

The Bateman–Horn conjecture: Heuristic, history, and applications

Soren Laing Aletheia-Zomlefer^b, Lenny Fukshansky^{a,1},
Stephan Ramon Garcia^{b,*,2}

^a Department of Mathematics, Claremont McKenna College, 850 Columbia Ave, Claremont, CA 91711, USA

^b Department of Mathematics, Pomona College, 610 N. College Ave., Claremont, CA 91711, USA

Received 26 July 2018; received in revised form 4 April 2019; accepted 26 April 2019

Abstract

The Bateman–Horn conjecture is a far-reaching statement about the distribution of the prime numbers. It implies many known results, such as the prime number theorem and the Green–Tao theorem, along with many famous conjectures, such the twin prime conjecture and Landau’s conjecture. We discuss the Bateman–Horn conjecture, its applications, and its origins.

© 2019 Elsevier GmbH. All rights reserved.

MSC 2010: primary 11N32; secondary 11N05; 11N13

Keywords: Prime number; Bateman–Horn conjecture; Primes in arithmetic progressions; Landau’s conjecture; Twin prime conjecture; Ulam spiral

1. Introduction

Given a collection of polynomials with integer coefficients, how often should we expect their values at integer arguments to be simultaneously prime? This general

* Corresponding author.

E-mail addresses: lenny@cmc.edu (L. Fukshansky), stephan.garcia@pomona.edu (S.R. Garcia).

URL: <http://pages.pomona.edu/~sg064747> (S.R. Garcia).

¹ LF supported by the Simons Foundation grant #519058, USA.

² SRG supported by a David L. Hirsch III and Susan H. Hirsch Research Initiation Grant, the Institute for Pure and Applied Mathematics (IPAM) Quantitative Linear Algebra program, and NSF Grant DMS-1800123, USA.

question subsumes a large number of different directions and investigations in analytic number theory. A comprehensive answer is proposed by the famous Bateman–Horn conjecture, first formulated by Paul T. Bateman and Roger A. Horn in 1962 [4,5]. This conjecture is a far-reaching statement about the distribution of the prime numbers. Many well-known theorems, such as the prime number theorem and the Green–Tao theorem, follow from it. The conjecture also implies a variety of unproven conjectures, such as the twin prime conjecture and Landau’s conjecture. We hope to convince the reader that the Bateman–Horn conjecture deserves to be ranked among the Riemann hypothesis and *abc*-conjecture as one of the most important unproven conjectures in number theory.

The amount of literature related to the Bateman–Horn conjecture is large: MathSciNet, for example, shows over 100 citations to the original Bateman–Horn papers in which the conjecture was formulated. Somewhat surprisingly, however, we did not find many expository accounts besides a short note by Serge Lang [51] with just a quick overview of the conjecture. It is a goal of this paper to provide a detailed exposition of the conjecture and some of its ramifications. We assume no knowledge beyond elementary undergraduate number theory. We introduce the necessary algebraic and analytic prerequisites as need arises. We do not attempt a comprehensive survey of all the literature related to the Bateman–Horn conjecture. For example, recent variations of the conjecture, say to multivariate polynomials [18,61] or to polynomial rings over finite fields [12,13], are not treated here.

The organization of this paper is as follows. Section 2 introduces asymptotic equivalence, the logarithmic integral, and the prime number theorem. In Section 3, we go through a careful heuristic argument based upon the Cramér model that explains most of the key restrictions and predictions of the Bateman–Horn conjecture. Before proceeding to various examples and applications of the conjecture, Section 4 revisits some of the historical background. In particular, we include many personal recollections of Roger Horn that have never before been published.

One of the main features of the Bateman–Horn conjecture is an explicit constant in the main term of the asymptotic formula for the number of integers below a given threshold at which a collection of polynomials simultaneously assume prime values. The expression for this constant, however, is complicated and involves an infinite product. It is nontrivial to see that this product converges and we are not aware of a detailed proof of this fact anywhere in the literature. The original Bateman–Horn paper sketches the main idea of this proof, but omits almost all of the details. We present this argument in detail in Section 5.

Section 6 is devoted to a number of important instances and consequences of the single polynomial case of the conjecture, while ramifications of the multiple polynomial case are discussed in Section 7. Finally, we discuss some limitations of the Bateman–Horn conjecture in Section 8. With this brief introduction, we are now ready to proceed.

2. Preliminaries

We will often need to compare the rate of growth of two real-valued functions of a real variable as their arguments tend to infinity. To this end, we require a bit of notation. Readers familiar with asymptotic equivalence, Big- O and little- o notation, and the prime number theorem should proceed to Section 3. A good source of information on classical analytic number theory is [17].

2.1. Asymptotic equivalence

In what follows, we assume that $f(x)$ and $g(x)$ are continuous, real-valued functions that are defined and nonzero for sufficiently large x . We write $f \sim g$ to mean that

$$\lim_{x \rightarrow \infty} \frac{f(x)}{g(x)} = 1. \quad (2.1.1)$$

We say that f and g are *asymptotically equivalent* when this occurs. The limit laws from calculus show that \sim is an equivalence relation; we use this fact freely.

Two polynomials are asymptotically equivalent if and only if they have the same degree and the same leading coefficient. For example, $2x^2 \sim 2x^2 + x + 1$ since

$$\lim_{x \rightarrow \infty} \frac{2x^2 + x + 1}{2x^2} = \lim_{x \rightarrow \infty} \left(1 + \frac{1}{x} + \frac{1}{x^2}\right) = 1.$$

It is important to note, however, that asymptotic equivalence does not necessarily mean that “ f and g are close together” in the sense that $f - g$ is small. Although $2x^2 \sim 2x^2 + x + 1$, their difference $(2x^2 + x + 1) - 2x^2 = x + 1$ is unbounded.

2.2. Big- O and little- o notation

When we write $f(x) = O(g(x))$, we mean that there is a constant C such that $|f(x)| \leq C|g(x)|$ for sufficiently large x . For example,

$$4x^2 + 7x \log x = O(x^2) \quad \text{and} \quad \sin x = O(1).$$

What is the relationship between Big- O notation and asymptotic equivalence? If $f \sim g$, then $f(x) = O(g(x))$ and $g(x) = O(f(x))$. Indeed, (2.1.1) and the definition of limits ensure that $|f(x)| \leq 2|g(x)|$ and $|g(x)| \leq 2|f(x)|$ for sufficiently large x (the number 2 in the preceding inequalities can be replaced by any constant greater than 1). On the other hand, $2x = O(x)$ and $x = O(2x)$, although x and $2x$ are not asymptotically equivalent. Hence the statement “ $f \sim g$ ” is stronger than the statement “ $f(x) = O(g(x))$ and $g(x) = O(f(x))$ ”, but both of these statements are asymptotic in their nature.

We say $f(x) = o(g(x))$ if

$$\lim_{x \rightarrow \infty} \frac{f(x)}{g(x)} = 0.$$

For instance, $x = o(x^2)$ as $x \rightarrow \infty$. Notice that if $f \sim g$, then

$$1 = \lim_{x \rightarrow \infty} \frac{f(x)}{g(x)} = \lim_{x \rightarrow \infty} \frac{f(x) - g(x) + g(x)}{g(x)} = \lim_{x \rightarrow \infty} \frac{f(x) - g(x)}{g(x)} + 1,$$

and so $\lim_{x \rightarrow \infty} \frac{f(x) - g(x)}{g(x)} = 0$. Thus, the error term satisfies $|f(x) - g(x)| = o(g(x))$. On the other hand, the assertion that $f(x) = O(g(x))$ and $g(x) = O(f(x))$ does not guarantee a smaller order error term. Indeed, $x = O(2x)$ and $2x = O(x)$, but $|x - 2x| = |x|$ is not $o(x)$ or $o(2x)$.

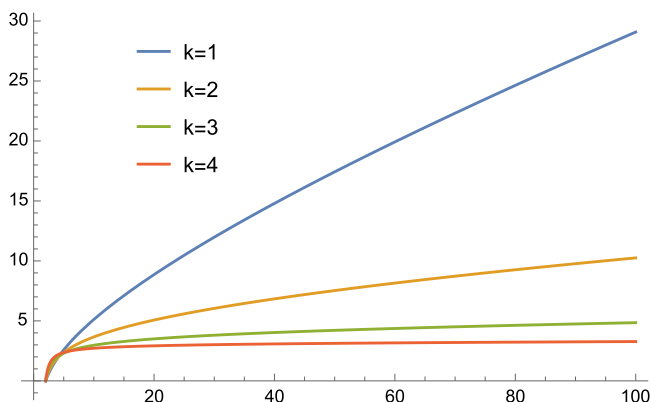


Fig. 1. The functions $\int_2^x \frac{dt}{(\log t)^k}$ for $k = 1, 2, 3, 4$ and $x \geq 2$.

2.3. The logarithmic integral

In the theory of prime numbers the *offset logarithmic integral*³

$$\text{Li}(x) = \int_2^x \frac{dt}{\log t} \quad (2.3.1)$$

and its close relatives frequently arise. Here $\log t$ denotes the natural logarithm⁴ of t . Unfortunately, the integral (2.3.1) cannot be evaluated in closed form. As a consequence, it is convenient to replace $\text{Li}(x)$ and its relatives (see Fig. 1) with simpler functions that are asymptotically equivalent.

Lemma 2.3.2. $\int_2^x \frac{dt}{(\log t)^k} \sim \frac{x}{(\log x)^k}$ for $k = 1, 2, \dots$

Proof. L'Hôpital's rule and the fundamental theorem of calculus imply that

$$\lim_{x \rightarrow \infty} \frac{\int_2^x \frac{dt}{(\log t)^k}}{x/(\log x)^k} \stackrel{L}{=} \lim_{x \rightarrow \infty} \frac{1/(\log x)^k}{1/(\log x)^k - k/(\log x)^{k+1}} = \lim_{x \rightarrow \infty} \frac{1}{1 - k/\log x} = 1. \quad \square$$

One can be a little more precise than Lemma 2.3.2. Integration by parts provides:

$$\text{Li}(x) = \frac{x}{\log x} + O\left(\frac{x}{(\log x)^2}\right)$$

and

$$\int_2^x \frac{dt}{(\log t)^k} = \frac{x}{(\log x)^k} + O\left(\frac{x}{(\log x)^{k+1}}\right).$$

³ The function (2.3.1) is a close relative of the standard *logarithmic integral* $\text{li}(x)$, in which the lower limit of integration in (2.3.1) is 0 and the singularity at $x = 1$ is avoided by using a Cauchy principal value. Since we are interested in large x , we use (2.3.1) instead.

⁴ The notation $\ln t$ may be more familiar to calculus students.

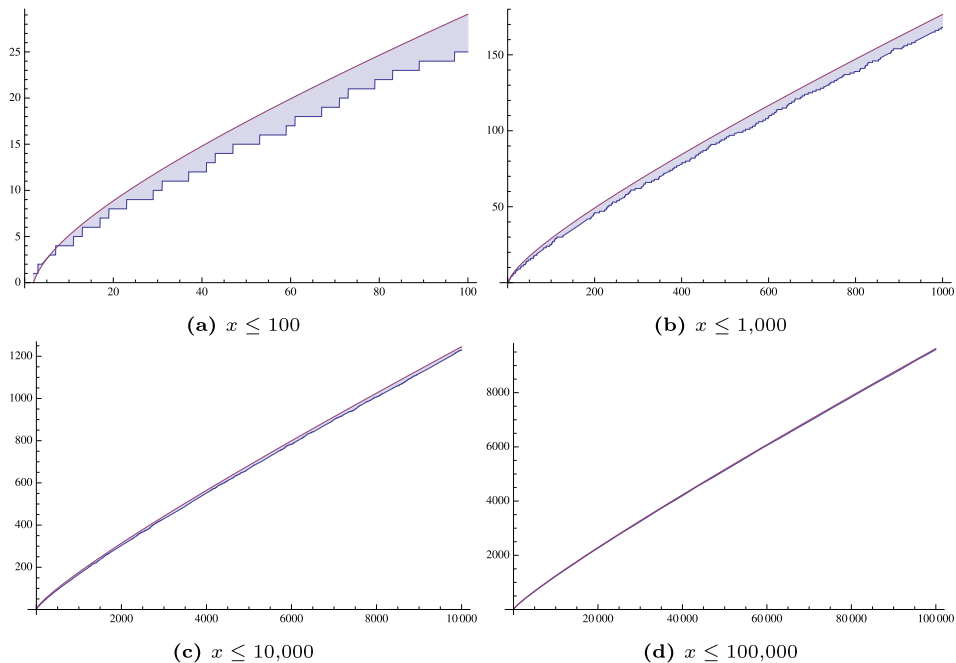


Fig. 2. Graphs of $\text{Li}(x)$ versus $\pi(x)$ on various scales.

2.4. Prime number theorem

The first signpost toward the Bateman–Horn conjecture is the prime number theorem, which describes the gross distribution of the primes. Let $\pi(x)$ denote the number of primes at most x . For example, $\pi(10.5) = 4$ since $2, 3, 5, 7 \leq 10.5$. The following result was proved independently by Hadamard and de la Vallée Poussin in 1896; see Fig. 2.

Theorem 2.4.1 (Prime Number Theorem). $\pi(x) \sim \text{Li}(x)$.

Although $\text{Li}(x) \sim x/\log x$, the logarithmic integral provides a more accurate approximation to $\pi(x)$; see Table 1. For simplicity, we work now with the approximation $\pi(x) \sim x/\log x$ and develop a probabilistic model of the prime numbers that will guide our progress toward the Bateman–Horn conjecture [78].

For fixed $c > 0$ and large x , the prime number theorem tells us to expect about

$$\frac{x + cx}{\log(x + cx)} - \frac{x - cx}{\log(x - cx)} \sim \frac{2cx}{\log x}$$

primes in the interval $[x - cx, x + cx]$. Dividing by the length $2cx$ of the interval, it follows that the probability that a natural number in the vicinity of x is prime is roughly $1/\log x$. We use this repeatedly as a guide in our heuristic arguments.

Table 1

The logarithmic integral $\text{Li}(x)$ is a better approximation to the prime counting function $\pi(x)$ than is $x/\log x$. The entries in the table have been rounded to the nearest integer.

x	$\pi(x)$	$\text{Li}(x)$	$x/\log x$
1 000	168	177	145
10,000	1,229	1,245	1,086
100,000	9,592	9,629	8,686
1,000,000	78,498	78,627	72,382
10,000,000	664,579	664,917	620,421
100,000,000	5,761,455	5,762,208	5,428,681
1,000,000,000	50,847,534	50,849,234	48,254,942
10,000,000,000	455,052,511	455,055,614	434,294,482
100,000,000,000	4,118,054,813	4,118,066,400	3,948,131,654
1,000,000,000,000	37,607,912,018	37,607,950,280	36,191,206,825

3. A heuristic argument

Now that we know about the gross distribution of the primes, it is natural to ask about the distribution of primes of certain forms. For example, are there infinitely many primes of the form $n^2 + 1$? This was asked at the 1912 International Congress of Mathematicians by Edmund Landau (1877–1938) and remains open today.⁵

3.1. A single polynomial

We let $\mathbb{Z}[x]$ denote the set of polynomials in x with coefficients in \mathbb{Z} , the set of integers. We denote by \mathbb{N} the set $\{1, 2, \dots\}$ of natural numbers. For $f \in \mathbb{Z}[x]$, we define

$$Q(f; x) = \#\{n \leq x : f(n) \text{ is prime}\},$$

in which $\#S$ denotes the number of elements of a set S . We investigate some conditions that f must satisfy if it is to generate infinitely many distinct primes. To avoid trivialities, suppose that f is nonconstant and that $Q(f; x) \rightarrow \infty$.

- **Leading coefficient.** The degree of f , denoted $\deg f$, must be at least one. Moreover, the leading coefficient of f must be positive.
- **Irreducible.** We claim that f is irreducible; that is, it cannot be factored as a product of two polynomials in $\mathbb{Z}[x]$, neither of which is ± 1 .⁶ Suppose that $f = gh$, in which $g, h \in \mathbb{Z}[x]$. Without loss of generality, we may assume that the leading coefficients of g and h are positive. Then $g(n) = 1$ or $h(n) = 1$ for infinitely many n since f assumes prime values infinitely often. Consequently, $g - 1$ or $h - 1$ is a polynomial with infinitely many roots and hence g or h is identically 1. Thus, f is irreducible.

⁵ Although commonly known as Landau's conjecture, its first appearance is in a 1752 letter from Leonhard Euler (1707–1783) to Christian Goldbach (1690–1764) [22, p. 2–3].

⁶ Gauss' lemma ensures that a primitive $f \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$ if and only if it is irreducible in $\mathbb{Q}[x]$, the ring of polynomials with rational coefficients [21, Prop. 5, p. 303].

- **Nonvanishing modulo every prime.** A nonconstant $f \in \mathbb{Z}[x]$ may be irreducible, yet fail to be prime infinitely often. For example, $f(x) = x^2 + x + 2$ is irreducible, but $f(n)$ is divisible by 2 for all $n \in \mathbb{Z}$. Similarly, $f(x) = x^3 - x + 3$ is irreducible and

$$x^3 - x + 3 \equiv x^3 - x \equiv x(x-1)(x+1) \equiv 0 \pmod{3},$$

so $f(n)$ is divisible by 3 for all $n \in \mathbb{Z}$. Thus, we must insist that f does not vanish identically modulo any prime.

3.2. Effect of the degree.

Suppose that $f \in \mathbb{Z}[x]$ is nonconstant, irreducible, and does not vanish identically modulo any prime. Let $d = \deg f$ and suppose that f has a positive leading coefficient, c . Then $f(x) \sim cx^d$ and our heuristic from the prime number theorem suggest that the probability $f(n)$ is prime is about

$$\frac{1}{\log f(n)} \sim \frac{1}{\log(cx^d)} = \frac{1}{d \log x + \log c} \sim \frac{1}{d \log x}. \quad (3.2.1)$$

This suggests that

$$Q(f; x) \sim \sum_{n=2}^{\lfloor x \rfloor} \frac{1}{d \log x} \sim \frac{1}{\deg f} \int_2^x \frac{dt}{\log t}. \quad (3.2.2)$$

Is this correct? We should do some computations to see whether this pans out.

3.3. A sanity check

Consider the polynomial

$$f(x) = x^2 + 1,$$

which is nonconstant, irreducible, and has a positive leading coefficient. Since $f(0) = 1$, it follows that f does not vanish identically modulo any prime. Landau's conjecture is that f assumes infinitely many prime values; that is, $Q(f; x) \rightarrow \infty$.

According to (3.2.2)

$$Q(f; N) \sim \frac{1}{2} \text{Li}(N). \quad (3.3.1)$$

However, the numerical evidence disagrees; see Table 2. On the positive side, the loss is not total since it appears that our estimate is only off by a constant factor. What is this constant factor and where does it come from?

3.4. Making a correction

We were too quick to celebrate the fact that f does not vanish identically modulo any prime. Our prediction needs to take into account how likely it is that $f(n) \equiv 0 \pmod{p}$. For example, $f(n) \equiv n + 1 \pmod{2}$ and hence $f(n)$ is even with probability $\frac{1}{2}$.

Table 2

The estimate (3.3.1) is clearly incorrect. However, the ratio between the correct answer and our prediction appears to converge slowly to a constant (the value of $\frac{1}{2} \text{Li}(N)$ is rounded to the nearest integer for display purposes).

N	$Q(f; N)$	$\frac{1}{2} \text{Li}(N)$	$Q(f; N)/\frac{1}{2} \text{Li}(N)$
100	19	15	1.3067
1,000	112	88	1.26866
10,000	841	623	1.3509
100,000	6,656	4,814	1.38252
1,000,000	54,110	39,313	1.37638
10,000,000	456,362	332,459	1.37269
100,000,000	3,954,181	2,881,104	1.37245
1,000,000,000	34,900,213	25,424,617	1.37269

If we assume for the sake of our heuristic argument that divisibility by distinct primes p and q are independent events, then we should weight our prediction by⁷

$$\prod_p \left(1 - \frac{\omega_f(p)}{p}\right), \quad (3.4.1)$$

in which $\omega_f(p)$ is the number of solutions to $f(x) \equiv 0 \pmod{p}$.

However, there is a problem. The constant factor suggested by Table 2, approximately 1.372, is greater than one, whereas (3.4.1) is not. Therefore, the preceding analysis cannot be correct. More seriously, there are convergence issues with (3.4.1); see Section 5.1 for information about infinite products.

We need to weight the factors in (3.4.1) against the probabilities that randomly selected integers are not divisible by p . This suggests that we adjust (3.3.1) by

$$C(f) = \prod_p \left(1 - \frac{1}{p}\right)^{-1} \left(1 - \frac{\omega_f(p)}{p}\right) = \prod_p \frac{p - \omega_f(p)}{p - 1}. \quad (3.4.2)$$

Does this agree with our numerical computations? To compute $\omega_f(p)$, we need to count the number of solutions to $x^2 + 1 \equiv 0 \pmod{p}$. Since -1 is a square modulo p if and only if $p = 2$ or $p \equiv 1 \pmod{4}$ [62],

$$\omega_f(p) = \begin{cases} 1 & \text{if } p = 2, \\ 2 & \text{if } p \equiv 1 \pmod{4}, \\ 0 & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

The hundred millionth partial product of (3.4.2) yields

$$C(f) \approx 1.37281,$$

which agrees with the data in Table 2. In particular, this suggests an affirmative answer to Landau's problem.

⁷ An important convention we adhere to throughout this paper is that the letter p always denotes a prime number. A product or sum indexed by p indicates that product or sum runs over all prime numbers.

Let us pause to summarize the discussion so far. For a single polynomial f , we suspect that

$$Q(f; x) \sim \frac{C(f)}{\deg f} \int_2^x \frac{dt}{\log t},$$

in which

$$C(f) = \prod_p \left(1 - \frac{1}{p}\right)^{-1} \left(1 - \frac{\omega_f(p)}{p}\right). \quad (3.4.3)$$

This is the Bateman–Horn conjecture for a single polynomial. What about families of multiple polynomials?

3.5. More than one polynomial

Suppose that $f_1, f_2, \dots, f_k \in \mathbb{Z}[x]$ are distinct irreducible polynomials with positive leading coefficients. The same reasoning in (3.2.1) tells us the probability that all of the $f_i(n)$ are prime is

$$\prod_{i=1}^k \frac{1}{\log f_i(n)} \sim \prod_{i=1}^k \frac{1}{d_i \log n} = \frac{1}{(\prod_{i=1}^k \deg f_i)(\log n)^k}.$$

Thus, the expected number of n at most x for which $f_1(n), f_2(n), \dots, f_k(n)$ are simultaneously prime is around

$$\int_2^x \frac{1}{(\prod_{i=1}^k \deg f_i)(\log n)^k} = \frac{1}{\prod_{i=1}^k \deg f_i} \int_2^x \frac{dt}{(\log t)^k}.$$

As before, we must amend this with a suitable correction factor.

Although perhaps no single f_i vanishes identically modulo a prime, these polynomials might conspire to make

$$f = f_1 f_2 \cdots f_k \quad (3.5.1)$$

vanish identically modulo some prime. For example, neither $f_1(x) = x$ nor $f_2(x) = x - 1$ vanish identically modulo a prime, although their product $f(x) = x(x - 1)$ vanishes identically modulo 2. This “congruence obstruction” prevents n and $n + 1$ from being simultaneously prime infinitely often. Consequently, we must require that f does not vanish identically modulo any prime.

With f as in (3.5.1), one final adjustment to (3.4.3) is necessary. Instead of dividing by $1 - 1/p$ in (3.4.3), we must now divide by $(1 - 1/p)^k$, the probability that a randomly selected k -tuple of integers has no element divisible by p .

3.6. The Bateman–Horn conjecture

The preceding heuristic deductions make a compelling argument in favor of the following conjecture.

Bateman–Horn Conjecture. Let $f_1, f_2, \dots, f_k \in \mathbb{Z}[x]$ be distinct irreducible polynomials with positive leading coefficients, and let

$$Q(f_1, f_2, \dots, f_k; x) = \#\{n \leq x : f_1(n), f_2(n), \dots, f_k(n) \text{ are prime}\}. \quad (3.6.1)$$

Suppose that $f = f_1 f_2 \cdots f_k$ does not vanish identically modulo any prime. Then

$$Q(f_1, f_2, \dots, f_k; x) \sim \frac{C(f_1, f_2, \dots, f_k)}{\prod_{i=1}^k \deg f_i} \int_2^x \frac{dt}{(\log t)^k}, \quad (3.6.2)$$

in which

$$C(f_1, f_2, \dots, f_k) = \prod_p \left(1 - \frac{1}{p}\right)^{-k} \left(1 - \frac{\omega_f(p)}{p}\right) \quad (3.6.3)$$

and $\omega_f(p)$ is the number of solutions to $f(x) \equiv 0 \pmod{p}$.

Under the hypotheses of the Bateman–Horn conjecture, the infinite product (3.6.3) always converges. However, the proof is delicate and nontrivial; see Section 5 for the details.

The only case of the Bateman–Horn conjecture that has been proven is the prime number theorem for arithmetic progressions (Theorem 6.1.1). However, an upper bound similar to (3.6.2) is known to be true. The Brun sieve provides a constant B that depends only on k and the degrees of the polynomials involved such that

$$Q(f_1, f_2, \dots, f_k; x) \leq \frac{B C(f_1, f_2, \dots, f_k)}{\prod_{i=1}^k \deg f_i} \int_2^x \frac{dt}{(\log t)^k}$$

for sufficiently large x [81, Thm. 3, Sect. I.4.2]. Thus, the prediction afforded by the Bateman–Horn conjecture is not unreasonably large.

4. Historical background

Before proceeding to applications and examples of the Bateman–Horn conjecture, we first discuss its historical context. In particular, we briefly examine several important antecedents that the conjecture generalizes. We are fortunate to have available the personal recollections of Roger A. Horn, who was kind enough to provide his account of the events leading up to the formulation of the conjecture.

4.1. Predecessors of the conjecture

The Bateman–Horn conjecture is the culmination of hundreds of years of theorems and conjectures about the large-scale distribution of the prime numbers [32]. In Section 3 we arrived at the conjecture from the prime number theorem and heuristic reasoning based upon the Cramér probabilistic model of the primes (see [30] for a nice exposition of this model). Although this is easy to do in hindsight, in reality the Bateman–Horn conjecture evolved naturally from a family of interrelated conjectures, all of which remain open.

We state these conjectures in modern terminology and with our present notation for the sake of uniformity and clarity.

Bunyakovsky conjecture [9] (1854): Suppose that $f \in \mathbb{Z}[x]$ is irreducible, $\deg f \geq 1$, the leading coefficient of f is positive, and the sequence $f(1), f(2), \dots$ is relatively prime. Then $f(n)$ is prime infinitely often.

This conjecture, which concerns prime values assumed by a single polynomial, was proposed by Viktor Yakovlevich Bunyakovsky (1804–1889). It implies, for example, Landau’s conjecture on the infinitude of primes of the form $n^2 + 1$. The condition that $f(1), f(2), \dots$ is relatively prime is equivalent to the assumption that f does not vanish identically modulo any prime, which appears in the Bateman–Horn conjecture. Dirichlet’s theorem on primes in arithmetic progressions (1837) is the degree-one case of the Bunyakovsky conjecture.

Dickson’s conjecture [20] (1904): If $f_1, f_2, \dots, f_k \in \mathbb{Z}[x]$ are of the form $f_i(x) = a_i x + b_i$, in which each a_i is positive, and there is no congruence obstruction, then $f_1(n), f_2(n), \dots, f_k(n)$ are simultaneously prime infinitely often.

This was conjectured by Leonard Eugene Dickson (1874–1954) as an extension of Dirichlet’s theorem. By a “congruence obstruction” we mean that the f_1, f_2, \dots, f_k are not prevented from assuming infinitely many prime values by some combination of congruences. For example, $f_1(x) = x + 3$, $f_2(x) = x + 7$, and $f_3(x) = x - 1$ are congruent modulo 3 to x , $x + 1$, and $x + 2$, respectively. For each $n \in \mathbb{N}$, at least one of $f_1(n), f_2(n), f_3(n)$ is divisible by three. Since these polynomials are nonconstant, this prevents them from being simultaneously prime infinitely often.

First Hardy–Littlewood Conjecture [33] (1923): Let $0 < m_1 < m_2 < \dots < m_k$. Unless there is a congruence obstruction, the number of primes $q \leq x$ such that $q + 2m_1, q + 2m_2, \dots, q + 2m_k$ are prime is asymptotic to

$$2^k \prod_{p \text{ odd}} \left(1 - \frac{1}{p}\right)^{-(k+1)} \left(1 - \frac{w(p; m_1, m_2, \dots, m_k)}{p}\right) \int_2^x \frac{dt}{(\log t)^{k+1}},$$

in which $w(p; m_1, m_2, \dots, m_k)$ is the number of distinct residues of $0, m_1, m_2, \dots, m_k$ modulo p .

Unlike the conjectures of Bunyakovsky and Dickson, the first Hardy–Littlewood conjecture provides an asymptotic expression for the number of primes of a given form. It is a special case of the Bateman–Horn conjecture with

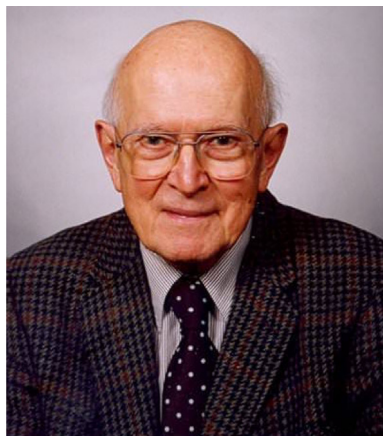
$$f_1(x) = x, \quad f_2(x) = x + 2m_1, \dots, \quad f_{k+1}(x) = x + 2m_k.$$

There are $k + 1$ polynomials involved, which accounts for the power $k + 1$ that appears in the product and the integrand.

The classic paper [33] of Hardy and Littlewood is full of conjectures, labeled “Conjecture A” through “Conjecture P”. Most of these are subsumed under what is now known as the First Hardy–Littlewood conjecture, which we have just stated. Hardy and Littlewood end their paper with the remark:



(a) Paul and Felice Bateman in January 1980. Photo courtesy of Harold G. Diamond.



(b) Photo courtesy of the University of Illinois mathematics department

Fig. 3. Paul T. Bateman (1919–2012).

We trust that it will not be supposed that we attach any exaggerated importance to the speculations which we have set out in this last section. We have not forgotten that in pure mathematics, and in the Theory of Numbers in particular, ‘it is only proof that counts’. It is quite possible, in the light of the history of the subject, that the whole of our speculations may be ill-founded. Such evidence as there is points, for what it is worth, in the opposite direction. In any case it may be useful that, finding ourselves in possession of an apparently fruitful method, we should develop some of its consequences to the full, even where accurate investigation is beyond our powers.

At least one of their conjectures is “ill-founded”. The second Hardy–Littlewood conjecture asserts that $\pi(x + y) \leq \pi(x) + \pi(y)$ for $x \geq 2$. In 1974, Douglas Hensley and Ian Richards proved that the second conjecture is incompatible with the first; see [38], as well as [37,68]. It is not known which of the two conjectures is true, although most number theorists favor the first.

Schinzel’s Hypothesis H [71] (1958): *Let f_1, f_2, \dots, f_k be distinct irreducible, integer-valued polynomials that have positive leading coefficients. If for each prime p there exists an $m \in \mathbb{N}$ such that none of the values $f_1(m), f_2(m), \dots, f_k(m)$ are divisible by p , then there are infinitely many $n \in \mathbb{N}$ such that $f_1(n), f_2(n), \dots, f_k(n)$ are prime.*

This general qualitative predecessor of the Bateman–Horn conjecture was formulated by Andrzej Schinzel (1937–) in 1958. At that time, Schinzel was a student of Wacław Sierpiński (1882–1969) at Warsaw University, and the hypothesis was first stated in its general form in their joint paper [71]. In fact, Schinzel wrote the reviews of the two papers of Bateman and Horn [4,5] for Mathematical Reviews and Zentralblatt MATH, the main reviewing services of the American and European Mathematical Societies, respectively.

The Bateman–Horn conjecture is a quantitative version of Hypothesis H. The hypotheses of both conjectures are essentially the same. The condition that for each prime p there exists an integer m such that none of the values $f_1(m), f_2(m), \dots, f_k(m)$ are divisible by p is equivalent to the condition that the product $f_1 f_2 \cdots f_k$ does not vanish identically modulo any prime.

The Bateman–Horn conjecture unifies all of the conjectures above in one bold prediction. It provides an asymptotic expression for the relevant counting function and, moreover, its predictions agree well with numerical computation. We will chronicle many consequences of the conjecture in Sections 6 and 7.

4.2. Bateman, Horn, and the ILLIAC

Paul T. Bateman (1919–2012) earned his Ph.D. in 1946 under Hans Rademacher (1892–1969) at the University of Pennsylvania (Fig. 3). He joined the mathematics department of the University of Illinois, Urbana–Champaign in 1950 and stayed there until his retirement in 1989, after which he was Professor Emeritus. He was department head from 1965 until 1980 and is credited by many for his leadership, incredible memory, and work ethic. Harold G. Diamond [19] tells us

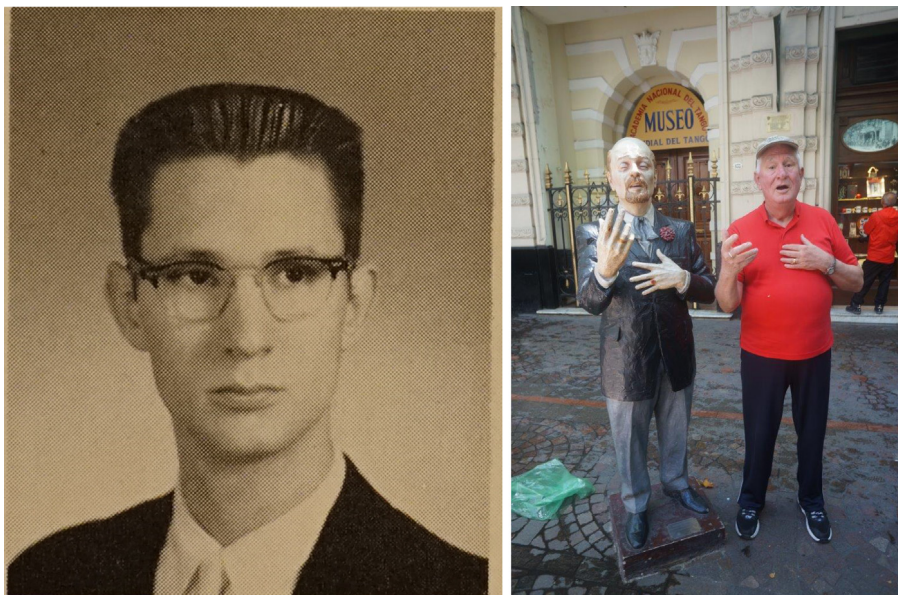
Paul is perhaps best known to the number theory community for the Bateman–Horn conjectural asymptotic formula for the number of k -tuples of primes generated by systems of polynomials... Their formula extended and quantified several famous conjectures of Hardy and J.E. Littlewood, and of Andrzej Schinzel, and they illustrated its quality with calculations. This topic has been treated in dozens of subsequent papers.

Hugh Montgomery adds

Bateman not only organized an active number theory group in Urbana, with such people as John Selfridge, Walter Philipp, Harold Diamond, and Heini Halberstam, but he also did a lot to promote number theory around the country, and also he did a huge amount of service to the AMS. Later, when Bateman died, he didn't get all the honor and credit he deserved. He had lived so long, that the (comparatively young) editor of the AMS Notices had no idea who Bateman had been. He insisted on just a very short (1 page or so) obituary, so many of the reminiscences never saw the light of day. Harold Diamond may still have drafts of what we wanted to publish [58].

Fortunately, it appears that Diamond was able to publish much of the desired memorial tribute online [19].

Roger A. Horn (1942–) received his Ph.D. from Stanford in 1967, under the direction of Donald Spencer (1912–2001) and Charles Loewner (1893–1968); see Fig. 4. He worked briefly at Santa Clara University before moving to Johns Hopkins in 1968, where he founded the Department of Mathematical Sciences (now the Department of Applied Mathematics and Statistics in 1972) He remained at Johns Hopkins until 1992, when he moved to the University of Utah as Research Professor. He retired in 2015 and currently resides in Tampa.



(a) Roger Horn in his 1963 Cornell graduation photo, (b) Roger Horn on vacation in Buenos Aires, January 2017.

Fig. 4. Photographs provided courtesy of Roger A. Horn.

Horn is known best for his long and storied career in matrix analysis. Among his chief publications are the classic texts *Matrix Analysis* [42] and *Topics in Matrix Analysis* [41], both coauthored with Charles Johnson. Of his many papers, only two are on number theory; both of these date from the early 1960s and concern the Bateman–Horn conjecture [4,5]. Consequently, many of his close colleagues are unaware of his connection to a famous conjecture in number theory.⁸ For example, the third named author wrote a linear algebra textbook [26] with Roger Horn before he learned, in the course of a number theory project [27,28], that Roger was “the” Horn from Bateman–Horn!

How did Roger Horn co-propose an important conjecture in a field so far from his own? We are fortunate to have access to his detailed recollections [39].

In the early 1960s, the National Science Foundation funded several summer programs intended to introduce college mathematics students to computing. In 1962 I applied to, and was accepted into, one of those programs, which was hosted by the Computing Center at the University of Illinois in Urbana–Champaign.

There were about 10 participants, from all over the country. We were housed in university dorm rooms, attended classes in the Computing Center,

⁸ A common misconception is that Roger Horn is the “Horn” from the famed Horn conjecture about the eigenvalues of a sum of two Hermitian matrices, settled in 1999 by Knutson–Tao [49] and Klyachko [47]. That distinction belongs to Alfred Horn (1918–2001), who made the conjecture in 1962 [40], the same year in which the Bateman–Horn conjecture appeared [4].



Fig. 5. The ILLIAC I computer around 1952. Courtesy of the University of Illinois Archives.

and had unlimited access to the hottest computer on campus, the ILLIAC, which later was known as the ILLIAC I when its successor, the ILLIAC II was built.

The ILLIAC (Illinois Automatic Computer), which powered up on September 22, 1952, was the first computer to be built and owned by a United States academic institution; see Fig. 5. It was the second of two identical computers, the first of which was the ORDVAC (Ordnance Discrete Variable Automatic Computer), built by the University of Illinois for the government’s Ballistics Research Laboratory. The two machines employed the architecture proposed by John von Neumann in 1945.

In those days, universities built their own computers: IBM hardware was of the punch-card variety, for which businesses were the primary customers; they were not well suited for scientific work. It was the size of a small house and it consumed a prodigious amount of electric power. It stopped working frequently when one of its thousands of vacuum tubes died. We programmed it in hexadecimal machine code; no high-level user language (BASIC or FORTRAN, for example) was ever written for it.

According to the archives of the University of Illinois, the ILLIAC weighed two tons, measured $10 \times 2 \times 8.5$ feet,⁹ and required approximately 2800 vacuum tubes to operate [1]. A later survey, published in 1961 and based upon observations made in 1959, gives quite

⁹ Horn says “this was only the console, the big box visible in Fig. 5. All this stuff, and a huge power supply, was in a big adjoining room (the size of a small house)”.

different figures: 4427 vacuum tubes of twenty-seven different types [83]. It is likely that the system was somewhat expanded and upgraded in the period since its construction in 1951 and the latter figure perhaps more closely approximates the system that Bateman and Horn used.

Some classes were organized for us. One was on Boolean logic and circuit design, taught by one of the engineers who was working on the design of ILLIAC II. Another was on numerical analysis, taught by Herb Wilf, who was a young assistant professor and author (with Anthony Ralston) of a new numerical analysis textbook [Mathematical Methods for Digital Computers]. I first learned about interpolation and orthogonal polynomials in that class.

Initially, we were given small problems to program for the ILLIAC to develop our programming skills. Programs were typed onto paper tape with the same Teletype machines used by Western Union. Noisy! We submitted our tapes to the ILLIAC operator, who fed them into the machine. We did that a lot because most of the time our programs crashed. The ILLIAC had a small speaker hooked up to a bit in its accumulator register, and gave out a high-pitched whine when it went into a loop. The operator had to flip a “kill” switch to stop it, and that was embarrassing.

The ILLIAC could read punched paper tape at a rate of 300 characters per second. Moreover, “five hole teletype tape is used. Numerical data are read with a 4-hole code. Alphanumerical data employs a 5-hole code and a special instruction” [83]. Output appeared on paper tape at 60 characters per second, or on a page printer at a sluggish 10 characters per second.

After a couple of weeks we started work on some projects. The organizers had lined up some faculty who were willing to mentor us and supervise projects. I chose two: One was as part of a team of three supervised by Herb Wilf. We did a lot of calculations in an attempt to find a counterexample to the Pólya–Schoenberg conjecture (if two normalized univalent analytic functions on the unit disk have the property that each maps the unit disk onto a convex domain, then their Hadamard product has the same property). Part of the computation required testing some very large Hermitian matrices for positive definiteness, so I learned something about that topic. All of our runs produced negative results...no counterexamples found. This was a good thing, because about 10 years later the conjecture became a theorem.

The conjecture, stated in 1958 by George Pólya (1887–1985) and Isaac Schoenberg (1903–1990) [66], became a theorem in 1973 when it was proved by Stephan Ruscheweyh and Terence Sheil-Small [70]. Although we do not wish to drift too far afield, there are a few tangential remarks of mild historical interest that are worth making. First, Herbert Saul Wilf (1931–2012) was at Illinois from 1959 to 1962, after which he moved to the University of Pennsylvania. Thus, Horn must have worked with Wilf just before his departure. Wilf’s 1963 paper on the Pólya–Schoenberg conjecture also mentions Horn’s contribution and identifies several other participants of the 1962 summer research program:

The machine program was planned and executed by Messrs. Roger A. Horn (Cornell University), Forrest R. Miller Jr. (University of Oklahoma) and Gerald Shapiro (Massachusetts Institute of Technology) who visited the Digital Computer Laboratory at Illinois during a summer program for undergraduates in Applied Mathematics sponsored by the National Science Foundation. These calculations were made possible largely by their dedication and enthusiasm [84].

Now back to number theory and Roger Horn’s account of the origins of the Bateman–Horn conjecture [39].

My other project was a lone effort supervised by Paul T. Bateman, a famous analytical number theorist; I think he was chair of the math department at the time. His Ph.D. advisor was Hans Rademacher. He had me read some papers that dealt with a variety of number-theoretic conjectures (there were then, and still are now, a LOT of them!) with the goal of choosing something that might be amenable to experimental computation. Eventually, we settled on the problem reported on in our 1962 Math. Comp. paper. I burned up about 7 h of ILLIAC time, but the results were very interesting and gave increased confidence in the conjectures.

The UIUC mathematics department website and two short biographies of Bateman assert that he was department head (not chair) from 1965 until 1980 [19,64]. Hugh Montgomery tells us that “Bateman was not the chair of the math dept when I arrived as a freshman in 1962. The chair at that time was M.M. Day. But during my sophomore year, Day became ill with an ulcer, and Bateman was then asked to take over. He was probably chair first, and then head later” [58].¹⁰

Of greater interest to us are the computations mentioned above. The paper [4], in which the Bateman–Horn conjecture is stated, says the following.

The second-named author [Roger Horn] used the ILLIAC to prepare a list of the 776 primes of the form $p^2 + p + 1$ with p a prime less than 113,000. (The program used was a straightforward one, and the running time was about 400 min.) The first 209 of these primes are listed by Bateman and Stemmler who considered primes of the form $p^2 + p + 1$ in connection with a problem in algebraic number theory.

The “Stemmler” mentioned above is Rosemarie M.S. Stemmler, a student of Bateman who received her Ph.D. in 1959 [6]. Bateman and Horn computed $Q(f_1, f_2; x)$ for various $x \leq 113,000$ with $f_1(t) = t$ and $f_2(t) = t^2 + t + 1$. On the third named author’s late-2013 iMac, the same computation takes only a tenth of a second!

¹⁰ Montgomery also remarks “I was interested in number theory already when I was in high school. At Illinois I started taking their honors math courses. I got to know Bateman during the second half of my sophomore year, when I took his graduate-level problem-solving class. I worked around 40 h per week on that one class, while carrying a full load of other courses, but it was worth it. During the summer after my junior year, he had me stay in Urbana and do a research project, probably on the same grant that Horn had been on. It was sort of a precursor of REU”.

Although the summer drew to a close, Horn continued to work on the project:

When the summer was over, I went back to Cornell for my senior year and found that they had taken delivery of a brand new CDC [Control Data Corporation] 1604 computer. It took a while for folks to discover that it was in operation and move their work to a new programming environment, so I was able to get quite a lot of overnight time on the machine, which was much faster than the ILLIAC and a lot more reliable. It had FORTRAN, too! I ran a lot of additional experiments that were reported in our 1965 Symposia in Pure Math VIII paper [5]. And then I graduated, went to graduate school, took other directions in my research, and haven't thought about these number theory issues since 1963.

We wrap things up with a humorous anecdote connected to the Bateman–Horn conjecture. Serge Lang (1927–2005), in his book *Math Talks for Undergraduates* provides one of the few expositions of the conjecture [52]. In the introduction, he claims that his tone was too conversational and informal for certain editors:

[Paul] Halmos once characterized this style as “vulgar”, and obstructed publication of excerpts in the *Math Monthly*. A decade later, in the 1990s, the present talk was offered for publication again in the *Math Monthly*, and was turned down by the editor (Roger Horn, this time) because of the spoken style. Well, I like the spoken style, and I find it effective. Go figure. [52, p. 1]

There is a remarkable confluence here. Paul Halmos, the academic grandfather of the third named author, was editor(-in-chief) of the *American Mathematical Monthly* from 1982 to 1986. Herbert S. Wilf, who we met above in connection to the Pólya–Schoenberg conjecture, was the editor from 1987 to 1991. Roger Horn was editor from 1997 to 2001!

Horn recalls that he “had a memorable bad experience once with Lang, while I was Editor of the *Monthly*”. Although he has no recollection of a submission related to the Bateman–Horn conjecture, he does remember several submissions on other topics. He also vividly remembers a phone call in which “[Lang] shouted at me for ten minutes or so, and then hung up”.

5. Why does the product converge?

We now discuss the convergence of the product (3.6.3) that defines the Bateman–Horn constant $C(f_1, f_2, \dots, f_k)$. This is a delicate argument that requires elements of both algebraic and analytic number theory, along with a few tricks to deal with conditionally convergent infinite products. In [17, p. 36], the authors state:

It is not even clear that in formula (2.18) the expression $C(f_1, f_2, \dots, f_k)$ represents a product which converges to a positive limit.

We wish to provide a thorough account here since most of these details are suppressed in the original source [4].

5.1. Infinite products

Before we can proceed with the proof that the product (3.6.3) that defines the Bateman–Horn constant converges, we require a few general words about infinite products.

The only way that a zero factor can appear in the evaluation of $C(f_1, f_2, \dots, f_k)$ is if $\omega_f(p) = p$ for some prime p ; that is, if f vanishes identically modulo p . This is prohibited by the hypotheses of the Bateman–Horn conjecture, so we can safely ignore this possibility. Let a_n be a sequence in $\mathbb{C} \setminus \{-1\}$. Fix a branch of $\log z$ the logarithm with $\log 1 = 0$ and for which $\log(1 + a_n)$ is defined.

- We say that $\prod_{n=1}^{\infty} (1 + a_n)$ converges to $L \neq 0$ if and only if $\sum_{n=1}^{\infty} \log(1 + a_n)$ converges to $\log L$. Otherwise the infinite product diverges.
- If a_n is a sequence of real numbers and $\sum_{n=1}^{\infty} \log(1 + a_n)$ diverges to $-\infty$, then we say that $\prod_{n=1}^{\infty} (1 + a_n)$ diverges to zero. In particular, this means that the partial products $\prod_{n=1}^N (1 + a_n)$ tend to zero as $N \rightarrow \infty$.

It turns out that the infinite products that arise in the Bateman–Horn conjecture are often rather finicky. To handle them, we require the following convergence criterion. Although it is well known in analysis circles as a folk theorem, we are unable to find a reference that contains a proof. For the sake of completeness, we provide the proof below.

Lemma 5.1.1. *Let a_n be a sequence in $\mathbb{C} \setminus \{-1\}$. If $\sum_{n=1}^{\infty} |a_n|^2 < \infty$, then $\sum_{n=1}^{\infty} a_n$ and $\prod_{n=1}^{\infty} (1 + a_n)$ converge or diverge together.*

Proof. For $|z| \leq \frac{1}{2}$,

$$\log(1+z) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1} z^n}{n} = z + \left(-\frac{1}{2} + \frac{z}{3} - \frac{z^2}{4} + \dots \right) z^2 = z + z^2 L(z), \quad (5.1.2)$$

in which

$$|L(z)| \leq \sum_{n=0}^{\infty} \frac{1}{(n+2)2^n} = -2 + \log 16 = 0.77258\dots < 1.$$

If $\sum_{n=1}^{\infty} |a_n|^2 < \infty$, then there is an N such that $|a_n| \leq \frac{1}{2}$ for $n \geq N$. Therefore,

$$\sum_{n=N}^{\infty} \log(1 + a_n) = \sum_{n=N}^{\infty} a_n + \sum_{n=N}^{\infty} a_n^2 L(a_n),$$

in which the second series on the right-hand side converges absolutely by the comparison test. Thus,

$$\begin{aligned} \sum_{n=1}^{\infty} a_n \text{ converges} &\iff \sum_{n=1}^{\infty} \log(1 + a_n) \text{ converges} \\ &\iff \prod_{n=1}^{\infty} (1 + a_n) \text{ converges.} \quad \square \end{aligned}$$

Example 5.1.3. The hypothesis $\sum_{n=1}^{\infty} |a_n|^2 < \infty$ is necessary in [Lemma 5.1.1](#). If

$$a_n = \frac{(-1)^n}{\sqrt{n \log n}}$$

for $n \geq 2$, then

$$\sum_{n=2}^{\infty} |a_n|^2 = \sum_{n=2}^{\infty} \frac{1}{n \log n} \quad (5.1.4)$$

diverges by the integral test. However, $\sum_{n=2}^{\infty} a_n$ converges by the alternating series test while the second series on the right-hand side of

$$\sum_{n=4}^{\infty} \log(1 + a_n) = \sum_{n=4}^{\infty} a_n + \sum_{n=4}^{\infty} \frac{L(a_n)}{n \log n}$$

diverges by the limit comparison test against [\(5.1.4\)](#) since $L(a_n) \rightarrow -\frac{1}{2}$ by [\(5.1.2\)](#).¹¹

The infinite product $\prod_{n=1}^{\infty} (1 + a_n)$ converges absolutely if $\prod_{n=1}^{\infty} (1 + |a_n|)$ converges; this is equivalent to the convergence of $\sum_{n=1}^{\infty} |a_n|$. An infinite product that converges but does not converge absolutely is *conditionally convergent*.

5.2. Algebraic prerequisites

Let \mathbb{K} be a number field; that is, a finite algebraic extension of \mathbb{Q} . This implies that each element of \mathbb{K} is algebraic over \mathbb{Q} and that the dimension of \mathbb{K} as a \mathbb{Q} -vector space is finite. This dimension is called the *degree* of \mathbb{K} over \mathbb{Q} and denoted by $[\mathbb{K} : \mathbb{Q}]$.

For each $\alpha \in \mathbb{K}$, there is a unique irreducible polynomial $m_{\alpha}(x) \in \mathbb{Z}[x]$ with relatively prime coefficients and positive leading coefficient such that $m_{\alpha}(\alpha) = 0$. This is the *minimal polynomial* of α . The *degree of α* , denoted by $\deg \alpha$, is the degree of the polynomial m_{α} , which is at most $[\mathbb{K} : \mathbb{Q}]$. One can show that

$$\mathcal{O}_{\mathbb{K}} := \{\alpha \in \mathbb{K} : m_{\alpha}(x) \text{ is monic}\}$$

is a subring of \mathbb{K} (see, for instance, Theorem 2.9 of [\[77\]](#) or p.16 of [\[54\]](#)); it is the *ring of algebraic integers* of \mathbb{K} . Since $m_n(x) = x - n$ is irreducible for each $n \in \mathbb{Z}$, it follows that $\mathbb{Z} \subseteq \mathcal{O}_{\mathbb{K}}$.

For $\alpha \in \mathbb{K}$, let $\mathbb{Q}(\alpha)$ denote the smallest (with respect to inclusion) subfield of \mathbb{K} that contains \mathbb{Q} and α . The following important theorem asserts that every number field is generated by a single algebraic integer [\[77, Thm. 2.2 & Cor. 2.12\]](#).

Theorem 5.2.1 (*Primitive Element Theorem*). *If \mathbb{K} is a number field, then there is a $\theta \in \mathcal{O}_{\mathbb{K}}$ such that $\mathbb{K} = \mathbb{Q}(\theta)$.*

If $\mathbb{K} = \mathbb{Q}(\theta)$, then we have the field isomorphism

$$\mathbb{K} \cong \mathbb{Q}[x]/\langle m_{\theta}(x) \rangle,$$

¹¹ To use [\(5.1.4\)](#) we require $|a_n| \leq \frac{1}{2}$. Note that $|a_3| > \frac{1}{2}$ and $|a_n| \leq \frac{1}{2}$ for $n \geq 4$.

in which $\langle m_\theta(x) \rangle$ is the (maximal) ideal in $\mathbb{Q}[x]$ generated by the irreducible polynomial $m_\theta(x)$. In this case, $[\mathbb{K} : \mathbb{Q}] = \deg \theta$. Observe that $\mathbb{Z}[\theta]$, the set of integral linear combinations of powers of θ , is a subring of $\mathcal{O}_{\mathbb{K}}$ and hence $\mathcal{O}_{\mathbb{K}}$ is a ring extension of $\mathbb{Z}[\theta]$. The index of $\mathbb{Z}[\theta]$ inside $\mathcal{O}_{\mathbb{K}}$ (as abelian groups), which is finite, is denoted $[\mathcal{O}_{\mathbb{K}} : \mathbb{Z}[\theta]]$.

We say that p is a *rational prime* if it is a prime in the ring \mathbb{Z} ; that is, if p is prime in the traditional sense. For each rational prime p , the set $p\mathcal{O}_{\mathbb{K}}$ is an ideal in $\mathcal{O}_{\mathbb{K}}$. Although this ideal might not be a prime ideal in $\mathcal{O}_{\mathbb{K}}$, it can be factored as a product of prime ideals [77, Thm. 5.6]. Thus, for each rational prime p there exist distinct prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_k \subset \mathcal{O}_{\mathbb{K}}$ and positive integers e_1, e_2, \dots, e_k such that

$$p\mathcal{O}_{\mathbb{K}} = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_k^{e_k}. \quad (5.2.2)$$

This factorization is unique up to permutation of factors. Each prime ideal $\mathfrak{p} \subset \mathcal{O}_{\mathbb{K}}$ can be present in the factorization for only one rational prime [77, Thm. 5.14c].

If $e_i > 1$ for some i in (5.2.2), then p *ramifies* in \mathbb{K} ; the exponents e_1, e_2, \dots, e_k are called *ramification indices*. There are only finitely many rational primes p that ramify in a given number field [54, Cor. 2, p. 73]. Since prime ideals in $\mathcal{O}_{\mathbb{K}}$ are maximal [77, Thm. 5.3d], it follows that $\mathcal{O}_{\mathbb{K}}/\mathfrak{p}_i$ is a field for each \mathfrak{p}_i in the factorization (5.2.2). In fact, it is a finite field of characteristic p [54, p. 56] and hence its cardinality is p^{f_i} for some f_i , which is called the *inertia degree* of p at \mathfrak{p}_i (the notation f_i is standard and should not be confused with the polynomials in the statement of the Bateman–Horn conjecture). The *norm* of the ideal \mathfrak{p}_i is

$$N(\mathfrak{p}_i) = |\mathcal{O}_{\mathbb{K}}/\mathfrak{p}_i| = p^{f_i} \quad (5.2.3)$$

and there are only finitely many prime ideals in $\mathcal{O}_{\mathbb{K}}$ of a given norm [77, Thm. 5.17c]. The factorization (5.2.2) is related to the factorization of $m_\theta(x)$ modulo p . This connection is given by the Dedekind factorization criterion (see [52, Prop. 25, p. 27]).

Theorem 5.2.4 (Dedekind Factorization Criterion). *Let $\mathbb{K} = \mathbb{Q}(\theta)$, in which $\theta \in \mathcal{O}_{\mathbb{K}}$, and let p a rational prime whose ideal $p\mathcal{O}_{\mathbb{K}}$ factors as in (5.2.2). If $p \nmid [\mathcal{O}_{\mathbb{K}} : \mathbb{Z}[\theta]]$, then there is a factorization*

$$m_\theta(x) \equiv g_1(x)^{e_1} g_2(x)^{e_2} \cdots g_k(x)^{e_k} \pmod{p}$$

into powers of irreducible polynomials $g_i(x)$ modulo p , in which $\deg g_i(x) = f_i$, the inertia degree of p at the corresponding prime ideal \mathfrak{p}_i .

One immediate and important implication of this theorem is that

$$\deg \theta = \sum_{i=1}^k e_i f_i.$$

Observe also that $m_\theta(a) \equiv 0 \pmod{p}$ for some $a \in \mathbb{Z}$ if and only if $(x - a) \mid m_\theta(x)$ modulo p . This occurs if and only if $g_i(x) = x - a$ for some i , in which case $f_i = \deg g_i = 1$ and (5.2.3) tells us that the corresponding prime ideal \mathfrak{p}_i in the factorization (5.2.2) has norm p . Since there are only finitely many primes that divide the index $[\mathcal{O}_{\mathbb{K}} : \mathbb{Z}[\theta]]$, we have the following corollary.

Corollary 5.2.5. *Let $g(x) \in \mathbb{Z}[x]$ be a monic irreducible polynomial with root θ and let $\mathbb{K} = \mathbb{Q}(\theta)$. For all but finitely many rational primes p , the number $\omega_g(p)$ of solutions to $g(x) \equiv 0 \pmod{p}$ equals the number of prime ideals of norm p in the prime ideal factorization of $p\mathcal{O}_{\mathbb{K}}$.*

5.3. Analytic prerequisites

Later on we will need the following theorem of Leonhard Euler. We present a proof due to Clarkson [11]; see [82] for a survey of various proofs.

Theorem 5.3.1 (*L. Euler, 1737*). $\sum_p \frac{1}{p}$ diverges.

Proof. Let p_n denote the n th prime number and suppose toward a contradiction that $\sum_{n=1}^{\infty} \frac{1}{p_n}$ converges. Since the tail end of a convergent series tends to zero, let K be so large that

$$\sum_{j=K+1}^{\infty} \frac{1}{p_j} < \frac{1}{2}.$$

Let $Q = p_1 p_2 \cdots p_K$ and note that none of the numbers

$$Q + 1, 2Q + 1, 3Q + 1, \dots$$

is divisible by any of the primes p_1, p_2, \dots, p_K . Now observe that

$$\sum_{n=1}^N \frac{1}{nQ+1} \leq \sum_{m=1}^{\infty} \left(\sum_{j=K+1}^{\infty} \frac{1}{p_j} \right)^m < \sum_{m=1}^{\infty} \left(\frac{1}{2} \right)^m = 1$$

for $N \geq 1$; the reason for the first inequality is the fact that the sum in the middle, when expanded term-by-term, includes every term on the left-hand side (and with a coefficient greater than or equal to 1). This is a contradiction, since $\sum_{n=1}^{\infty} \frac{1}{nQ+1}$ diverges by the integral test. \square

A more precise version of the preceding lemma was obtained by Franz Mertens (1840–1927). Since the proof of Mertens' theorem would draw us too far afield, we refer the reader to Terence Tao's exposition for details [79].

Theorem 5.3.2 (*Mertens, 1874*).

$$\sum_{p \leq x} \frac{1}{p} = \log \log x + B + O\left(\frac{1}{\log x}\right)$$

in which $B = 0.2614972128476 \dots$ is the Meissel–Mertens constant.

Much of the analytic theory of prime numbers goes through to prime ideals, *mutatis mutandis*. Define

$$\pi_{\mathbb{K}}(x) = |\{\mathfrak{p} \subset \mathcal{O}_{\mathbb{K}} : \mathfrak{p} \text{ is a prime ideal and } N(\mathfrak{p}) \leq x\}|,$$

which is a generalization of the usual prime counting function $\pi(x) = \pi_{\mathbb{Q}}(x)$. The prime number theorem asserts that $\pi(x) \sim x/\log x$. This is a special case of Landau's prime ideal theorem [50], [59, p. 194, p. 267].

Theorem 5.3.3 (Prime Ideal Theorem). *If \mathbb{K} is a number field, then $\pi_{\mathbb{K}}(x) \sim \text{Li}(x)$.*

Thus, the asymptotic distribution of prime ideals (by norm) in a number field mirrors that of the prime numbers in the integers. Therefore, it is not surprising to find an analogue of Mertens' theorem (Theorem 5.3.2) that holds for prime ideals [69, Lemma 2.4] or [53, Prop. 2].

Theorem 5.3.4 (Mertens Theorem for Number Fields). *If \mathbb{K} is an algebraic number field, then there is a constant C such that*

$$\sum_{N(\mathfrak{p}) \leq x} \frac{1}{N(\mathfrak{p})} = \log \log x + C + O\left(\frac{1}{\log x}\right),$$

in which the sum runs over all nonzero prime ideals \mathfrak{p} in $\mathcal{O}_{\mathbb{K}}$ of norm at most x .

We are now in a position to prove the following convergence result (recall that p always denotes a prime number and that \sum_p means that we sum over all primes).

Lemma 5.3.5. *Let $g(x) \in \mathbb{Z}[x]$ be monic and irreducible. For each rational prime p , let $\omega(p)$ denote the number of solutions to $g(x) \equiv 0 \pmod{p}$. Then*

$$\sum_p \frac{\omega(p) - 1}{p}$$

converges.

Proof. Let $\mathbb{K} = \mathbb{Q}(\theta)$, in which θ is a root of g . Then Corollary 5.2.5 implies that

$$\sum_{p \leq x} \frac{\omega(p)}{p} = \sum_{N(\mathfrak{p}) \leq x} \frac{1}{N(\mathfrak{p})} + A,$$

in which the constant A arises from the finitely many rational primes p that are excluded from Corollary 5.2.5. Theorems 5.3.2 and 5.3.4 imply that

$$\begin{aligned} \sum_{p \leq x} \frac{\omega(p) - 1}{p} &= \sum_{N(\mathfrak{p}) \leq x} \frac{1}{N(\mathfrak{p})} - \sum_{p \leq x} \frac{1}{p} + A \\ &= \left[\log \log x + C + O\left(\frac{1}{\log x}\right) \right] \\ &\quad - \left[\log \log x + B + O\left(\frac{1}{\log x}\right) \right] + A \\ &= A - B + C + O\left(\frac{1}{\log x}\right) \end{aligned}$$

converges to $A - B + C$ as $x \rightarrow \infty$. \square

5.4. Convergence of the product

We are now ready to prove the convergence of the product (3.6.3) that defines the Bateman–Horn constant. Let $f_1, f_2, \dots, f_k \in \mathbb{Z}[x]$ be irreducible and define $f = f_1 f_2 \cdots f_k$. Let $\omega_i(p)$ and $\omega(p)$ denote the number of solutions in $\mathbb{Z}/p\mathbb{Z}$ to $f_i(x) \equiv 0 \pmod{p}$ and $f(x) \equiv 0 \pmod{p}$, respectively.

Lemma 5.4.1. *For all but finitely many primes p ,*

$$\omega(p) = \omega_1(p) + \cdots + \omega_k(p). \quad (5.4.2)$$

Proof. Since p is prime, each zero of f in $\mathbb{Z}/p\mathbb{Z}$ is a zero of some f_i . Thus,

$$\omega(p) \leq \omega_1(p) + \cdots + \omega_k(p).$$

On the other hand, every zero of each f_i in $\mathbb{Z}/p\mathbb{Z}$ is a zero of f . Hence it suffices to show that f_i and f_j have no common zeros in $\mathbb{Z}/p\mathbb{Z}$ if p is sufficiently large. Since the polynomials $f_i(x)$ are irreducible in $\mathbb{Z}[x]$ they are irreducible in $\mathbb{Q}[x]$. If $i \neq j$ then $\gcd(f_i, f_j) = 1$ in $\mathbb{Q}[x]$, which is a Euclidean domain. Hence there exist polynomials $u_{ij}(x)$ and $v_{ij}(x)$ in $\mathbb{Q}[x]$ such that

$$u_{ij}(x)f_i(x) + v_{ij}(x)f_j(x) = 1.$$

Let d_{ij} be the least common denominator of the coefficients of $u_{ij}(x)$ and $v_{ij}(x)$, then $g_{ij}(x) = d_{ij}u_{ij}(x)$ and $h_{ij}(x) = d_{ij}v_{ij}(x)$ are in $\mathbb{Z}[x]$, and we have:

$$g_{ij}(x)f_i(x) + h_{ij}(x)f_j(x) = d_{ij}.$$

Suppose that $f_i(x) \pmod{p}$ and $f_j(x) \pmod{p}$ have a common root $r \in \mathbb{Z}/p\mathbb{Z}$ for some prime p . Substituting r for x in the equation above and reducing modulo p yields

$$d_{ij} \equiv 0 \pmod{p},$$

meaning that p divides d_{ij} , which is only possible for finitely many primes p since p has to be smaller than d_{ij} . Hence for all sufficiently large primes p the polynomials f_i and f_j have no common zeros in $\mathbb{Z}/p\mathbb{Z}$. This completes proof. \square

The product that defines the Bateman–Horn constant need not converge absolutely. Consequently, we must take care to justify its convergence. We are now ready to prove the main result of this section.

Theorem 5.4.3. *The product that defines $C(f_1, f_2, \dots, f_k)$ converges.*

Proof. Lemma 5.4.1 implies that

$$\sum_{p \leq x} \frac{\omega(p) - k}{p} = \sum_{i=1}^k \sum_{p \leq x} \frac{\omega_i(p) - 1}{p} + D$$

for all $x \geq 0$; the constant D arises because of the finitely many exceptions to (5.4.2). The preceding lemma and Lemma 5.3.5 ensure that

$$\sum_p \frac{k - \omega(p)}{p} \text{ converges.} \quad (5.4.4)$$

Then a binomial expansion yields

$$\left(1 - \frac{1}{p}\right)^{-k} \left(1 - \frac{\omega(p)}{p}\right) = 1 + \frac{k - \omega(p)}{p} + \frac{B(p)}{p^2},$$

in which

$$B(p) = \frac{k(k-1)}{2} - \omega(p) + O\left(\frac{1}{p}\right)$$

is uniformly bounded because $|\omega(p)| \leq \deg f$. Let

$$a_p = \frac{k - \omega(p)}{p} + \frac{B(p)}{p^2}$$

and observe that

$$\sum_p a_p = \sum_p \frac{k - \omega(p)}{p} + \sum_p \frac{B(p)}{p^2}$$

converges by (5.4.4) and the comparison test. Since

$$|a_p|^2 = \left(\frac{k - \omega(p)}{p} + \frac{B(p)}{p^2}\right)^2 = \frac{(k - \omega(p))^2}{p^2} + \frac{2B(p)(k - \omega(p))}{p^3} + \frac{B(p)^2}{p^4},$$

the comparison test ensures that $\sum_p |a_p|^2$ converges. Consequently, Lemma 5.1.1 tells us that $\prod_p (1 + a_p)$, the product that defines $C(f_1, f_2, \dots, f_k)$, converges. \square

The preceding argument, first envisioned in its general form by Bateman and Horn (but also in some special cases by Nagell (1921), Rademacher (1924) and Ricci (1937); see [15] for a discussion), shows that the constant $C(f_1, f_2, \dots, f_k)$ is well defined. However it is still hard to compute due to the fact that the convergence of the product in question is not necessarily absolute or rapid. This consideration leaves an open problem: express the constant $C(f_1, f_2, \dots, f_k)$ in terms of an absolutely convergent product. This was done in some special cases in a subsequent paper [5] of Bateman and Horn, and then generally by Davenport and Schinzel [15]. Several methods to accelerate the convergence rate of infinite products for approximation purposes use L -functions; see [43,60].

6. Single polynomials

The Bateman–Horn conjecture implies a wide range of known theorems and unproved conjectures. In this section we examine several such results in the case of a single polynomial. This provides us with some practical experience computing Bateman–Horn constants and it also highlights some delicate convergence issues. Applications of the Bateman–Horn conjecture to families of two or more polynomials are studied in Section 7.

6.1. Prime number theorem for arithmetic progressions

In 1837, Peter Gustav Lejeune Dirichlet (1805–1859) proved that if a and b are relatively prime natural numbers, then there are infinitely many primes of the form $at + b$,

in which $t \in \mathbb{N}$. For example, there are infinitely many primes that end in 123,456,789. To see this, apply Dirichlet's result with $a = 10,000,000$ and $b = 123,456,789$.¹²

Let $\pi_{a,b}(x)$ denote the number of primes at most x that are of the form $at + b$. The complex-variables proof of the prime number theorem can be modified to provide the following asymptotic formulation of Dirichlet's result [80] (see [73] and the discussion on [65, p. 236] for information about elementary approaches).

Theorem 6.1.1 (*Prime Number Theorem for Arithmetic Progressions*). *If a and b are relatively prime natural numbers, then*

$$\pi_{a,b}(x) \sim \frac{1}{\phi(a)} \text{Li}(x). \quad (6.1.2)$$

Here

$$\phi(n) = \#\{k \in \{1, 2, \dots, n\} : \gcd(k, n) = 1\}$$

denotes the *Euler totient function*. Its value equals the order of the group $(\mathbb{Z}/n\mathbb{Z})^\times$ of units in $\mathbb{Z}/n\mathbb{Z}$. The totient function is multiplicative, in the sense that $\phi(mn) = \phi(m)\phi(n)$ whenever $\gcd(m, n) = 1$. It enjoys the product decomposition

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right), \quad (6.1.3)$$

in which the expression $p|n$ denotes that the product is taken over all primes p that divide n . For example, $\phi(6) = 2$ since only 1 and 5 are in the range $\{1, 2, \dots, 6\}$ and relatively prime to 6. The product formulation (6.1.3) tells us the same thing:

$$\phi(6) = 6(1 - 1/2)(1 - 1/3) = 6(\frac{1}{2})(\frac{2}{3}) = 2.$$

What is the intuitive explanation behind the prime number theorem for arithmetic progressions? If $\gcd(a, b) \neq 1$, then a and b share a common factor and hence $at + b$ is prime for at most one t . Thus, $\gcd(a, b) = 1$ is a necessary condition for the polynomial $at + b$ to generate infinitely many primes. For each fixed a , this yields exactly $\phi(a)$ admissible values of $b \pmod{a}$. Since the prime number theorem tells us that $\pi(x) \sim \text{Li}(x)$, (6.1.2) tells us that each of the $\phi(a)$ admissible congruence classes modulo a receives an approximately equal share of primes.

The prime number theorem for arithmetic progressions (Theorem 6.1.1) is a straightforward consequence of the Bateman–Horn conjecture. Let $f(t) = at + b$, in which $\gcd(a, b) = 1$. Then

$$f(t) \equiv 0 \pmod{p} \iff at \equiv -b \pmod{p}. \quad (6.1.4)$$

If $p \nmid a$, then a is invertible modulo p and the preceding congruence has a unique solution. If $p|a$, then (6.1.4) has no solutions since $\gcd(a, b) = 1$. Therefore,

$$\omega_f(p) = \begin{cases} 1 & \text{if } p \nmid a, \\ 0 & \text{if } p|a, \end{cases}$$

¹² The values of $t \leq 100$ for which $at + b$ is prime are 11, 29, 43, 50, 59, 64, 68, 73, 97, 98.

and hence

$$C(f; p) = \prod_p \left(1 - \frac{1}{p}\right)^{-1} \left(1 - \frac{\omega_f(p)}{p}\right) = \prod_{p|a} \left(1 - \frac{1}{p}\right)^{-1} = \frac{a}{\phi(a)}$$

by (6.1.3). In particular, the potentially infinite product reduces to a finite product indexed only over the prime divisors of a . Since

$$at + b \leq x \iff t \leq \frac{x-b}{a},$$

we have

$$\begin{aligned} \pi_{a,b}(x) &= Q\left(f; \frac{x-b}{a}\right) \\ &\sim \frac{a}{\phi(a)} \cdot \frac{(x-b)/a}{\log((x-b)/a)} \\ &= \frac{a}{\phi(a)} \cdot \frac{(x/a) - (b/a)}{\log(x-b) - \log a} \\ &\sim \frac{a}{\phi(a)} \cdot \frac{x/a}{\log(x-b)} \\ &\sim \frac{x}{\phi(a) \log x} \sim \frac{1}{\phi(a)} \operatorname{Li}(x), \end{aligned}$$

which is the desired result.

The weaker statement about simply the infinitude of primes in an arithmetic progression is a special case of the Bunyakovsky conjecture and is currently the only case of that conjecture which has been settled. The conjecture is open for quadratic and cubic polynomials, as we discuss next.

6.2. Landau's conjecture and its relatives

In our heuristic argument (Section 3), we explained how Landau's conjecture (there are infinitely many primes of the form $n^2 + 1$) follows from the Bateman–Horn conjecture. For $f(t) = t^2 + 1$, we showed that

$$Q(f; x) \sim (0.68640\dots) \operatorname{Li}(x);$$

in particular, the conjecture suggests that Landau's intuition was correct. Let $\pi_{\text{Landau}}(x)$ denote the number of primes of the form $n^2 + 1$ that are at most x . Since

$$t^2 + 1 \leq x \iff t \leq \sqrt{x-1},$$

it follows that

$$\begin{aligned} \pi_{\text{Landau}}(x) &= Q(f; \sqrt{x-1}) \sim (0.68640\dots) \operatorname{Li}(\sqrt{x-1}) \\ &\sim (0.68640\dots) \frac{\sqrt{x-1}}{\log(\sqrt{x-1})} \\ &\sim (1.3728\dots) \frac{\sqrt{x}}{\log x}. \end{aligned}$$

Thus, $\pi_{\text{Landau}}(x)$ grows like a constant times $\pi(x)/\sqrt{x}$.

The Bateman–Horn conjecture also implies important variants of Landau’s conjecture. For example, Friedlander and Iwaniec proved that there are infinitely many primes of the form $x^2 + y^4$ (they also provided asymptotics for the counting function of such primes) [24]. For each fixed $y \geq 1$, the Bateman–Horn conjecture suggests that there are infinitely many primes of the form $x^2 + y^4$. A result of Heath-Brown [35] guarantees the existence of infinitely many primes (with an asymptotic formula for the growth of their number) of the form $x^3 + 2y^3$, thereby confirming the conjecture of Hardy and Littlewood on the infinitude of primes expressible as a sum of three cubes. These are results in the interesting and promising direction of representing primes by multivariate polynomials, see the survey [61] and the recent preprint [18].

Let us briefly turn to cubic polynomials in one variable. A result of [23] states, roughly speaking, that on the average polynomials of the form $t^3 + k$ for squarefree $k > 1$ assume infinitely many prime values at integer points, in some well-defined sense. We are not aware of a definitive published result on any specific example of such a polynomial: an existence of an infinitude of prime values of a cubic polynomial is a special case of the Bunyakovsky conjecture that is sometimes called the “cubic primes conjecture”. For example, $f(t) = t^3 - 2$ is irreducible and does not vanish identically modulo any prime. The Bateman–Horn conjecture predicts that this polynomial assumes prime values infinitely often.

6.3. Tricking Bateman–Horn?

What happens if we replace $n^2 + 1$ with $n^2 - 1 = (n - 1)(n + 1)$? The only prime of this form is 3. Of course, the polynomial in question is reducible and hence is not even a permissible candidate for the conjecture. Does the Bateman–Horn conjecture “detect this” attempted fraud, or does it just plow ahead and suggest to the unwary that there are infinitely many primes of this form? For the sake of curiosity, let us try it and see what happens.

If $f(n) = n^2 - 1$, then $f(n) \equiv 0 \pmod{p}$ becomes $n^2 \equiv 1 \pmod{p}$ and hence

$$\omega_f(p) = \begin{cases} 1 & \text{if } p = 2, \\ 2 & \text{otherwise.} \end{cases}$$

Thus,

$$C(f) = \prod_{p \geq 3} \frac{p-2}{p-1} = \prod_{p \geq 3} \left(1 - \frac{1}{p-1}\right). \quad (6.3.1)$$

Let P_n denote the set of the first n odd primes. For example, $P_1 = \{3\}$, $P_2 = \{3, 5\}$, $P_3 = \{3, 5, 7\}$, and so forth. Numerical evidence (Table 3) suggests that

$$\lim_{n \rightarrow \infty} \prod_{p \in P_n} \left(1 - \frac{1}{p-1}\right) = 0; \quad (6.3.2)$$

that is, the product that defines $C(f)$ diverges to zero (this is the case). If this application of the Bateman–Horn conjecture were admissible (it is not since f is reducible), we would expect no primes of the form $n^2 - 1$. This is not too far from the truth: we were

Table 3The partial products $\prod_{p \in P_n} \left(1 - \frac{1}{p-1}\right)$ appear to diverge to zero.

n	$\prod_{p \in P_n} \left(1 - \frac{1}{p-1}\right)$
10	0.210114
100	0.117208
1,000	0.0824772
10,000	0.0641136
100,000	0.0526554
1,000,000	0.044777
10,000,000	0.0390052

off by only one. The Bateman–Horn conjecture is surprisingly robust; in some sense, it detected our trickery and rejected it.

Why does (6.3.1) diverge to zero? Euler’s result (Theorem 5.3.1) ensures that

$$\sum_{p \in P_n} \frac{1}{p-1} > \sum_{p \in P_n} \frac{1}{p},$$

which diverges as $n \rightarrow \infty$. An application of Lemma 5.1.1 implies that (6.3.1) diverges (to zero); that is, $C(f) = 0$. Thus, the Bateman–Horn conjecture detected, in a subtle way, the difference between the polynomials $n^2 + 1$ (which is believed to generate infinitely many prime values) and $n^2 - 1$, which is prime exactly once.

6.4. Prime-generating polynomials

Euler observed in 1772 that the polynomial $f(t) = t^2 + t + 41$ assumes prime values for $t = 0, 1, \dots, 39$. However, $f(40) = 1681 = 41^2$ is composite. Is there a nonconstant polynomial that assumes only prime values?

Theorem 6.4.1. *Let $f \in \mathbb{Z}[x]$. If $f(n)$ is prime for all $n \geq 0$, then f is constant.*

Proof. Let $p = f(0)$, which is prime by assumption. For each $n \geq 0$, the prime $f(pn)$ is divisible by p . Then $f(pn) = p$ for $n \geq 0$ and hence $f(pn) - p$ has infinitely many roots and is therefore zero. Thus, f is the constant polynomial p . \square

This shows that no single-variable polynomial can assume only prime values for all natural arguments. Surprisingly, there is a polynomial of degree twenty-five in twenty-six variables whose positive integral range is precisely the set of prime numbers [45]. This startling fact is related to Matiyasevich’s solution to Hilbert’s tenth problem [55] and the work of Davis–Putnam–Robinson [16]. It is not known what is the smallest number of variables a prime-generating polynomial must have, but it is definitely less than twenty-six: a polynomial with this property in twelve variables is also known; see [17, Sect. 2.1].

What is so special about 41? Suppose that $f(t) = t^2 + t + k$ generates primes for the first few nonnegative integral values of t . Then $k = f(0)$ is prime. In 1913, Georg Yuri Rainich (1886–1968) proved if p is prime, then $n^2 + n + p$ is prime for $n = 0, 1, \dots, p-2$

if and only if the imaginary quadratic field $\mathbb{Q}(\sqrt{1-4p})$ has class number one [67]¹³; for our purposes it suffices to say that this means that $\mathbb{Q}(\sqrt{1-4p})$ is a unique factorization domain. The Baker–Heegner–Stark theorem ensures that there are only finitely many primes p with this property [3,36,75,76]. The largest of these, $p = 41$, corresponds to the quadratic field $\mathbb{Q}(\sqrt{-163})$. Thus, we cannot beat Euler at his own game.

Perhaps we can beat Euler on average. Can we find an Euler-type polynomial that produces an asymptotically greater number of primes than Euler’s polynomial? Let us first examine what the Bateman–Horn conjecture says about $f(t) = t^2 + t + 41$.

Since $f(t)$ is identically 1 modulo 2, $\omega_f(2) = 0$. In what follows we use the “completing the square” identity

$$4a(at^2 + bt + c) = (2at + b)^2 - (b^2 - 4ac). \quad (6.4.2)$$

For $p \geq 3$, this ensures that

$$t^2 + t + 41 \equiv 0 \pmod{p} \iff (2t + 1)^2 \equiv -163 \pmod{p}.$$

Thus, everything boils down to whether -163 is a quadratic residue or nonresidue modulo the odd prime p :

$$\omega_f(p) = 1 + \left(\frac{-163}{p} \right).$$

Here $\left(\frac{-163}{p} \right)$ is a *Legendre symbol*, defined by

$$\left(\frac{\ell}{p} \right) = \begin{cases} 0 & \text{if } p|\ell, \\ 1 & \text{if } \ell \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } \ell \text{ is a quadratic nonresidue modulo } p. \end{cases}$$

Numerical computation confirms that -163 is a quadratic nonresidue modulo

$$3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, \quad (6.4.3)$$

the first eleven odd primes. Thus, $\omega_f(p) = 0$ for these primes and hence

$$\begin{aligned} C(t^2 + t + 41) &= \prod_p \left(1 - \frac{1}{p} \right)^{-1} \left(1 - \frac{\omega_f(p)}{p} \right) \\ &= 2 \prod_{3 \leq p \leq 37} \frac{p}{p-1} \prod_{p \geq 41} \left(1 + \frac{1 - \omega_f(p)}{p-1} \right) \end{aligned} \quad (6.4.4)$$

$$\approx 2 \cdot 3.31993 = 6.63985. \quad (6.4.5)$$

The factors corresponding to $p = 2, 3, \dots, 37$ are each greater than one, which drives $C(f)$ up. We have little control over the second product, although we may hope that

¹³ Rainich published [67] under his original birth name, Rabinowitsch. According to [63], “Rainich was giving a lecture in which he made use of a clever trick which he had discovered. Someone in the audience indignantly interrupted him pointing out that this was the famous Rabinowitsch trick and berating Rainich for claiming to have discovered it. Without a word Rainich turned to the blackboard, picked up the chalk, and wrote ‘RABINOWITSCH.’ He then put down the chalk, picked up an eraser and began erasing letters. When he was done what remained was ‘RA IN I CH.’ He then went on with his lecture”.

$1 - \omega_f(p)$ changes sign regularly enough to keep it in check. Although it is not clear at first glance that the second product in (6.4.4) converges, the product that defines the Bateman–Horn constant is guaranteed to converge (see Section 5) and thus the second product must as well.

The Bateman–Horn conjecture suggests that

$$Q(t^2 + t + 41; x) \sim (3.31993 \dots) \text{Li}(x). \quad (6.4.6)$$

Can we find a second-degree polynomial $f(t)$ for which $Q(f; x)$ exceeds this amount asymptotically? To this end, we want each factor in the product (3.6.3) to be as large as possible. Unfortunately, we cannot arrange for $\omega_f(p) = 0$ for all primes p since the corresponding infinite product

$$\prod_p \left(1 - \frac{1}{p}\right)^{-1} = \prod_p \frac{p}{p-1} = \prod_p \left(1 + \frac{1}{p-1}\right)$$

would diverge by Lemma 5.1.1 and Theorem 5.3.1. However, this would contradict Theorem 5.4.3.

In fairness to Euler, we should try to beat him with a polynomial of the same type. Thus, we search for an integer k such that the polynomial $f(t) = t^2 + t + k$ satisfies $\omega_f(p) = 0$ for the first several dozen or so primes. We first need $k \equiv 1 \pmod{2}$ such that $\omega_f(2) = 0$. The identity (6.4.2) shows that for odd p ,

$$f(t) \equiv 0 \pmod{p} \iff (2t+1)^2 \equiv 1 - 4k \pmod{p}.$$

Consequently, we need to choose an odd k such that $1 - 4k$ is a quadratic nonresidue modulo p for a long initial string of odd primes.

Let P_n denote the set of odd primes at most n . For each $p \in P_n$, let r_p be a quadratic nonresidue modulo p . The Chinese Remainder Theorem provides an odd k_n , unique modulo $2 \prod_{p \in P_n} p$, such that $k_n \equiv 4^{-1}(1 - r_p) \pmod{p}$ for each $p \in P_n$. Then $1 - 4k_n \equiv r_p \pmod{p}$ is a quadratic nonresidue and hence $\omega_p(f) = 0$ for each $p \in P_n$. The corresponding Bateman–Horn constant is

$$C(t^2 + t + k_n) = 2 \prod_{3 \leq p \leq n} \frac{p}{p-1} \prod_{p > n} \frac{p - \omega_f(p)}{p-1}.$$

If $n = 547$, the hundredth odd prime, and we let r_p equal the least primitive root of p , the corresponding constant

$$C(t^2 + t + k_{100}) \approx 2 \cdot (5.4972 \dots) = 10.9945$$

easily beats the constant (6.4.5) corresponding to Euler's polynomial. Unfortunately, k_{100} is not as easily remembered as Euler's 41:

3682528442873462645493394982418837604455310384084190749577
 5453041420103519734083583186615204669729662489042369819157
 7358565650719425670030967384568941667322171286195075149379
 680113340447535104953498545635385597443028681.

It is conceivable that other choices of r_p might lead to a smaller constant, although we have not looked into the matter.¹⁴ The Bateman–Horn conjecture suggests that

$$Q(t^2 + t + k_{100}; x) \sim (5.4972 \dots) \text{Li}(x),$$

which is asymptotically larger than the corresponding prediction (6.4.6) for Euler’s polynomial.

Before we pat ourselves on the back for beating Euler, we should point out that the search for prime-producing polynomials using these sorts of arguments has a long history [7,25,43]. Moreover, without the Bateman–Horn conjecture or one of its weaker relatives (Section 4.1), we do not even know if any quadratic polynomial produces infinitely many primes. Thus, this is all speculative.

6.5. A conjecture of Hardy and Littlewood

A general conjecture about the asymptotic distribution of prime values assumed by quadratic polynomials is due to G.H. Hardy (1877–1947) and John E. Littlewood (1885–1977) [33, p. 48] (see also [34, p. 19]). The more convenient formulation below is from [43, p. 499].

Hardy–Littlewood Conjecture (F). *If a, b, c are relatively prime integers, a is positive, $a + b$ and c are not both even, and $b^2 - 4ac$ is not a perfect square, then there are infinitely many primes of the form $f(t) = at^2 + bt + c$. The number of such primes at most x is asymptotic to*

$$\epsilon \prod_{\substack{p \geq 3 \\ p \mid \gcd(a,b)}} \frac{p}{p-1} \prod_{\substack{p \geq 3 \\ p \nmid a}} \left(1 - \frac{(\Delta/p)}{p-1}\right) \text{Li}(x), \quad (6.5.1)$$

in which

$$\epsilon = \begin{cases} \frac{1}{2} & \text{if } 2 \nmid (a+b), \\ 1 & \text{otherwise.} \end{cases}$$

This is a consequence of the Bateman–Horn conjecture. Let us see why, paying careful attention to the relevance of Hardy and Littlewood’s hypotheses. Suppose that $f(t) = at^2 + bt + c$, in which $a > 0$. What conditions on a, b, c are necessary for f to be prime infinitely often? Since

$$at^2 + bt + c \equiv \begin{cases} c & \text{if } t \equiv 0 \pmod{2}, \\ a + b + c & \text{if } t \equiv 1 \pmod{2}, \end{cases}$$

we want either $a + b$ or c (or both) to be odd. Consequently,

$$\omega_f(2) = \begin{cases} 0 & \text{if } a + b \text{ is even and } c \text{ is odd,} \\ 1 & \text{if } a + b \text{ is odd and } c \text{ is odd,} \\ 1 & \text{if } a + b \text{ is odd and } c \text{ is even.} \end{cases} \quad (6.5.2)$$

¹⁴ If we choose the least primitive roots 2, 2, 3, 2, 3, 2, 5, 2, 3, 2 of the primes (6.4.3), respectively, and apply the algorithm above we obtain $k_{37} = 1,448,243,016,041$.

Suppose that p is an odd prime. There are two cases.

- If $p|a$, then $f(t) \equiv bt + c \pmod{p}$. Since $\gcd(a, b, c) = 1$, we conclude that

$$\omega_f(p) = \begin{cases} 0 & \text{if } p|b, \\ 1 & \text{if } p \nmid b. \end{cases}$$

- If $p \nmid a$, then (6.4.2) ensures that

$$f(t) \equiv 0 \pmod{p} \iff (2at + b)^2 \equiv \Delta \pmod{p},$$

in which $\Delta = b^2 - 4ac$ is the discriminant of f . Thus,

$$\omega_f(p) = 1 + \left(\frac{\Delta}{p}\right).$$

Thus, the Bateman–Horn constant (3.6.3) is

$$\begin{aligned} C(f) &= (2 - \omega_f(2)) \prod_{\substack{p \geq 3, p|a \\ p \nmid b}} \frac{p-0}{p-1} \prod_{\substack{p \geq 3, p|a \\ p \nmid b}} \frac{p-1}{p-1} \prod_{\substack{p \geq 3 \\ p \nmid a}} \frac{p - (1 + (\Delta/p))}{p-1} \\ &= 2\epsilon \prod_{\substack{p \geq 3 \\ p | \gcd(a, b)}} \frac{p}{p-1} \prod_{\substack{p \geq 3 \\ p \nmid a}} \left(1 - \frac{(\Delta/p)}{p-1}\right). \end{aligned} \quad (6.5.3)$$

There is a subtle point here that we wish to highlight. If Δ is a perfect square, then $(\Delta/p) = 1$ and the second factor in (6.5.3) diverges (to zero) by Lemma 5.1.1 and Theorem 5.3.1. This does not contradict the Bateman–Horn conjecture, since f is not irreducible in this case. If Δ is a perfect square, then the two roots

$$\frac{-b + \sqrt{\Delta}}{2a} \quad \text{and} \quad \frac{-b - \sqrt{\Delta}}{2a}$$

of f belong to \mathbb{Q} . Then f would be reducible over \mathbb{Q} and hence, by Gauss' lemma [21, Prop. 5, p. 303], reducible over \mathbb{Z} . Thus, Δ cannot be a perfect square if f is to be prime infinitely often: this is why Hardy and Littlewood assume that $b^2 - 4ac$ is not a perfect square. If Δ is not a perfect square, then the prediction (3.6.1) of the Bateman–Horn conjecture provides the asymptotic formula (6.5.1) proposed by Hardy and Littlewood.

6.6. Ulam's spiral

In 1963, Stanisław Ulam (1909–1984) discovered a startling pattern in the primes, allegedly while doodling at a scientific meeting; see Fig. 6. The story was popularized by Martin Gardner (1914–2010) in his much-loved *Scientific American* column “Mathematical Games” [29]:

Last fall Stanislaw M. Ulam of the Los Alamos Scientific Laboratory, attended a scientific meeting at which he found himself listening to what he describes as a “long and very boring paper”. To pass the time he doodled a grid of horizontal

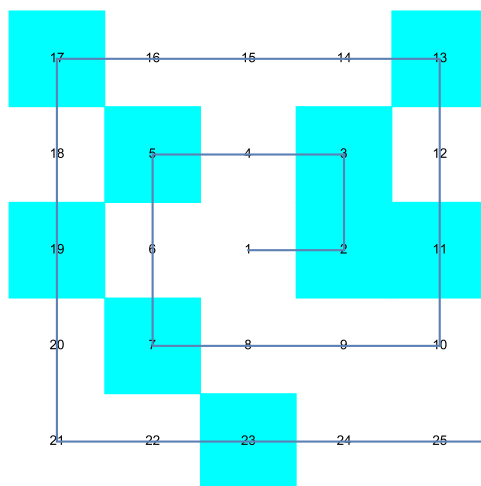


Fig. 6. The natural numbers spiral outward counterclockwise from the origin. A colored box is placed over each prime.

and vertical lines on a sheet of paper. His first impulse was to compose some chess problems, then he changed his mind and began to number the intersections, starting near the center with 1 and moving out in a counterclockwise spiral. With no special end in view, he began circling all the prime numbers. To his surprise the primes seemed to have an uncanny tendency to crowd into straight lines.

The patterns observed by Ulam are evident in Fig. 7. There are certain diagonals that the primes prefer and others that they eschew. Less prominent, but still noticeable, are the scarcity or abundance of primes on some horizontal or vertical lines. Others seem to have more than their fair share of primes. The primes, which are often assumed to be “random” in their overall distribution (Section 2.4), manage to conspire over great distances to form these intriguing patterns. What is the explanation for this behavior?

In what follows, it is more fruitful to consider “rays” in the Ulam spiral instead of “lines”. This is no loss of generality since each line is the union of two rays.

Example 6.6.1. Consider Fig. 8, in which the horizontal ray

$$8, 9, 10, 27, 52, 85, 126, 175, 232, 297, 370, 451, 540, \dots \quad (6.6.2)$$

in the Ulam spiral appears devoid of primes. Why does this occur? Let us truncate our sequence slightly to avoid the short stretch of consecutive integers at the beginning. This yields the sequence

$$10, 27, 52, 85, 126, 175, 232, 297, 370, 451, 540, \dots \quad (6.6.3)$$

To pass from 10 to 27, we walk around the exterior of the 3×3 square

$$\begin{array}{ccc} 5 & 4 & 3 \\ 6 & 1 & 2 \\ 7 & 8 & 9 \end{array}$$

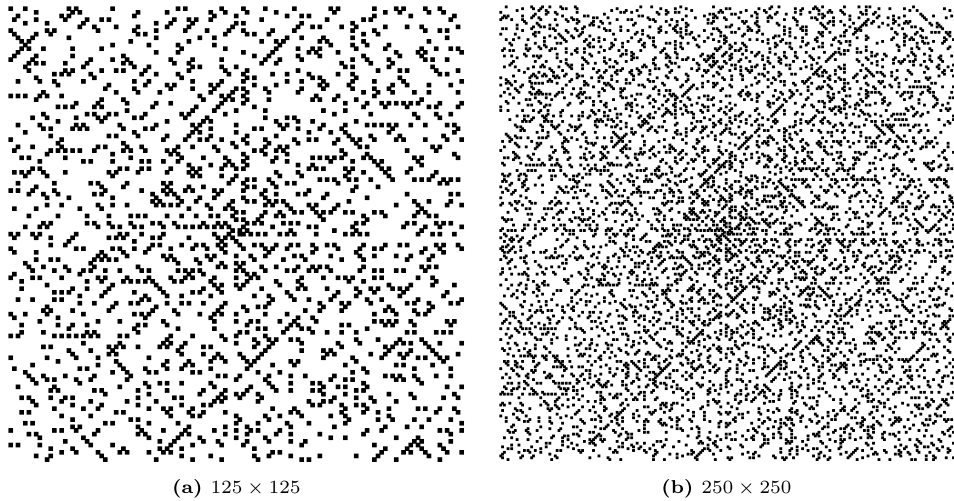


Fig. 7. Plots of the Ulam spiral on grids of several sizes. There are certain diagonals that the primes (black) prefer and others that they eschew. Less prominent, but still noticeable, are the scarcity or abundance of primes on some horizontal or vertical lines. The existence of these patterns is a consequence of the Bateman–Horn conjecture.

and take one more step; this requires $4 \cdot 4 + 1 = 17$ total steps. Similarly, to pass from 27 to 52 we must traverse the exterior of a 5×5 square and take an additional step; this requires $4 \times 6 + 1 = 25$ total steps. Let $f(n)$ denote the n th number on the list (6.6.3). Then induction confirms that

$$f(n) - f(n-1) = 8n + 1,$$

and hence

$$\begin{aligned}
 f(n) &= \sum_{i=2}^n (f(i) - f(i-1)) + f(1) \\
 &= 10 + \sum_{i=2}^n (8i + 1) \\
 &= 10 + (n-1) + 8 \sum_{i=2}^n i \\
 &= n + 9 + 8 \left(\frac{n(n+1)}{2} - 1 \right) \\
 &= 4n^2 + 5n + 1 \\
 &= (4n+1)(n+1).
 \end{aligned} \tag{6.6.4}$$

This ensures that none of the numbers on the horizontal ray (6.6.2) is prime.

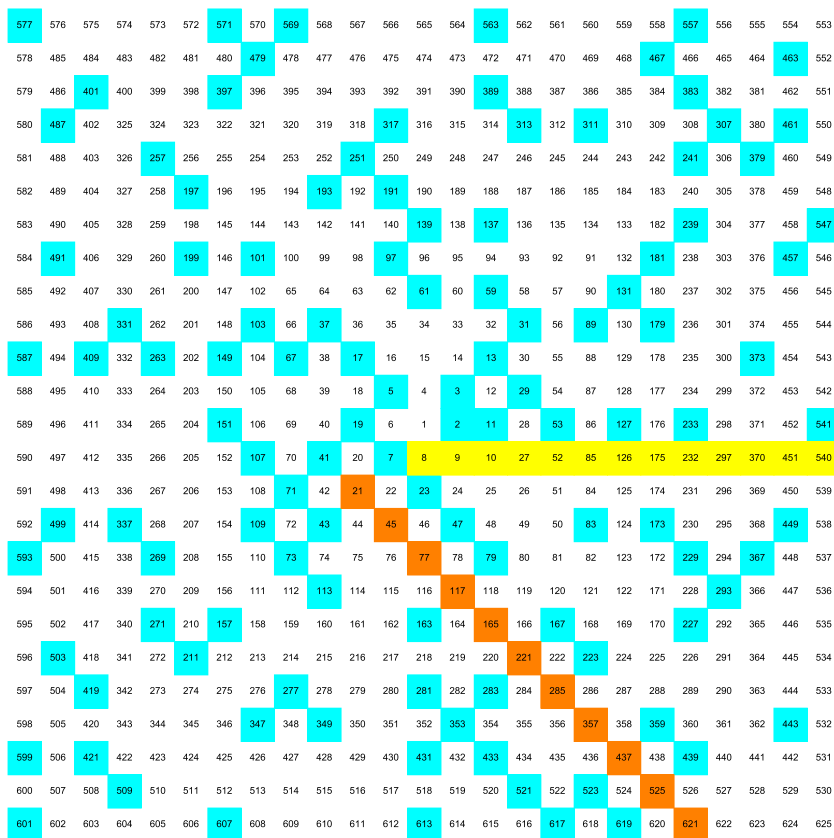


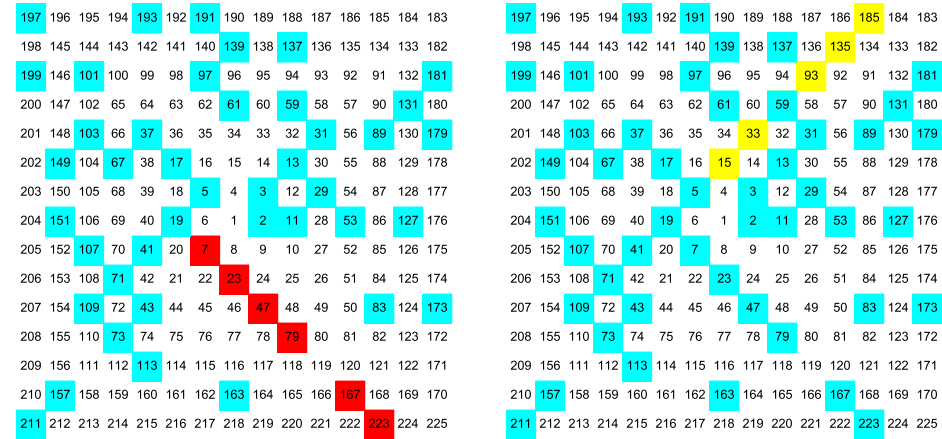
Fig. 8. The horizontal ray depicted in yellow is prime free. If we ignore the initial 8 and 9, and start with $f(1) = 10$, then the n th element on this list is $f(n) = (4n + 1)(n + 1)$, which is composite (see [Example 6.6.1](#)). Similarly, the diagonal ray depicted in orange is prime free. The n th number on this ray is $4n^2 + 12n + 5 = (2n + 1)(2n + 5)$ (see [Example 6.6.5](#)).

Example 6.6.5. The diagonal ray 21, 45, 77, 117, 165, 221, 285, 357, 437, 525, 621, ... in [Fig. 8](#) is similarly devoid of primes. An argument similar to that used in [Example 6.6.1](#) confirms that the n th number on this list is $4n^2 + 12n + 5 = (2n + 1)(2n + 5)$.

The prime-free rays of [Examples 6.6.1](#) and [6.6.5](#) (see [Fig. 8](#)) are governed by a reducible quadratic polynomial. What about prime-rich rays?

Example 6.6.6. Consider [Fig. 9a](#), in which the particularly prime-rich diagonal that includes the primes 7, 19, 23, 47, 67, 79, 103, 167, 199, 223 stands out. As before, it is more convenient to consider a single ray, in which the first differences increase monotonically. We therefore study the ray

$$7, 23, 47, 79, 119, 167, 223, \dots \quad (6.6.7)$$



(a) The diagonal ray $7, 19, 23, 47, 67, 79, \dots$ contains an abundance of primes (red). The n th number on the ray is $f(n) = 4n^2 + 4n - 1$. The Bateman–Horn constant of this polynomial is approximately 3.70.

(b) The diagonal ray $5, 15, 33, 59, 93, \dots$ contains a few primes. The n th number on the ray is $f(n) = 4n^2 - 2n + 3$. The Bateman–Horn constant of this polynomial is approximately 1.02.

Fig. 9. The relative number of primes on diagonal rays is governed by the Bateman–Horn conjecture .

Of these numbers only 119 is composite. If $f(n)$ denotes the n th number on the list (6.6.7), then an argument similar to that of Example 6.6.1 shows that

$$f(n) - f(n - 1) = 8n$$

and hence

$$\begin{aligned} f(n) &= \sum_{i=2}^n (f(i) - f(i - 1)) + f(1) \\ &= 7 + \sum_{i=2}^n 8i \\ &= 8 \left(\frac{n(n+1)}{2} - 1 \right) + 7 \\ &= 4n^2 + 4n - 1. \end{aligned} \tag{6.6.8}$$

Unlike (6.6.4), this polynomial is irreducible. Since it has at most two roots modulo any prime and it does not vanish identically modulo 2, it does not vanish identically modulo any prime. Consequently, the Bateman–Horn conjecture suggests that it assumes infinitely many prime values. Since the discriminant of the polynomial (6.6.8) is 32, the general computation (6.5.3) tells us that

$$Q(f; x) \sim \frac{1}{2} C(f) \text{Li}(x),$$

in which

$$C(f) = 2 \prod_{p \geq 3} \left(1 - \frac{(32/p)}{p-1} \right).$$

Among the odd primes at most 67 we have

$$\left(\frac{32}{p} \right) = \begin{cases} 1 & \text{if } p = 7, 17, 23, 31, 41, 47, \\ -1 & \text{if } p = 3, 5, 11, 13, 19, 29, 37, 43, 53, 59, 61, 67. \end{cases}$$

This substantial imbalance among the first few odd primes makes $C(f)$ unusually large and explains the particularly prime-rich diagonal that corresponds to this polynomial. In particular, numerical computations suggest that $\frac{1}{2}C(f) \approx 3.70$.

Example 6.6.9. Consider the diagonal ray $5, 15, 33, 59, 93, 135, 185, \dots$; see Fig. 9b. Although it contains some primes, it does not appear as prime rich as the ray from Example 6.6.6. Its values correspond to $f(t) = 4t^2 - 2t + 3$, which has discriminant -44 . Since $(-44/3) = (-44/5) = 1$, the primes 3 and 5 conspire to make $C(f)$ smaller; see (6.5.3). The coefficient of $\text{Li}(x)$ provided by the Bateman–Horn conjecture is approximately 1.02. This is substantially lower than in the previous example.

In summary, the patterns that Ulam observed can be explained as follows. If we agree to omit the first several consecutive terms on a given ray, then there are integers b and c such that the n th number on the ray is

$$f(n) = 4n^2 + bn + c.$$

If b is even, then the ray is diagonal. If b is odd, then the ray is horizontal or vertical. Certain combinations of b and c yield reducible polynomials; in these cases the ray contains at most one prime. Other combinations of b and c yield irreducible polynomials; the Bateman–Horn conjecture predicts the relative number of primes along each such ray.

7. Multiple polynomials

We are now ready to apply the Bateman–Horn conjecture to families of irreducible polynomials $f_1, f_2, \dots, f_k \in \mathbb{Z}[x]$ with positive leading coefficients, no two of which are multiples of each other. Recall that the product $f = f_1 f_2 \cdots f_k$ should not vanish modulo any prime. Then the conjecture predicts that the number $Q(f_1, f_2, \dots, f_k; x)$ of $n \leq x$ for which $f_1(n), f_2(n), \dots, f_k(n)$ are simultaneously prime is asymptotic to

$$\frac{C(f_1, f_2, \dots, f_k)}{\prod_{i=1}^k \deg f_i} \int_2^x \frac{dt}{(\log t)^k},$$

in which

$$C(f_1, f_2, \dots, f_k) = \prod_p \left(1 - \frac{1}{p} \right)^{-k} \left(1 - \frac{\omega_f(p)}{p} \right).$$

In particular, observe that the number k of polynomials involved appears in the exponents that occur in the integrand and the product that defines the Bateman–Horn constant.

7.1. Twin prime conjecture

If p and $p + 2$ are prime, then p and $p + 2$ are *twin primes*. The long-standing twin prime conjecture asserts that there are infinitely many twin primes. Although this question likely puzzled thinkers since Euclid's time, the earliest extant record of the conjecture (in a more general form, see Section 7.2) is from Alphonse de Polignac (1826–63) in 1849. While it remains unproven, recent years have seen an explosion of closely-related work [10,56,86].

In 1919, Viggo Brun (1885–1978) proved that the sum

$$\left(\frac{1}{3} + \frac{1}{5}\right) + \left(\frac{1}{5} + \frac{1}{7}\right) + \left(\frac{1}{11} + \frac{1}{13}\right) + \left(\frac{1}{17} + \frac{1}{19}\right) + \cdots \quad (7.1.1)$$

of the reciprocals of the twin primes converges. This stands in stark contrast to Euler's discovery that $\sum_p 1/p$ diverges (Theorem 5.3.1). Thus, the twin primes must be far sparser, in the sense of reciprocal sums, than the primes themselves. The sum (7.1.1), which is now known as *Brun's constant*, is greater than 1.83 and less than 2.347 [48] (numerical evidence suggests a value of approximately 1.9).

What does the Bateman–Horn conjecture have to say about twin primes? Let $f_1(t) = t$ and $f_2(t) = t + 2$. Then $f_1(t)$ and $f_2(t)$ are simultaneously prime if and only if t is the lesser element of a twin-prime pair. Let $f = f_1 f_2$. Then

$$f(t) \equiv 0 \pmod{p} \quad \Longleftrightarrow \quad t(t + 2) \equiv 0 \pmod{p},$$

and hence

$$\omega_f(p) = \begin{cases} 1 & \text{if } p = 2, \\ 2 & \text{if } p \geq 3. \end{cases}$$

The corresponding Bateman–Horn constant is

$$\begin{aligned} C(f_1, f_2) &= \prod_p \left(1 - \frac{1}{p}\right)^{-2} \left(1 - \frac{\omega_f(p)}{p}\right) \\ &= 2 \prod_{p \geq 3} \frac{p^2}{(p-1)^2} \cdot \frac{p-2}{p} \\ &= 2 \prod_{p \geq 3} \frac{p(p-2)}{(p-1)^2} \\ &= 2C_2, \end{aligned}$$

in which

$$C_2 = \prod_{p \geq 3} \frac{p(p-2)}{(p-1)^2} \approx 0.660161815$$

is the *twin primes constant*. The Bateman–Horn conjecture predicts that

$$Q(f_1, f_2; x) \sim 2C_2 \int_2^x \frac{dt}{(\log t)^2}.$$

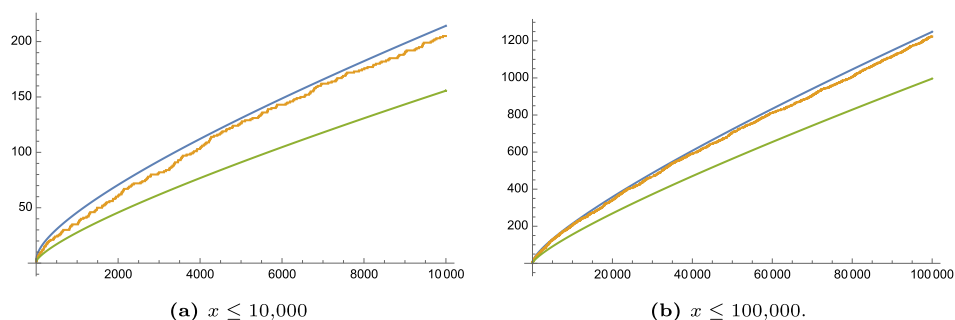


Fig. 10. Graph of $\pi_2(x)$ (orange) versus $2C_2 \int_2^x (\log t)^{-2} dt$ (blue) and $2C_2 x / (\log x)^2$ (green). The more complicated integral expression apparently provides a much better approximation than does the simpler expression.

It is more traditional to express this in terms of the twin prime counting function. Let $\pi_2(x)$ denote the number of primes p at most x for which $p + 2$ is prime. Then $\pi_2(x) = Q(f_1, f_2; x)$ and (by [Lemma 2.3.2](#))

$$\pi_2(x) \sim 2C_2 \int_2^x \frac{dt}{(\log t)^2} \sim \frac{2C_2 x}{(\log x)^2};$$

see [Fig. 10](#). This asymptotic estimate for $\pi_2(x)$ was first postulated by Hardy and Littlewood [\[33\]](#).

7.2. Cousin primes, sexy primes, and more

If p and $p + 4$ are prime, then p and $p + 4$ are *cousin primes*. If p and $p + 6$ are prime, then p and $p + 6$ are *sexy primes*. Thankfully the nomenclature appears to expire after this point, although it is still fruitful to consider prime pairs $p, p + k$, in which $k \geq 2$ is even.

Alphonse de Polignac conjectured in 1849 that for each even number k , there are infinitely many prime pairs $p, p + k$. This is now known as *Polignac's conjecture*. The case $k = 2$ of Polignac's conjecture is the twin prime conjecture ([Section 7.1](#)), which remains unproven. In light of the work of Yitang Zhang (1955–) [\[86\]](#) and the Polymath8b Project [\[10\]](#) on bounded gaps between primes, we know that there is an even $k \leq 246$ for which infinitely many prime pairs $p, p + k$ exist. Unfortunately, we do not know a specific value of k for which this occurs.

The Bateman–Horn conjecture goes much further than even Polignac's conjecture. It implies the existence of infinitely many pairs $p, p + k$ of primes for each even k and also supplies asymptotic predictions that are backed up by numerical computations. The following calculations were worked out in [\[28\]](#). Let $f_1(t) = t$ and $f_2(t) = t + k$, and let $f = f_1 f_2$. Then

$$f(t) \equiv 0 \pmod{p} \quad \Longleftrightarrow \quad t(t + k) \equiv 0 \pmod{p},$$

and hence

$$\omega_f(p) = \begin{cases} 1 & \text{if } p|k, \\ 2 & \text{if } p \nmid k. \end{cases}$$

The Bateman–Horn constant is

$$\begin{aligned} C(f_1, f_2; x) &= \prod_p \left(1 - \frac{1}{p}\right)^{-2} \left(1 - \frac{\omega_f(p)}{p}\right) \\ &= \prod_{p|k} \left(1 - \frac{1}{p}\right)^{-1} \prod_{p \nmid k} \left(1 - \frac{1}{p}\right)^{-2} \left(1 - \frac{2}{p}\right) \\ &= \prod_{p|k} \frac{p}{p-1} \prod_{p \nmid k} \frac{p(p-2)}{(p-1)^2}. \end{aligned} \quad (7.2.1)$$

To highlight the dependence on k and match the historically established notation in the twin prime setting (Section 7.1), we denote the preceding constant by $2C_k$; that is,

$$C_k = \prod_{\substack{p|k \\ p \geq 3}} \frac{p}{p-1} \prod_{p \nmid k} \frac{p(p-2)}{(p-1)^2}. \quad (7.2.2)$$

We do not define C_k for odd k ; this would be pointless since for each odd k there is at most one prime pair $p, p+k$. Since $\sum_p 1/p^2$ converges, the infinite product (7.2.2) that defines C_k converges absolutely since

$$\frac{p(p-2)}{(p-1)^2} = 1 - \frac{1}{(p-1)^2}. \quad (7.2.3)$$

Numerical approximations for C_2, C_4, \dots, C_{150} are given in Table 4. If $\pi_k(x)$ denotes the number of primes $p \leq x$ for which $p+k$ is prime, then the Bateman–Horn conjecture predicts that

$$\pi_k(x) \sim 2C_k \int_2^x \frac{dt}{(\log t)^2} \sim \frac{2C_k x}{(\log x)^2}.$$

There are several important observations to make.

- The conjectured rate of growth in π_k depends only upon the constant C_k . Furthermore, C_k depends only upon the primes that divide k .
- In light of (7.2.3), an examination of (7.2.1) reveals that C_k is minimized when k is a power of two, in which case $C_2 = C_4 = C_8 = C_{16} = \dots \approx 0.660162$.
- $\lim_{p \rightarrow \infty} C_{2p} = C_2$. That is, C_k can be made arbitrarily close to the twin primes constant C_2 by letting $k = 2p$, in which p is a sufficiently large prime.
- C_k can be made arbitrarily large by selecting k to have sufficiently many small prime factors. The first factor in (7.2.1) is

$$\prod_{\substack{p|k \\ p \geq 3}} \frac{p}{p-1} = \prod_{\substack{p|k \\ p \geq 3}} \left(1 + \frac{1}{p-1}\right).$$

Table 4Numerical approximations of the constants C_k based upon the first 1,000,000 terms of the product (7.2.1).

k	C_k	k	C_k	k	C_k	k	C_k	k	C_k
2	0.660162	32	0.660162	62	0.682926	92	0.691598	122	0.671351
4	0.660162	34	0.704173	64	0.660162	94	0.674832	124	0.682926
6	1.32032	36	1.32032	66	1.46703	96	1.32032	126	1.58439
8	0.660162	38	0.698995	68	0.704173	98	0.792194	128	0.660162
10	0.880216	40	0.880216	70	1.05626	100	0.880216	130	0.960235
12	1.32032	42	1.58439	72	1.32032	102	1.40835	132	1.46703
14	0.792194	44	0.733513	74	0.679024	104	0.720177	134	0.670318
16	0.660162	46	0.691598	76	0.698995	106	0.673106	136	0.704173
18	1.32032	48	1.32032	78	1.44035	108	1.32032	138	1.3832
20	0.880216	50	0.880216	80	0.880216	110	0.978018	140	1.05626
22	0.733513	52	0.720177	82	0.677089	112	0.792194	142	0.669729
24	1.32032	54	1.32032	84	1.58439	114	1.39799	144	1.32032
26	0.720177	56	0.792194	86	0.676263	116	0.684612	146	0.66946
28	0.792194	58	0.684612	88	0.733513	118	0.671744	148	0.679024
30	1.76043	60	1.76043	90	1.76043	120	1.76043	150	1.76043

Table 5

Values of the counting functions $\pi_k(x)$ at p_{10^n} , the 10^n th prime. The asymptotic predictions of the Bateman–Horn conjecture are identical for π_2 , π_4 , and π_8 (blue), and for π_6 and π_{12} (green). The computations appear to corroborate this.

n	$\pi_2(p_{10^n})$	$\pi_4(p_{10^n})$	$\pi_6(p_{10^n})$	$\pi_8(p_{10^n})$	$\pi_{10}(p_{10^n})$	$\pi_{12}(p_{10^n})$	$\pi_{30}(p_{10^n})$
2	25	27	48	24	33	48	61
3	174	170	343	178	230	340	456
4	1,270	1,264	2,538	1,303	1,682	2,515	3,450
5	10,250	10,214	20,472	10,336	13,653	20,462	27,434
6	86,027	85,834	170,910	85,866	114,394	171,618	228,548
7	738,597	738,718	1,477,321	738,005	984,809	1,477,496	1,970,049
8	6,497,407	6,496,372	12,992,625	6,497,273	8,667,364	12,994,918	17,331,689

If k is the product of the first n primes (that is, k is the n th *primorial* $p_n\#$), then the preceding diverges as $n \rightarrow \infty$.

The patterns predicted by the Bateman–Horn conjecture are evident in Table 5, which provides the numerical values of $\pi_k(10^n)$ for several k and $n = 2, 3, \dots, 8$. For example, Table 4 suggests that primes p for which $p + 30$ is prime should be about

$$\frac{1.76043}{0.660162} \approx 2.6667$$

times more numerous than twin primes. Among the first 10^8 primes, Table 5 gives the proportion

$$\frac{17,331,689}{6,497,407} \approx 2.66748.$$

The agreement is remarkable.

7.3. Sophie Germain primes

A prime number p is a *Sophie Germain prime* if $2p + 1$ is also a prime. Such primes were first introduced and investigated by the legendary French mathematician, physicist, and philosopher Marie-Sophie Germain (1776–1831) in the course of her work on some early cases of Fermat’s Last Theorem; see [74, Sect.5.5.5] for further information.

If p is a Sophie Germain prime, then $2p + 1$ is the corresponding *safe prime*. This terminology reflects the usefulness of such primes in cryptography. Specifically, the famous RSA (Rivest–Shamir–Adleman) cryptosystem is an asymmetric cryptoscheme using a public key to encrypt a message and a private key to decrypt it [46]. The public key is a product of two large prime numbers (for example, a product of two safe primes) and the hardness of a hostile attack is based on the difficulty of factoring such a product. Factorization is especially difficult if the primes in question are of comparable size. Cryptographic applications provide a strong modern motivation for studying such prime numbers, and it is conjectured that there are infinitely many Sophie Germain (and hence safe) primes. This conjecture is currently open, and the largest Sophie Germain prime known has 51 780 digits [44].

The search for Sophie Germain primes can be rephrased in the language of the Bateman–Horn conjecture. Let $f_1(t) = t$ and $f_2(t) = 2t + 1$. Then p is a Sophie Germain prime if and only if $f_1(p)$ and $f_2(p)$ are simultaneously prime. The infinitude of these primes follows from the Bateman–Horn conjecture, which also provides an asymptotic estimate on their counting function. The polynomial

$$f(t) = f_1(t)f_2(t) = t(2t + 1)$$

does not vanish identically modulo any prime since $f(1) \equiv 1 \pmod{2}$ and f has at most two roots modulo any odd prime. Since f vanishes at 0 and $(p - 1)/2$ for every odd prime p , we deduce that

$$\omega_f(p) = \begin{cases} 1 & \text{if } p = 2, \\ 2 & \text{if } p \text{ is odd.} \end{cases}$$

Thus,

$$C(f_1, f_2) = 2 \prod_{p \neq 2} \left(1 - \frac{1}{p}\right)^{-2} \left(1 - \frac{2}{p}\right) = 2 \prod_{p \neq 2} \frac{p(p-2)}{(p-1)^2} \approx 1.32032 \dots$$

Since $\deg f_1 = \deg f_2 = 1$, we obtain the estimate

$$Q(f_1, f_1; x) \sim (1.32032 \dots) \int_2^x \frac{dt}{(\log t)^2}.$$

This is the same asymptotic prediction as in the twin-prime case (Section 7.1).

7.4. Cunningham chains

A sequence p_1, p_2, \dots, p_n of primes is a *Cunningham chain* of the first kind if $p_{i+1} = 2p_i + 1$ for each $1 \leq i \leq n - 1$ and of the second kind if $p_{i+1} = 2p_i - 1$. That is, every p_i in a Cunningham chain of the first kind, except for p_n , is a Sophie Germain

prime and every p_i , except for p_1 , is a safe prime. Cunningham chains are named after the British mathematician Allan Joseph Champneys Cunningham (1842–1928) who first introduced and studied them [14]. Here are a few examples of Cunningham chains of the first kind

$$(2, 5, 11, 23, 47), (3, 7), (89, 179, 359, 719, 1439, 2879),$$

and of the second kind

$$(2, 3, 5), (7, 13), (19, 37, 73).$$

The longest known Cunningham chains have length 19 [2].

The existence of arbitrary long Cunningham chains follows from the first Hardy–Littlewood conjecture, and hence from the Bateman–Horn conjecture. Indeed, let

$$f_1(t) = t, \quad f_2(t) = 2f_1(t) \pm 1, \dots, \quad f_k(t) = 2f_{k-1}(t) \pm 1.$$

We need these all to be prime simultaneously. Bateman–Horn guarantees the existence of infinitely many such k -tuples and even gives an asymptotic estimate on the growth of their number that is analogous to the argument above for Sophie Germain primes. On the other hand, it has been proved that a Cunningham chain of infinite length cannot exist. Indeed, suppose for instance that odd primes p_1, p_2, \dots form a Cunningham chain of the first kind. Then

$$p_{i+1} = 2p_i + 1 = 2(2p_{i-1} + 1) + 1 = \dots = 2^i p_1 + \sum_{j=0}^{i-1} 2^j = 2^i p_1 + (2^i - 1)$$

and hence $p_{i+1} \equiv 2^i - 1 \pmod{p_1}$. On the other hand, Fermat's little theorem implies that

$$2^{p_1-1} - 1 \equiv 0 \pmod{p_1},$$

meaning that p_{p_1} would be divisible by p_1 , and so cannot be prime. This implies that, in fact, a Cunningham chain starting with an odd prime p_1 cannot have more than $p_1 - 1$ terms in it. If $p_1 = 2$, then the same argument can be applied to the chain p_2, p_3, \dots . Further information about Cunningham chains and their use in cryptography can be found in [85].

7.5. Green–Tao theorem

One of the most spectacular results in twenty-first century number theory is the Green–Tao theorem [31], which asserts that the primes contain arbitrarily long arithmetic progressions. That is, given $k \geq 1$ there is a k -term arithmetic progression

$$b, \quad b + a, \quad b + 2a, \dots, \quad b + (k - 1)a$$

of prime numbers. For example, 5, 11, 17, 23, 29 is a 5-term arithmetic progression of primes with $b = 5$ and $a = 6$.

Consider the k linear polynomials

$$f_1(t) = t, \quad f_2(t) = t + a, \dots, \quad f_k(t) = t + (k - 1)a,$$

each of which is obviously irreducible. Let $f = f_1 f_2 \cdots f_k$ denote their product. The congruence $f(t) \equiv 0 \pmod{p}$ is

$$t(t+a)(t+2a) \cdots (t+(k-1)a) \equiv 0 \pmod{p}.$$

Thus,

$$\omega_f(p) = \begin{cases} 1 & \text{if } p|a, \\ \min\{k, p\} & \text{if } p \nmid a. \end{cases}$$

If $p \leq k$ and $p \nmid a$, then f vanishes identically modulo p . Consequently, we require that $p|a$ for all primes $p \leq k$. This suggests that we take $a = p_k\#$, the product of the first k prime numbers. Then

$$\mathcal{Q}(f_1, f_2, \dots, f_k; x) \sim C(f_1, f_2, \dots, f_k) \int_2^x \frac{dt}{(\log t)^k},$$

in which

$$C(f_1, f_2, \dots, f_k) = \prod_{n=1}^k \left(1 - \frac{1}{p_n}\right)^{-k+1} \prod_{n=k+1}^{\infty} \left(1 - \frac{1}{p}\right)^{-k} \left(1 - \frac{k}{p}\right)$$

is a nonzero constant. This yields the following famous result [31, Thm. 1.1].

Theorem 7.5.1 (Green–Tao, 2004). *For each positive integer k , the prime numbers contain infinitely many arithmetic progressions of length k .*

8. Limitations of the Bateman–Horn conjecture

Although we have touted the Bateman–Horn conjecture as “one conjecture to rule them all”, it has its limitations. We briefly discuss a number of topics in number theory that the conjecture does not appear to address.

First of all, the Bateman–Horn conjecture is a statement about the overall distribution of prime numbers. It says little about what happens on small scales. For example, it does not appear to resolve Legendre’s conjecture (for each n there is a prime between n^2 and $(n+1)^2$). Bateman–Horn also does not tell us much about the additive properties of the prime numbers. For instance, it does not seem to imply the Goldbach conjecture (every even number greater than 4 is the sum of two odd prime numbers).

The Bateman–Horn conjecture does an excellent job predicting the asymptotic distribution of primes generated by families of polynomials. However, it does not tell us much about primes generated by non-polynomial functions. For example, it has nothing to say about the number of primes of the form $2^{2^n} + 1$ (Fermat primes) or $2^n - 1$ (Mersenne primes).

The conjecture has little to say about diophantine equations, such as the Fermat equation $x^n + y^n = z^n$ [77] or the Catalan equation $x^n - y^m = 1$ [57]. For example, the Bateman–Horn conjecture appears to have little overlap with the *abc*-conjecture and its applications; see [17, Ch. 11] or [8, Ch. 12] for a detailed overview of the far-reaching *abc*-conjecture and its numerous connections.

The Bateman–Horn conjecture provides asymptotics for counting functions related to primes, but does not bound the size of the error terms. For example, it implies the prime number theorem (Theorem 2.4.1), which asserts that $\pi(x) \sim \text{li}(x)$. However, BH does not tell us about $|\pi(x) - \text{li}(x)|$. On the other hand, Schoenfeld [72] proved that the Riemann hypothesis yields

$$|\pi(x) - \text{li}(x)| < \frac{1}{8\pi} \sqrt{x} \log x, \quad x \geq 2657.$$

Thus, the Riemann hypothesis implies the prime number theorem with a well-controlled error term. Serge Lang says:

I regard it as a major problem to give an estimate for the error term in the Bateman–Horn conjecture similar to the Riemann hypothesis. This could possibly lead to a vast reconsideration of the context for Riemann’s explicit formulas. [52, p. 11].

Number theory is one of the central branches of mathematics and connects with analysis, algebra, combinatorics, and many other fields. It has enjoyed a great number of exciting advances and breakthroughs in recent years, several of which have led to Fields medals and other prestigious awards. It also contains a great number of difficult and deep open problems and conjectures. To a large extent these influence the course of modern mathematics. Some problems, like the Riemann hypothesis, the *abc*-conjecture, the twin prime conjecture, or the Goldbach conjecture are well known and rightfully celebrated by the mathematical community. Others, like the Bateman–Horn conjecture, although of equally great stature, are not as well known. The goal of this paper was to present an overview of this important problem, its connections, and its consequences. It is our hope that we have convinced the reader that the Bateman–Horn conjecture deserves to be ranked among the most pivotal unproven conjectures in the theory of numbers.

Acknowledgments

We thank Keith Conrad for many technical corrections, Harold G. Diamond for permitting us to use two photographs of Paul Bateman, Jeff Lagarias for several suggestions about the exposition, Florian Luca for introducing us to the Bateman–Horn conjecture, and Hugh Montgomery for his remarks about Bateman. We especially thank Roger A. Horn for supplying us with his extensive recollections and several photographs, and for many comments on an initial draft of this paper. Special thanks goes to the anonymous referee for suggesting dozens of improvements to the exposition.

Disclaimer

This paper originally appeared on the arXiv under the title “One conjecture to rule them all: Bateman–Horn” (<https://arxiv.org/abs/1807.08899>).

References

- [1] Bethany Anderson, The Birth of the Computer Age at Illinois, University of Illinois Archives, <https://archives.library.illinois.edu/blog/birth-of-the-computer-age/>.
- [2] D. Augustin, Cunningham Chain records, http://primerecords.dk/Cunningham_Chain_records.htm.
- [3] A. Baker, Linear forms in the logarithms of algebraic numbers. I, II, III, *Mathematika* 13 (1966) 204–216; *Mathematika* 14 (1967) 102–107; *Mathematika* 14 (1967) 220–228, MR 0220680.
- [4] Paul T. Bateman, Roger A. Horn, A heuristic asymptotic formula concerning the distribution of prime numbers, *Math. Comp.* 16 (1962) 363–367, MR 0148632.
- [5] Paul T. Bateman, Roger A. Horn, Primes represented by irreducible polynomials in one variable, in: *Proc. Sympos. Pure Math.*, Vol. VIII, Amer. Math. Soc., Providence, R.I., 1965, pp. 119–132, MR 0176966.
- [6] Paul T. Bateman, Rosemarie M. Stemmler, Waring’s problem for algebraic number fields and primes of the form $(p^r - 1)/(p^d - 1)$, *Illinois J. Math.* 6 (1962) 142–156, MR 0138616.
- [7] N.G.W.H. Beeger, Report on some calculations of prime numbers, *Nieuw Arch. Wiskde.* 20 (1939) 48–50, MR 0000393.
- [8] E. Bombieri, W. Gubler, *Heights in Diophantine Geometry*, in: *New Mathematical Monographs*, vol. 4, Cambridge University Press, Cambridge, 2006, p. 652.
- [9] V.Y. Bouniakowsky, Nouveaux théorèmes relatifs à la distinction des nombres premiers et à la décomposition des entiers en facteurs, *Mém. Acad. Sci. St. Pétersbourg* (6) (1857) 305–329.
- [10] Wouter Castryck, Étienne Fouvry, Gergely Harcos, Emmanuel Kowalski, Philippe Michel, Paul Nelson, Eytan Paldi, János Pintz, Andrew V. Sutherland, Terence Tao, Xiao-Feng Xie, New equidistribution estimates of Zhang type, *Algebra Number Theory* 8 (9) (2014) 2067–2199, MR 3294387.
- [11] James A. Clarkson, On the series of prime reciprocals, *Proc. Amer. Math. Soc.* 17 (1966) 541, MR 0188132.
- [12] Keith Conrad, Irreducible values of polynomials: a non-analogy, in: *Number Fields and Function Fields—Two Parallel Worlds*, in: *Progr. Math.*, vol. 239, Birkhäuser Boston, Boston, MA, 2005, pp. 71–85, MR 2176587.
- [13] Brian Conrad, Keith Conrad, Robert Gross, Prime specialization in genus 0, *Trans. Amer. Math. Soc.* 360 (6) (2008) 2867–2908, MR 2379779.
- [14] A.J.C. Cunningham, On hyper-even numbers and on Fermat’s numbers, *Proc. London Math. Soc.* (2) 5 (1907) 237–274.
- [15] H. Davenport, A. Schinzel, A note on certain arithmetical constants, *Illinois J. Math.* 10 (1966) 181–185.
- [16] Martin Davis, Hilary Putnam, Julia Robinson, The decision problem for exponential diophantine equations, *Ann. of Math.* (2) 74 (1961) 425–436, MR 0133227.
- [17] J.-M. De Koninck, F. Luca, *Analytic Number Theory. Exploring the Anatomy of Integers*, *Graduate Studies in Mathematics*, vol. 134, American Mathematical Society, Providence, RI, 2012, p. 414.
- [18] Kevin Destagnol, Efthymios Sofos, Prime and square-free values of polynomials in moderately many variables, <https://arxiv.org/abs/1801.03082>.
- [19] Harold G. Diamond, Paul T. Bateman, *Celebratio Mathematica*, http://celebratio.org/Bateman_PT/cove-r/323/, 2015.
- [20] Leonard Eugene Dickson, A new extension of Dirichlet’s theorem on prime numbers, *Messenger Math.* 33 (1904) 155–161.
- [21] D.S. Dummit, R.M. Foote, *Abstract Algebra*, third ed., John Wiley & Sons, Inc., 2004, p. 944.
- [22] Leonhard Euler, Lettre CXLIX (Euler à Goldbach), The Euler Archive, <http://eulerarchive.maa.org/correspondence/letters/OO0877.pdf>.
- [23] T. Foo, L. Zhao, On primes represented by cubic polynomials, *Math. Z.* 274 (1–2) (2013) 323–340.
- [24] John Friedlander, Henryk Iwaniec, The polynomial $X^2 + Y^4$ captures its primes, *Ann. of Math.* (2) 148 (3) (1998) 945–1040, MR 1670065.
- [25] G.W. Fung, H.C. Williams, Quadratic polynomials which have a high density of prime values, *Math. Comp.* 55 (191) (1990) 345–353, MR 1023759.
- [26] Stephan Ramon Garcia, Roger A. Horn, *A Second Course in Linear Algebra*, *Cambridge Mathematical Textbooks*, Cambridge University Press, 2017.

- [27] Stephan Ramon Garcia, Elvis Kahoro, Florian Luca, Primitive root bias for twin primes, *Experiment. Math.* 28 (2) (2019) 151–160, <https://doi.org/10.1080/10586458.2017.1360809>.
- [28] Stephan Ramon Garcia, Florian Luca, Timothy Schaaff, Primitive root biases for prime pairs I: Existence and non-totality of biases, *J. Number Theory* 185 (2018) 93–120, MR 3734344.
- [29] Martin Gardner, *Mathematical games: The remarkable lore of the prime numbers*, *Sci. Am.* 210 (1964) 120–128.
- [30] A. Granville, Harald Cramér and the distribution of prime numbers. Harald Cramér Symposium (Stockholm, 1993), *Scand. Actuar. J.* 1 (1995) 12–28.
- [31] Ben Green, Terence Tao, The primes contain arbitrarily long arithmetic progressions, *Ann. of Math.* (2) 167 (2) (2008) 481–547, MR 2415379.
- [32] Richard K. Guy, *Unsolved problems in number theory*, third ed., *Problem Books in Mathematics*, Springer-Verlag, New York, 2004, p. xviii+437, MR 2076335.
- [33] G.H. Hardy, J.E. Littlewood, Some problems of ‘partitio numerorum’; III: On the expression of a number as a sum of primes, *Acta Math.* 114 (3) (1923) 215–273, MR 1555183.
- [34] G.H. Hardy, E.M. Wright, *An introduction to the theory of numbers*, sixth ed., Oxford University Press, Oxford, 2008, p. xxii+621, Revised by D.R. Heath-Brown and J. H. Silverman, With a foreword by Andrew Wiles, MR 2445243.
- [35] D.R. Heath-Brown, Primes represented by $x^3 + 2y^3$, *Acta Math.* 186 (1) (2001) 1–84.
- [36] Kurt Heegner, Diophantische Analysis und Modulfunktionen, *Math. Z.* 56 (1952) 227–253, MR 0053135.
- [37] D. Hensley, I. Richards, On the incompatibility of two conjectures concerning primes, in: *Analytic Number Theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972)*, Amer. Math. Soc., Providence, R.I, 1973, pp. 123–127.
- [38] D. Hensley, I. Richards, Primes in intervals, *Acta Arith.* 25 (1973/74) 375–391.
- [39] Roger A. Horn, personal communication.
- [40] Alfred Horn, Eigenvalues of sums of Hermitian matrices, *Pacific J. Math.* 12 (1962) 225–241, MR 0140521.
- [41] Roger A. Horn, Charles R. Johnson, *Topics in matrix analysis*, Cambridge University Press, Cambridge, 1994, p. viii+607, Corrected reprint of the 1991 original, MR 1288752 (95c:15001).
- [42] Roger A. Horn, Charles R. Johnson, *Matrix analysis*, second ed., Cambridge University Press, Cambridge, 2013, p. xviii+643, MR 2978290.
- [43] Michael J. Jacobson Jr., Hugh C. Williams, New quadratic polynomials with high densities of prime values, *Math. Comp.* 72 (241) (2003) 499–519, MR 1933834.
- [44] Jarai, et al., The Prime Database: 1372119412921952171960-1, <http://primes.utm.edu/primes/page.php?id=77705>.
- [45] James P. Jones, Daihachiro Sato, Hideo Wada, Douglas Wiens, Diophantine representation of the set of prime numbers, *Amer. Math. Monthly* 83 (6) (1976) 449–464, MR 0414514.
- [46] J. Katz, Y. Lindell, *Introduction to Modern Cryptography*, second ed., Chapman and Hall/CRC, 2014, p. 603.
- [47] Alexander A. Klyachko, Stable bundles, representation theory and Hermitian operators, *Sel. Math. (N.S.)* 4 (3) (1998) 419–445, MR 1654578.
- [48] Dominic Klyve, Explicit bounds on twin primes and Brun’s Constant, ProQuest LLC, Ann Arbor, MI, 2007, p. 226, Thesis (Ph.D.)–Dartmouth College, MR 2712414.
- [49] Allen Knutson, Terence Tao, The honeycomb model of $GL_n(\mathbb{C})$ tensor products. i. proof of the saturation conjecture, *J. Amer. Math. Soc.* 12 (4) (1999) 1055–1090, MR 1671451.
- [50] Edmund Landau, Neuer Beweis des Primzahlsatzes und Beweis des Primidealsatzes, *Math. Ann.* 56 (4) (1903) 645–670, MR 1511191.
- [51] S. Lang, La conjecture de Bateman-Horn, *Gaz. Math.* 67 (1996) 82–84.
- [52] Serge Lang, *Math talks for undergraduates*, Springer-Verlag, New York, 1999, p. x+121, MR 1697559.
- [53] Philippe Lebacque, Generalized Mertens and Brauer-Siegel theorems, *Acta Arith.* 130 (4) (2007) 333–350.
- [54] Daniel A. Marcus, *Number fields*, Springer-Verlag, New York-Heidelberg, 1977, p. viii+279, Universitext, MR 0457396.

- [55] Ju. V. Matijasevič, The diophantineness of enumerable sets, Dokl. Akad. Nauk SSSR 191 (1970) 279–282, MR [0258744](#).
- [56] James Maynard, Small gaps between primes, Ann. of Math. (2) 181 (1) (2015) 383–413, MR [3272929](#).
- [57] Preda Mihailescu, Primary cyclotomic units and a proof of catalan’s conjecture, J. Reine Angew. Math. 572 (2004) 167–195, MR [2076124](#).
- [58] Hugh L. Montgomery, personal communication.
- [59] [H.L. Montgomery, R.C. Vaughan, Multiplicative Number Theory I: Classical Theory, Reprint, Cambridge Studies in Advanced Mathematics \(Book 97\), 2012, p. 572.](#)
- [60] P. Moree, Approximation of singular series and automata, Manuscripta Math. 101 (2000) 385–399.
- [61] B. Z. Moroz, On the representation of primes by polynomials: a survey of some recent results, Preprints of the Max-Planck-Institut für Mathematik, Bonn 21 (2008).
- [62] Ivan Niven, Herbert S. Zuckerman, Hugh L. Montgomery, An introduction to the theory of numbers, Fifth, John Wiley & Sons, Inc., New York, 1991, p. xiv+529, MR [1083765](#).
- [63] [Bruce P. Palka, Editor’s endnotes, Amer. Math. Monthly 111 \(5\) \(2004\) 456–460.](#)
- [64] T. Paul, Bateman—biography, Int. J. Number Theory 11 (5) (2015) xv–xviii, MR [3376239](#).
- [65] Paul Pollack, Not Always Buried Deep: A Second Course in Elementary Number Theory, American Mathematical Society, Providence, RI, 2009, p. xvi+303, MR [2555430](#) (2010i:11003).
- [66] G. Pólya, I.J. Schoenberg, Remarks on de la Vallée Poussin means and convex conformal maps of the circle, Pacific J. Math. 8 (1958) 295–334, MR [0100753](#).
- [67] Georg Rabinowitsch, Eindeutigkeit der Zerlegung in Primzahl faktoren in quadratischen Zahlkörpern, J. Reine Angew. Math. 142 (1913) 153–164, MR [1580865](#).
- [68] Ian Richards, On the incompatibility of two conjectures concerning primes; a discussion of the use of computers in attacking a theoretical problem, Bull. Amer. Math. Soc. 80 (1974) 419–438, MR [0337832](#).
- [69] [Michael Rosen, A generalization of Mertens’ theorem, J. Ramanujan Math. Soc. 14 \(1\) \(1999\) 1–19.](#)
- [70] St. Ruscheweyh, T. Sheil-Small, Hadamard products of Schlicht functions and the Pólya-Schoenberg conjecture, Comment. Math. Helv. 48 (1973) 119–135, MR [0328051](#).
- [71] [A. Schinzel, W. Sierpiński, Sur certaines hypothèses concernant les nombres premiers, Acta Arith. 4 \(1958\) 185–208; erratum 5 \(1958\) 259, MR 0106202.](#)
- [72] Lowell Schoenfeld, Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$. II, Math. Comp. 30 (134) (1976) 337–360, MR [0457374](#).
- [73] Atle Selberg, An elementary proof of the prime-number theorem for arithmetic progressions, Canad. J. Math. 2 (1950) 66–78, MR [0033306](#).
- [74] [V. Shoup, A Computational Introduction to Number Theory and Algebra, second ed., Cambridge University Press, 2009, p. 600.](#)
- [75] H.M. Stark, A complete determination of the complex quadratic fields of class-number one, Michigan Math. J. 14 (1967) 1–27, MR [0222050](#).
- [76] H.M. Stark, On the “gap” in a theorem of heegner, J. Number Theory 1 (1969) 16–27, MR [0241384](#).
- [77] Ian Stewart, David Tall, Algebraic number theory and Fermat’s last theorem, Fourth, CRC Press, Boca Raton, FL, 2016, p. xix+322, MR [3443702](#).
- [78] Terence Tao, 254A, Supplement 4: Probabilistic models and heuristics for the primes (optional), <http://terrytao.wordpress.com/tag/cramers-random-model/>.
- [79] Terence Tao, Mertens’ theorems, <https://terrytao.wordpress.com/2013/12/11/mertens-theorems/>.
- [80] Terence Tao, The prime number theorem in arithmetic progressions, and dueling conspiracies, <https://terrytao.wordpress.com/2009/09/24/the-prime-number-theorem-in-arithmetic-progressions-and-dueling-conspiracies/>.
- [81] Gérald Tenenbaum, Introduction to analytic and probabilistic number theory, third ed., Graduate Studies in Mathematics, vol. 163, American Mathematical Society, Providence, RI, 2015, p. xxiv+629, Translated from the 2008 French edition by Patrick D. F. Ion, MR [3363366](#).
- [82] Charles Vanden Eynden, Proofs that $\sum 1/p$ diverges, Amer. Math. Monthly 87 (5) (1980) 394–397, MR [567727](#).
- [83] Martin H. Weik, ILLIAC, A Third Survey of Domestic Electronic Digital Computing Systems, <http://www.ed-thelen.org/comp-hist/BRL61-ibm7070.html#ILLIAC>, 1961.

- [84] Herbert S. Wilf, Calculations relating to a conjecture of Pólya and Schoenberg, *Math. Comp.* 17 (1963) 200–201, MR [0160892](#).
- [85] A. Young, M. Yung, Finding length-3 positive cunningham chains and their cryptographic significance, in: *Algorithmic Number Theory: Third International Symposium, ANTS-III*, Springer, New York, 1998, pp. 289–298.
- [86] Yitang Zhang, Bounded gaps between primes, *Ann. of Math.* (2) 179 (3) (2014) 1121–1174, MR [3171761](#).