Primes & GCD

We've discussed divisibility before. An integral part of divisibility is prime numbers.

Def $p \in \mathbb{N}$ is <u>prime</u> iff $p > 1$ & if $k \mid p$ then $k = 1, p$.

If $p \in \mathbb{N}$ is <u>not</u> prime it is called <u>Composite</u>.

<u>Ex</u>: 7 is prime, no number $2, \ldots, 6$ divides 7.

9 is composite, $3 \mid 9$.

Fundamental Theorem of Arithmetic

<u>Theorem</u>: Every integer greater than 1 can be written uniquely as a prime or as the product of 2 or more primes, where primes are written in non decreasing order.

<u>Ex</u>: $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 5^2$

$107 = 107$

$2700 = 2 2 \cdot 3 \cdot 3 \cdot 3 \cdot 5 5 = 2^2 \cdot 3^3 \cdot 5^2$

$128 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2$

Prime numbers are very important in cryptography. Thus we need ways to determine when numbers are prime.

<u>Theorem</u>: If n is a composite number then n has a prime divisor less than or equal to $\sqrt{n}$.

<u>pf</u>: If n is Composite, we know it has a factor, say a. So we can write $n = a \cdot b$ & we know $1 < a < n$ $b \in \mathbb{N}$ $b > 1$.

If $a > \sqrt{n}$ & $b > \sqrt{n}$ then $ab > \sqrt{n} \cdot \sqrt{n} = n$. Thus at least one of a & b must be less than $\sqrt{n}$. Thus n has a <u>factor</u> less than $\sqrt{n}$.

AWLOG $a < \sqrt{n}$. If a is prime done, otherwise we can factor a into primes w/ fundamental thm of Arith. $\square$

Ex: prove 101 is prime

pf $\sqrt{101} \approx 10$ primes less than $\sqrt{101}$ = 2, 3, 5, 7

$2, 3, 5, 7 \nmid 101$ So 101 must be prime.

$\square$

Prime factorizations are also important, so we discuss some methods here.

Ex: Find the prime factorization of 3692

We begin by dividing by primes:

$\frac{3692}{2} = 1846$

$\frac{1846}{2} = 923$

$2, 3, 5, 7, 11 \nmid 923$

$\frac{923}{13} = 71$

71 is prime.

Thus $3692 = 2^2 \cdot 13 \cdot 71$.

This method of factoring requires a list of primes. There are many ways to generate a list. A popular way is via the Sieve of Eratosthenes.

(Era - toss - then os)

First you choose how large you want your list to be. Say we want all primes less than 35.

~~1~~	$\boxed{2}$	$\boxed{3}$	~~4~~	$\boxed{5}$	~~6~~	$\boxed{7}$
~~8~~	~~9~~	~~10~~	$\boxed{11}$	~~12~~	$\boxed{13}$	~~14~~
~~15~~	~~16~~	$\boxed{17}$	~~18~~	$\boxed{19}$	~~20~~	~~21~~
~~22~~	$\boxed{23}$	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~
$\boxed{29}$	~~30~~	$\boxed{31}$	~~32~~	~~33~~	~~34~~	~~35~~

Then 1 is marked not prime.

The procedure is as follows: the next unmarked number (2) is prime. Mark all multiples as not-prime.

repeat

This is very easy to program

(You should try it now! possibly helpful for project)

Some primes have particular names: primes of the form $2^k - 1$ are called Mersenne primes, & are useful for crypto.

We only know of 49 Mersenne primes, largest: $2^{74,207,281} - 1$

We know there are infinitely many primes, but how common are they?

Theorem: The number of primes less than $n \approx \frac{n}{\ln n}$.

Greatest Common divisors:

Def: Let $a, b \in \mathbb{Z}$ a, b not both 0. The largest integer d s.t. $d | a$ & $d | b$ is called the greatest common divisor of a & b. Denoted $\gcd(a,b)$ or (a,b).

Ex What is $\gcd(18, 24)$?

Divisors of 18: 1, 2, 3, 6, 9, 18

Divisors of 24: 1, 2, 3, 4, 6, 8, 12, 24 ← ever play that make 24 game in elementary school?

Draw 4 cards use any operations to make 24.

e.g. 1, 1, 4, 4

$(4+1+1) \cdot 4 = 24$

$\gcd(18, 24) = 6$.

Def: The integers a,b are relatively prime if $\gcd(a,b) = 1$.

Embarrassing relatively prime story.

A common method to find $\gcd(a,b)$ is to find the prime factorizations of both:

$a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$

$b = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$

then $\gcd(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_k^{\min(a_k,b_k)}$