Mathematics for Computer Science

MIT 6.042J/18.062J

GCD's & linear combinations: The Pulverizer

GCD is a linear combination

Theorem:

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

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

GCD is a linear combination

Corollary:

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

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

Proof: Show how to find coefficients s,t.

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

Extending Euclid

In Euclid have

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

Track coeff's c,d,e,f

$ca+db= x$ and $ea+fb= y$

Extending Euclid

In Euclid have

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

Track coeff's c,d,e,f

$ca+db= x$ and $ea+fb= y$

to start:

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

Extending Euclid

In Euclid have

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

Track coeff's c,d,e,f

$ca+db= x$ and $ea+fb= y$

to start:

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

Extending Euclid

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

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

$$x-qy =$$

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

Extending Euclid

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

$$y_{next} = rem(x,y) = x-qy = (c-qe)a+(d-qf)b$$

Finding s and t

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

$899 = 1\cdot 493 + 406$	so $406 = 1\cdot a + -1\cdot b$
$493 = 1\cdot 406 + 87$	so $87 = 1\cdot b - 1\cdot 406$
	$= -1\cdot a + 2\cdot b$
$406 = 4\cdot 87 + 58$	so $58 = 1\cdot 406 - 4\cdot 87$
	$= 5\cdot a + -9\cdot b$
$87 = 1\cdot 58 + 29$	so $29 = 1\cdot 87 - 1\cdot 58$
	$= -6\cdot a + 11\cdot b$
$58 = 2\cdot 29 + 0$	
	done, gcd = 29

Finding s and t

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

$899 = 1\cdot 493 + 406$	so $406 = 1\cdot a + -1\cdot b$
$493 = 1\cdot 406 + 87$	so $87 = 1\cdot b - 1\cdot 406$
	$= -1\cdot a + 2\cdot b$
$406 = 4\cdot 87 + 58$	so $58 = 1\cdot 406 - 4\cdot 87$
	$= 5\cdot a + -9\cdot b$
$87 = 1\cdot 58 + 29$	so $29 = 1\cdot 87 - 1\cdot 58$
	$= -6\cdot a + 11\cdot b$
$58 = 2\cdot 29 + 0$	
	done, gcd = 29

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

Finding s>0 and t

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

get positive coeff. for 899?:

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

let k be 1:

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

Pulverizer is efficient

Same number of transitions as Euclid

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