Primes. An integer $p > 1$ is called prime if the only positive factors of p are 1 and p. A positive integer that is greater than 1 is not prime is called composite.

Theorem 1. Fundamental Theorem of Arithmetic.

Every integer > 1 can be written uniquely as a prime or as a product of primes. (factors are prime written in nondecreasing size.

Theorem 2 Trial Division.

If n is a composite integer, then n has a prime divisor $\leq \sqrt{n}$.

proof. If n is composite, we can write $n = ab$ with $1 < a \leq b < n$. If both a and b are $> \sqrt{n}$, then $n = ab > \sqrt{n} \cdot \sqrt{n} = n$ is a contradiction. Thus, one of a or b must be $\leq \sqrt{n}$. As $a \leq b$, it must be $a \leq \sqrt{n}$ (Note that we could also have $b \leq \sqrt{n}$ but we have $a \leq b \leq \sqrt{n}$ in that case)

The Sieve of Eratosthenes

In the list of N positive integers $1, \cdots, N$, cross out multiples (not itself) of prime $p \le \sqrt{N}$. The remaining integers are prime

Theorem 3. There are infinitely many primes.

Definition. $2^n - 1$ with positive integer n, is called Mersenne number. If a Mersenne number becomes a prime, such primes are called Mersenne primes.

Conjecture. There are infinitely many Mersenne primes

Theorem 4 Prime Number Theorem. (Hadamard, Vallée-Poussin 1896) Let $\pi(x) = \sum_{p \le x} 1$ be the number of primes $\le x$. Then

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1.$$

Theorem 5. Dirichlet's Theorem on Primes in Arithmetic Progression If a and b are relatively prime, the arithmetic progression $ak+b$ captures infinitely many primes. (1837)

Theorem 6 (Green, Tao) There are arbitrarily long arithmetic progressions composed entirely of prime numbers. (2006)

Goldbach's Conjecture

Goldbach → Euler : $\forall$ odd $n > 5$, is a sum of 3 primes?

Euler → Goldbach : $\forall$ even $n > 2$, is a sum of 2 primes?

"Every even number $n > 2$ is a sum of 2 primes"
is now known as Goldbach's conjecture.

Theorem (O. Ramaré) Every even integer > 2 is a sum of at most 6 primes.

Twin Prime Conjecture.

Definition If p and $p+2$ are both primes, we say that $p, p+2$ are twin primes.

Conjecture: There are infinitely many twin primes

Theorem (Chen J. R) (1966)

Toward Goldbach conjecture: Every sufficiently large even positive integer is a sum of a prime and P_2 number

(P_2: prime or product of two primes)

Toward Twin Prime conjecture:

There are infinitely many pairs $p, p+2$ such that p is a prime and $p+2$ is a P_2 number.

Prime Gaps. Let p' be the next prime to p, so that p and p' are consecutive primes. Then

$p' - p \leq 246$ infinitely often.

(Polymath 8b, 2014 after Zhang, Maynard's progress)
70000000 600

GCD: Greatest common Divisor.

$a = p_1^{e_1} \cdots p_k^{e_k}$
$b = p_1^{f_1} \cdots p_k^{e_k}$ $\rightsquigarrow$ $\gcd(a,b) = p_1^{\min(e_1,f_1)} \cdots p_k^{\min(e_k,f_k)}$

LCM: Least common multiple

$a = p_1^{e_1} \cdots p_k^{e_k}$
$b = p_1^{f_1} \cdots p_k^{f_k}$ $\rightarrow$ $\operatorname{lcm}(a,b) = p_1^{\max(e_1,f_1)} \cdots p_k^{\max(e_k,f_k)}$

GCD can be regarded as intersection of multisets
LCM can be regarded as union of multisets.

GCD, LCM of tuples

Given $m_1, \cdots, m_k$,

$\gcd(m_1, \cdots, m_k) = \gcd(\gcd(m_1, \cdots, m_{k-1}), m_k)$

$\operatorname{lcm}(m_1, \cdots, m_k) = \operatorname{lcm}(\operatorname{lcm}(m_1, \cdots, m_{k-1}), m_k)$