

Integers

- These are the integers: $\{\dots, -3, -2, -1, 0, 1, 2, \dots\}$
- These are the natural numbers: $\{0, 1, 2, \dots\}$
- We will be concerned at first with the divisibility properties of the integers and natural numbers

Multiple

- 10 is a multiple of 2
- 21 is a multiple of 7
- 100 is a multiple of 10
- 42 is a multiple of -6
- -90 is a multiple of 15
- -20 is a multiple of -4

- In general, given two integers a and b , we say b is a *multiple* of a if $b = ma$ for some integer m .

Divides

- | | |
|---------------------|-----------------|
| ▪ 4 divides 20 | ▪ $4 \mid 20$ |
| ▪ 10 divides 100 | ▪ $10 \mid 100$ |
| ▪ -9 divides 81 | ▪ $-9 \mid 81$ |
| ▪ 6 divides -30 | ▪ $6 \mid -30$ |
| ▪ 1 divides 7 | ▪ $1 \mid 7$ |
| ▪ -1 divides -8 | ▪ $-1 \mid -8$ |
- In general, we say that a *divides* b if b is a multiple of a . This is written: $a \mid b$

Factors and Divisor

- If a and b are integers, and a divides b , then we call a a *factor* of b
- “divisor” and “factor” mean the same thing
- Can you list all factors of 10?
< $-10, -5, -2, -1, 1, 2, 5, 10$
- Can you list all positive factors of 20?
< 1, 2, 4, 5, 10, 20
< Can you see why you need only the first half of that list?
< Will there always be an even number of factors?
- Can you list all the positive factors of 36?
< 1, 2, 3, 4, 6, 9, 12, 18, 36

Prime Numbers

- An integer p greater than 1 is called *prime* if its only positive divisors are 1 and p
- Which of the following are prime:
< 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17
- A *prime factor* is a factor which is prime
< What are the prime factors of 60?
< 2, 3 and 5
- The *prime factorization* of an integer n is an expression of n as the product of primes
< $100 = 2 \cdot 2 \cdot 5 \cdot 5$
< $99 = 3 \cdot 3 \cdot 11$

Greatest Common Divisor

- Reduce the fraction: $30/100$
- Reduce the fraction: $18/33$
- Given two integers a and b , we call the greatest divisor common to both a and b their *greatest common divisor*, denoted $\gcd(a, b)$.
- $\gcd(30, 100) = 10$
- $\gcd(18, 33) = 3$
- $\gcd(20, 60) =$
< 20
- $\gcd(105, 154) =$
< 7

Prime Factorization and gcd

- We can easily find the gcd of two integers given their prime factorizations:
< $a = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 \cdot 11 \cdot 19 \cdot 41 \cdot 47$ (= 604114500)
< $b = 2 \cdot 5 \cdot 5 \cdot 11 \cdot 41 \cdot 101 \cdot 103$ (= 234587650)
- We consider the greatest amount of each prime factor that they have in common
- The product of these prime factors gives the greatest common divisor
< $\gcd = 2 \cdot 5 \cdot 5 \cdot 11 \cdot 41$ (= 22550)
- This gives us an algorithm for determining the gcd of two integers, assuming we can find prime factorizations.

Our algorithm for finding gcd

- Find $\gcd(19841693512938, 189341078342178)$
< Do you want to find the prime factorizations of those two numbers?
< $(2) \cdot (3) \cdot (11) \cdot (41) \cdot (42139) \cdot (174007)$
< $(2) \cdot (3) \cdot (7) \cdot (23) \cdot (103) \cdot (1902963661)$
- How would you decide that 1,902,963,661 is prime?
< Can you come up with an algorithm for deciding this?
< Would your algorithm work on
1389417289417832798974189341892378192741843197?
- Thus, our gcd algorithm is not very good. We will find a better one on Thursday

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 $N(30)$

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 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