Primes : Results (3 pages; 21/5/25)

See also “Series - Results”.

Terminology

Composite (positive integer): not a prime

References

(A) “Euler – The master of us all” (William Dunham; The Mathematical Association of America)

(1) Fundamental theorem of arithmetic (aka Prime factorisation theorem): Every integer greater than 1 can be represented uniquely as a product of prime numbers (ignoring the ordering of the factors).

(2) Euclid’s theorem: There are infinitely many prime numbers.

Proof

Suppose that the only primes are $p_1, p_2, \dots, p_n$. Consider

$N = p_1 p_2 \dots p_n + 1$ [we will then find a further prime number]

As $p_1, p_2, \dots, p_n$ are the only primes, N cannot be prime.

But then there will be some p_i in the list which are factors of both N and $N - 1$.

Thus $N = p_k F$ and $N - 1 = p_k G$ (where F & G are positive integers, and $F > G$), for some p_k in the list $p_1, p_2, \dots, p_n$.

Hence $p_k(F - G) = 1$.

But this is not possible if p_k is prime, and so it contradicts the assumption that there is a finite number of primes.

[This shows that, if all we know all the prime numbers up to p_n, then there is an upper bound of $p_1 p_2 \ldots p_n + 1$ for the next prime.]

(3) Prime Number theorem (initially a conjecture by Gauss [30/4/1777-23/2/1855]), and proved in 1896, states that $\frac{\pi(x)}{x} \to \frac{1}{lnx}$ as $x \to \infty$, where $\pi(x)$ is the number of primes less than or equal to x

(4) Mersenne primes: Primes of the form $2^n - 1$

Results:

(i) If n is composite, then so is $2^n - 1$ (so that if $2^n - 1$ is prime, then n is prime).

(ii) If n is prime, then it doesn't follow that $2^n - 1$ is prime

(eg $2^{11} - 1 = 2047 = 23 \times 89$)

(iii) The largest prime discovered so far (as at 19 May 2025, and discovered on 12 October 2024), is the Mersenne prime $2^{136279841} - 1$ (it has 41024320 digits).

(5) For every positive integer n, there is a prime number between $2n$ & $4n$. [STEP 2018, P2, Q6] (A big help in finding the next prime number: If p is prime, then let $n = \frac{p+1}{2}$, so that another prime must lie between $p + 1$ and $2(p + 1)$.)

(6) Fermat's Little theorem:

If p is a prime number and a is any integer, then $a^p \equiv a \pmod{p}$.

(7) Conjectures

(i) Goldbach's conjecture

Every even positive integer greater than 2 can be written as the sum of two primes.

(ii) Opperman's conjecture

There is always a prime between n^2 and $(n+1)^2$

(iii) Fermat's conjecture (found to be false)

All numbers of the form $2^{2^n} + 1$ are prime.