Cambridge University Press & Assessment
978-1-108-83183-3 — The Discrete Mathematical Charms of Paul Erdos
Vašek Chvátal
Excerpt
More Information

Introduction

The lecture notes that form the basis of this book have been distributed to graduate students, but the model readers I had in mind when writing them were contestants in a mathematical olympiad. As I did not want to intimidate such youngsters, I chose to include prerequisites that they might not be familiar with even if these prerequisites could be taken for granted when addressing graduates. (They are collected in Appendix A.) The term ‘simple’ in the subtitle of the book is the operative word: I aimed to make the material accessible to as wide an audience as possible.

I used the lecture notes in a course that consisted of twelve 90-minute lectures and a screening of George Csicsery’s brilliant documentary “N is a number” [92]. In each of its editions, I covered at most nine of the following eleven chapters (and once also a large part of Appendix A) at a leisurely pace.

Here is how I arrived at the order of the chapters.

1. Erdős’s first important achievement, his 1932 paper proving Bertrand’s postulate, seemed a logical choice for the first chapter.
2. His next widely acclaimed result, published in a 1935 paper co-authored with George Szekeres, was the Happy Ending Theorem. Erdős’s proof of it, chronologically second and quantitatively far superior to the first, is the starting point of Chapter 2. Its geometric nature suggests continuing with another early geometric interest of Paul Erdős, his conjecture that was confirmed by Tibor Gallai (né Grünwald) and became known as the Sylvester–Gallai theorem. As pointed out by Erdős in 1943, this theorem has a pretty corollary involving points and lines in the plane. In a 1948 paper, Erdős and Nicolaas de Bruijn proved a combinatorial theorem that subsumes this corollary and extends it far beyond the reaches of geometry. This De Bruijn–Erdős theorem and its several proofs round up Chapter 2.
3. Not to leave the reader in suspense for too long, we then backtrack to the Happy Ending Theorem and present its proof by Szekeres. This is done in Chapter 3, whose main theme is Ramsey’s theorem. At the end of this chapter, I indulge myself by discussing my second joint paper with Erdős.
4. Another instance of such self-indulgence comes in Chapter 4, where I point out how a qualitative version of the Erdős–Rado theorem on Δ-systems can be viewed as a corollary of Ramsey’s theorem. This observation is linked to a

conjecture of Erdős and Lovász on weak and strong Δ-systems, whose beautiful proof by Michel Deza concludes the chapter.

5. The Erdős–Rado theorem on Δ-systems opens the gates of extremal set theory, which is the subject of Chapter 5. One of the two results closing this chapter is Erdős's lower bound on the number of hyperedges in a k-uniform hypergraph of chromatic number greater than s.
6. This bound subsumes not only Erdős's lower bound on diagonal Ramsey numbers but also a lower bound on van der Waerden numbers, and so van der Waerden's theorem on arithmetic progressions is treated in Chapter 6.
7. In Chapter 7, we return to extremal set theory and survey its rich autonomous branch, extremal graph theory.
8. Chapter 8 stands out by having no links to other chapters. It begins with the Friendship Theorem of Erdős, Alfréd Rényi, and Vera Sós. Its proof by Herbert Wilf connects it to strongly regular graphs and the dazzling theorem on Moore graphs of diameter two by Alan Hoffman and R. R. Singleton.
9. After the detour, the next chapter begins with a reference to the Erdős–Stone–Simonovits formula of Chapter 7, which features the chromatic number of a graph. This invariant is the sole subject of Chapter 9. Several proof techniques used there are early instances of what has become known as the probabilistic method, and so it seems natural to continue with graph theory and probability.
10. The first two sections of Chapter 10 reproduce two fragments of the Erdős–Rényi theory of random graphs; the next section reports without proofs the fascinating results on the evolution of random graphs, with an emphasis on the double jump and its critical window; the concluding section puts the preceding material in its natural context of finite probability spaces.
11. Chapter 11 is more of an appendix than a genuine chapter: its theme, Hamiltonian graphs, was far from central among Erdős's interests in discrete mathematics. I have taken the liberty of recounting in its first section how a result of mine was directly inspired by Erdős's delightful algorithmic proof of Turán's theorem and presenting in the second section my first joint paper with Erdős. (Please note that I have displayed admirable restraint by not mentioning our third joint paper anywhere in this book. Except here.) A brief survey of results on Hamilton cycles in random graphs rounds up this chapter.

I regret the omission of two brilliant and important results, Lovász Local Lemma [249] and Szemerédi's Regular Partition Lemma [257]. I could not find a way of weaving them smoothly into the narrative.

Non-mathematical parts of the text are set in sans serif against a lightly shaded background like this.

Definitions that are used more than once are collected in Appendix B.

Cambridge University Press & Assessment
978-1-108-83183-3 — The Discrete Mathematical Charms of Paul Erdos
Vašek Chvátal
Excerpt
More Information

1 A Glorious Beginning: Bertrand's Postulate

In 1845, Joseph Bertrand (1822–1900) conjectured [29] 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* [211, 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 1852, it was proved [67] by Pafnuty Chebyshev (1821–94).

In March 1931, the 18-year-old Erdős found an elegant elementary proof of Bertrand's postulate; the following year, this proof appeared in his first publication [106].[a] 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 [106] was rewritten by László Kalmár (1905–76), a professor at the University of Szeged; as Erdős recalls in [131], he said in the introduction that Srinivasa Ramanujan (1887–1920) found [322] a somewhat similar proof. Erdős's proof and its background are described in the next five sections; Ramanujan's proof is sketched in section 1.7. Six years after Erdős's proof appeared, Godfrey Harold Hardy (1877–1947) and Edward Maitland Wright (1906–2005) included it in their textbook [211], a classic with its sixth edition appearing in 2008.

1.1 Binomial Coefficients

NOTATION: When m and k are nonnegative integers, the symbol $\binom{m}{k}$ – read "m choose k" – denotes the number of k-point subsets of a fixed m-point set. For

[a] Erdős must have considered his 1929 article [105] in a Hungarian mathematics and physics journal for high school students unimportant: In [131] he refers to [106] as "[my paper . . .] which was actually my very first."

example, $\{1, 2, \ldots, 5\}$ has precisely ten 3-point subsets, namely,

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

and so $\binom{5}{3} = 10$.

This combinatorial definition leads directly to a number of identities such as

$$\sum_{k=0}^{m} \binom{m}{k} = 2^m \tag{1.1}$$

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

$$\binom{m}{k} = \binom{m}{m-k} \tag{1.2}$$

(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

$$\binom{m}{k} k = \binom{m}{k-1} (m-k+1) \tag{1.3}$$

(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, (1.1) with $m = 2n+1$ and (1.2) with $m = 2n+1$, $k = n$ imply that

$$\binom{2n+1}{n} \leq 4^n. \tag{1.4}$$

Second, (1.3) with $m = 2n$ guarantees that $\binom{2n}{n}$ is the largest of the $2n+1$ numbers $\binom{2n}{k}$ 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 (1.1) with $m = 2n$; we conclude that

$$\binom{2n}{n} \geq \frac{4^n}{2n} \text{ whenever } n \geq 1. \tag{1.5}$$

DEFINITION: The product $1 \cdot 2 \cdot \ldots \cdot m$ of the first m positive integers is called the *factorial of m* and denoted $m!$. The factorial of 0 is defined as $0! = 1$.

Induction on k using identity (1.3) shows that

$$\binom{m}{k} = \frac{m!}{k!(m-k)!}\,. \tag{1.6}$$

This formula is also used in Erdős's proof.

The 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 having the form $a^k b^{m-k}$. The binomial formula reduces to (1.1) by setting $a = b = 1$.

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

$$\prod_{p \le m} p < 4^m \quad \text{for every positive integer } m. \tag{1.7}$$

Some eight years after Erdős first proved (1.7), he and Kalmár found independently and almost simultaneously a simpler proof (see [131]). This proof goes by induction on m. The induction basis verifies (1.7) 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

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

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

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

Using the induction hypothesis and (1.4), we conclude that

$$\prod_{p \le m} p < 4^{n+1} \cdot 4^n = 4^m.$$

1.3 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.*

> *For every positive integer n and for all primes p,*
> *there are uniquely defined nonnegative integers* $e(p,n)$ *such that*

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

(In the right-hand-side product, p runs through the infinite set of primes, but for every 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.

Some people attribute the Unique Factorization Theorem to Euclid [212, Proposition 14 of Book IX], whose *Elements* appeared around 300 BC, and others to Carl Friedrich Gauss (1777–1855), whose *Disquisitiones Arithmeticae* [184] appeared in the summer of 1801. The controversy is analyzed in [86].

1.4 Legendre's Formula

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 four such terms,
- every fourth one contributes at least two units to the total, and there are two such terms,
- every eighth one contributes at least three units to the total, and there is one 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 (1752–1833) in the second edition of his book [273] published in 1808.

1.5 Erdős's Proof of Bertrand's Postulate

1.5.1 The Plan

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

$$\prod_{p\leq n}p^{e(p,N)}<\prod_{p\leq 2n}p^{e(p,N)}, \tag{1.8}$$

which obviously implies Bertrand's postulate. Our choice is $N = \binom{2n}{n}$. Since formula (1.6) with $m = 2n$ and $k = n$ reads

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

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

$$\prod_{p\le n} p^{e(p,N)} < \frac{4^n}{2n}. \tag{1.9}$$

Since (1.5) reads $4^n/2n \le N$, inequality (1.8) will then follow.

1.5.2 A Formula for $e(p, N)$

We will use the formula

$$e(p,N) = \sum_{i=1}^{\infty}\left(\left\lfloor\frac{2n}{p^i}\right\rfloor - 2\left\lfloor\frac{n}{p^i}\right\rfloor\right), \tag{1.10}$$

which follows directly from (1.6) 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

$$\left\lfloor\frac{2n}{p^i}\right\rfloor - 2\left\lfloor\frac{n}{p^i}\right\rfloor \;=\; 0 \text{ or } 1 \text{ for all } i. \tag{1.11}$$

1.5.3 An Upper Bound on $p^{e(p,N)}$

Given p and n, consider the largest integer j such that $p^j \le 2n$. By (1.10) and (1.11), 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

$$p^{e(p,N)} \le 2n. \tag{1.12}$$

1.5.4 Splitting the Left-Hand Side of (1.9)

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 $2n/3 < p \leq n$.

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

$$p \in M \Rightarrow e(p,N) \leq 1, \tag{1.13}$$

$$p \in L \ \Rightarrow e(p,N) = 0. \tag{1.14}$$

Our proof of these implications relies on formula (1.10): since

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

we have

$$p > \sqrt{2n} \Rightarrow e(p,N) = \left\lfloor \frac{2n}{p} \right\rfloor - 2\left\lfloor \frac{n}{p} \right\rfloor. \tag{1.15}$$

Implication (1.13) follows directly from (1.15) and (1.11); implication (1.14) follows from (1.15) combined with the observation that $p \in L$ implies $\lfloor 2n/p \rfloor = 2$ and $\lfloor n/p \rfloor = 1$.

1.5.5 Putting the Pieces Together

By definition, we have

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

by (1.12), we have

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

by (1.13) and by (1.7) with $m = \lfloor 2n/3 \rfloor$, we have

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

by (1.14), we have

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

altogether, we have

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

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

To prove (1.9), we prove that

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

which can be written as

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

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 (1.9) 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

$$5, 7, 11, 19, 31, 59, 113, 223, 443, 883. \tag{1.16}$$

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

1.6 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 1.1 *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 $n < p < 2n$ implies $\lfloor 2n/p \rfloor = 1$ and $\lfloor n/p \rfloor = 0$, formula (1.15) shows that

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

and so

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

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

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