

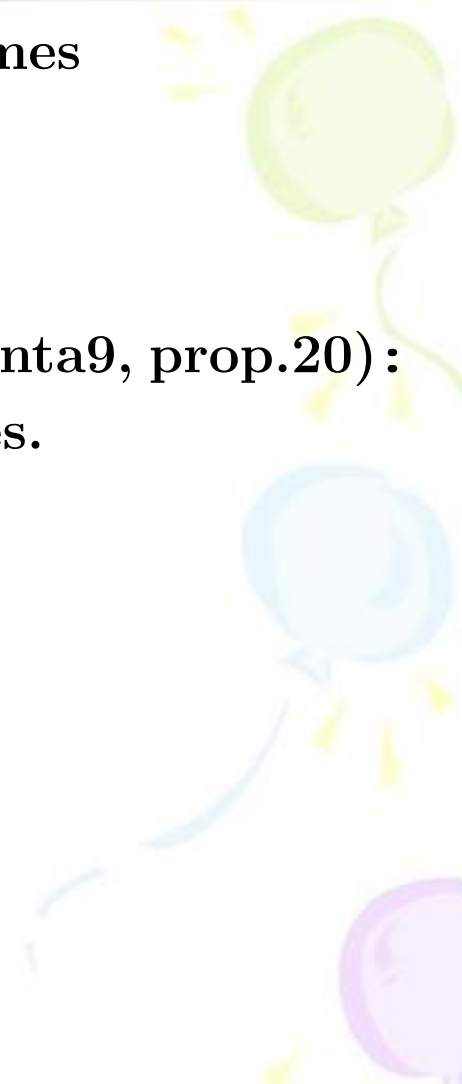
初等数论

吴伊涛

2022 年春

The distribution of Primes

**Theorem(Euclid, 300B.C. Elementa9, prop.20):
There are infinitely many primes.**





Lemma: Let n be an integer, then

$$\gcd(n, n + 1) = 1$$

Proof 1:

By the definition of greatest common divisor,

$$\gcd(n, n + 1) | n, \quad \gcd(n, n + 1) | n + 1$$

So

$$\gcd(n, n + 1) | n + 1 - n = 1$$

Since $\gcd(n, n + 1) \geq 0$, So $\gcd(n, n + 1) = 1$. □



Proof 2:

It suffices to prove $(n, n + 1) = (1)$.

Obviously, $(n, n + 1) \subseteq (1) = \mathbb{Z}$.

Conversely, $1 = (n + 1) \cdot 1 + n \cdot (-1) \in (n, n + 1)$, thus, $\forall x \in (1)$,

$$x = (n + 1) \cdot x + n \cdot (-x) \in (n, n + 1)$$

So $(1) \subseteq (n, n + 1)$.

Hence $(n, n + 1) = (1)$.

□

The distribution of Primes

Theorem: There are infinitely many primes.

Proof 1 (Euclid) :

Assume there are just finite primes:

$$p_1, p_2, \dots, p_n$$

Construct $N = p_1 p_2 \cdots p_n + 1$.

Obviously $N > 1$, thus N has prime factors. Let q be a prime factor, then $q \in \{p_1, p_2, \dots, p_n\}$, so $q | p_1 p_2 \cdots p_n = N - 1$. Thus $\gcd(N, N - 1) \geq q > 1$.

But by the lemma above, N is coprime to $N - 1$, a contradiction.

Thus there are infinitely many primes.

□

Proof 2 (Hermite) :

For any positive integer n , $n! + 1$ is coprime to $n!$. So all prime factors of $n! + 1$ is greater than n .

So, for any positive integer n , there exists a prime greater than n .

Thus there are infinitely many primes. □

Proof 3 (Cohen) :

Assume there are just finite primes:

$$p_1, p_2, \dots, p_l$$

Recall that

$$n! = \prod_p p^{\text{ord}_p(n!)}$$

where

$$\text{ord}_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \dots = \sum_{r=1}^{\infty} \left[\frac{n}{p^r}\right]$$

Thus,

$$\text{ord}_p(n!) \leq \frac{n}{p} + \frac{n}{p^2} + \frac{n}{p^3} + \dots = \frac{n}{p-1}$$

Hence

$$n! \leq \prod_p p^{\frac{n}{p-1}}$$

So

$$\sqrt[n]{n!} \leq \prod_p p^{\frac{1}{p-1}} = p_1^{\frac{1}{p_1-1}} \cdot p_2^{\frac{1}{p_2-1}} \cdots p_l^{\frac{1}{p_l-1}}$$

which is bounded above.

Claim: $\lim_{n \rightarrow \infty} \sqrt[n]{n!} = +\infty$

In fact, it's a direct corollary from Stirling's formula. In case you don't know Stirling's formula, then you use the following argument:

$$(n!)^2 = [1 \cdot n] \cdot [2 \cdot (n-1)] \cdot [3 \cdot (n-2)] \cdots [n \cdot 1]$$

Each product in the bracket is larger than or equal to $n(k \cdot (n+1-k) \geq n)$

So

$$(n!)^2 \geq n^n, \quad \sqrt[n]{n!} \geq \sqrt{n}$$

Thus $\lim_{n \rightarrow \infty} \sqrt[n]{n!} = +\infty$.

A contradiction.

□

Proof 4 (Goldbach) :

Idea (Goldbach) : Construct an infinite sequence $\{a_n\}_{n \geq 1}$, where $a_n > 1$ and pairwise coprime.

Lemma: Let a be a positive integer, $n > m$ be two positive integers, then:

when a is even, $\gcd(a^{2^n} + 1, a^{2^m} + 1) = 1$.

when a is odd, $\gcd(a^{2^n} + 1, a^{2^m} + 1) = 2$.

Sketch of Proof:

When $n = m + 1$,

$$a^{2^{m+1}} - 1 = (a^{2^m})^2 - 1 = (a^{2^m} - 1)(a^{2^m} + 1)$$

So $a^{2^m} + 1 \mid a^{2^{m+1}} - 1$.

When $n = m + 2$,

$$a^{2^{m+2}} - 1 = (a^{2^{m+1}})^2 - 1 = (a^{2^{m+1}} - 1)(a^{2^{m+1}} + 1)$$

So $a^{2^{m+1}} - 1 \mid a^{2^{m+2}} - 1$, thus $a^{2^m} + 1 \mid a^{2^{m+2}} - 1$.

.....

In general, we can prove, by induction(induction on what? Write out the complete proof yourself), for all $n > m$,

$$a^{2^m} + 1 \mid a^{2^n} - 1$$

Hence

$$\gcd(a^{2^n} + 1, a^{2^m} + 1) \mid a^{2^n} + 1 - (a^{2^n} - 1) = 2$$

So

$$\gcd(a^{2^n} + 1, a^{2^m} + 1) = 1 \text{ or } 2$$

when a is even, both $a^{2^n} + 1$ and $a^{2^m} + 1$ are odd numbers, the greatest common divisor of them shouldn't be 2, so $\gcd(a^{2^n} + 1, a^{2^m} + 1) = 1$.

when a is odd, both $a^{2^n} + 1$ and $a^{2^m} + 1$ are even numbers, the greatest common divisor of them should be at least 2, so $\gcd(a^{2^n} + 1, a^{2^m} + 1) = 2$.

□

Proof 4:

Consider an infinite series $\{2^{2^n} + 1\}_{n \geq 1}$, each term $2^{2^n} + 1 \geq 1$, and by the lemma above, they are pairwise coprime. Thus there are infinitely many primes. □

Remarks

- obviously, the proof still holds if we replace the infinite series $\{2^{2^n} + 1\}_{n \geq 1}$ by $\{a^{2^n} + 1\}_{n \geq 1}$ (where a is an even positive integer), so we get infinitely many proofs of "there are infinitely many primes".
- Numbers of the form $2^{2^n} + 1$ are called Fermat Numbers, denoted by $F_n = 2^{2^n} + 1$. Let's write out the first few terms of $\{2^{2^n} + 1\}_{n \geq 1}$

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537$$

Clearly, these are all primes, so Fermat made a conjecture:

For all natural numbers n , F_n is a prime.

However, Euler gave a contradiction:

$$F_5 = 641 \times 6700417$$



(We will explain it later)

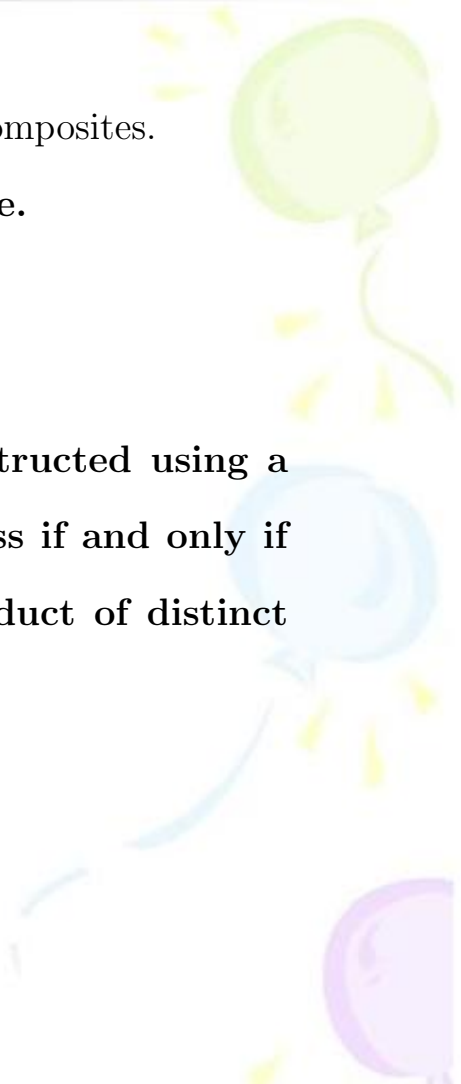
Later, People found out that F_6, F_7, \dots are all composites.

Conjecture: If $n \geq 5$, then F_n is a composite.

(See Section 3.6 in the textbook.)

- Fermat primes and geometry

A regular polygon of n sides can be constructed using a straightedge (unmarked ruler) and compass if and only if n is the product of a power of 2 and product of distinct Fermat primes.



Prime Number Theorem


Let n be an integer, $\pi(n)$ be the number of primes smaller than or equal to n . e.g.

$$\pi(8) = 4, \quad \pi(11) = 5$$

Prime Number Theorem

Let n be an integer, $\pi(n)$ be the number of primes smaller than or equal to n . Then

$$\lim_{n \rightarrow \infty} \frac{\pi(n)}{n / \ln n} = 1$$



Example: Estimate the number of primes smaller than or equal to 10^{100} (Take $\ln 10 \approx 2.302$).


Solution:

We need to estimate the size of $\pi(10^{100})$.

By Prime Number Theorem,

$$\pi(10^{100}) \approx \frac{10^{100}}{\ln 10^{100}} = \frac{10^{100}}{100 \ln 10} \approx 4.344 \times 10^{97}$$

So there are approximately 4.344×10^{97} primes smaller than or equal to 10^{100} .



An important Corollary

Corollary: Let n be a positive integer, p_n be the n -th prime, Then $p_n \sim n \ln n$. i.e.

$$\lim_{n \rightarrow \infty} \frac{p_n}{n \ln n} = 1$$

Proof:

Since $\pi(p_n) = n$, by Prime Number Theorem, we have

$$\frac{p_n}{\ln p_n} \sim n \quad (n \rightarrow \infty)$$

Take logarithm,

$$\ln p_n - \ln \ln p_n \sim \ln n \quad (n \rightarrow \infty)$$

So

$$p_n \left(1 - \frac{\ln \ln p_n}{\ln p_n}\right) \sim n \ln n \quad (n \rightarrow \infty)$$

Since $p_n \rightarrow \infty (n \rightarrow \infty)$, so $\frac{\ln \ln p_n}{\ln p_n} \rightarrow 0 (n \rightarrow \infty)$. Thus $1 - \frac{\ln \ln p_n}{\ln p_n} \rightarrow 1 (n \rightarrow \infty)$.

Hence

$$p_n \sim n \ln n \quad (n \rightarrow \infty)$$

□



Example: Estimate the size of the 10^{100} th prime (Take $\ln 10 \approx 2.302$).

Solution:

We need to estimate the size of $p_{10^{100}}$.

By the corollary of Prime Number Theorem,

$$p_{10^{100}} \approx 10^{100} \times \ln 10^{100} \approx 2.302 \times 10^{102}$$

So the 10^{100} th prime is approximately 2.302×10^{102} .



Remarks

We can also use Prime Number Theorem to estimate the size of n -th composite:

Let c_n be the n -th composite, then

$$c_n = 1 + \pi(c_n) + n$$


Since $\pi(c_n) \approx \frac{c_n}{\ln c_n}$, thus

$$c_n \approx \frac{c_n}{\ln c_n} + n$$

and therefore that

$$c_n \left(1 - \frac{1}{\ln c_n}\right) \approx n$$

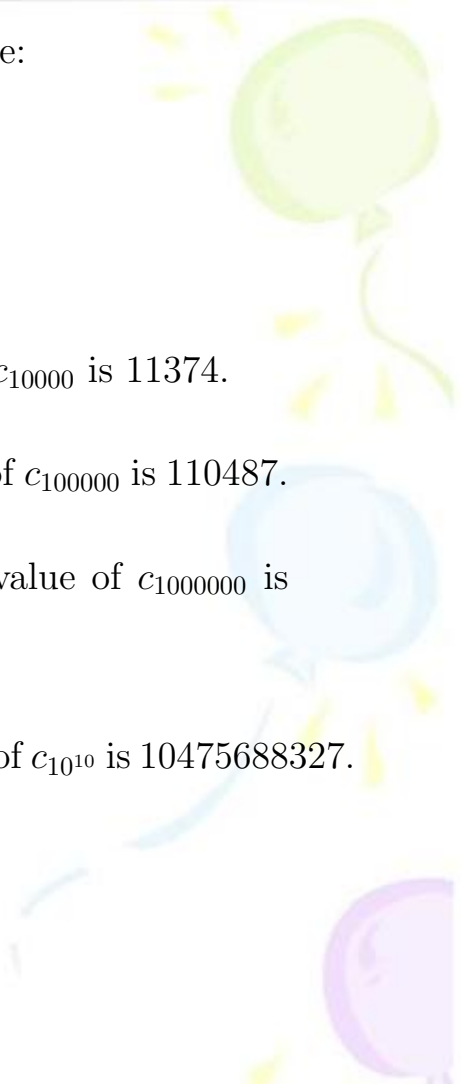
We can simplify the above (approximate)equality via $\ln c_n \approx \ln n$, thus



we get the approximation of the size of n -th composite:

$$c_n \approx \frac{n}{1 - \frac{1}{\ln n}}$$

Example:


- $n = 10000$, $c_{10000} \approx 11218$, and the true value of c_{10000} is 11374.
 - $n = 100000$, $c_{100000} \approx 109512$, and the true value of c_{100000} is 110487.
 - $n = 1000000$, $c_{1000000} \approx 1078030$, and the true value of $c_{1000000}$ is 1084605.
 - $n = 10^{10}$, $c_{10^{10}} \approx 10454011971$, and the true value of $c_{10^{10}}$ is 10475688327.
- 

Summarize and some Extensions


Recall: Given an integer n greater than 1, by Fundamental Theorem of Arithmetic, n can be written uniquely as the product of primes

$$n = p_1^{a_1} p_2^{a_2} \cdots p_l^{a_l}$$

where p_1, p_2, \dots, p_l are pairwise different primes, a_1, a_2, \dots, a_l are positive integers.



Primality Test and Factorization: “Trial division” (Eratosthenes Sieve),
Fermat’s factorization method. Both are inefficient.





The first result we learned on the distribution of prime numbers:

There are infinitely many primes.

Some related topics: "There are infinitely many XXX-type primes."


- Dirichlet Theorem

Let a, b be two coprime positive integers, then the arithmetic progression $\{a, a+b, a+2b, a+3b, \dots\}$ contains infinitely many primes.

e.g. By Dirichlet theorem, There are infinitely many $2022k+5$ -type primes.

- Maynard(2019)

Let $a_0 \in \{0, 1, 2, 3, \dots, 9\}$, there are infinitely many primes which do not have the digit a_0 in their decimal expansion.



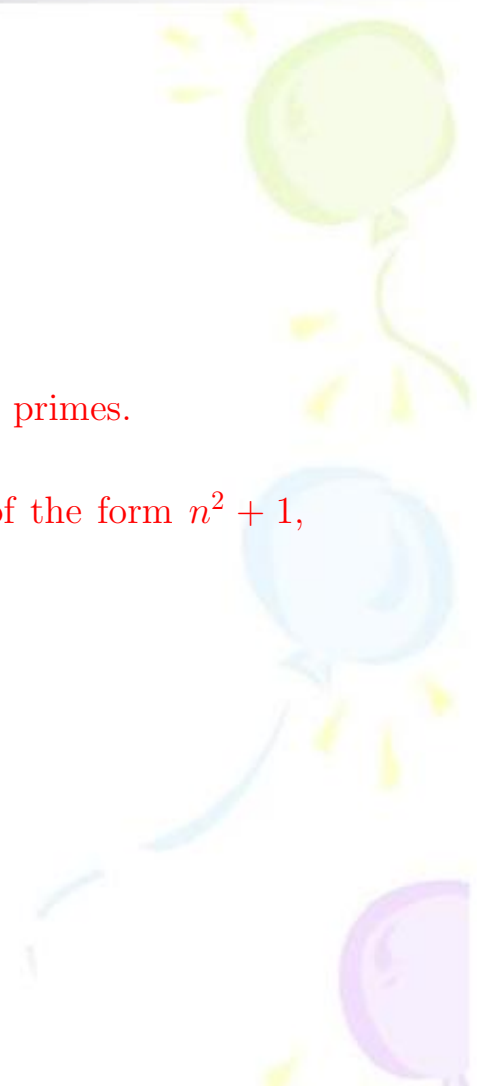
- Euler(1737)

$$\sum_p \frac{1}{p} = +\infty$$

where p runs through all primes.

(See Lecture notes)

- Conjecture: There are infinitely many Mersenne primes.
- Conjecture: There are infinitely many primes of the form $n^2 + 1$,
where n is a positive integer.



“Gaps between primes”

Clearly, all primes are odd except 2. So the gap between two consecutive primes greater than 2 is an even positive integer.


We can prove the gap between two consecutive primes can be arbitrary large(Leave to you as an exercise.), but this doesn't mean that we can not estimate the size of the gap between two consecutive primes.

Bertrand's postulate(Proved by Chebyshev in 1852):

$$p_{n+1} < 2p_n$$

or equivalently,

If x is an integer greater than 1, then there is a prime p s.t. $x < p < 2x$.



Examples. The prime 3 is between 2 and 4, the prime 5 is between 3 and 6, and the prime 5 is between 4 and 8.


Theorem(Nagura,1952). Let $n \geq 25$ be a positive integer, then there is always a prime p between n and $1.2n$.


For instance, if $n = 25$, then Nagura' s theorem says that there is a prime between 25 and 30 and, indeed, 29 is such a prime. If $n = 40$, then there is a prime $p = 41$ (also 43,47) between 40 and 48, and so on.

Note that, by Nagura' s theorem, when $n \geq 25$, then there are at least three primes between n and $2n$.

Legendre' s conjecture:

Let n be a positive integer, then there exists a prime between n^2 and $(n + 1)^2$.





Now, let's see the least gap between consecutive primes:

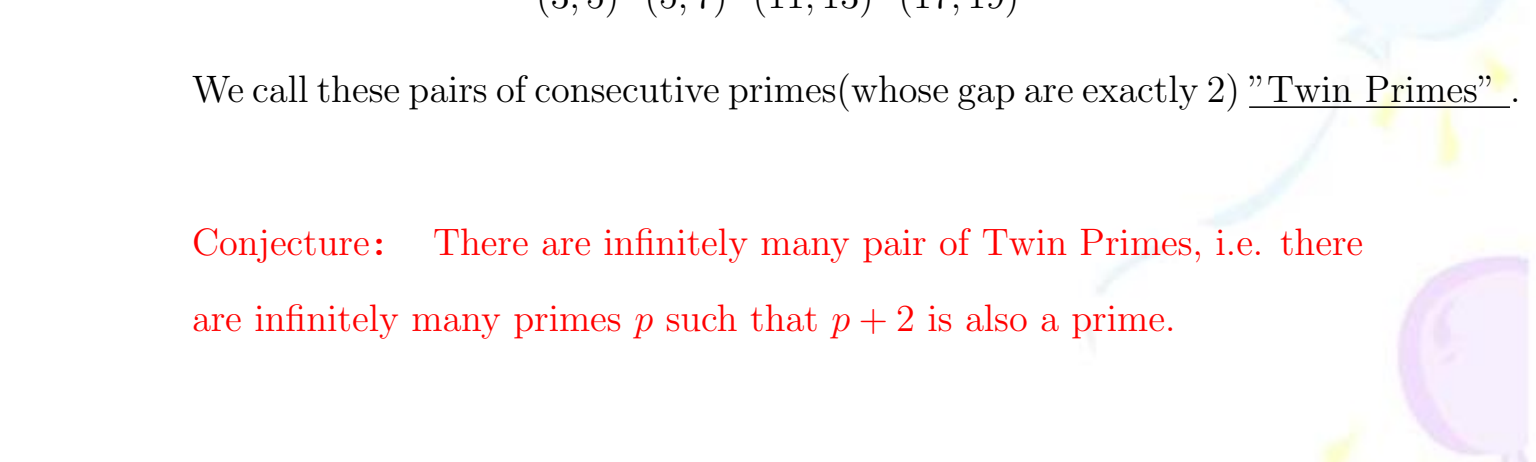
We already see the gap between two consecutive primes greater than 2 is an even positive integer, thus larger than 2.

Now we consider those pairs of consecutive primes whose gap are exactly 2, e.g.

$$(3, 5) \quad (5, 7) \quad (11, 13) \quad (17, 19)$$

We call these pairs of consecutive primes (whose gap are exactly 2) "Twin Primes".

Conjecture: There are infinitely many pair of Twin Primes, i.e. there are infinitely many primes p such that $p + 2$ is also a prime.




- Brun(1919)

$$\sum_p \frac{1}{p} < +\infty$$

where p runs through all primes satisfying the condition: $p + 2$ is also a prime.






值得骄傲的是，在这个领域，两位中国数学家做出了目前最好的结果或是突破性进展：

陈景润（1966）：

存在无穷多个素数 p ，使得 $p + 2$ 或者是素数，或者是两个素数的乘积。

张益唐（2013）：

存在无穷多对素数 (p, q) ，使得 $|p - q| < 70000000$ 。



"Density of Primes"

Prime Number Theorem

Let n be an integer, $\pi(n)$ be the number of primes smaller than or equal to n . Then

$$\lim_{n \rightarrow \infty} \frac{\pi(n)}{n / \ln n} = 1$$

Corollary: Let n be a positive integer, p_n be the n -th prime, Then $p_n \sim n \ln n$. i.e.

$$\lim_{n \rightarrow \infty} \frac{p_n}{n \ln n} = 1$$

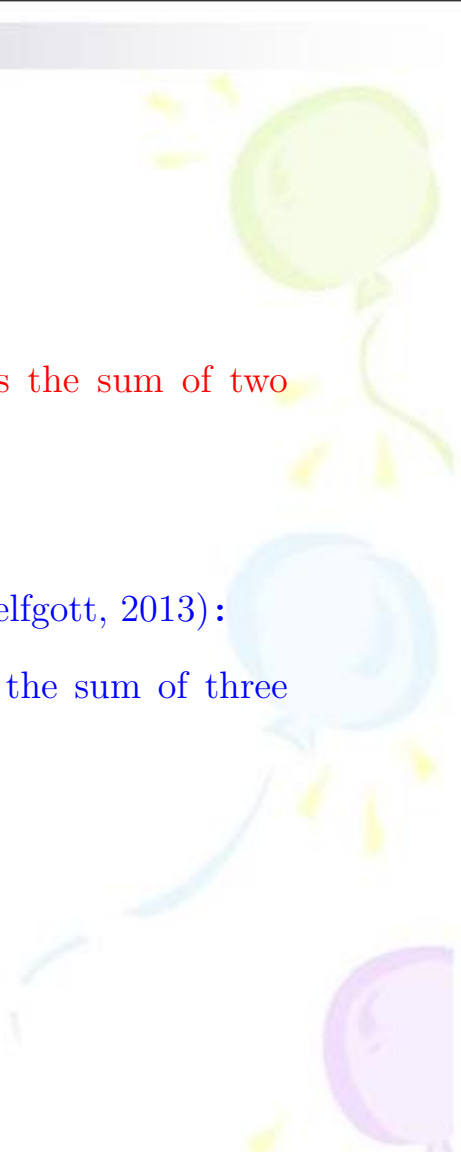



Goldbach Conjecture(哥德巴赫猜想):

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

ternary(odd,weak) Goldbach Conjecture(proved by Helfgott, 2013):

Every odd integer greater than 5 can be written as the sum of three primes.






目前最好的结果：


陈景润（1966）：

一个充分大的偶数可以写成1个素数和1个至多是2个素数乘积的数之和。

推荐书目：徐迟，《哥德巴赫猜想》


（1978年的春天，徐迟的报告文学《哥德巴赫猜想》使得数学家陈景润成了家喻户晓的人物，激起了无数人研究哥德巴赫猜想的热情，是值得一读的作品。）





“陈景润所做的工作，犹如在喜马拉雅山颠上行走，一旦成功，必将影响世人。”

“您移动了群山！”



谢谢！

