Primes

Def: A prime p is an integer > 1, with no positive integer divisors except 1 and p.

$$2, 3, 5, 7, 11, 13, 17, \ldots$$

Theorem 3.1

Assume theorem holds for all m, $2 \leq m < k$

If k is not prime,

$$k = k_1 k_2, \quad 1 < k_1, k_2 < k$$

So by assumption k_1, k_2 both ~~factor~~ are prime, or factor into products of primes.

say $k_1 = p_1 \cdots p_r$, $k_2 = q_1 \cdots q_s$, primes p_i, q_i

Then $k = p_1 \cdots p_r q_1 \cdots q_s$.

So k is a product of primes, and the theorem holds for k.

So by strong induction, theorem true for all $n \geq 2$. $\blacksquare$

eg $100 = 2^2 \cdot 5^2$

Theorem 3.2

There are infinitely many primes

Proof: This is a proof by contradiction. So let's assume there are only finitely many primes, and the complete list is

$$p_1, p_2, p_3, \ldots\ldots, p_N.$$

Then consider the integer

$$M = (p_1 p_2 p_3 \cdots p_N) + 1.$$

Apply Th. 3.1 to M. But M can't be prime, as $M > p_i$, for $1 \le i \le N$.

So therefore M can be expressed as the product of some of the p_i (maybe with ~~repetitions~~ repetitions).

So M has at least one prime factor, call it p_j, for some $1 \le j \le N$.

Then notice that

$$1 = M - (p_1 p_2 \overset{p_j}{\cdots} p_N)$$

$\Rightarrow$ $p_j \mid 1$, since $p_j \mid M$, and $p_j \mid (p_1 \cdots p_N)$

and by theorem 2.1 (3) divisibility of lin. combs.

$\Rightarrow \{p_j = 1\}$, as 1 is the only pos. divisor of 1.

This contradicts the definition of prime number.

So our assumption at the start is wrong, so there are infinitely many primes.

Can also look at this in an algorithmic way as an algorithm to produce an infinite list of primes.

- Start with $\underbrace{2, 3, 5}$
- Take their product and add 1

$$2 \cdot 3 \cdot 5 + 1 = 31$$

By theorem 3.1, 31 is either prime or has prime divisors, and by the argument in 3.2, these primes will be new

- Add these to ~~the~~ the list 2, 3, 5, 31

Lemma 3.4 Euclid's Lemma

$\boxed{\begin{array}{l}\text{Let } a, b, p \in \mathbb{Z}, \text{ with } p \text{ prime.} \\ \text{If } p \mid ab \text{ then } p \mid a \text{ or } p \mid b.\end{array}}$

eg. $3 \mid 36 = 4 \cdot \underline{9}$ and $3 \mid 9$

$4 \mid 36 = \underline{2} \cdot \underline{18}$ and $4 \nmid 2$ and $4 \nmid 18$

Proof (not relying on prime factorisations)

Let's assume $p \mid ab$, ie. $ab = \alpha p$, $\alpha \in \mathbb{Z}$.

"A or B" $\equiv$ "$A \vee B$" $\equiv$ "$(\neg A) \Rightarrow B$"

We also assume $\boxed{p \nmid a.}$

Then $\gcd(p, a) = 1$ since p is a prime

And by Euclid's algorithm we can find a Bezout's Identity

$$1 = np + ma, \quad \text{for some integers } n, m$$

$$\Rightarrow b = npb + m\underline{ab}$$

$$\Rightarrow b = \underbrace{(nb + m\alpha)}\, p$$

$$\Rightarrow \boxed{p \mid b.}$$

So $p \mid a$ <u>or</u> $p \mid b$. ∎

<u>Corollary</u> $p \mid a_1 \cdots a_n$

then $p \mid a_i$, for at least one $1 \le i \le n$

Can prove this by induction using lemma.

Proof of the F.T.A.

Again by strong induction.

So assume FTA for every integer k, $\boxed{1 < k < n}$. Now we'll prove it for n.

Suppose $n = p_1 \cdots p_r = q_1 \cdots q_s$ which are two prime factorisations with primes p_i, q_i

Clearly $p_1 \mid n$.

$\Rightarrow p_1 \mid (q_1 \cdots q_s)$

by corollary $p_1 \mid q_j$, for some $1 \le j \le s$

Can assume that $p_1 | q_1$ (by relabelling if necessary).

$\implies p_1 = q_1$, since both are prime.

Now consider

$$\frac{n}{p_1} = p_2 \dots p_r = q_2 \dots q_s \quad (*)$$

But $\boxed{1 \leq \frac{n}{p_1} < n}$

So by assumption the ~~factor~~ two factorizations in $(*)$ are the same so $r = s$, $p_i = q_i$ for $2 \leq i \leq s$.

$$\implies n = p_1 \dots p_r = \overset{\overset{p_1}{\shortparallel}}{q_1} \dots q_s$$

So these two prime factorisations

are the same also.

$\boxed{\text{So the FTA holds for } n.}$

So by strong induction F.T.A. holds for all integers. ∎

Prime factorizations will be quite useful. Sometimes called the canonical form of integer n

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} = \prod_{i=1}^{r} p_i^{\alpha_i}$$

for the primes p_i in increasing order.

<u>Ex 3.1</u> Can we judge gcd and l.c.m. of a, b from their canonical forms.

$a = 11340 = 2^2 \cdot 3^4 \cdot 5 \cdot 7$

$b = 990 = 2 \cdot 3^2 \cdot 5 \cdot 11$

$\gcd(a, b) = 2 \cdot 3^2 \cdot 5 =$

$\operatorname{lcm}(a, b) = 2^2 \cdot 3^4 \cdot 5 \cdot 7 \cdot 11 =$

$\hookrightarrow$ least integer, that is a multiple of a and b.

In a sense, the gcd (a,b) is the intersection of two prime factorizations.

lcm (a,b) is the union of the two factorizations.

FTA $\Rightarrow$ Existence of irrationals.

<u>Theorem</u> $\sqrt{2}$ is Irrational.

<u>Proof</u> By contradiction.

Assume $\sqrt{2} = \frac{a}{b}$, $\underline{\underline{a, b \in \mathbb{Z}}}$.

and assume $\gcd(a, b) = 1$

$\Rightarrow \quad b\sqrt{2} = a$

$\Rightarrow b^2 \cdot 2 = a^2$

$\Rightarrow b \mid a^2$

Either $b = 1$ or $b > 1$

If $b = 1$ then $2 = a^2$, clearly false.

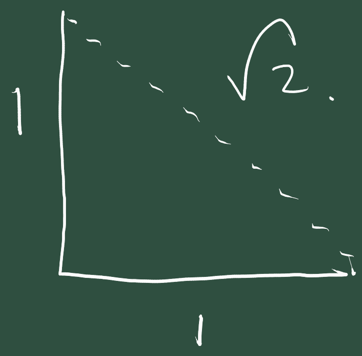
So $b > 1$, so it has a prime factor p.

$p \mid b$

$\Rightarrow p \mid a^2$, by transitivity

$\Rightarrow p \mid a$, by Euclid's Lemma.

This contradicts the fact that $\gcd(a, b) = 1$. so $\sqrt{2}$ cannot be expressed as $\frac{a}{b}$, $a, b \in \mathbb{Z}$.



This argument can be generalised to:

Theorem 3.6.

Given any integer $n \in \mathbb{Z}$.

Either $\sqrt{n}$ is an integer.

or $\sqrt{n}$ is irrational.

For large x, $\pi(x) =$ # primes $\leq x$, asymptotically behaves like

$$\pi(x) \sim \frac{x}{\log x}.$$

Twin Prime conjecture.

Twin primes are pairs,

$p, p+2$ both of which are

prime

eg. $(5,7)$, $(11,13)$, $(29,31)$

, ...

<u>many</u> of these have been found

and conjectured that there are

infinitely many.

However we can prove that

there exist arbitrarily large

gaps between consecutive primes.

i.e. for any integer N we can

find a run of at least
N consecutive composite
numbers.

Idea: Use the factorial to
find a location where
the composites begins.
run of

Consider $M = (N+1)! = (N+1)N(N-1)\ldots 4\cdot 3\cdot 2\cdot 1$

M is composite.

$M+1$ is ?

$\boxed{M+2}$ is composite as $2 \mid M$

$M+3$ is composite $3 \mid M$

$M+4$ is composite $4 \mid M$

$\vdots$

$\vdots$

$M+(N+1)$ is composite $(N+1) \mid M$

This is a run of N consecutive integer.