Primes

Def 3.1 An integer p is prime if $p > 1$ and the only positive divisors of p are 1 and p.

If n is not prime it is called composite.

The primes

$2, 3, 5, 7, 11, 13, 17, 19,$

$23, \ldots$

Theorem 3.1 Every integer $n \geq 2$ factors as a product of primes.

Proof (using strong induction)

To prove $\forall n \geq 1 \; P(n)$ it is to show that $\forall n \geq 1$

$$\left(\forall 0 < k < n \; P(k) \right) \Rightarrow P(n)$$

Then we have shown $\forall n \geq 1 \; P(n)$.

Assume theorem holds $\forall \; 2 \leq m < k$

Consider k. Maybe it's prime.

If not $k = k_1 k_2$ for two integers

$2 \leq k_1, k_2 < k$.

So k_1 & k_2 factor into primes.

Concatenate these factorizations

to give a factorization of k.

So by the principle of strong induction the theorem is true.

F.T.A. adds the uniqueness condition to this theorem

200

2×100 4×50 8×25

40×5

10×20

<u>Theorem 3.2</u> There are an infinite number of prime integrs.

<u>Proof</u> (Proof by contradiction).
Assume there are only a finite number. Let's say they are the primes

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

Consider the large integer M

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

$$= \left(\prod_{i=1}^{N} p_i \right) + 1.$$

Think of what theorem 3.1 says of M.

M is not prime since it is greater than all the p_i. Therefore M factors into primes.

So for some j, $1 \le j \le N$, we can say

$$p_j \mid M.$$

Consider

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

By theorem 2.1 part (3) "divisibility of linear combinations"

$$\therefore \quad p_j \mid 1.$$

$$\Rightarrow \boxed{p_j \le 1}$$

Contradicts the definition of prime. ($p > 1$)

So the assumption at the beginning is false, and therefore there are an infinite numbers of prime numbers. $\blacksquare$

Lemma **Euclid's Lemma**

Let $a, b \in \mathbb{Z}$ and p a prime.

$$p \mid ab \Rightarrow (p \mid a \text{ or } p \mid b).$$

This is **not** true of composite numbers.

$$25 \mid 200$$

ie $25 \mid 10 \times 20$ But $25 \nmid 10$ and $25 \nmid 20$.

$5 \mid 10 \times 20$ and $5 \mid 10$, $5 \mid 20$

Proof Assume $p \mid ab$.

$$A \text{ or } B \equiv A \vee B \equiv ((\neg A) \Rightarrow B)$$

So we will prove that

$$p \nmid a \Rightarrow p \mid b.$$

Assume $p \nmid a$.

Therefor $\gcd(p, a) = 1$

So there exists a Bezout identity, i.e. $\exists \; n, m \in \mathbb{Z}$.

$$np + ma = 1.$$

$$\Rightarrow \cancel{bnp}\; npb + mab = b.$$

$\Rightarrow p \mid b$, as p divides both terms on the left.

Therefore $p \mid a$ or $p \mid b$ as required.

12:05

By induction we can prove

Corollary

$p \mid (a_1 \cdots a_n) \Rightarrow p \mid a_i$ for at least one $1 \leq i \leq n$.

Proof of the F.T.A.

We just need to prove uniqueness. Use strong induction. So assume F.T.A. is true for all $1 < k \leq n$.

Suppose

$n = p_1 \cdots p_r = q_1 \cdots q_s \quad (*)$

where p_i, q_i are primes. and

$r, s \geq 1$, ie. n factors into potentially two different collections of prime factors.

Clearly $p_1 \mid n$.

$\Longrightarrow \quad p_1 \mid (q_1 \cdots q_s)$

$\Longrightarrow \quad p_1$ divides a least one q_j
$1 \leq j \leq s$.

Without loss of generality we can assume that $j = 1$,

ie. $p_1 \mid q_1$. ie. $p_1 = q_1$

Consider $\quad n_1 = n/p_1 = n/q_1$

$$n_1 = p_2 \cdots p_r = q_2 \cdots q_s$$

But $\quad n_1 < n$.

and by our induction assumption F.T.A. applies to n_1, ie. n_1 has a unique prime factorisation.

$\Rightarrow$ (WLOG)

$$p_i = q_i \quad \text{and} \quad r = s$$

for $1 \le i \le r = s$.

$\Rightarrow$ The two factorisations in $(*)$ are exactly the same.

Therefore by the principle of strong induction the F.T.A is true for all $n > 1$ $\blacksquare$

<u>Def 3.2</u>. We often write a general prime factorisation / canonical form as

$$n = \prod_{i=1}^{r} p_i^{\alpha_i}$$

and $p_1, \ldots, p_r$ are distinct primes.

Ex 3.1 Consider the example.

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

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

$$\gcd(11340, 990) = 2 \cdot 3^2 \cdot 5 = 90$$

$$\mathrm{lcm}(11340, 990) = 2^2 \cdot 3^4 \cdot 5 \cdot 7 \cdot 11$$

So in effect the $\gcd(a,b)$ is the intersection of their factorisations. The $\mathrm{lcm}(a,b)$ is the union of their factorisations.

A second application of the FTA is in proving the existence of irrational numbers.

Theorem 3-6

For any integer n

$\sqrt{n}$ is either an integer

or irrational

Eg $\sqrt{2}$. is not an integer.

So suppose $\sqrt{2}$ is rational.

ie. $\exists\ a, b \in \mathbb{Z}$.

$$\sqrt{2} = \frac{a}{b}$$

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

$\Longrightarrow \sqrt{2}\,b = a$

$\Longrightarrow 2b^2 = a^2$

$\Longrightarrow b \mid a^2$

Case 1. $b=1$

Case 2 = $b>1$.

$\Rightarrow \sqrt{2} = a \in \mathbb{Z}$.

clearly fase.

So $b > 1$. and by the FTA has a prime factor p.

so $p \mid b$

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

$\Rightarrow p \mid a$,

So $p \mid b$ and $p \mid a$

$\Rightarrow \gcd(a,b) \geq p > 1$

This contradicts our assumption that $\gcd(a,b) = 1$.

And so $\sqrt{2}$ is irrational.