

Returning to the GCD

P Our previous algorithm for finding the gcd of two integers required us to find the prime factorization of each of those integers

P That can be a hard step

P We want to consider an algorithm for finding the gcd that does not require that step

Some Observations about Common Divisors

P What is $\gcd(43, 44)$?

P What is $\gcd(50, 52)$?

P What is $\gcd(8331, 8333)$?

P What is $\gcd(1420, 1426)$?

P Some helpful theorems:

< Theorem: if $d \mid a$ and $d \mid b$, then $d \mid (a + b)$

< Theorem: if $d \mid a$ and $d \mid b$, then $d \mid (a - b)$

< Theorem: if $d \mid a$ and $d \mid b$, then $d \mid (as + bt)$ for any integers s and t

A Proof

P Theorem: if $d \mid a$ and $d \mid b$, then $d \mid (a + b)$

P Proof:

< If $d \mid a$, then $a = kd$ for some $k \in \mathbb{Z}$

< If $d \mid b$, then $b = ld$ for some $l \in \mathbb{Z}$

< Then we can write $(a + b)$ as $(kd + ld) = d(k + l)$

< Which means $a + b$ is a multiple of d

< Which implies $d \mid (a + b)$

P Let's find $\gcd(133, 98)$ with our new ideas

The Euclidean Algorithm

The Euclidean algorithm for finding greatest common divisors is just an iteration of that simple observation

$$< 133 = 1 \times 98 + 35$$

$$< 98 = 2 \times 35 + 28$$

$$< 35 = 1 \times 28 + 7$$

$$< 28 = 4 \times 7 + 0$$

P The last non-zero remainder gives the gcd

Another Example

PFind the gcd(412, 1423)

$$< 1423 = 3 \times 412 + 187$$

$$< 412 = 2 \times 187 + 38$$

$$< 187 = 4 \times 38 + 35$$

$$< 38 = 1 \times 35 + 3$$

$$< 35 = 11 \times 3 + 2$$

$$< 3 = 1 \times 2 + \boxed{1}$$

$$< 2 = 2 \times 1 + 0$$

PSo these numbers are relatively prime

Your Turn

PFind gcd(412, 56)

$$< 412 = 7 \times 56 + 20$$

$$< 56 = 2 \times 20 + 16$$

$$< 20 = 1 \times 16 + 4$$

$$< 16 = 4 \times 4 + 0$$

< So 4 is the gcd

PFind gcd(144, 233)

$$< 233 = 1 \times 144 + 89$$

$$< 144 = 1 \times 89 + 55$$

$$< 89 = 1 \times 55 + 34$$

$$< 55 = 1 \times 34 + 21$$

$$< 34 = 1 \times 21 + 13$$

<

$$< 21 = 1 \times 13 + 8$$

$$< 13 = 1 \times 8 + 5$$

$$< 8 = 1 \times 5 + 3$$

$$< 5 = 1 \times 3 + 2$$

$$< 3 = 1 \times 2 + 1$$

$$< 2 = 2 \times 1 + 0$$

<