

Relatively Prime

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

The Phi-Function

- For prime p , $N(p) = p - 1$
< True
- What is the value of $N(p^2)$ (again, for prime p)?
- Conjecture: $N(ab) = N(a)N(b)$
< Wouldn't this be nice?
 - $N(30)$
 - $N(3)N(10)$
 - $N(3)N(5)N(2)$
 - $2 \cdot 4 \cdot 1$
 - 8
- But is it always true? If not, then *when* is it true?
- Work in groups to figure this out... Quiz 4

The Division Algorithm

- Sometimes $a \mid b$, and sometimes it doesn't.
- If $a \nmid b$ (a does not divide b), then the division $b \div a$ leaves some remainder, r
- 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?
- 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:

$$n = qd + r$$

$$0 \leq r < d$$

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

Returning to the GCD

- Our previous algorithm for finding the gcd of two integers required us to find the prime factorization of each of those integers
- That can be a hard step
- We want to consider an algorithm for finding the gcd that does not require that step

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