Prime Numbers

And a bit of modular arithmetic, maybe defining the rationals

Recall

- p is prime if $p>1$ & its only divisors are 1 & p

Fact

1. if p is prime & $p \mid ab$, then $p \mid a$ or $p \mid b$
2. There are infinitely many primes

Proof: Suppose, by way of contradiction, that there are only finitely many primes, say $p_1, p_2, \dots, p_n$

Let $p = p_1 \cdot p_2 \cdot p_3 \cdot \dots \cdot p_n + 1$

claim: p is prime (this gives the contradiction since $p > p_k$ for all k)

$p_k \nmid p$ for all $k = 1, \dots, n$ since otherwise:

$p_k \mid (p - p_1 \cdot p_2 \cdot \dots \cdot p_n)$ ie $p_k \mid 1$ (contradiction b/c $p_k \neq 1$)

- if $p_1, \dots, p_n$ is a list of all the primes then p must be composite but then some prime must divide p...

Proposition: Suppose n is a positive integer ($\neq 1$), then n can be written as a product of prime numbers

Proof: By induction on $n \geq 2$

Base step: ($n=2$)

2 is prime & $2=2$ is its own product

Induction hypothesis: ($n=k$)

Every m with $2 \leq m \leq k$ can be written as a product of primes

Inductive Step: ($n=k \Rightarrow n=k+1$)

Suppose $n=k+1$ then either

a) $n=k+1$ is prime

→ in which case we're done

or

b) $n=k+1$ is not prime

→ ie $n = k+1 = c \cdot d$ for some c & d such that $1 < c < n$ & $1 < d < n$

In this case, c & d are both products of primes by the induction hypothesis

→ & so $n = k+1 = cd$ can also be written as a product of primes (multiply the products for c & d together)

∴ by induction... //

Modular Arithmetic

Arithmetic "mod n" ($n \geq 2$)

- Define $\equiv_n$ by $a \equiv_n b$ if $n \mid (b-a)$

$\mathbb{Z}_n = \{ [a]_{\equiv n} \mid a \in \mathbb{Z} \}$

$[a]_{\equiv n} + [b]_{\equiv n} = [a+b]_{\equiv n}$ & $[a]_{\equiv n} \cdot [b]_{\equiv n} = [ab]_{\equiv n}$ etc...

- in practice, we work with $0, 1, 2, \dots, n-1$ & roll over to 0 @ n

Fact

1. Suppose $n = d_k d_{k-1} \dots d_1 d_0$ is the decimal version of $n > 0$ (i.e. $n = d_k 10^k + d_{k-1} 10^{k-1} + \dots + d_1 10^1 + d_0$)

→ then: $3 \mid n \iff 3 \mid (d_k + d_{k-1} + \dots + d_1 + d_0)$

→ Ex: what is $3 \mid 1125$?

$3 \mid (1+1+2+5)$

$\parallel$

9

Proof: $3 \mid n \iff n \equiv 0 \pmod 3$ (i.e. $[n]_{\equiv_3} = [0]_{\equiv_3}$)

$\iff d_k 10^k + d_{k-1} 10^{k-1} + \dots + d_1 10^1 + d_0 10^0 \equiv 0 \pmod 3$

$\iff d_k 1^k + d_{k-1} 1^{k-1} + \dots + d_1 1^1 + d_0 1^0 \equiv 0 \pmod 3$ since $10 \equiv 1 \pmod 3$

$\iff d_k + d_{k-1} + \dots + d_1 + d_0 \equiv 0 \pmod 3$

$\iff 3 \mid (d_k + d_{k-1} + \dots + d_1 + d_0)$