

Some Observations about Common Divisors

- What is $\gcd(43, 44)$?
- What is $\gcd(50, 52)$?
- What is $\gcd(8331, 8333)$?
- 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
- What is $\gcd(133, 98)$?

A Proof

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

- < $133 = 1 \times 98 + 35$
- < $98 = 2 \times 35 + 28$
- < $35 = 1 \times 28 + 7$
- < $28 = 4 \times 7 + 0$

- The last non-zero remainder gives the gcd

Another Example

- Find the $\gcd(412, 1423)$

- < $1423 = 3 \times 412 + 187$
- < $412 = 2 \times 187 + 38$
- < $187 = 4 \times 38 + 35$
- < $38 = 1 \times 35 + 3$
- < $35 = 11 \times 3 + 2$
- < $3 = 1 \times 2 + 1$
- < $2 = 2 \times 1 + 0$

- So these numbers are relatively prime

Your Turn

- Find 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

- Find gcd(144, 233)

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

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

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

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

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

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

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

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

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

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

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

Congruence

- Believe it or not, the idea of the remainder is very important, and is used in many contexts
- It is so important, that we have a whole new definition related to it:
- Two integers a and b are called *congruent* (mod m) if they leave the same remainder when divided by m . This is written $a/b \pmod{m}$
 - T F $14 / 40 \pmod{13}$
 - T F $33 / 76 \pmod{20}$
 - T F $-4 / 34 \pmod{19}$

Congruence Classes

- Given a modulus m , the set of possible remainders modulo that modulus is $\{0, 1, \dots, m-1\}$
- If you pick an integer n , then we can consider the set of all integers which are congruent to n
- This is called the *congruence class* of $n \pmod{m}$

$$= \{x \in \mathbb{Z} \mid x \equiv n \pmod{m}\}$$
- For example, the congruence class of $13 \pmod{5}$ is $\{\dots, -17, -12, -7, -2, 3, 8, 13, 18, \dots\}$



There are m congruence classes modulo m , and any two integers in the same class are congruent (mod m)

Another Definition of $a/b \pmod{m}$



Any two integers in the same class are congruent (mod m)

- From the picture above, can you think of another way to say that two integers are in the same congruence class? (That is, that they have the same color)
- For example, will 104 and 123 have the same color?
- Theorem: $a/b \pmod{m} \iff m \mid (b-a)$

$a \bmod m$

- There is one other usage of the “mod” notation
- When you see the expression $a \bmod m$, (without the “/” symbol) then it refers to the remainder when a is divided by m
- For example:
 - < $100 \bmod 4 = 0$
 - < $21 \bmod 5 = 1$
 - < $3 \bmod 14 = 3$
 - < $-2 \bmod 7 = 5$