

Relatively Prime

- P Two integers a and b are called *relatively prime* if $\gcd(a, b) = 1$
- P That is, they are relatively prime if they have no non-trivial common divisor
- P Which integers from 1 to 10 are rel. prime to 10?
▶ 1, 3, 7, 9
- P We define the *phi-function* $\phi(n)$ to be the number of integers in the range $\{1, 2, \dots, n\}$ which are relatively prime to n
▶ Everyone: Find $\phi(30)$

The Division Algorithm

- P Sometimes $a \mid b$, and sometimes it doesn't.
- P If $a \nmid b$ (a does not divide b), then the division $b \div a$ leaves some remainder, r
- P Suppose we go around dividing integers by 6 and looking at the remainders. What remainders are given by each of the following:
▶ 1, 2, 3, 4, 5, ..., 29, 30?
- P The division algorithm says this: Whenever we divide one integer by another, we get a quotient and a remainder
▶ But what do you think we should say about that remainder?

The Division Algorithm

The Division Algorithm:

Given an integer n and a positive integer d , we can divide n by d to get a quotient q and a remainder r such that:

$$\begin{aligned}n &= qd + r \\ 0 &\leq r < d\end{aligned}$$

- P Use the division algorithm to:
- ▶ divide 30 by 7
 - ▶ divide 100 by 9
 - ▶ divide -84 by 20
 - ▶ divide -100 by 9

Congruence

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

Congruence Classes

P Given a modulus m , the set of possible remainders modulo that modulus is $\{0, 1, \dots, m - 1\}$

P If you pick an integer n , then we can consider the set of all integers which are congruent to n

P This is called the *congruence class* of $n \pmod{m}$
▶ $= \{x \in \mathbb{Z} \mid x \equiv n \pmod{m}\}$

P 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 \pmod{m}

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



Any two integers in the same class are congruent \pmod{m}

P 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)

P For example, will 104 and 123 have the same color?

P Theorem: $a \equiv b \pmod{m} \leftrightarrow m \mid (b - a)$

$a \bmod m$

P There is one other usage of the “mod” notation

P When you see the expression $a \bmod m$, (without the “ \equiv ” symbol) then it refers to the remainder when a is divided by m

P For example:

- ▶ $100 \bmod 4 = 0$
- ▶ $21 \bmod 5 = 1$
- ▶ $3 \bmod 14 = 3$
- ▶ $-2 \bmod 7 = 5$

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