Lecture notes for Discrete mathematics of Paul Erdős - NDMI107


# A GLORIOUS BEGINNING

In 1845, Joseph Bertrand [3] conjectured that for every integer $n$ greater than 3 there is at least one prime $p$ such that $n < p < 2n - 2$. The slightly weaker proposition,

> for every positive integer $n$
> there is at least one prime $p$ such that $n < p \leq 2n$,

is known as *Bertrand's postulate* [19, Theorem 418]. (As all primes except 2 are odd, its constraint $n < p \leq 2n$ amounts to $n < p < 2n$ except when $n = 1$.)

In March 1931, the eighteen-year old Erdős found an elegant elementary proof of Bertrand's postulate; the following year, this proof appeared in his first publication [7]. [1] Later, Erdős became fond of quoting Nathan Fine's couplet that celebrated this achievement,

> *Chebyshev said it and I say it again:*
> *There is always a prime between* $n$ *and* $2n$.

The first draft of [7] was rewritten by László Kalmár, a professor at the University of Szeged and Erdős's senior by eight years; as Erdős recalls in [11], he said in the introduction that Srinivasa Ramanujan [25] found a somewhat similar proof. Erdős's proof (which was later reproduced in Hardy and Wright's classic monograph [19]) and its background are described in the next five sections; Ramanujan's proof is reproduced in section 8.

## 1 Binomial coefficients

When $m$ and $k$ are nonnegative integers, symbol $\binom{m}{k}$ — read "$m$ choose $k$" — denotes the number of $k$-point subsets of a fixed $m$-point set. For example, $\{1, 2, \ldots, 5\}$ has precisely ten 3-point subsets, namely,

$$\{1,2,3\}, \{1,2,4\}, \{1,2,5\}, \{1,3,4\}, \{1,3,5\},$$
$$\{1,4,5\}, \{2,3,4\}, \{2,3,5\}, \{2,4,5\}, \{3,4,5\},$$

[1] Erdős must have considered his 1929 article [6] in a Hungarian mathematics and physics journal for high school students unimportant: in [11] he refers to [7] as "[my paper ...] which was actually my very first".

and so $\binom{5}{3} = 10$. This combinatorial definition leads directly to a number of identities such as

$$\sum_{k=0}^{m} \binom{m}{k} = 2^m \tag{1}$$

(both sides count all subsets of a fixed $m$-point set, the left-hand side groups them by their size $k$),

$$\binom{m}{k} = \binom{m}{m-k} \tag{2}$$

(complementation $S \leftrightarrow T - S$ sets up a one-to-one correspondence between the set of all $k$-point subsets $S$ of a fixed $m$-point set $T$ and the set of all $(m-k)$-point subsets of $T$), and

$$\binom{m}{k} k = \binom{m}{k-1} (m-k+1) \tag{3}$$

(for a fixed $m$-point set $T$, both sides count the number of pairs $(S, x)$ such that $S \subseteq T$, $|S| = k$, and $x \in S$: the left-hand side chooses first $S$ and then $x$, the right-hand side chooses first $S - \{x\}$ and then $x$).

Erdős's proof of Bertrand's postulate employs two standard inequalities which follow easily from these identities. First, (1) with $m = 2n+1$ and (2) with $m = 2n+1$, $k = n$ imply that

$$\binom{2n+1}{n+1} \leq 4^n. \tag{4}$$

Second, (3) with $m = 2n$ guarantees that $\binom{2n}{n}$ is the largest of the $2n+1$ binomial coefficients $\binom{2n}{k}$ with $k = 0, 1, \ldots, 2n$, and so it is the largest of the $2n$ terms in the sum $2 + \sum_{k=1}^{2n-1} \binom{2n}{k}$, which totals $4^n$ by (1) with $m = 2n$; we conclude that

$$\binom{2n}{n} \geq \frac{4^n}{2n} \text{ whenever } n \geq 1. \tag{5}$$

By definition, we have $0! = 1$; induction on $k$ using identity (3) shows that

$$\binom{m}{k} = \frac{m!}{k!(m-k)!}\,. \tag{6}$$

This formula is also used in Erdős's proof.

Quantities $\binom{m}{k}$ are referred to as the *binomial coefficients* since they are featured in the *binomial formula*

$$(a+b)^m = \sum_{k=0}^{m} \binom{m}{k} a^k b^{m-k}.$$

Validity of this formula can be perceived by contemplating how its left-hand-side

$$(a+b)(a+b)\cdots(a+b)$$

distributes into a sum of $2^m$ terms, each of them having the form $a^k b^{m-k}$. The binomial formula reduces to (1) by setting $a = b = 1$.

## 2 A lemma

Bertrand's postulate asserts that, in a sense, primes appear in the sequence of positive integers relatively often. Paradoxically, Erdős's proof of the postulate relies on a lemma asserting that they do not appear too often: the product of all primes not exceeding a positive integer $m$ is less than $4^m$.

In number theory it is customary to reserve the letter $p$ for primes; in particular, Erdős's lemma can be recorded as

$$\prod_{p\le m} p < 4^m \quad \text{for every positive integer } m. \tag{7}$$

In 1939, a proof of (7) simpler than Erdős's original proof was found independently and almost simultaneously by Erdős and by Kalmár (see [11]). This proof goes by induction on $m$. The induction basis verifies (7) when $m \le 2$. In the induction step, we consider an arbitrary integer $m$ greater than 2 and assume that $\prod_{p\le k} p < 4^k$ whenever $k < m$; then we distinguish between two cases. If $m$ is even, then

$$\prod_{p\le m} p = \prod_{p\le m-1} p < 4^{m-1}.$$

If $m$ is odd, then $m = 2n+1$ with $n \ge 1$; since

$$\binom{2n+1}{n+1} = \frac{(n+2)\cdot(n+3)\cdot\ldots\cdot(2n+1)}{n!},$$

every prime in the range $n+1 < p \le 2n+1$ divides $\binom{2n+1}{n+1}$, and so

$$\prod_{p\le m} p = \left(\prod_{p\le n+1} p\right)\cdot\left(\prod_{n+1<p\le 2n+1} p\right) \le \left(\prod_{p\le n+1} p\right)\cdot\binom{2n+1}{n+1};$$

using the induction hypothesis and (4), we conclude that $\prod_{p\le m} p < 4^{n+1}\cdot 4^n = 4^m$.

## 3 The Unique Factorization Theorem

Every child knows that a prime is a positive integer divisible by no positive integer other than itself and the integer 1. However, not all children may be aware that the integer 1 is decreed to be not a prime, even though it is divisible by no positive integer other than itself. Ruling this integer out of the set of all primes is not an arbitrary decision: ruling it in would ruin the following theorem, known as the *Fundamental Theorem of Arithmetic* or the *Unique Factorization Theorem* [5].

> *For every positive integer* $n$ *and for all primes* $p$,
> *there are uniquely defined nonnegative integers* $e(p, n)$ *such that*
>
> $$n = \prod_p p^{e(p,\, n)}\,.$$

(For each $n$ only finitely many of the exponents $e(p, n)$ are nonzero: if $p > n$, then $e(p, n) = 0$.) Declaring 1 to be a prime would make the factorization no longer unique: $e(1, n)$ could assume any nonnegative integer value.

## 4 Legendre's formula

The product $1 \cdot 2 \cdot \ \ldots \ \cdot m$ of the first $m$ positive integers is denoted $m!$ and called the *factorial of* $m$. When $n$ is the factorial $m!$, the exponents $e(p, n)$ in the unique factorization

$$n = \prod_p p^{e(p,\, n)}$$

can be calculated from a neat formula. To begin, for every choice of positive integers $s$ and $t$ we have

$$st = \left(\prod_p p^{e(p,\, s)}\right) \cdot \left(\prod_p p^{e(p,\, t)}\right) = \prod_p p^{e(p,\, s)+e(p,\, t)},$$

and so

$$e(p,\, st) = e(p,\, s) + e(p,\, t).$$

It follows that

$$e(p, m!) = e(p, 1) + e(p, 2) + \ldots + e(p, m).$$

We are going to express the right-hand side sum in a more transparent way. Let us begin with the example of $p = 2$ and $m = 9$. Here,

$$e(2, 1) + e(2, 2) + \ldots + e(2, 9) = 0 + 1 + 0 + 2 + 0 + 1 + 0 + 3 + 0;$$

of the nine terms,

- every second one contributes at least one unit to the total
  and there are 4 such terms,

- every fourth one contributes at least two units to the total and there are 2 such terms,
- every eighth one contributes at least three units to the total and there is 1 such term,
- every 16th one contributes at least four units to the total and there are no such terms;

these observations make it clear that

$$0+1+0+2+0+1+0+3+0 = 4+2+1+0.$$

This identity can be illustrated by the array

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| $i=4$ | | | | | | | | | |
| $i=3$ | | | | | | | | ○ | |
| $i=2$ | | | | ○ | | | | ○ | |
| $i=1$ | | ○ | | ○ | | ○ | | ○ | |
| | $j=1$ | $j=2$ | $j=3$ | $j=4$ | $j=5$ | $j=6$ | $j=7$ | $j=8$ | $j=9$ |

where column $j$ holds a stack of $e(2,j)$ coins: the sum $0+1+0+2+0+1+0+3+0$ of the heights of the nine stacks counts the total number of coins and the sum $4+2+1+0$ counts the same number row by row. In general, for any choice of $p$ and $m$, there are stacks $1, 2, \ldots, m$ and stack $j$ holds $e(p,j)$ coins. Counting the total number $e(p,1)+e(p,2)+\ldots+e(p,m)$ of coins row by row, we end up with the sum $\lfloor m/p \rfloor + \lfloor m/p^2 \rfloor + \lfloor m/p^3 \rfloor + \cdots$ (where, as usual, $\lfloor x \rfloor$ denotes $x$ rounded down to the nearest integer): a coin appears in row $i$ and column $j$ if and only if $e(p,j) \geq i$, which is the case if and only if $j$ is a multiple of $p^i$. It follows that

$$e(p, m!) = \sum_{i=1}^{\infty} \left\lfloor \frac{m}{p^i} \right\rfloor$$

(where only finitely many terms in the infinite sum are not zero). This formula was presented by Adrien-Marie Legendre in the second edition of his *Essai sur la Théorie des Nombres*, published in 1808.

# 5 Erdős's proof of Bertrand's postulate

## 5.1 The plan.

Given a positive integer $n$, we shall choose a positive integer $N$ and prove that

$$\prod_{p \leq n} p^{e(p,\,N)} < \prod_{p \leq 2n} p^{e(p,\,N)}\,, \tag{8}$$

which obviously implies Bertrand's postulate. Our choice is $N = \binom{2n}{n}$. Since formula (6) with $m = 2n$ and $k = n$ reads

$$N \;=\; \frac{2n\cdot(2n-1)\cdot(2n-2)\cdot\ldots\cdot(n+1)}{n!}\;,$$

it is clear that all prime divisors of $N$ are at most $2n$, and so

$$\prod_{p\le 2n} p^{e(p,\,N)} = N.$$

We propose to prove that

$$\prod_{p\le n} p^{e(p,\,N)} < \frac{4^n}{2n}; \tag{9}$$

since (5) reads $4^n/2n \le N$, inequality (8) will then follow.

## 5.2 A formula for $e(p,N)$.

We will use the formula

$$e(p,N) = \sum_{i=1}^{\infty}\left(\left\lfloor\frac{2n}{p^i}\right\rfloor - 2\left\lfloor\frac{n}{p^i}\right\rfloor\right), \tag{10}$$

which follows directly from (6) combined with Legendre's formula. Note that

$$\lfloor 2x\rfloor - 2\lfloor x\rfloor \;=\; \begin{cases} 0 & \text{if} \quad 0 \le x - \lfloor x\rfloor < 1/2\;, \\ 1 & \text{if} \quad 1/2 \le x - \lfloor x\rfloor < 1\;, \end{cases}$$

and so

$$\left\lfloor\frac{2n}{p^i}\right\rfloor - 2\left\lfloor\frac{n}{p^i}\right\rfloor \;=\; 0 \text{ or } 1 \text{ for all } i. \tag{11}$$

## 5.3 An upper bound on $p^{e(p,\,N)}$.

Given $p$ and $n$, consider the largest integer $j$ such that $p^j \le 2n$. By (10) and (11), we have

$$e(p,N) = \sum_{i=1}^{j}\left(\left\lfloor\frac{2n}{p^i}\right\rfloor - 2\left\lfloor\frac{n}{p^i}\right\rfloor\right) \;\le\; j.$$

and so

$$p^{e(p,\,N)} \le 2n. \tag{12}$$

## 5.4 Splitting the left-hand side of (9).

We will partition the set of all primes not exceeding $n$ into three classes:

- the set $S$ of primes $p$ such that $p \le \sqrt{2n}$,
- the set $M$ of primes $p$ such that $\sqrt{2n} < p \le 2n/3$,
- the set $L$ of primes $p$ such that $2n/3 < p \le n$.

This classification reflects the size of $e(p, N)$: as we are about to prove,

$$p \in M \quad \Rightarrow \quad e(p, N) \le 1, \tag{13}$$

$$p \in L \quad \Rightarrow \quad e(p, N) = 0. \tag{14}$$

Our proof of these implications relies on formula (10): since

$$p > \sqrt{2n} \text{ and } i \ge 2 \quad \Rightarrow \quad 2n/p^i < 1 \quad \Rightarrow \quad n/p^i < 1,$$

we have

$$p > \sqrt{2n} \quad \Rightarrow \quad e(p, N) = \left\lfloor \frac{2n}{p} \right\rfloor - 2\left\lfloor \frac{n}{p} \right\rfloor. \tag{15}$$

Implication (13) follows directly from (15) and (11); implication (14) follows from (15) combined with the observation that $p \in L$ implies $\lfloor 2n/p \rfloor = 2$ and $\lfloor n/p \rfloor = 1$.

## 5.5 Putting the pieces together.

By definition, we have

$$\prod_{p \le n} p^{e(p,\,N)} = \prod_{p \in S} p^{e(p,\,N)} \cdot \prod_{p \in M} p^{e(p,\,N)} \cdot \prod_{p \in L} p^{e(p,\,N)};$$

by (12), we have

$$\prod_{p \in S} p^{e(p,\,N)} \le (2n)^{\sqrt{2n}-1};$$

by (13) and by (7) with $m = \lfloor 2n/3 \rfloor$, we have

$$\prod_{p \in M} p^{e(p,\,N)} \le \prod_{p \in M} p \le \prod_{p \le 2n/3} p < 4^{2n/3};$$

by (14), we have

$$\prod_{p \in L} p^{e(p,\,N)} = 1;$$

altogether, we have

$$\prod_{p \le n} p^{e(p,\, N)} < (2n)^{\sqrt{2n}-1} \cdot 4^{2n/3}.$$

We let $\lg x$ stand for the binary logarithm $\log_2 x$.

To prove (9), we prove that

$$(2n)^{\sqrt{2n}-1} \cdot 4^{2n/3} \le \frac{4^n}{2n},$$

which can be written as

$$(2n)^{\sqrt{2n}} \le 4^{n/3}$$

and then (taking binary logarithms of both sides) as $\sqrt{2n}\lg(2n) \le 2n/3$, and finally as

$$3\lg(2n) \le \sqrt{2n}\ :$$

a routine exercise in calculus shows that $3\lg x \le \sqrt{x}$ whenever $x \ge 1024$, and so (9) holds whenever $n \ge 512$.

To complete the proof of Bertrand's postulate, we have to verify its validity for the remaining 511 values of $n$. To do this, just observe that each interval $(n, 2n]$ with $1 \le n \le 511$ includes at least one of the primes

$$2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631\ :$$

each prime in the sequence is less than twice its predecessor.

## 6 A strengthening of of Bertrand's postulate

In [7, page 198], Erdős also explains how his arguments can be adapted to prove that

> there is a positive constant $c$ such that for every positive integer $n$ there are at least $cn/\log n$ primes $p$ such that $n < p \le 2n$.

## 7 Proof of Bertrand's original conjecture

It is a routine matter to adjust Erdős's proof of Bertrand's postulate so as to prove Bertrand's stronger original conjecture. Let us spell out the details.

**Theorem 7.1.** *For every integer $n$ greater than 3, there is a prime $p$ such that $n < p < 2n-2$.*

*Proof.* As in Erdős's proof of Bertrand's postulate, write $N = \binom{2n}{n}$. Since $n < p \le 2n$ implies $\lfloor 2n/p \rfloor = 1$ and $\lfloor n/p \rfloor = 0$, formula (10) shows that

$$n < p \le 2n \;\Rightarrow\; e(p, N) = 1,$$

and so

$$\begin{aligned}\prod_{n<p<2n-2} p &= \frac{N}{\prod_{p\le n} p^{e(p,\,N)} \cdot \prod_{2n-2\le p\le 2n} p^{e(p,\,N)}} \\ &\ge \frac{N}{\prod_{p\le n} p^{e(p,\,N)} \cdot (2n-1)};\end{aligned}$$

as in Erdős's proof of Bertrand's postulate, we have

$$\frac{N}{\prod_{p\le n} p^{e(p,\,N)}} \;>\; \frac{4^{n/3}}{(2n)^{\sqrt{2n}}}.$$

It follows that

$$\prod_{n<p<2n-2} p^{e(p,\,N)} \;>\; \frac{4^{n/3}}{(2n)^{1+\sqrt{2n}}}\,.$$

A routine exercise in calculus shows that

$$3 \lg x < \sqrt{x} - 1 < \frac{x}{1+\sqrt{x}} \;\text{ whenever } x \ge 1024,$$

and so

$$\frac{4^{n/3}}{(2n)^{1+\sqrt{2n}}} \;>\; 1 \;\text{ whenever } n \ge 512;$$

if $3 < n < 512$, then the interval $(n, 2n-2)$ includes at least one of the primes

$$5, 7, 11, 19, 31, 59, 113, 223, 443, 883.$$

□

# 8 Earlier proofs of Bertrand's postulate

## 8.1 Chebyshev.

In [4], Pafnuty Chebyshev (1821–1894) introduced functions

$$\begin{aligned}\theta(x) &= \sum_{p\le x} \ln p, \\ \psi(x) &= \sum_{i=1}^{\infty} \theta(x^{1/i})\end{aligned}$$

(here, only finitely many terms in the infinite sum are nonzero) and proved the identity

$$\sum_{j=1}^{\infty} \psi\left(\frac{x}{j}\right) = \ln\left(\lfloor x \rfloor !\right) \tag{16}$$

(again, only finitely many terms in the infinite sum are nonzero). With the notation

$$a(i,j,p,x) = \begin{cases} 1 & \text{if } jp^i \le x, \\ 0 & \text{otherwise} \end{cases}$$

his argument can be stated as

$$\begin{aligned} \sum_{j=1}^{\infty} \psi\left(\frac{x}{j}\right) &= \sum_{j=1}^{\infty}\sum_{i=1}^{\infty} \theta\left(\left(\frac{x}{j}\right)^{1/i}\right) = \sum_{j=1}^{\infty}\sum_{i=1}^{\infty}\sum_{p} a(i,j,p,x)\ln p \\ &= \sum_{p}\sum_{i=1}^{\infty}\sum_{j=1}^{\infty} a(i,j,p,x)\ln p = \sum_{p}\sum_{i=1}^{\infty}\left\lfloor \frac{x}{p^i}\right\rfloor \ln p \\ &= \sum_{p}\sum_{i=1}^{\infty}\left\lfloor \frac{\lfloor x \rfloor}{p^i}\right\rfloor \ln p = \sum_{p} e(p, \lfloor x \rfloor !)\ln p = \ln(\lfloor x \rfloor !). \end{aligned}$$

From (16) and from Stirling's approximation

$$0 < \ln(n!) - \left(n\ln n - n + \tfrac{1}{2}\ln(2\pi n)\right) < \frac{1}{12n},$$

he deduced by a lengthy arithmetical argument that $\theta(2n) - \theta(n) > 0$ (and so there is a prime $p$ such that $n < p \le 2n$) whenever $n > 160$.

## 8.2 Landau.

Chebyshev's proof of Bertrand's postulate reappeared, with slight modifications, in §17 – §20 of a monograph [21] written by Edmund Landau (1877–1938). One of Landau's shortcuts involves the observation (inequalities (1), (2) in §18 of [21]) that (16) implies

$$\begin{aligned} &\ln\left(\lfloor x \rfloor !\right) - 2\ln\left(\lfloor \tfrac{1}{2}x \rfloor !\right) \\ &\qquad = \psi(x) - \psi\left(\tfrac{1}{2}x\right) + \psi\left(\tfrac{1}{3}x\right) - \psi\left(\tfrac{1}{4}x\right) + \psi\left(\tfrac{1}{5}x\right) - \psi\left(\tfrac{1}{6}x\right) + \cdots, \end{aligned}$$

and so, as $\psi$ is nondecreasing and nonnegative,

$$\psi(x) - \psi\left(\tfrac{1}{2}x\right) \le \ln\left(\lfloor x \rfloor !\right) - 2\ln\left(\lfloor \tfrac{1}{2}x \rfloor !\right) \le \psi(x). \tag{17}$$

This observation is reminiscent of Chebyshev's observation (inequalities (6) in §5 of [4]) that

$$\begin{aligned} \psi(x) - \psi\left(\sqrt{x}\right) &= \theta(x) + \theta(x^{1/3}) + \theta(x^{1/5}) + \cdots \\ \psi(x) - 2\psi\left(\sqrt{x}\right) &= \theta(x) - \theta(x^{1/2}) + \theta(x^{1/3}) - \theta(x^{1/4}) + \theta(x^{1/5}) - \theta(x^{1/6}) + \cdots \end{aligned}$$

and so, as $\theta$ is nondecreasing and nonnegative,

$$\psi(x) - 2\psi\left(\sqrt{x}\right) \;\le\; \theta(x) \;\le\; \psi(x) - \psi\left(\sqrt{x}\right). \tag{18}$$

### 8.3 Ramanujan.

In [25], Srinivasa Ramanujan (1887–1920) started out with a refinement of (17),

$$\psi(x) - \psi\left(\tfrac{1}{2}\,x\right) \;\le\; \ln\left(\lfloor x\rfloor!\right) - 2\ln\left(\lfloor \tfrac{1}{2}x\rfloor!\right) \;\le\; \psi(x) - \psi\left(\tfrac{1}{2}\,x\right) + \psi\left(\tfrac{1}{3}\,x\right), \tag{19}$$

and a cruder version of of (18),

$$\psi(x) - 2\psi\left(\sqrt{x}\right) \;\le\; \theta(x) \;\le\; \psi(x). \tag{20}$$

He argued that Stirling's approximation implies

$$\begin{aligned} \ln\left(\lfloor x\rfloor!\right) - 2\ln\left(\lfloor \tfrac{1}{2}x\rfloor!\right) &< \tfrac{3}{4}x \quad \text{whenever } x > 0, \\ \ln\left(\lfloor x\rfloor!\right) - 2\ln\left(\lfloor \tfrac{1}{2}x\rfloor!\right) &> \tfrac{2}{3}x \quad \text{whenever } x > 300; \end{aligned}$$

these bounds combined with (19) give

$$\psi(x) - \psi\left(\tfrac{1}{2}x\right) \;<\; \tfrac{3}{4}x \quad \text{whenever } x > 0, \tag{21}$$

$$\psi(x) - \psi\left(\tfrac{1}{2}x\right) + \psi\left(\tfrac{1}{3}x\right) \;>\; \tfrac{2}{3}x \quad \text{whenever } x > 300. \tag{22}$$

Then he noted that

$$\psi(x) \;<\; \tfrac{3}{2}x \quad \text{whenever } x > 0: \tag{23}$$

this inequality holds trivially when $0 < x < 2$ and can be verified by induction on $\lfloor \lg x\rfloor$ when $x > 2$, with (21) taking care of the induction step. If $n \ge 162$, then (20), (22), and (23) guarantee that

$$\begin{aligned} \theta(2n) - \theta(n) \;\ge\; & \psi(2n) - 2\psi\left(\sqrt{2n}\right) - \psi\left(n\right) \;>\; \tfrac{4}{3}n - \psi\left(\tfrac{2}{3}n\right) - 2\psi\left(\sqrt{2n}\right) \\ >\; & \tfrac{1}{3}n - 3\sqrt{2n} \;\ge\; 0. \end{aligned}$$

## 9 Further results and problems concerning primes

### 9.1 Landau's problems

In his invited address at the fifth International Congress of Mathematicians, held at Cambridge in 1912, Landau mentioned four conjectures, which he declared to be "unattackable at the present state of science":

1. The conjecture that there are infinitely many primes of the form $n^2 + 1$.

2. *The Goldbach conjecture:* Every even integer greater than 2 is the sum of two primes.

3. *Twin prime conjecture:* There are infinitely many primes $p$ such that $p+2$ is prime.

4. Legendre's conjecture that for every positive integer $m$ there is a prime between $m^2$ and $(m+1)^2$.

These four conjectures are now known as *Landau's problems* and they remain open.

## 9.2 Small gaps between consecutive primes

In number theory, it is customary to let $p_n$ denote the $n$-th prime:

$$p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ p_4 = 7,\ p_5 = 11,\ p_6 = 13,\ p_7 = 17,\ p_8 = 19,\ \dots\ .$$

In this notation, Bertrand's postulate asserts that

$$p_{n+1} - p_n \leq p_n \text{ for all } n.$$

Roger Baker, Glyn Harman, and János Pintz [2] strengthened this to

$$p_{n+1} - p_n \leq p_n^{0.525} \text{ for all sufficiently large } n.$$

If this bound could be strenghtened to $p_{n+1} - p_n \leq 2p_n^{0.5}$ for all $n$, then Legendre's conjecture would follow: with $p_n$ the largest prime less than $m^2$, we would have $m^2 < p_{n+1} < m^2 + 2m$. Conversely, Legendre's conjecture implies that $p_{n+1} - p_n \leq 4p_n^{0.5} + 4$ for all $n$: given $p_n$, consider the $m$ such that $(m-1)^2 < p_n < m^2$ and note that $p_{n+1} < (m+1)^2$ implies $p_{n+1} - p_n < 4m$.

The twin prime conjecture asserts that

$$p_{n+1} - p_n = 2 \text{ for infinitely many } n.$$

In progress towards proving this conjecture, an epoch-making breakthrough was made in April 2013 by Yitang Zhang [27]:

$$p_{n+1} - p_n \leq 70{,}000{,}000 \text{ for infinitely many } n.$$

The challenge of reducing this upper bound was answered in April 2014 by an online collaborative project *Polymath 8* [24]:

$$p_{n+1} - p_n \leq 246 \text{ for infinitely many } n.$$

## 9.3 Large gaps between consecutive primes

Since $m! + k$ is divisible by $k$ whenever $k$ is one of $2, 3, \dots, m$, integers

$$m! + 2, \;\; m! + 3, \;\; \dots, \;\; m! + m$$

include no primes. It follows that gaps $p_{n+1} - p_n$ between consecutive primes $p_n$ and $p_{n+1}$ can be arbitrarily large. In [26], Robert Rankin (1915—2001) proved that for some positive $c$ and infinitely many $n$

$$p_{n+1} - p_n \;>\; c \cdot \frac{\ln p_n \ln\ln p_n \ln\ln\ln\ln p_n}{(\ln\ln\ln p_n)^2} \tag{24}$$

In [12], Erdős wrote

> I offered (perhaps somewhat rashly) \$ 10 000
> for a proof that (24) holds for every $c$.

Two distinct proofs were found simultaneously and independently by a team of Kevin Ford, Ben Green, Sergei Konyagin, and Terence Tao [15] and by James Maynard [22].

## 9.4 Primes in arithmetic progressions

An *arithmetic progression* is a (finite or infinite) sequence of numbers

$$a, \; a + d, \; a + 2d, \; a + 3d, \; a + 4d, \; \dots . \tag{25}$$

and its *length* is the number of its terms. For instance, $5, 11, 17, 23, 29$ is an arithmetic progression of length five (and it consists exclusively of primes). The set of all primes contains no infinite arithmetic progressions: if (25) has at least $a + 1$ terms and if its first term, $a$, is a prime, then its term $a + ad$ is composite. Nevertheless, Ben Green and Terence Tao proved [16] that

*the set of all primes contains arbitrarily long arithmetic progressions.*

This was an old conjecture, implicit in investigations carried out by Joseph-Louis Lagrange (1736–1813) and Edward Waring (1736–1798) around 1770 and subsumed in a special case of the "first Hardy-Littlewood conjecture" [18].

In 1974, Erdős [9, 10] offered \$2,500 for a proof or disproof of his conjecture that

> *every increasing sequence* $a_1, a_2, a_3, \dots$ *of positive integers such that* $\sum_{i=1}^{\infty} 1/a_i = \infty$ *contains arbitrarily long arithmetic progressions.*

This conjecture remains open; since the sum of the reciprocals of prime numbers diverges (a classical result of Euler), its validity would imply the Green-Tao theorem.

### 9.5 On revient toujours à ses premiéres amours

Number theory remained one Erdős's most important interests throughout his life: the inventory [14] of his papers up to 1998 [2] lists

- 229 on extremal problems and Ramsey theory,
- 191 on additive number theory,
- 176 on graph theory,
- 158 on multiplicative number theory,
- 149 on analysis,
- 77 on geometry,
- 69 on combinatorics,
- 52 on set theory,
- 41 on probability.

Erdős kept returning not only to the area of his first paper, but also to its proof technique. In this first paper, he established the existence of an object with specified properties (namely, a prime $p$ such that $n < p \leq 2n$) without providing an efficient algorithm to find such an object. Such proofs of existence are called *non-constructive.* This particular non-constructive proof is a prototype of a scheme that Erdős used again and again in his subsequent papers unrelated to number theory. In the general setting, its condensed outline goes as follows:

A finite set $\Omega$ of objects is divided into disjoint subsets $A$ (for 'acceptable') and $B$ (for 'bad'). T prove the existence of an acceptable object, assign a nonnegative weight $w(p)$ to every object $p$ in $\Omega$ and show that $\sum_{w\in B} w(p) < \sum_{w\in\Omega} w(p)$.

In the special case where all objects in $\Omega$ are assigned weight 1, this way of proving the existence of an acceptable object amounts to a computation showing that $|B| < |\Omega|$. Erdős used even this crudest variant with astounding success [8]. Its enhancements eventually developed into the *probabilistic method* [13, 1, 23].

In the special case of Bertrand's postulate, $\Omega$ consists of all prime divisors of $\binom{2n}{n}$; a $p$ in $\Omega$ is acceptable if $n < p \leq 2n$ and bad if $p \leq n$; for every $p$ in $\Omega$, Erdős sets $w(p) = e(p, N) \log p$ with $N = \binom{2n}{n}$. We have $\sum_{w\in\Omega} w(p) = \log N$ by definition and Erdős proves that $\sum_{w\in B} w(p) < \log N$. (This overview explains the paradox mentioned at the beginning of Section 2: in order to bound $\sum_{w\in A} w(p)$ from below, we bound $\sum_{w\in B} w(p)$ from above.)

[2] Papers co-authored with Erdős kept appearing even after 1998 and the list of his publications [17] compiled in January 2013 consists of 1525 items, the latest one dating from 2008.

## References


[1] N. Alon and J. H. Spencer, *The probabilistic method. Third edition,* John Wiley & Sons, Hoboken, New York, 2008.

[2] R. C. Baker, G. Harman, J. Pintz , The difference between consecutive primes, II, *Proc. London Math. Soc. (3)* **83**, (2001) 532–562.

[3] J. Bertrand, Mémoire sur le nombre de valeurs que peut prendre une fonction quand on y permute les lettres qu'elle renferme, *J. de l'École Polytechnique* **18** (1848), 123 – 140.

[4] P. L. Chebyshev, Mémoire sur les nombres premiers, *J. Math. Pures Appl.* **17** (1852), 366 – 390. Also in: *Oeuvres de P.L. Tchebychef* (A. Markoff and N. Sonin, eds.),St. Petersburg, 1899 – 1907, Vol. 1, pp. 49 – 70. (Reprint Chelsea,New York, 1952)

[5] M. J. Collison, The Unique Factorization Theorem: From Euclid to Gauss, *Mathematics Magazine* **53** (1980), 96–100.

[6] P. Erdős, A magasabb rendű számtani sorokról, Kózépiskolai Matematikai és Fizikai Lapok (1929), 187–189.

[7] P. Erdős, Beweis eines Satzes von Tschebyschef, *Acta Litt. Sci. Szeged* **5** (1932), 194 – 198.

[8] P. Erdős, Some remarks on the theory of graphs, *Bull. Amer. Math. Soc.* **53** (1947), 292–294.

[9] P. Erdős, Remarks on some problems in number theory, *Math. Balkanica* **4** (1974), 197 – 202

[10] P. Erdős, Problems and results in combinatorial number theory, *Journées Arithmétiques de Bordeaux* (Conf., Univ. Bordeaux, Bordeaux, 1974), *Astérisque*, Nos. 24–25 , pp. 295 – 310, Soc. Math. France, Paris, 1975

[11] P. Erdős, Ramanujan and I. *Number theory, Madras 1987*, Lecture Notes in Math. 1395, Springer, Berlin, 1989, pp. 1 – 20.

[12] P. Erdős, Some of my favourite unsolved problems. In: *A tribute to Paul Erdős* (A. Baker, B. Bollobás, A. Hajnal, eds.), Cambridge University Press, 1990, pp. 467–469.

[13] P. Erdős and J. Spencer, *Probabilistic methods in combinatorics*, Academic Press, New York, 1974.

[14] European Mathematical Society & FIZ Karlsruhe & Springer- Verlag, Publications of (and about) Paul Erdős, `https://www.emis.de/classics/Erdos/zbl.htm`, 1998.

[15] K. Ford, B. Green, S. Konyagin, and T. Tao, Large gaps between consecutive prime numbers, *Annals of Mathematics* **183** (2016), 935–974.

[16] B. Green and T. Tao, The primes contain arbitrarily long arithmetic progressions, *Annals of Mathematics* **167** (2008), 481–547.

[17] J. Grossman, List of publications of Paul Erdős, January 2013, in: *The Mathematics of Paul Erdős II. Second Edition* (R. L. Graham, J. Nešetřil, and S. Butler, eds.), Springer, New York, Heidelberg, 2013. pp. 497–603.

[18] G. H. Hardy and J. E. Littlewood, Some problems of 'partitio numerorum'. III. On the expression of a number as a sum of primes, *Acta Math.* **44** (1923), 1 − 70.

[19] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers,* Oxford University Press, Oxford, 1938.

[20] T. L. Heath, ed., *The thirteen books of Euclid's Elements,* St. John's College Press, 1947.

[21] E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen,* B. G. Teubner, Leipzig, Berlin, 1909. Reprinted (with an Appendix by P. T. Bateman) by Chelsea Publishing Co., New York, 1953.

[22] J. Maynard, Large gaps between primes, *Annals of Mathematics* **183** (2016), 915–933.

[23] M. Molloy and B. Reed, *Graph colouring and the probabilistic method*, Springer-Verlag, Berlin, 2002.

[24] D. H. J. Polymath, Variants of the Selberg sieve, and bounded intervals containing many primes, *Research in the Mathematical Sciences* **1** (2014), Article 12, 83 pages.

[25] S. Ramanujan. A proof of Bertrand's postulate, *Journal of the Indian Math. Soc.* **11** (1919), 181 − 182. Also in *Collected Papers of Srinivasa Ramanujan* (G. H. Hardy, P. V. Seshu Aiyar, B. M. Wilson, eds.), AMS/Chelsea Publication, 2000,pp. 208 − 209.

[26] R. A. Rankin, The difference between consecutive primes, *Journal of the London Mathematical Society* **13** (1938), 242–247.

[27] Y. Zhang, Bounded gaps between primes, *Annals of Mathematics* **179** (2014): 1121-1174.