Lecture 9

Prime numbers (overview)

a is a factor of b

Let $a, b \in \mathbb{Z}$. We say a divides b or a is a divisor of b if $a \neq 0$ and $b = ac$ for some $c \in \mathbb{Z}$.

We write $a \mid b$ read 'a divides b'

> $a \mid b$ does not mean $\frac{a}{b}$
>
> $a \mid b$ is 'NOT' a number it is a relationship between two numbers

Natural numbers $\mathbb{N}$

A proper divisor of a nat. number is one which is neither 1 nor the number itself.

A nat. no. $p \geq 2$ is called prime if the only divisors of p are proper divisors.

A nat no. $n \geq 2$ is called Composite if it is not prime.

A factorization of a nat. no. n

means writing it in the form $n = ab$

where a, b are nat. no's. Or, more generally

$n = a_1 \dots a_r$.

To decide if a no. is prime or Composite

Let n be a nat no. $n \geq 2$.
We wish to determine if n is prime or Composite. Carry out trial divisions of n by all prime no's $p \leq \sqrt{n}$.

- If none of them works, n is prime
- If one of them works, n is Composite

If n is Composite, the above process can be iterated.

Example Is 97 prime or composite?

$\sqrt{97} = 9.84\ldots$.

Carry out trial divisions by 2, 3, 5, 7.

None of them works so 97 is prime.

Fundamental theorem of arithmetic

Each nat. no. $n \geq 2$ is either prime or a product of primes. The prime numbers that occur, & the no. of times they occur is uniquely det'd by n.

We usually write $n = p_1^{a_1} \ldots p_r^{a_r}$

where $p_1 < \ldots < p_r$.

This is called the prime factorization of n

Example Write 525 as a product of powers of primes.

There are obvious factorizations of this number which is ~~value~~ where I would usually begin but I shall follow the method above.

$\sqrt{525} \approx 22$ Carry out trial divisions by 2, 3, 5, ...

$525 = 3 \cdot 175$

↑ prime factor

$\sqrt{175} \approx 13$ Carry out trial divisions by 2, 3, 5, ..

$175 = 5 \cdot 35$

↑ prime factor

$\sqrt{35} \approx 5.$ 2, 3, 5.

$35 = 5 \cdot 7$

↑ ↑ both prime.

$525 = 3 \cdot 5 \cdot 5 \cdot 7$

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

The following is useful

Lemma If n is not prime then its smallest proper divisor is prime.

(Why is this true?)

Theorem (Euclid, 300 BCE)

There are infinitely many primes.

Proof. Let $p_1, \dots, p_n$ be the first n primes.

We prove there is a bigger prime.

Put $N = p_1 \cdots p_n + 1$.

Either N is itself prime (as $N > p_n, \dots, p_n$)

or N is composite. If N is composite then

smallest proper divisor p is a prime. So $p \mid N$.

But does, $p \neq p_1, \dots, p_n$. So $p > p_n$.

In either case, there is a larger prime ∎

Using advanced methods from Calculus, we can say how the primes are distributed.

$\pi(n) = \#$ primes $\leq n$.

Prime Number Theorem

(Hadamard, de la Vallée Poussin, 1896)

$$\pi(x) \simeq \frac{x}{\ln(x)}$$