

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

Mathematics for Computer Science  
MIT 6.042J/18.062J

# GCD's & linear combinations: The Pulverizer



Albert R Meyer

March 6, 2015

pulverizer.1

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

GCD is a linear combination

Theorem:

$\gcd(a,b)$  is an integer  
linear combination of  
 $a$  and  $b$ .

$$\gcd(a,b) = sa + tb$$



Albert R Meyer

March 6, 2015

pulverizer.2

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

GCD is a linear combination

Corollary:

The multiples of  $\gcd(a,b)$   
are exactly the linear  
combinations of  $a$  and  $b$ .



Albert R Meyer

March 6, 2015

pulverizer.3

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

$$\gcd(a,b) = sa + tb$$

Proof: Show how to find  
coefficients  $s, t$ .

Method: apply Euclidean  
algorithm, finding  
coefficients as you go.



Albert R Meyer

March 6, 2015

pulverizer.4

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

## Extending Euclid

In Euclid have

$$\gcd(x,y) = \gcd(a,b).$$

Track coeff's  $c,d,e,f$

$$ca+db = x \text{ and } ea+fb = y$$



Albert R Meyer

March 6, 2015

pulverizer.5

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

## Extending Euclid

In Euclid have

$$\gcd(x,y) = \gcd(a,b).$$

Track coeff's  $c,d,e,f$

$$ca+db = x \text{ and } ea+fb = y$$

to start:

$$x = a = 1a+0b$$



Albert R Meyer

March 6, 2015

pulverizer.6

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

## Extending Euclid

In Euclid have

$$\gcd(x,y) = \gcd(a,b).$$

Track coeff's  $c,d,e,f$

$$ca+db = x \text{ and } ea+fb = y$$

to start:

$$y = b = 0a+1b$$



Albert R Meyer

March 6, 2015

pulverizer.7

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

## Extending Euclid

$$x_{\text{next}} = y = ea+fb$$

$$y_{\text{next}} = \text{rem}(x,y) =$$

$$x - qy =$$

$$ca+db - q(ea+fb)$$



Albert R Meyer

March 6, 2015

pulverizer.8

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

## Extending Euclid

$$x_{\text{next}} = y = ea + fb$$

$$y_{\text{next}} = \text{rem}(x, y) =$$

$$x - qy =$$

$$(c - qe)a + (d - qf)b$$



Albert R Meyer

March 6, 2015

pulverizer.9

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

## Finding $s$ and $t$

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

$$899 = 1 \cdot 493 + 406 \quad \text{so } 406 = 1 \cdot a + (-1) \cdot b$$

$$493 = 1 \cdot 406 + 87 \quad \text{so } 87 = 1 \cdot b - 1 \cdot 406$$

$$= -1 \cdot a + 2 \cdot b$$

$$406 = 4 \cdot 87 + 58 \quad \text{so } 58 = 1 \cdot 406 - 4 \cdot 87$$

$$= 5 \cdot a + (-9) \cdot b$$

$$87 = 1 \cdot 58 + 29 \quad \text{so } 29 = 1 \cdot 87 - 1 \cdot 58$$

$$= -6 \cdot a + 11 \cdot b$$

$$58 = 2 \cdot 29 + 0$$

done,  $\text{gcd} = 29$



Albert R Meyer

March 6, 2015

pulverizer.10

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

## Finding $s$ and $t$

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

$$899 = 1 \cdot 493 + 406 \quad \text{so } 406 = 1 \cdot a + (-1) \cdot b$$

$$493 = 1 \cdot 406 + 87 \quad \text{so } 87 = 1 \cdot b - 1 \cdot 406$$

$$= -1 \cdot a + 2 \cdot b$$

$$406 = 4 \cdot 87 + 58 \quad \text{so } 58 = 1 \cdot 406 - 4 \cdot 87$$

$$= 5 \cdot a + (-9) \cdot b$$

$$87 = 1 \cdot 58 + 29 \quad \text{so } 29 = 1 \cdot 87 - 1 \cdot 58$$

$$= -6 \cdot a + 11 \cdot b$$

$$58 = 2 \cdot 29 + 0$$

done,  $\text{gcd} = 29$

the Pulverizer  $s = -6$ ,  $t = 11$



Albert R Meyer

March 6, 2015

pulverizer.11

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

## Finding $s > 0$ and $t$

$$\text{gcd}(899, 493) = -6 \cdot 899 + 11 \cdot 493$$

get positive coeff. for 899?:

$$= (-6 + 493k) \cdot 899 + (11 - 899k) \cdot 493$$

let  $k$  be 1:

$$= 487 \cdot 899 - 888 \cdot 493$$



Albert R Meyer

March 6, 2015

pulverizer.12

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

**Pulverizer is efficient**  
Same number of transitions as  
Euclid



Albert R Meyer

March 6, 2015

pulverizer.13

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

**Pulverizer is efficient**  
Same number of transitions as  
Euclid, a few more adds/mults  
per transition.  
So halts after at most  
 $10\log_2 b$  operations



Albert R Meyer

March 6, 2015

pulverizer.14