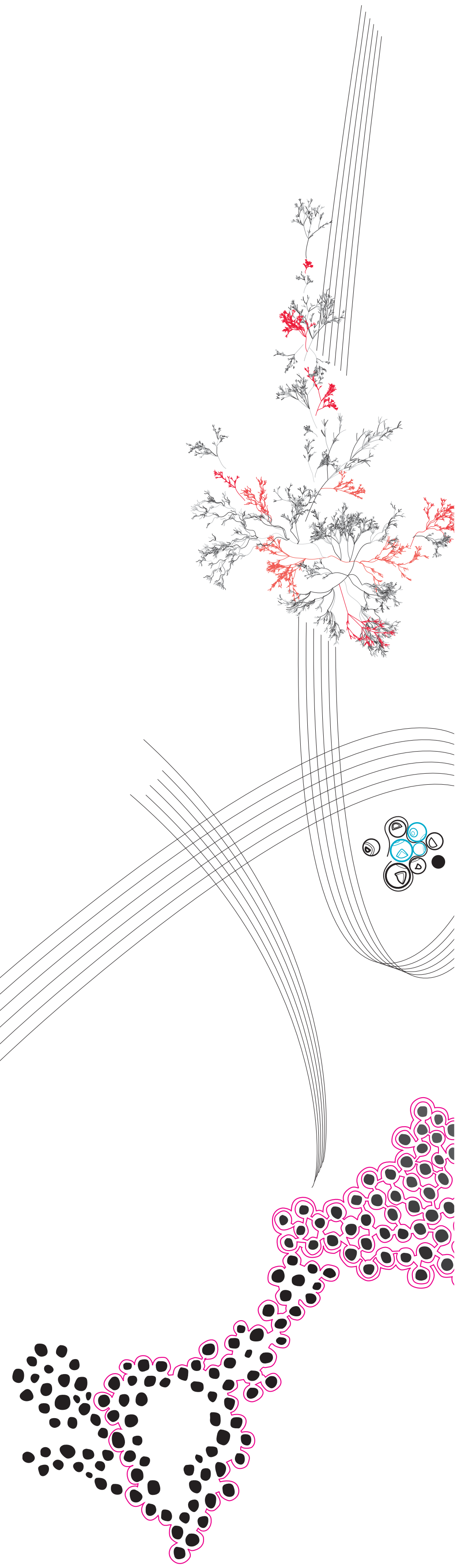
BSc Thesis Applied Mathematics



# Twin primes: classical results and new developments

Sam van Dijk

Supervisor: Georg Still

February, 2019

Department of Applied Mathematics
Faculty of Electrical Engineering,
Mathematics and Computer Science

UNIVERSITY OF TWENTE.

# Contents

# Twin primes:
# classical results and new developments

Sam van Dijk*

February, 2019

**Abstract**

While the notion of prime numbers has existed for millennia, twin primes have only been around for little over a century. Although it is not known whether there are infinitely many twin primes, the prime gap was very recently shown to be no greater than 246. The fact that the summed reciprocals of twin primes converge to approximately 1.9 has also been demonstrated. It has further been established that there *do* exist infinitely many primes $p$ for which $p + 2$ is the product of no more than two primes. A criterion for twin primes does exist but it is neither sufficient to show the existence of an infinite number of them, nor feasible as a computational tool.

*Keywords*: Prime numbers, Twin primes, Sieve theory.

## 1 Introduction

This thesis comprises a review of several historic landmarks in the theory of twin primes. To mention them by name, Brun's theorem, the $k$-tuple conjecture, Chen's theorem and the bounds for the prime gap established by Zhang and Maynard will be explored in further detail. A large proportion of earlier research on twin primes led only to conjectural results. In addition, many of the proven results on twin primes display a heavy internal reliance on the theory of regular primes. Because of this, the theory of twin primes will be explored by in each case first observing the analogous result for the prime numbers themselves. Special attention is also devoted to the development of sieve techniques, from which almost all extant results on twin primes derive. The thesis is structured chronologically, with each chapter representing a subsequent development in the bodies of prime and twin prime theory. It begins therefore, as it must, by looking at the origins of prime numbers and twin primes themselves.

*Email: s.g.vandijk@student.utwente.nl

## 2 Humble beginnings

Before stating the definitions of prime numbers and twin primes some historical context is provided. The notion of prime numbers is perhaps as old as the concept of division itself, dating back at least several thousand years. The *Elements*, written by Euclid circa 300 BC, provides a now-famous proof of the infinitude of primes. Appendix A contains a translation of this proof. Both this and his proof of the fundamental theorem of arithmetic clearly show that by Euclid's time the notion of prime numbers was already understood to some extent. It might therefore surprise the reader that the idea of twin primes would not appear for another two millennia. During all this time the issue of whether 1 is prime, or if it even qualified as a number to begin with, would stay unresolved. According to Caldwell and Xiong in [4], the number one would not widely be considered as such until the introduction of decimals and the real number system to Europe by Simon Stevin in his 1585 publication *De Thiende*. Two hundred years thereafter, in 1798, Carl Friedrich Gauss wrote the *Disquisitiones Arithmeticae*. It is argued in [4] that this work laid a foundation for modern number theory which consolidated the definition of prime numbers as it is known today. A fair proposition, given the fact that Gauss had stated and proved modern forms of both the fundamental theorem of arithmetic and the Chinese remainder theorem in this work. The idea of one as a prime number would however not completely vanish until well into the 20th century, with the 1921 third edition printing of *A Course of Pure Mathematics* by G.H. Hardy still counting 1 amongst the primes in several cases.

### 2.1 Preliminaries

The contemporary definitions of primes and twin primes are now ready to be set forth.

**Definition 2.1** (Prime numbers). *Any natural number with exactly two distinct positive divisors is prime or, equivalently, a prime number.*

**Definition 2.2** (Twin primes). *A twin prime is any prime number $p$ such that $p+2$ is also prime.*

The pair $\{p, p+2\}$ is a twin prime pair if $p$ is a twin prime. By grace of these definitions both primes and twin primes are individual numbers rather than one of the two referring to numbers and the other to number sets. This choice was made for ease of reference moreso than any other reason. The (obvious) exclusion of the number one from the primes by definition 2.1 must also be duly noted by the reader. Each positive integer is then either a unit, a composite number, or a prime.[1] The notation $\mathbb{P}$ identifies the set of prime numbers and $\mathbb{P}_2$ similarly corresponds to the set of twin primes. Table 1 below contains the twenty smallest twin prime pairs. The largest currently known twin prime is $2996863034895 * 2^{1290000} - 1$, a number over $3 * 10^6$ digits in length. This record is taken from The Prime Pages at `https://primes.utm.edu`.

[1]If convenient, such a partitioning could easily be extended to include the number zero. In order to achieve this the unit partition should be replaced by an identity partition containing the identities 0 and 1 both.

| Twin prime pairs | | | | |
|---|---|---|---|---|
| 3 | 5 | | 149 | 151 |
| 5 | 7 | | 179 | 181 |
| 11 | 13 | | 191 | 193 |
| 17 | 19 | | 197 | 199 |
| 29 | 31 | | 227 | 229 |
| 41 | 43 | | 239 | 241 |
| 59 | 61 | | 269 | 271 |
| 71 | 73 | | 281 | 283 |
| 101 | 103 | | 311 | 313 |
| 137 | 139 | | 347 | 349 |

Table 1: Twenty twins

The following pair of analogous statements about the cardinality of $\mathbb{P}$ and $\mathbb{P}_2$ are further presented.

**Theorem 2.3** (The infinitude of primes)**.** *There are infinitely many primes.*

**Conjecture 2.4** (The twin prime conjecture)**.** *There are infinitely many twin primes.*

As is shown in appendix A the first of these statements has long since been proved. The latter remains undecided to date. The twin prime conjecture has occupied the minds of many great thinkers since its conception, as will soon become evident from this thesis. Even so, it can not be stated for precisely how long it has been an open problem as it was originally part of a more general conjecture. The circumstances of that origin are elucidated in the remainder of this section.

## 2.2 The origins of twin primes and the twin prime conjecture

The origin of the twin prime conjecture can be attributed to Alphonse de Polignac only with some reservations. Although he was in fact the first to present some form of it in writing the circumstances of this event are at best described as dubious, at worst as downright shameful. De Polignac, born in 1826, was a nobleman whose father had briefly served as prime minister of France at the end of the Bourbon Restoration. In the october 1849 issue of *Comptes rendus*, a publication of the still-renowned *École Polytechnique*, he offered a pair of statements as theorems in a research paper on prime numbers. The first of these is known today as Polignac's conjecture.

**Conjecture 2.5** (Polignac's conjecture)**.** *For any even positive integer $n$ there exist infinitely many primes $p$ such that $p + n$ is the first prime subsequent to $p$.*

The twin prime conjecture corresponds to the case $n = 2$ of this conjecture. His second claim was the strictly false proposition that all odd numbers can be expressed as the sum of a prime and a power of two. He goes so far as to insist this statement had been verified for numbers up to 3 million. This claim, falsifiable by the fourth Mersenne prime[2], had in fact already been discredited by Euler 100 years prior. He would acknowledge his error within months, blaming subordinates for faulty calculations [8]. He had made no specific

[2]The reader is invited to confirm that the fourth Mersenne prime $2^7 - 1 = 127$ cannot be written as a sum $2^k + p$. To those readers who consider this too trivial an excercise, I propose de Polignac's claim may alternatively be falsified by a composite number.

mention of twin primes and had furthermore presented his conjecture (as a theorem) alongside a known falsehood. This casts, to say the least, some doubt on his academic credibility.

Thirty years later, in 1879, James Whitbread Lee Glaisher would at last do the twin prime conjecture justice. As editor of the *Quarterly Journal of Mathematics* he authored an article introducing the notion of "prime-pairs". Though without naming it as such, he also states the twin prime conjecture explicitly in this article. An image of the original text containing this statement may be found in [8] by Dunham. Dunham further asserts there that twin primes were to replace prime-pairs within decades through translations of the term into German and French. He notes that by the time of Viggo Brun, whose work is discussed in section 3, twin primes had become the standard terminology.

# 3 Reciprocal primes

The first major theorem published on the topic of twin primes was in some ways a disheartening result. It was first established in 1919 by Viggo Brun. In [3] he managed to show that the sum of reciprocals of twin prime pairs is convergent. Considering the fact that the summed reciprocals of primes

$$\sum_{p\in\mathbb{P}} \frac{1}{p} = \infty \tag{1}$$

diverge, this is remarkable indeed. The result established by Brun was somewhat disheartening in the sense that the twin prime conjecture would have followed directly from the divergence of the summed reciprocals.[3] A proof of his theorem which is both clear and concise can be found in [21] and section 3.3 will treat this result in further detail. The value of the sum

$$\sum_{p\in\mathbb{P}_2} (\frac{1}{p} + \frac{1}{p+2}) = \mathfrak{B} \tag{2}$$

is known as Brun's constant. The explicit bound $\mathfrak{B} < 2.4$ is demonstrated in [18] and its value was computed in [24] to be approximately 1.9 by Thomas Nicely. Nicely's calculation is mentioned in section 7 as it turned out to reveal the existence of the Pentium FDIV bug. Brun established his result with the aid of a most ingenious method known as Brun's sieve. This method was based on a refinement of the sieve of Erathosthenes that has been around for several millennia. There had been virtually no interest in sieves up to this point, but Brun's sieve would mark the beginning of an entire field of study nowadays known as sieve theory. Like most modern sieves it utilizes the fundamental theorem of arithmetic alongside the Chinese remainder theorem in order to allow a sum to be turned into a product for which meaningful bounds can be obtained. The Riemann zeta function $\zeta(s)$ is used in [3] to achieve that transformation. This zeta function is the analytical continuation of a remarkably simple sum

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \zeta(s), \quad \mathrm{Re}(s) > 1$$

which even more remarkably transforms into an equally simple product (see (4)). While Riemann was first to elaborate on the possibility of analytical continuation, it was Euler

[3]Note that while divergence would imply the twin prime conjecture, convergence does not disprove it.

who first studied its most basic form. The key significance of zeta functions to applications in sieve theory rests on the ability to transform sums into products. When a sum counts (or bounds) the number of members in a set, its product equivalent can then be analysed to assess the magnitude of the set. This is often advantageous as such products are more suitable than sums for the application of techniques involving integration. A general method by which to achieve such transformations is therefore now explained before the reader's attention is turned towards proofs of the equations 1 and 2.

### 3.1 Euler products

The idea of expressing a series as an infinite product instead of an infinite sum is introduced in order to assist the reader's comprehension of Brun's sieve. The aforementioned divergence of the reciprocals of primes proved in section 3.2 was in fact first proved by Leonhard Euler in [12] through use of just such an idea. The idea of these so-called Euler products is again crucial in proving the prime number theorem discussed in section 4.1. It additionally pervades the original derivation of the so-called Hardy-Littlewood conjectures treated there. More modern research often relies upon it as an elementary tool. The reader is referred to [19] for a more in-depth explanation of generalized Euler products. Although the details of its application in many of the sources used (such as [16],[25],[31], and [9] to name a few) had to be omitted here, it must be stressed that its importance cannot be overstated. The method, in technical terms, consists of replacing a Dirichlet $L$-series

$$\sum_{n=1}^{\infty} \frac{\chi_k(n)}{n^s} \quad ,$$

wherein the Dirichlet character $\chi_k(n)$ is a totally multiplicative[4] complex function modulo $k$, with an infinite product

$$\prod_{p\in\mathbb{P}} \sum_{n=1}^{\infty} a_n(p) z_p^n$$

of power series. This product must be carried out over all primes. The prime terms of the $L$-series are used as the variables $z_p$ for each of the power series. Since most would prefer the variable of a power series to be a plain number rather than containing a function, the Dirichlet character $\chi_k$ occuring in the terms of the $L$-series ought to be taken out. This is easily achieved by simply eliminating it from the variable and instead setting it to form the coefficients $a_n(p)$ of the power series. The coefficients of each power series are then given by the Dirichlet character of the corresponding prime.[5] By grace of unique prime factorization such a product of power series at prime indices covers every natural number's term from the original $L$-series exactly once. The equality

$$\sum_{n=1}^{\infty} \frac{\chi_k(n)}{n^s} = \prod_{p\in\mathbb{P}} \sum_{n=1}^{\infty} \frac{\chi_k(p^n)}{p^{sn}} = \prod_{p\in\mathbb{P}} \frac{1}{1-\chi_k(p)p^{-s}} \tag{3}$$

is thus obtained whenever $s$ is chosen such that the power series are convergent. Whilst I managed to arrive at this equation through a personal investigation of the subject matter,

[4] The totally multiplicative quality amounts to the statement $\forall a, b : \chi_k(ab) = \chi_k(a)\chi_k(b)$, allowing for assertion of the fact that $\chi_k(a^n) = \chi_k^n(a)$.

[5] More specifically: the $n$th coefficient in the sum of the power series for a given prime is the Dirichlet character of the $n$th power of that prime, which is equivalent to the $n$th power of that prime's Dirichlet character.

Wuthrich asserts its validity in [29] with greater detail. Note that setting $\chi_k(n) = 1$ in equation 3 turns the middle expression's power series into simple geometric series. An extremely elegant but algebraically simplistic analog of this method allowed Euler to arrive in [12] at the product formula

$$\prod_{p\in\mathbb{P}} \frac{1}{1-\frac{1}{p^s}} = \sum_{n=1}^{\infty} \frac{1}{n^s} \tag{4}$$

for the much-renowned Riemann zeta function. This particular equation would come to be known as Euler's product. Equation 1 and several other equally impressive results are subsequently demonstrated in [12] by what effectively amounts to algebraic manipulations involving this type of product. Much later works (e.g. [19],[28]) would come to invoke the name 'Euler products' for all algebraic transformations of this general type. It must be noted that Euler's product is certainly the most prevalent of all Euler products and arguably the most important. A general notion of Euler products has nevertheless been presented here (as equation 3) because of its profound connections to sieve theory and its tremendous potential as an analytical tool.

### 3.2 Divergence of the summed prime reciprocals

Despite Euler's extraordinary genius his notation occasionally lacks finesse by modern standards (or perhaps it is us, mere mortals, who lack the master's understanding). In particular several ultimately inconsequential liberties were taken with regard to the values of divergent series and the relative magnitude of infinitesimal terms. The reader is referred to [2] for further insights into the specific technicalities that are omitted in Euler's work. These are inconsequential in the sense that any potential gaps in the proof have long since been closed, some even by Euler's own subsequent publications. They however remain of consequence to the intricacy and length of a formal proof for equation 1 derived from the immensely powerful result titled 'Theorem 19' in [12]. Luckily a brief and remarkably simple proof of equation 1 instead attributable to Paul Erdõs can yet be provided here. The proof is by contradiction. Assume the summed reciprocals of primes to converge. Then for some $k$ we must have

$$\sum_{n=k+1}^{\infty} \frac{1}{p_n} < \frac{1}{2} \quad .$$

Now consider the function $S_k(x)$ which counts those integers smaller than $x$ whose only prime factors are amongst the first $k$ primes. By writing each of these integers as $nm^2$ with $n$ squarefree it is quickly observed that

$$S_k(x) < 2^k\sqrt{x}$$

since $m^2 \leq nm^2 < x$ and the number of possible choices for $n$ is at most $2^k$, the number of combinations of the first $k$ primes. The number of positive integers smaller than $x$ which are divisible by the prime $p$ is at most $\frac{x}{p}$, so the number of integers smaller than $x$ divisible by any prime other than the first $k$ primes is then at most

$$\sum_{n=k+1}^{\infty} \frac{x}{p_n} < \frac{x}{2}$$

by assumption. However, the number of such integers must additionally equal $x - S_k(x)$ since every integer except 1 has a prime divisor. Now $x - S_k(x) < \frac{x}{2}$ gives

$$\frac{x}{2} < S_k(x) < 2^k\sqrt{x} \quad .$$

Setting $x$ to be at least $2^{2k+2}$ then gives the contradiction $2^{2k+1} < 2^{2k+1}$ so the assumption must be false and the sum $\sum_{p\in\mathbb{P}} \frac{1}{p}$ therefore diverges. $\square$

Erdõs was extremely prolific throughout the twentieth century and the precise provenance of this proof could hence not be ascertained. In addition to this and many other contributions Erdõs was involved in the development of an elementary proof of the prime number theorem from section 4.1 by way of events which [13] extensively documents.

### 3.3 Brun's sieve

Brun did not show the convergence of equation 2 directly. Rather, he demonstrated an upper bound for the twin prime counting function which was in turn used to establish convergence. The twin prime counting function is the function $\pi_2$ defined as

$$\pi_2(x) = \sum_{\substack{p\in\mathbb{P}_2 \\ p\leq x}} 1 + \sum_{\substack{p\in\mathbb{P}_2 \\ (p+2)\leq x}} 1 \quad \text{for } x \in \mathbb{N} \quad .$$

It counts the number of members of twin prime pairs not exceeding $x$ in magnitude. The bound Brun established is sometimes known as Brun's theorem.[6]

**Theorem 3.1** (Brun's theorem). *There exists a positive constant $C$ so that the number $\pi_2(x)$ of members of twin prime pairs not exceeding $x$ satisfies*

$$\pi_2(x) < C * x * \Big(\frac{\log\log x}{\log x}\Big)^2, \quad \forall x \geq 3 \quad .$$

The proof of Brun's theorem effectively consists of three steps. For the first step, the goal is to separate a suitable remainder from the twin prime counting function. In the second step the magnitude of this remainder is analysed. An upper bound for $\pi_2(x)$ is thus constructed. The third step consists of identifying a choice of variables that allows the upper bound to be conveniently expressed in terms of the argument of the twin prime counting function alone. In this three-step approach the reasoning of [26] is followed closely. As another less lengthy alternative to Brun's original paper [3], a somewhat different approach is offered in [21]. The only shortcoming of the proof in [21] is that it fails to analyse the size of a particular error term. This is however not a total loss as understanding of the proof is significantly facilitated by the omission, and said error term can in fact be analysed with the aid of the prime number theorem. In one further alternative, slides $10 - 13$ in a talk given by Sun [27] also demonstrate the idea behind the proof succinctly. A rudimentary outline of the proof for Brun's theorem now follows. It is intended not only to shed light on the inner workings of Brun's sieve itself, but also to hopefully provide some insight into the way in which bounds can be obtained by sieving techniques in general.

As previously mentioned the proof begins by separating a suitable remainder from $\pi_2(x)$, the twin prime counting function. This is achieved by separating it into a 'head' ($H$) and a 'tail' ($T$) segment, with the cut-off point $y < x$ to be determined later. The 'head' segment

[6] In other cases, the name "Brun's theorem" might be used to refer to equation 2 directly.

simply counts all primes smaller than some chosen number. Of course not all of these are twin primes, but overcounting in the 'head' is of minor importance as the proof instead rests on clever analysis of the 'tail' and an appropriate choice for the cut-off point. The 'tail' segment counts all odd numbers $n < x$ for which the product $n(n+2)$ is not divisible by any of the odd primes smaller than the chosen cut-off. The reader should convince theirself at this point that the two segments

$$H(y) + T(x, y) \geq \pi_2(x)$$

have together accounted at least for every twin prime no greater than $x$. The 'tail' is then written as all of the odd numbers smaller than $x$ minus an alternating sum

$$T(x, y) = \left\lceil \frac{x}{2} \right\rceil + \sum_{i=1}^{H(y)} (-1)^i \sum_{j=1}^{\binom{H(y)}{i}} D(x, i, j) \tag{5}$$

where $D(x, i, j)$ counts the amount of odd numbers $k < x$ for which $k(k+2)$ is divisible by some product of precisely $i$ specific primes all smaller than $H(y)$, and $j$ is an index for the combinations of such primes. The point of the alternating sum is to exclude precisely those odd numbers for which $n(n+2)$ *is* divisible by any prime smaller than the chosen cut-off. This is achieved by the principle of inclusion-exclusion through alternate subtraction and addition of the odd numbers for which $n(n+2)$ is divisible by some individual prime (smaller than the cut-off), some product of two primes, et cetera until the product of all primes up to the cut-off is reached. Also by the principle of inclusion-exclusion, whenever this alternating sum is truncated at an even number of terms $l$ it remains assured that

$$T(x, y) \leq \left\lceil \frac{x}{2} \right\rceil + \sum_{i=1}^{l} (-1)^i \sum_{j=1}^{\binom{H(y)}{i}} D(x, i, j)$$

and thus no more than the required amount of odd numbers has been eliminated. Subsequently the Chinese remainder theorem allows the establishment of values for the individual terms $D(x, i, j)$ occuring inside the alternating sum. It is vital that the sum be truncated at an even number of terms not only because this is required by the inclusion-exclusion principle, but also since the remainder theorem would not otherwise permit for such evaluation. Together, these methods make it possible to write the 'tail' segment in a fashion that can be feasibly evaluated. Performing this evaluation is the second step of the proof. Here the method of Euler products is utilized, alongside a bound on the value of specific partial sums known as Mertens' second theorem, in order to simplify the expression derived in step one. This eliminates the most problematic terms from the original expression for the 'tail'. The remaining terms can be analysed with the aid of bounds on the prime counting function developed from the prime number theorem treated in the next chapter. This produces an expression now devoid of summations, although it still contains the chosen cut-off point $y$ as an argument. The third step of choosing a suitable function of $x$ as a value for the cut-off point is then comparatively simple. An appropriate choice for the cut-off point always takes the form $y = x^{1/c \log \log(x)}$ wherein the specific value of $c$ hinges on the trunctation point $l$ chosen for the alternating sum in step one, and on the degree of care observed with regard to the establishment of bounds on the summands in step two.

To arrive at equation 2 from Brun's theorem is a fairly straightforward endeavour. It is achieved here in a fashion taken from [27]. By Brun's theorem a constant $\tilde{C}$ exists such that

$$\pi_2(x) < C * x * \Big(\frac{\log\log x}{\log x}\Big)^2 \leq \tilde{C}\frac{x}{(\log x)^{1.5}} \quad \forall x \geq 3 \quad .$$

Let $t_n$ be the $n$-th twin prime. Then

$$n = \pi_2(t_n) < \tilde{C}\frac{t_n}{(\log t_n)^{1.5}} \quad \text{and so} \quad \frac{1}{t_n} < \frac{\tilde{C}}{n(\log n)^{1.5}} \quad .$$

By now summing over all twin primes it is seen that

$$\sum_{p\in\mathbb{P}_2}\frac{1}{p} = \sum_{n=1}^{\infty}\frac{1}{t_n} < \sum_{n=1}^{\infty}\frac{\tilde{C}}{n(\log n)^{1.5}} < \infty$$

since $\sum 1/n(\log n)^{1+\varepsilon}$ converges for $\varepsilon > 0$. Because

$$2\sum_{p\in\mathbb{P}_2}\frac{1}{p} > \sum_{p\in\mathbb{P}_2}(\frac{1}{p} + \frac{1}{p+2})$$

equation 2 follows directly from this observation. □

With this conclusion, the exploration of reciprocal sums has been completed. The upcoming chapter deals with the notion of prime number distributions, beginning with an important result that permeates throughout the crevices of number-theoretic results.

# 4 The prime number theorem

Knowledge of the distribution (or density function) of primes is arguably one of the most basic tools available in contemporary number theory. Although perhaps to a slightly lesser extent than the Riemann zeta function, it underpins many findings in this field of study.

## 4.1 On the density function of prime numbers

No concrete theorems have yet been confirmed for the distribution of twin primes, but the distribution of prime numbers is well-established. This establishment originated with a theorem on the asymptotic distribution of primes known as the prime number theorem.

**Theorem 4.1** (Prime number theorem)**.** *The value of the prime counting function $\pi(x)$ asymptotically approaches $\frac{x}{\log x}$ as $x$ approaches infinity.*

This theorem can be stated as

$$\lim_{x\to\infty}\frac{\pi(x)}{x/\log x} = 1 \quad (\text{notation:} \quad \pi(x) \sim \frac{x}{\log x}) \quad .$$

There can be no such thing as the original prime number theorem given that Jacques Hadamard [15] discovered it independently of Charles-Jean de la Vallée Poussin [7]. In an interesting display of synchronicity, [13] notes that it was also first conjectured independently by two (much-renowned) mathematicians, Legendre and Gauss. A short proof of the prime number theorem reccommended to the reader is proffered in [30]. Although providing some extremely valuable insight into the distribution of the primes, as an approximation to $\pi(x)$ it leaves much to be desired. For instance, describing its asymptotic behavior fails to provide any lower or upper bounds on the prime counting function. It is therefore unsurprising that many refinements to the prime number theorem have since been devised. Strict lower and upper bounds on $\pi(x)$ are due to Dusart, who showed in [10] that

$$\pi(x) \geq \frac{x}{\log x}\left(1 + \frac{1}{\log x} + \frac{1.8}{\log^2 x}\right), \quad x \geq 32299 \quad ,$$
$$\pi(x) \leq \frac{x}{\log x}\left(1 + \frac{1}{\log x} + \frac{2.51}{\log^2 x}\right), \quad x \geq 355991 \quad ,$$

basing that result in part on earlier efforts by Chebyshev. The continued refinement of these bounds to increasingly tight derivate forms

$$\frac{x}{a + \log x} < \pi(x) < \frac{x}{A + \log x}, \quad \forall x \geq x_0$$

for real numbers $a, A, x_0$ is a work that remains ongoing. The most notable improvement of the prime number theorem is perhaps its approximation

$$\pi(x) \sim \mathrm{Li}(x) = \int_2^x \frac{dt}{\log t} \tag{6}$$

by the offset logarithmic integral $\mathrm{Li}(x)$. This was first speculated by Gauss before the prime number theorem was ever even proved. Modern methods have since revealed this approximation to be much more accurate than the original $x/\log x$. This is to say that the deviation $\pi(x) - (x/\log x)$ is $\mathcal{O}(x/\log^2 x)$, whereas it is $\mathcal{O}(x/e^{c\sqrt{\log x}})$ in the approximation by $\mathrm{Li}(x)$ (See pages 36-43 of Dusart's thesis [9] for the derivation, but be forewarned said pages are of exceeding complexity). Whilst these error terms are the result of modern (and ongoing) investigations, in [5] Chebyshev had already demonstrated prior to the prime number theorem's advent that $\mathrm{Li}(x)$ would be a better approximation of $\pi(x)$ than any rational function of $x/\log x$. Accuracy remains nevertheless a relative term: the difference $|\pi(x) - \mathrm{Li}(x)|$ does in fact still grow arbitrarily large, as Littlewood demonstrates in [20]. Riemann had postulated that $\mathrm{Li}(x) - \frac{1}{2}\mathrm{Li}(\sqrt{x})$ or any like expansion over some finite number of further terms might be an even better approximation, but Edwards' book [11] on the zeta function remarks that such a notion was later disproved by Littlewood. It was additionally Littlewood who, in collaboration with Hardy, contrived the 'best guess' currently available on the density of twin primes. This is to be the topic of the following section.

## 4.2 On the density function of twin primes

In analogy to the prime number theorem, a conjecture known as the $k$-tuple conjecture (originally called Theorem X in [16]) first posed by Littlewood and Hardy is the closest any have come to describing the density function of the twin primes. It rests on a rather complicated hypothesis which is here omitted from consideration. The notion of admissible sets must however be introduced.

**Definition 4.2** (Admissible set). *Let $H$ be a set of $k$ integers. When there exists no prime $p$ such that $\{h \mod p \mid h \in H\}$ contains all congruence classes modulo $p$, $H$ is said to be admissible.*

Sophisticated sieves like those later employed by Selberg and Zhang would come to utilize this very same notion of admissible $H$. The $k$-tuple conjecture is also commonly known as the first Hardy-Littlewood conjecture in honor of its creators. The conjecture does not make an explicit assertion about the density of twin primes but rather considers the density of all prime constellations. It is stated as follows:

**Conjecture 4.3** ($k$-tuple conjecture). *For every admissible $H$ there exist infinitely many primes $p$ such that the set $\{p+h\ |h \in H\}$ consists wholly of primes. Moreover, the asymptotic density of the function $\pi_H(x)$ counting the number of such primes below $x$ can be expressed in terms of the members of $H$ by the formula*

$$\pi_H(x) \sim 2^{k-1} \int_2^x \frac{dt}{\log^k t} \prod_{q \in \mathbb{P}\setminus 2} \frac{1 - \frac{r(H,q)}{q}}{\left(1 - \frac{1}{q}\right)^k}$$

*where $r(H,q)$ counts the amount of distinct residues modulo $q$ of the members of $H$.*

It is easy to derive (by the Chinese remainder theorem) that for *inadmissible* $H$, the existence of infinitely many prime sequences $\{p+h\ |h \in H\}$ can be ruled out. At a glance, the $k$-tuple conjecture might therefore appear to be just a wild guess much like Polignac's conjecture from earlier in this text (which is simply a weaker form for the case $k = 2$ of the $k$-tuple conjecture). Closer inspection of the hypothesis on which it rests and the fashion in which that was arrived at however reveals this not to be the case. The $k$-tuple conjecture is commonly believed to be true, despite the fact that a proof has thus far eluded the mathematical community. The special case $H = \{0, 2\}$ allows for a result of particular interest. It is sometimes referred to as the strong twin prime conjecture, and states that

$$\pi_2(x) \sim 2\Pi_2 \int_2^x \frac{dt}{\log^2 t}$$

wherein the twin primes constant

$$\Pi_2 = \prod_{p \in \mathbb{P}\setminus 2} \frac{p(p-2)}{(p-1)^2} \approx 0.66$$

arises from the right-hand term of the $k$-tuple conjecture. Note in particular the similarity of this expression to equation 6 up to the power of the logarithm. Although unproven, this statement provides the clearest insight into the distribution of twin primes currently available.

# 5 A criterion for twin primes

In spite of the apparent lack of fully proven results on twin primes a rock-solid criterion for twin primes does in fact exist. Like many of the results on twin primes it relates strongly to an analogous theorem on prime numbers. This result is known as Wilson's theorem.

**Theorem 5.1** (Wilson's Theorem). *A strictly positive number $n$ is prime if and only if $(n-1)! \equiv -1 \mod n$.*

This was subsequently used by Clement in [6] to arrive at a neccesary and sufficient condition for twin primes. Since

$$\begin{aligned} &(p-1)! + 1 \equiv 0 \mod p \quad \text{and} \\ &(p+1)! + 1 \equiv 0 \mod (p+2) \end{aligned}$$

both hold whenever $p$ is a twin prime, some simple modular arithmetic can be used to derive the following criterion for twin primes: $p$ is a twin prime if and only if

$$4\big((p-1)! + 1\big) + p \equiv 0 \mod p(p+2) \quad .$$

Sadly, this criterion is rendered computationally ineffective by the appearance of the factorial. The term on the left-hand side is simply too large to be of any use in establishing whether a number $p$ is a twin prime or not. With some additional effort, it can be derived from this criterion that all twin prime pairs excepting the first one are of the form $6n-1, 6n+1$ for some $n \in \mathbb{N}$. This is of somewhat greater utility both for the purpose of applying sieving techniques as well as to any exhaustive search for twin primes up to a given number.

## 6 Modern methods

Advancements in the fields of modular arithmetic and group theory at large have enabled several leaps of progress in the late 20th and early 21st centuries. A notable example is that of Selberg's sieve. Some notation must be introduced to express this idea. The notation used below was taken from [27]. Let (a,b) denote the greatest common divisor of $a$ and $b$. In this notation $(a,b)=1$ means $a$ and $b$ are coprime. Let $A$ be a finite sequence of integers and $P \subseteq \mathbb{P}$ any set of primes. Then

$$S(A,P,z) = \sum_{\substack{a\in A \\ (a,P_z)=1}} 1 \quad \text{where} \quad P_z = \prod_{\substack{p\in P \\ p\leq z}} p$$

is the amount of numbers in $A$ coprime to all primes from $P$ smaller than $z$. Roughly speaking, the purpose of the Selberg sieve technique is to derive an upper bound for $S(A,P,z)$ based on general functions $f$ which satisfy certain properties. The properties which are neccesary for such $f$ are omitted here for the sake of convenience (They are made explicit on slide 17 of [27]). Letting $|A|$ denote the number of members of $A$, the bound is given by

$$S(A,P,z) \leq \frac{|A|}{F} + \sum_{\substack{i\leq z^2 \\ i|P_z}} R(A,f,i) \quad \text{where} \quad F = \sum_{\substack{n\leq z \\ p|n\Rightarrow p\in P}} f(n) \tag{7}$$

and $R$ represents a positive remainder term that depends only on the set $A$ and the values $i$ and $f(i)$. This inequality can be observed by relying on Möbius inversion in order to separate a squared sum from $S(A,P,z)$ and applying the Cauchy-Schwartz inequality to the separated term in order to establish the equation. Omitting further discourse on Möbius transforms, it is remarked here merely that for squarefree $m = \prod_k p_k$, the sign of the Möbius function $\mu$ given by

$$\mu(m) = \mu(p_a p_b \cdots p_k) = \begin{cases} 0, & \text{if } \exists p \in \mathbb{P} : p^2|m \quad , \\ -1, & \text{if } k \text{ is odd and } m \text{ squarefree,} \\ 1, & \text{if } k \text{ is even and } m \text{ squarefree} \end{cases}$$

corresponds precisely to the sign of the alternating sum obtained for $T$ in equation 5. Using the Cauchy-Schwartz inequality unfortunately implies that this technique can only provide upper bounds. The sifting technique proposed however does not explicitly require use of Cauchy-Schwarz inequality, it is merely used by Selberg to conveniently arrive at the bound that equation 7 expresses. Reference [27] outlines only the particular application of Selberg's sieve treated here; a more detailed investigation of Selberg's sieve method within the wider context of sieve theory can be read back in [28]. Through use of clever constructions for $A$ and $f$, the Cauchy-Schwartz argument can be omitted to derive a broad spectrum of statements about the occurence of numbers fitting certain predicates in specific intervals.

This is precisely what was subsequently done by Chen Jingrun to arrive at a phenomenal result. Let $m$ be an even fixed integer. Chen attempted to count the number of primes $p$ whose difference $m - p$ could be expressed as a product $\prod_i p_i$ of no more than $k$ primes. He then established that for $k = 2$ and sufficiently large $m$, this number of primes *is bounded below by one*. The number one is used here in place of Chen's more sophisticated expression but the essence of the result remains unchanged. See [25] for a translated version of Chen's proof attributable to Ross. The truth of the proposition that

$$\exists n_0 \in \mathbb{N} : \forall n \in \mathbb{N} : 2n \geq n_0 \Rightarrow (2n = p_a + p_b \vee 2n = p_a + p_b p_c \text{ for some } p_a, p_b, p_c \in \mathbb{P})$$

is a direct consequence of that result. This statement comes remarkably close to the Goldbach conjecture. The constructed bound further implies the conclusion that $p+2$ can be written as a product of no more than two primes for infinitely many distinct $p$. These conjoined facts carry Chen's name by way of the following theorem:

**Theorem 6.1** (Chen's theorem)**.**

*(i) Large even numbers can be written as $p + n$, where $p \in \mathbb{P}$ and either $n \in \mathbb{P}$ or $n = p_a p_b$ for $p_a, p_b \in \mathbb{P}$.*

*(ii) There are infinitely many primes $p$ such that either $(p + 2) \in \mathbb{P}$ or $(p + 2) = p_a p_b$ for $p_a, p_b \in \mathbb{P}$.*

In a sense it can be argued that Chen's theorem is, simultaneously, the closest proven proximate to both the Goldbach and twin prime conjectures.

Yet another major breakthrough in the field arrived in 2013, when hitherto unknown mathematician Zhang Yitang managed to prove in [31] the existence of a bound on the prime gap. To see what is meant by this, first recall the definition (for arbitrary sequences $a_k$) of the limit inferior:

$$\liminf_{n\to\infty} a_n = \lim_{n\to\infty} \left( \inf_{m\geq n} a_m \right) = \sup_{n\geq 0} \inf_{m\geq n} a_m \quad .$$

The prime gap $\liminf_{n\to\infty}(p_{n-1} - p_n)$ therefore represents the minimal distance occuring in between consecutive primes of arbitrary magnitude. Note also that the prime gap represents a specific distance between prime numbers which must occur on an infinite number of distinct occasions. Zhang discovered that the prime gap was bounded by building on a result of Goldston, Pintz and Yildirim [14] who had previously managed to establish the similar but far less effectual bound

$$\liminf_{n\to\infty} \frac{(p_{n-1} - p_n)}{\sqrt{\log p_n}(\log\log p_n)^2} < \infty \quad .$$

Zhang used a slightly different approach developed by Motohashi and Pintz [23] combined with a strengthened version of the older Bombieri-Vinogradov theorem (published first by Barban [1]). The mentioned theorem and methods are conveniently compiled in [27] should the reader seek to investigate them more closely. Furthermore, he was able to arrive at a new bound for the partial sums of exponential functions that contain inverse values of modular residues. These techniques allowed Zhang to conclude his main result

$$\liminf_{n\to\infty}(p_{n-1} - p_n) < 7 * 10^7 \quad .$$

He proceeded to state about his result that to "replace the right-hand side... by a value as small as possible is an open problem that will not be discussed in this paper". This took mathematicians from all over the world by storm and a flurry of activities was set off to improve Zhang's bound. Terence Tao announced a collaborative project "Polymath8a" and the bound was eventually reduced to 4680. But the race was not yet run. James Maynard had been working in the meantime to revive Goldston, Pintz, and Yildirim's original approach and his efforts eventually proved successful, culminating in the 2015 publication of his work [22] in which a bound of 600 was obtained. The preprint of this article provoked another Polymath collaboration whereby the bound was further lowered to 246 in april 2014, where it continues to stand today. Publication of this latest Polymath bound is still pending.

## 7 Twin primes in practice

Although mathematicians have always been fascinated by primes, in centuries past these numbers have had little to no bearing on day-to-day existence. With the advent of RSA encryption, prime numbers have finally found their way into practical application. Sadly there is nothing to suggest that twin primes are of particular use to a secure and simple RSA encryption-decryption process. Outside of the RSA method, prime numbers still reside in relative obscurity from a pragmatic perspective. Thus it seems that twin primes, for now, must still wait their turn.

The two most obvious applications for twin primes that spring to mind could hardly be considered immediately practical by any stretch of the imagination. These are applications towards either the Goldbach conjecture or the Riemann hypothesis. Both equally famous statements, the Goldbach conjecture asserts that all even numbers greater than 2 can be written as the sum of two primes. The Riemann hypothesis is the statement that all non-trivial complex roots of the Riemann zeta function $\zeta(s)$ lie on the critical line $\mathrm{Re}(s) = \frac{1}{2}$. On top of the fact that both of these assertions lack immediate pragmatic merit, it is also unlikely that either of these statements would definitively follow from a result on twin primes. For the case of the Goldbach hypothesis, Chen's theorem is definitively the closest one could hope to obtain by existing methods in sieve theory (Tao explicitly states this in [28]). For the case of the Riemann Hypothesis, while it is possible that new insight into twin primes could reveal more information about the nature of *some* of the complex roots, it seems impossible that it could achieve this for *all* roots, given the simple fact that not every prime is a twin prime. Because of the nature of this relationship it has traditionally been the case that insight into the zeta function allowed for conclusions about twin primes (as was the case for Brun in [3]) rather than the other way around.

Only one clear-cut case where the study of twin primes did indeed foster an entirely pragmatic beneficial effect readily presents itself. This concerns the curious case of the Pentium FDIV bug. In an attempt to calculate Brun's constant starting in 1993, Thomas Nicely employed a then-common pentium processor to calculate Brun's constant through an enumeration of the terms of its sum up to $1.6 * 10^{15}$. To his great surprise, his inititial findings resulted in a contradiction. Laborious investigation of the computation revealed that it was not his method, but in fact the pentium chip itself that was at fault. For specific large integers, the FDIV division algorithm of the processor would return incorrect values. A considerable amount of media attention was given to this discovery, and Intel was soon forced to offer replacements for the defective chips to all customers. Although the majority of owners would ostensibly decline to take Intel up on this offer, the company still wrote off a loss of 475 million dollar in the month after the recall. While this was by no means an intended result, it arguably still represents the greatest practical impact that research on twin primes has ever produced up to this point.

## 8 Discussion

While Chen's theorem and a prime gap of 246 are both still a far cry from proof of the twin prime conjecture, it can safely be stated that the theory of twin primes has developed quite far in its now nearly 150-year old existence. Unfortunately, it was asserted through the Polymath project that the methods of Zhang and Maynard would never yield a bound below 6, even if they were to be shown to hold true in the most general setting imaginable. The method of Chen has already likewise been stretched to its limit. It is therefore unlikely that the twin prime conjecture is to be proven any time soon. Nonetheless this investigation has hopefully succeeded to provide some insight on not just the twin prime conjecture, but also into the nature of the sieve process that drives all these results. Several truly historic results and memorable pieces of literature have passed the review. In that regard, this author wishes to mention that Euler's [12] is in his mind an exceptionally insightful publication containing a great number of groundbreaking results. There remains a single case relating to the twin prime conjecture which I was unable to research due to time constraints. This concerns the 2004 publication by Arensdorf of a flawed proof for the twin prime conjecture that was later retracted. While it would be highly unlikely for a 15-year old retracted piece of research to be able to shed new light on an old and open problem, it does warrant mention as a piece of potentially significant literature that was deliberately omitted from these considerations.

## References


[1] MB Barban. New applications of Linnik's 'large sieve'. *Akad. Nauk Uzbek. SSR Trudy Inst. Mat*, 22:1–20, 1961.

[2] Lluís Bibiloni, Pelegrí Viader, and Jaume Paradís. On a series of Goldbach and Euler. *The American Mathematical Monthly*, 113(3):206–220, 2006.

[3] Viggo Brun. La serie 1/5+ 1/7+ 1/11+ 1/13+ 1/17+ 1/19+ 1/29+ 1/31+ 1/41+ 1/43+ 1/59+ 1/61+... ou les denominateurs sont" nombres premiers jumeaux" est convergente ou finie. *Bull. Sci. Math.(2)*, 43:124–128, 1919.

[4] Chris K Caldwell and Yeng Xiong. What is the Smallest Prime? *Journal of Integer Sequences*, 15(9.7):1–9, 2012.

[5] Pafnutiĭ L'vovich Chebyshev. *Oeuvres de PL Tchebychef*, volume 1, pages 711–714. Commissionaires de l'Académie impériale des sciences, 1899.

[6] PA Clement. Congruences for sets of primes. *The American Mathematical Monthly*, 56(1):23–25, 1949.

[7] Charles-Jean de la Vallée Poussin. *Recherches analytiques sur la théorie des nombres premiers.* Hayez, Imprimeur de l'Académie Royale de Belgique, 1897.

[8] William Dunham. A Note on the Origin of the Twin Prime Conjecture. In *Notices of the International Congress of Chinese Mathematicians*, volume 1, pages 63–65. International Press of Boston, 2013.

[9] Pierre Dusart. *Autour de la fonction qui compte le nombre de nombres premiers*. PhD thesis, Université de Limoges, 1998.

[10] Pierre Dusart. Inégalités explicites pour $\psi(x), \theta(x), \pi(x)$ et les nombres premiers. *Comptes Rendus Mathématiques de l'Académie des Sciences. La Societe Royale du Canada*, 2:53–59, 1999.

[11] Harold M Edwards. *Riemann's zeta function*, pages 34–36,87–88. Academic press, 1974.

[12] Leonhard Euler. Variae observationes circa series infinitas. *Commentarii academiae scientiarum imperialis Petropolitanae*, 9(1737):160–188, 1737.

[13] Dorian Goldfeld. The elementary proof of the prime number theorem: An historical perspective. In *Number Theory*, pages 179–192. Springer, 2004.

[14] Daniel A Goldston, János Pintz, Cem Yalçin Yıldırım, et al. Primes in tuples ii. *Acta mathematica*, 204(1):1–47, 2010.

[15] Jacques Hadamard. Sur la distribution des zéros de la fonction $\zeta$ (s) et ses conséquences arithmétiques. *Bull. Soc. Math. France*, 24(2):199–220, 1896.

[16] Godfrey H Hardy and John E Littlewood. Some problems of 'partitio numerorum'; iii: On the expression of a number as a sum of primes. *Acta Mathematica*, 44:52–68, 1923.

[17] David E Joyce. Euclid's Elements. Retrieved 20 december 2018 at `https://mathcs.clarku.edu/~djoyce/java/elements/elements.html`. Book IX, prop. 20.

[18] Dominic Klyve. *Explicit bounds on twin primes and Brun's Constant*. PhD thesis, Dartmouth College, New Hampshire, 2007.

[19] Robert P Langlands. *Euler products*, chapter 1+2, pages 3–8. Yale University Press New Haven, 1971.

[20] John E Littlewood. Sur la distribution des nombres premiers. *Comptes Rendus Mathématiques de l'Académie des Sciences, Paris*, 158:1869–1872, 1914.

[21] David Lowry-Duda. A Friendly Intro to Sieves with a Look Towards Recent Progress on the Twin Primes Conjecture. *arXiv preprint arXiv:1401.7555*, 2014.

[22] James Maynard. Small gaps between primes. *Annals of mathematics*, pages 383–413, 2015.

[23] Yoichi Motohashi and János Pintz. A smoothed GPY sieve. *Bulletin of the London Mathematical Society*, 40(2):298–310, 2008.

[24] Thomas R Nicely. Enumeration to 1.6e15 of the twin primes and Bruns constant. `http://www.trnicely.net/twins/twins2.html`, 1999.

[25] PM Ross. On Chen's theorem that each large even number has the form p1+ p2 or p1+ p2 p3. *Journal of the London Mathematical Society*, 2(4):500–506, 1975.

[26] Tjerand Silde. Elementary sieve methods and brun's theorem on twin primes. Retrieved 21 januari 2019 at `https://wiki.math.ntnu.no/_media/ma3001/2014v/analytisktallteori/tjerand_silde_project_ma3001.pdf`, 2014.

[27] Zhi-Wei Sun. Towards the twin prime conjecture, 2014. Conference talk slides.

[28] Terence Tao. 254a, Notes 4: Some sieve theory. Retrieved 21 januari 2019 at `https://terrytao.wordpress.com/2015/01/21/254a-notes-4-some-sieve-theory/`, januari 2019, January 2015. Supplementary notes to course 254A in analytic prime number theory.

[29] Christian Wuthrich. *Further Number Theory*, chapter 4. University of Nottingham, 2011.

[30] Don Zagier. Newman's short proof of the prime number theorem. *The American mathematical monthly*, 104(8):705–708, 1997.

[31] Yitang Zhang. Bounded gaps between primes. *Annals of Mathematics*, pages 1121–1174, 2014.

# A Euclid's proof of the infinitude of primes

From **Book IX** of Euclid's **Elements**

> Proposition 20:
> *Prime numbers are more than any assigned multitude of prime numbers.*
>
> Let $A$,$B$, and $C$ be the assigned prime numbers.
> I say that there are more primes than $A$, $B$, and $C$.
> Take the least number $DE$ measured by $A$, $B$, and $C$.
> Add the unit $DF$ to $DE$. Then $EF$ is either prime or not.
> First, let it be prime. Then the prime numbers $A$, $B$, $C$, and $EF$ have been found which are more than $A$, $B$, and $C$.
> Next, let $EF$ not be prime. Therefore it is measured by some prime number. (book VII, proposition 31: *any composite number is measured by some prime number*)
> Let it be measured by the prime number $G$.
> I say that $G$ is not the same with any of the numbers $A$, $B$, and $C$.
> If possible, let it be so. Now $A$, $B$, and $C$ measure $DE$, therefore $G$ also measures $DE$. But it also measures $EF$. Therefore $G$, being a number, measures the remainder, the unit $DF$, which is absurd.
> Therefore $G$ is not the same with any one of the numbers $A$, $B$, and $C$. And by hypothesis it is prime. Therefore the prime numbers $A$, $B$, $C$, and $G$ have been found which are more than the assigned multitude of $A$, $B$, and $C$.
> Therefore, *prime numbers are more than any assigned multitude of prime numbers.*

The English translation is by David E. Joyce of the Clark University Department of Mathematics and Computer Science [17]. A modern statement of the proof is as follows: assume there exist only finitely many primes $p$. Observe that for the product of these primes we have that $1 + \prod p$ is not divisible by any of the $p$. This contradicts the assumption that all primes have been included and proves the infinitude of primes by contradiction. □

It is of interest to note that the ancient Greeks spoke of measurement rather than division, and of the unit rather than the number one. This anumerical (rather geometrical) inclination might go some length towards explaining why twin primes were apparently never considered in Euclid's era. It also warrants mentioning that Euclid must rely on the well-ordering principle for several proofs in the *Elements*, but never states it as an axiom.

# B The fundamental theorem of arithmetic and the Chinese remainder theorem

Due to their ubiquity in the field of number theory the fundamental theorem of arithmetic and Chinese remainder theorem are here presented.

**Theorem B.1** (Fundamental theorem of arithmetic)**.** *Every integer greater than* 1 *is either a prime or a product of primes. Moreover, the product is unique up to the ordering of the primes. This is to say that if*

$$p_1 p_2 \cdots p_i = n = q_1 q_2 \cdots q_j$$

*for primes* $p_1$ *through* $p_i$ *and* $q_1$ *through* $q_j$*, then* $i = j$ *and the products on the left and right can be reordered so that* $p_k = q_k$ *for all* $k \leq i = j$*.*

**Theorem B.2** (Chinese remainder theorem)**.** *For two coprime positive integers* $n$ *and* $m$*, there exists a unique* $k < nm$ *for every pair of integers* $\{a, b\}$*such that the congruences*

$$\begin{aligned} &k \equiv a \mod n \quad \textit{and} \\ &k \equiv b \mod m \end{aligned}$$

*both hold true simultaneously.*

The Chinese remainder theorem can naturally be extended to any greater number of positive integers and congruences provided that the integers in question are all pairwise coprime.