $b \neq 0$

Proof:  $a = qb + r$

so  $a,b$  and  $b,r$  have  
the **same** divisors



Albert R Meyer March 6, 2015

gcdeuclid.3

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

## GCD example

Example:  $a = 899$ ,  $b = 493$

$$\text{GCD}(899, 493) =$$

$$\text{GCD}(493, 406) =$$

$$\text{GCD}(406, 87) =$$

$$\text{GCD}(87, 58) =$$

$$\text{GCD}(58, 29) =$$

$$\text{GCD}(29, 0) = 29$$



Albert R Meyer March 6, 2015

gcdeuclid.4

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

## Euclidean Algorithm

as a State Machine:

States ::=  $\mathbb{N} \times \mathbb{N}$

start ::=  $(a,b)$

state transitions defined by

$$(x,y) \rightarrow (y, \text{rem}(x,y))$$

for  $y \neq 0$



Albert R Meyer

March 6, 2015

gcdeuclid.5

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

## GCD partial correctness

By Lemma,  $\text{gcd}(x,y)$  is constant.

so preserved invariant is

$$P((x,y)) ::= [\text{gcd}(a,b) = \text{gcd}(x,y)]$$

$P(\text{start})$  is trivially true:

$$[\text{gcd}(a,b) = \text{gcd}(a,b)]$$



Albert R Meyer

March 6, 2015

gcdeuclid.6

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

## GCD partial correctness

at termination (if any)

$$x = \text{gcd}(a,b)$$

Proof: at termination,  $y = 0$ , so

$$x = \text{gcd}(x,0) = \underbrace{\text{gcd}(x,y)}_{\text{preserved invariant}} = \text{gcd}(a,b)$$

preserved invariant



Albert R Meyer

March 6, 2015

gcdeuclid.7

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

## GCD Termination

At each transition,  $x$  is replaced by  $y$ .



Albert R Meyer

March 6, 2015

gcdeuclid.8

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

## GCD Termination

At each transition,  $x$  is replaced by  $y$ . If  $y \leq x/2$ , then  $x$  gets halved at this step.



Albert R Meyer

March 6, 2015

gcdeuclid.9

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

## GCD Termination

At each transition,  $x$  is replaced by  $y$ . If  $y \leq x/2$ , then  $x$  gets halved at this step. If  $y > x/2$ , then  $\text{rem}(x,y) = x - y < x/2$ , so  $y$  gets halved when it is replaced by  $\text{rem}(x,y)$  after the next step.



Albert R Meyer

March 6, 2015

gcdeuclid.10

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

## GCD Termination

$y$  halves or smaller at every other step, so reaches minimum in  $\leq 2 \log_2 b$  steps.



Albert R Meyer

March 6, 2015

gcdeuclid.11