Prime number theorem

1896

THM (Euclid) 300 BC

There are infinitely many primes.

Pf Start with any finite list of primes:

$p_1, p_2, \dots, p_n$

$N := p_1 p_2 \cdots p_n + 1$

Each p_i divides $N-1$, so cannot divide N.

$\Rightarrow$ Any prime dividing N is missing on our list. $\square$

EG
p_1 $2 + 1 = 3$
p_2 $2 \cdot 3 + 1 = 7$
p_3 $2 \cdot 3 \cdot 5 + 1 = 31$
p_4 $2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$
p_5 $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$
p_6 $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$

all prime

$p_1, p_2, \dots, p_5$ "primorial" primes

next ones: $p_{11}, p_{75}, p_{171}, p_{172}, \dots$

OPEN: infinitely many primorial primes?

THM Prime number theorem

Up to x, there are roughly $\frac{x}{\ln(x)}$ primes.

$\log_e(x)$, $e \approx 2.71828\ldots$

EG Up to 10^6, roughly $\frac{10^6}{\ln(10^6)} = 72{,}382.4$ primes

actual number: 78,498

7.85%

proportion of primes: 7.24%

Crucial for cryptography:

need primes of size 2^{2048}

$\frac{1}{\ln(2^{2048})} = 0.0704\%$