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 larger 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.

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

e.g. 1, 1, 4, 4
$(4+4)\cdot 4 = 24$

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!

$a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$
$b = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_2}$

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

Ex: $\gcd(120, 500)$.

$120 = 2^3 \cdot 3 \cdot 5 \qquad 500 = 2^2 \cdot 5^3$

$\gcd(120,500) = 2^{\min(3,2)} \cdot 3^{\min(1,0)} \cdot 5^{\min(1,3)}$

$= 2^2 \cdot 3^0 \cdot 5$

$= 20$

Euclidean Algorithm: However the efficient way to find $\gcd(a,b)$ is the Euclidean algorithm.

Ex: $\gcd(91, 287)$

$287 = 91 \cdot 3 + 14$ note if $k \mid 287$ & $k \mid 91$ then $k \mid 3 \cdot 91$ & $k \mid 287 - 3 \cdot 91$ (14). Similarly any divisor of 91 & 14 divides 287!

$91 = 14 \cdot 6 + 7$ ← gcd

$14 = 7 \cdot 2 + 0$ ← stop

$\Rightarrow \gcd(91, 287) = 7.$

proof of this method in book.

$\gcd(a,b)$:

```
x = a
y = b
while y ≠ 0
    r = x mod y
    x = y
    y = r
return x.
```

Bézout's Theorem: If $a, b \in \mathbb{Z}^+$ $\exists\, s, t \in \mathbb{Z}$ s.t. $\gcd(a,b) = s \cdot a + b \cdot t$.

Can use an extended version of gcd alg to find s, t.

This is exactly the same as those problems from elementary math:

Can you get 6 gallons of water from a 5 gallon & 2 gallon jug?

[Fill 5 gallon, Pour into 2 gallon, empty, Pour into 2 gallon, what is in 5 gallon is 1 gallon. Put in two gallon, refill 5 gallon 1+5 = 6.