The Bateman–Horn Conjecture and its Applications

Alexandre Zvonkine

Joint work with **Gareth Jones** (University of Southampton)
with computational assistance from **Jean Bétréma**

Group de travail "Combinatoire et Applications"
Bordeaux, 16 May, 2022

It [the Bateman–Horn conjecture] implies many known results, such as the prime number theorem and the Green–Tao theorem, along with many famous 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.

From the paper "The Bateman–Horn conjecture: Heuristic, history, and applications", by S. L. Aletheia-Zomlefer, L. Fukshansky and S. R. Garcia, **2020**.

The conjecture belongs to the domain of Number theory.

Neither Jones nor I had ever heard of it before 2020. Our way to this conjecture went through the classification of permutation groups **of prime degree**.

Just in case, if there are young students in the audience:

degree — the number of points on which the group acts;
order — the number of elements in the group.

Symmetric group S_n:

degree $= n$,
order $= n!$.

Our interest is in the degree.

The groups of prime degree are few. . .

degree	2	3	4	5	6	7	8	9	10	11	12	13	14	15
#(groups)	1	2	5	5	16	7	50	34	45	8	301	9	63	104

degree	16	17	18	19	20	21	22	23	24	25
#(groups)	1954	10	983	8	1117	164	59	7	25 000	211

degree	26	27	28	29	30	31	32	33	34	35
#(groups)	96	2392	1854	8	5712	12	2 801 324	162	115	407

degree	36	37	38	39	40	41	42	43	44
#(groups)	121 279	11	76	306	315 842	10	9491	10	2113

degree	45	46	47	48
#(groups)	10 923	56	6	195 826 352

The last result, for the degree 48, is dated 2020. Its author, Derek Holt, carried out the computation for two years.

It is tempting to classify the groups of prime degree.

This work was started by Lagrange (1770) in terms of polynomials, continued by Galois (1830), then by Burnside (1906) and many others . . .

Finally, today, two and a half centuries after Lagrange and after the proof of the Mega-theorem of classification of the finite simple groups, the work may be considered as *almost* finished.

Why "almost"? — In fact, there still exists a fundamental question with an unknown answer. We will discuss it in a few minutes.

Remark. When I say that something is *unknown* I usually mean that there is, as yet, no proof. More often than not the true answer is "obvious" due to some indirect arguments and experimental results.

So. . .

The classification of permutation groups of prime degree goes as follows.

Case 1: Symmetric groups S_p and alternating groups A_p for p prime.

Nothing to add.

Let $\mathsf{AGL}_1(p)$ be the one-dimensional affine group over $\mathbb{Z}_p$:

$$\mathsf{AGL}_1(p) = \{t \mapsto at + b \mid a, b \in \mathbb{Z}_p, a \neq 0\} = \mathsf{C}_p \rtimes \mathsf{C}_{p-1}.$$

Then

Case 2: The groups G such that $\mathsf{C}_p \leq G \leq \mathsf{AGL}_1(p)$:

$$G = \mathsf{C}_p \rtimes \mathsf{C}_d$$

where d is a divisor of $p - 1$, so that $\mathsf{C}_d \leq \mathsf{C}_{p-1}$.

Galois proved that these are the only solvable groups of prime degree.

Sporadic cases

The projective groups $\mathrm{PSL}_2(p)$ act *naturally* on $p+1$ points of the projective line $\mathbb{Z}_p \cup \{\infty\}$.

But there are three of them (also known to Galois) which can also act on p points:

Case 3a: The groups $\mathrm{PSL}_2(5)$, $\mathrm{PSL}_2(7)$ and $\mathrm{PSL}_2(11)$ acting on 5, 7 and 11 points, respectively.

Beside these three groups, there are two more groups:

Case 3b: Mathieu groups M_{11} and M_{23} acting of 11 and 23 points, respectively.

The most interesting (and difficult) case

Case 4: Let p be a prime, and $q = p^e$ be a prime power, $e \geq 1$. Let $\mathbb{F}_q$ be the finite field with q elements. Let $n \geq 2$. Then the projective groups G such that

$$\mathsf{PSL}_n(q) \leq G \leq \mathsf{P\Gamma L}_n(q)$$

act on

$$m = \frac{q^n - 1}{q - 1} = 1 + q + q^2 + \cdots + q^{n-1}$$

points of the projective space of dimension $n - 1$.

If it so happens that m is prime then the degree of G is prime.

We call such numbers $\boxed{m}$ **projective primes**.

Of course, for a given prime m it is easy to verify if it can be represented as

$$m = 1 + q + q^2 + \cdots + q^{n-1}$$

with $q = p^e$ a prime power. Still, there is a largely open and quite fundamental question:

Open question: Are there infinitely many projective primes?

Equivalently, are there infinitely many projective groups of prime degree?

The same question may be formulated as follows. Let $f \in \mathbb{Z}[t]$ be the following polynomial:

$$f(t) = 1 + t^e + \cdots + t^{(n-1)e}.$$

Do there exist infinitely many $t \in \mathbb{N}$ such that both t and $f(t)$ are prime?

In this way we arrive at the question of

prime values of polynomials.

If you ask group theorists they will say that the classification of the groups of prime degree is already accomplished. This means that they have done their part of work. What remains is a job of Number Theory.

A few examples

1. Fermat primes: $q = 2^{2^k}$ $(k = 0, 1, 2, 3, 4)$, $n = 2$

$2^1 + 1 = 3, \quad 2^2 + 1 = 5, \quad 2^4 + 1 = 17, \quad 2^8 + 1 = 257, \quad 2^{16} + 1 = 65\,537.$

Conjecture: There are no more Fermat primes.

2. Mersenne primes: $q = 2$, various n (51 examples are known)

$2^2-1 = 3,\ 2^3-1 = 7,\ 2^5-1 = 31,\ 2^7-1 = 127,\ 2^{13}-1 = 8191,\ \ldots$

$$2^{82\,589\,933} - 1 \quad (24\,862\,048 \text{ digits}).$$

Conjecture: There are infinitely many Mersenne primes.

3. One more example: $q = 2^{59}$, $n = 59$

$$1 + 2^{59} + 2^{118} + \cdots + 2^{59\cdot 58} = \text{ a prime with 1031 digits.}$$

Primality verification

In order to carry out experiments we need to undertake a primality verification on a large scale. What is the "practical complexity" of this task?

December 2009: a 232-digit number was successfully factored into a product of two 116-digit numbers. This result was the outcome of two years of work by a team of 13 researchers, and was crowned with a \$50 000 prize. The computation "time" is 4400 GHz-years.

February 2020, the current record: a 250-digit number is factored.

A 260-digit number is a current challenge: it still waits for its turn to be factored.

However, the verification of the fact that this 260-digit number is composite takes < 0.0005 seconds on my laptop.
(I don't know the exact time: Maple gives the CPU time within the accuracy 0.001 seconds, and it outputs 0.)

The hero is the **Rabin–Miller algorithm**.

```
> N
      := 221128255295296664352810852550262309276120895024700153944 1\
     37483191288229414020019865127297265697465990859003300314000 51\
     17074220456085927635795375718595429883895870922923849100670 30\
     34124620545784566413664540684214361293017694020846391065875 91\
     47942514351444581 99:
> time(isprime(N));
                                    0.
> isprime(N);
                                  false
>
```

```
> M := (1201^1999 - 1)/1200 :
> number_of_digits := ceil(evalf(log10(M)));
                          number_of_digits := 6153
> time(isprime(M));
                               13.314
> isprime(M);
                                true
>
```

One more example: **the Goormaghtigh conjecture** (1917): the Diophantine equation

$$\frac{x^n-1}{x-1}=\frac{y^k-1}{y-1},\quad n,k\geq 3,\quad n\neq k$$

has only two solutions:

$$1+2+4+8+16=1+5+25=31$$

and

$$1+2+4+\cdots+2^{12}=1+90+90^2=8191.$$

Thus, 8191 is a projective prime for $(q,n)=(2,13)$; but 90 is not a prime power.

Hence, if the conjecture is true then there is only one "doubly projective" prime, namely, $\boxed{31}$. There are two different projective groups acting on 31 points: $\mathrm{PSL}_3(5)$ and $\mathrm{PSL}_5(2)$, and there are no other such examples. **Verified by Bétréma up to** 10^{18}.

I have mixed feelings concerning this conjecture: for about 20 years I thought that it was **my** conjecture.

Well... All the above was a starting point of our interest in prime values of polynomials. Here is a pioneering and really important but largely unknown conjecture.

Let $f(t) \in \mathbb{Z}[t]$ be a polynomial with integer coefficients. We would like it to have infinitely many prime values. There are three obvious necessary conditions:

1. The leading coefficient of f is positive.
2. f is irreducible over $\mathbb{Z}$.
3. The values of f do not have a common divisor > 1. (Another formulation: $f(t)$ is not identically zero modulo any prime.)

Examples that do not satisfy the 3rd condition:

- All the values of $f(t) = t^2 + t + 2 = t(t+1) + 2$ are even.

- All the values of $f(t) = t^9 - t^3 + 2520$ are divisible by 504.

Bunyakovsky conjecture (1857): The above three conditions are also sufficient. A polynomial satisfying conditions 1, 2, 3 takes prime values infinitely often.

The conjecture remains largely open. Even for $f(t) = t^2 + t + 1$ or $f(t) = t^2 + 1$ there is no proof in view.

Besides, there are 745 582 values of $t \leq 10^7$ such that $t^2 + t + 1$ is prime, and 456 362 values such that $t^2 + 1$ is prime.

However, the polynomial $t^{12} + 488\,669$ has only three prime values for $t \leq 10^6$, the least one being for $t = 616\,980$. Fortunately, Bunyakovsky did not know this example.

Bunyakovsky was a student of Cauchy.

In Russia, he is known for the *Cauchy–Bunyakovsky inequality* which, in the Western tradition, is called after Cauchy–Schwarz.

Schwarz proved this inequality in 1888, Bunyakovsky in 1859, thus 29 years earlier.

The only case of the Bunyakovsky conjecture which is proved is for polynomials of degree 1:

Theorem (Dirichlet, 1837): Let $a, b \in \mathbb{N}$ be coprime. Then the arithmetic progression $at + b$, $t \in \mathbb{N}$ contains infinitely many primes.

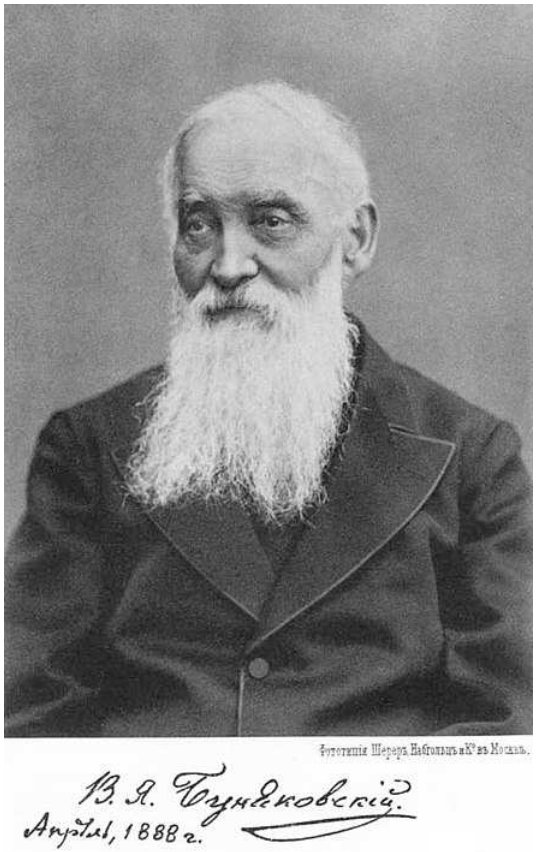
Example: There are infinitely many primes which terminate by $777\ldots7$ (17 times).

Proof: Take $a = 10^{17}$, $b = 777\ldots7$.

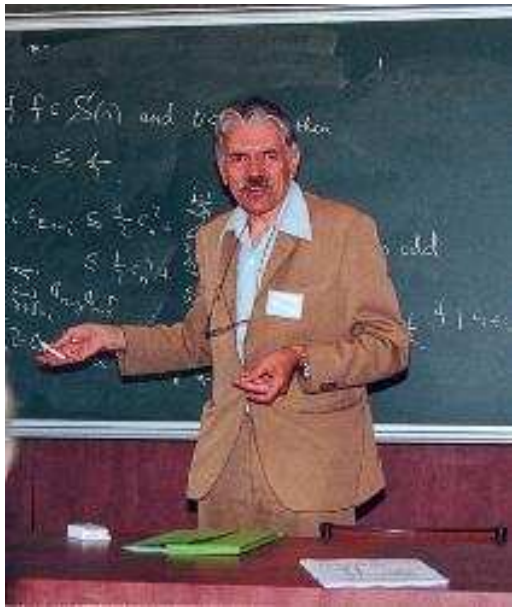
There followed a series of generalizations and special cases of the Bunyakovsky conjecture:

- Dickson's conjecture (1904)
- The Euler–Landau conjecture (1752, 1912)
- The Sophie Germain conjecture
- **Hardy and Littlewood (1923)**
- Schinzel's hypothesis H (1960)
- ...
- **Bateman and Horn (1962)**
- Weixiong Li (2019): improved version of the Bateman–Horn

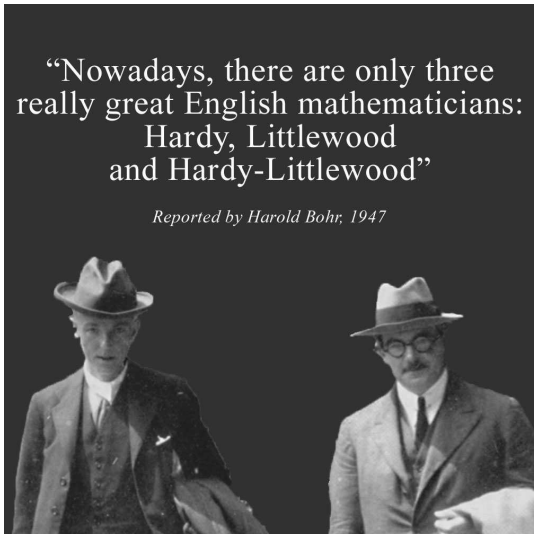
In what follows we will always use the version of the conjecture given by Li.



Viktor Yakovlevich Bunyakovsky (1804–1889)

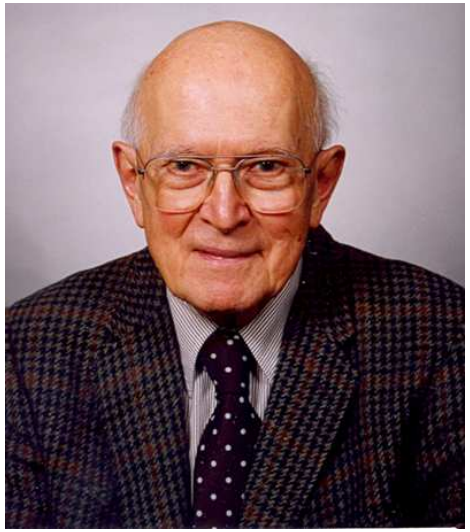


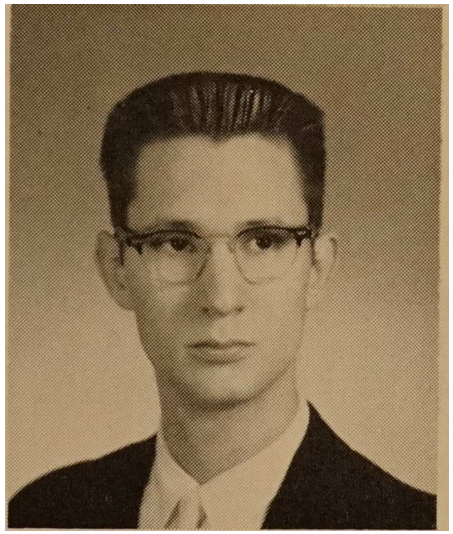
Left: Leonard Eugene Dickson (1874–1954).
Right: Andrzej Schinzel (born 1937) in Bordeaux at the conference in honour of Michel Mendès France (September 2000).



Left: Godfrey Harold Hardy (1877–1947)

Center: John Edensor Littlewood (1885–1977)





Paul T. Bateman (1919–2012) and Roger A. Horn (born 1942)

Bateman at the time (1962) was a renowned specialist in number theory, and Horn was an undergraduate student who was able to write programs for the ILLIAC computer. Later he became a specialist in matrix analysis.

Notice that there was no Maple at their disposal and no other mathematical packages: everything had to be programmed from scratch.

The Bateman–Horn conjecture (1962)

Let $f_1, f_2, \ldots, f_k \in \mathbb{Z}[t]$ be polynomials with integer coefficients which satisfy the following conditions (similar to Bunyakovsky):

1. All f_i are indecomposable over $\mathbb{Z}$ (and hence coprime).

2. The leading coefficients of all of them are positive.

3. The product $f = f_1 f_2 \ldots f_k$ is not identically zero modulo any prime.

Let $Q(x)$ be the number of $t \leq x$ such that $f_i(t)$ **are ALL prime**.

Then $Q(x)$ is asymptotically equivalent to the following expression (see the next pages)...

Recall that $f(t)$ is the product $f = f_1 f_2 \dots f_k$, and $Q(x)$ is the number of $t \leq x$ such that all $f_i(t)$ are prime. Then

$$\boxed{Q(x) \sim C(f) \int_a^x \frac{dt}{\prod_{i=1}^{k} \ln(f_i(t))}}$$

Here $C(f)$ is a constant factor to which I will return in a minute, and the lower limit of the integration, denoted here by a, should be adapted in such a way as to avoid the logarithmic singularities at $f_i(t) = 1$. Quite often one takes $a = 2$.

From the computational point of view to compute the integral is a matter of seconds while the computation of the constant $C(f)$ is a huge task and the subject of several publications.

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

where the product is taken over all primes p, and $\omega_f(p)$ is the number of solutions of $f(t) = 0 \mod p$.

Thus, $C(f)$ is an infinite product. Its computation may present serious difficulties. In particular, it may be difficult to find $\omega_f(p)$.

A bit of interpretation:

1. $\left(1 - \frac{1}{p}\right)^k$ is the "probability" that a "randomly chosen" k-tuple of integers contains no integer divisible by p.

2. $1 - \frac{\omega_f(p)}{p}$ is the probability that $f(t)$ is not divisible by p. Since the function f is the product of f_i, this is the probability that no one of $f_i(t)$ is divisible by p.

Lemma: The above product converges to a constant $C > 0$. (The convergence is not absolute!)

A detailed proof is published only in 2020 and takes seven pages. In the original paper by Bateman and Horn there are only a few hints.

Since the integral $\int_2^x \frac{dt}{\ln(t)^k}$ diverges for every $k \geq 1$ when $x \to \infty$ we have the following corollary:

Corollary (Schinzel's hypothesis): The polynomials $f_1, \ldots, f_k$ take prime values *simultaneously* infinitely many times.

The remaining part of the talk will mainly consist of

Examples

Example 1. Let us consider the simplest possible example: $k = 1$, so we have only one polynomial, and this polynomial is $f(t) = t$.

Then

$$Q(x) = \#(t \leq x) \text{ such that } t \text{ is prime.}$$

The equation $t = 0$ always has a unique solution modulo any p. Therefore

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

Conclusion: $Q(x) \sim \int_2^x \frac{dt}{\ln(t)} \sim \frac{x}{\ln(x)}$.

We recognize the Prime Number Theorem by Hadamard and de la Vallée Poussin (1896).

The estimations $\int_2^x \frac{dt}{\ln(t)}$ and $\frac{x}{\ln(x)}$ are asymptotically equivalent **BUT**...

The exact number of primes has been computed up to $x = 10^{28}$:

$$\pi(10^{28}) = 157\,589\,269\,275\,973\,410\,412\,739\,598.$$

The estimate by Hadamard and de la Vallée Poussin gives

$$\frac{10^{28}}{28 \cdot \ln 10} = 155\,105\,172\,108\,304\,224\,161\,117\,471.042$$

with the relative error $-1.576\,\%$.
The Bateman–Horn estimate gives

$$\int_2^{10^{28}} \frac{dt}{\ln t} = 157\,589\,269\,275\,974\,838\,158\,399\,970.696$$

with the relative error $0.000000000000906\,\% \approx 10^{-12}\,\%$.

The estimation using the integral was of course known both to Hadamard and de la Vallée Poussin and also to Dirichlet, but the first to conjecture it was Gauss.

My distinguished friend:

Your remarks concerning the frequency of primes were of interest to me in more ways than one. You have reminded me of my own endeavors in this field which I began in the very distant past, in 1792 or 1793, after I had acquired the Lambert supplements to the logarithmic tables. Even before I had begun my more detailed investigations into higher arithmetic, one of my first projects was to turn my attention to the decreasing frequency of primes, to which end I counted the primes in several chiliads and recorded the results on the attached white pages. I soon recognized that behind all of its fluctuations, this frequency is on the average inversely proportional to the logarithm, so that the number of primes below a given bound n is approximately equal to

$$\int \frac{dn}{\log n},$$

where the logarithm is understood to be hyperbolic.

(From a letter of Gauss to his former student,
the astronomer Johann Franz Encke, 1849.)

Twin primes

Let us take $f_1 = t$ and $f_2 = t + 2$. We want them to be simultaneously prime.

The equation $t(t+2) = 0 \bmod p$ has one solution for $p = 2$ and two solutions for all other primes p. Thus we have

$$\begin{aligned} C(f) &= \prod_p \left(1 - \frac{1}{p}\right)^{-2} \left(1 - \frac{\omega_f(p)}{p}\right) \\ &= 2 \prod_{p \geq 3} \left(1 - \frac{1}{p}\right)^{-2} \left(1 - \frac{2}{p}\right). \end{aligned}$$

This time, the constant is known with a high precision:

$$C(f) \;=\; 1.32032363169373914786\ldots$$

The number of pairs of twin primes is known up to 10^{18}: it is 808 675 888 577 436, while

$$C(f)\cdot\int_2^{10^{18}}\frac{dt}{\ln(t)^2} = 808\,675\,901\,493\,606.3.$$

The relative error is 0.0000016%.

To me, this is a kind of a paradox:

- The infinitude of the twin primes is a conjecture, widely open.

- In spite of that, we can predict their number, up to a given limit, with an incredibly high precision.

One may also invent his or her exercises. For example:

> How many neighboring twin pairs are there, like $(5, 7)$ and $(11, 13)$, or $(9431, 9433)$ and $(9437, 9439)$. It suffices to take four polynomials: $t, t + 2, t + 6, t + 8$.

As we can easily imagine, there are many applications of the Bateman–Horn conjecture to Number Theory. Their incomplete list looks as follows:

- The Sophie Germain primes: primes p such that $2p + 1$ is also prime;
- The Cunningham chains: sequences of primes $p_1, p_2, \ldots, p_k$ such that $p_{i+1} = 2p_i + 1$ (the longest know chain is of length 17);
- The Euler–Landau conjecture: primes of the form $t^2 + 1$;
- The Dirichlet theorem and its refinement (numbers of primes in arithmetic progressions);
- The Green–Tao theorem (2004): for any $k \in \mathbb{N}$, prime numbers contain infinitely many arithmetic progressions of length k;
- and certainly many others.

An application to block designs

A **2-block design** with parameters v, k, λ is a set V of size v of elements called *points* and a collection $\mathcal{B}$ of subsets of V, each of size k, called *blocks*, such that each pair of points lies in exactly λ blocks.

The 2 at the name "2-block design" corresponds to the *pairs* of points: in more general case one considers l-element subsets.

Example: Projective plane of the field $\mathbb{F}_q$: $v = 1 + q + q^2$, blocks are lines, $k = 1 + q$, and each pair of points lies on exactly one line (thus, $\lambda = 1$).

There also exist many other constructions.

An construction from a paper by Amara, Devillers and Praeger: block designs with large automorphism groups (some upper bounds are attained).

For their construction, they need the following: let $f_{n,r}$ be the polynomial

$$f_{n,r}(t) = 8n^2t^2 + 2n(2r-1)t + \left(\frac{r(r-1)}{2} - n\right)$$

with

$$r < 4n \quad \text{and} \quad \frac{r(r-1)}{2} \equiv n+1 \bmod (2n).$$

The construction needs $f_{n,r}(t)$ to be a prime power. The Bateman and Horn conjecture permits to treat the case of prime values.

Let us consider an example: $f_{2,3}(t) = 32t^2 + 20t + 1$.

The polynomial is of degree 2: there are no *theorems* which would imply whatsoever. The Bunyakovsky conjecture implies that there are infinitely many prime values. What do Bateman and Horn say?

In order to compute the constant $C(f)$ in front of the integral, we need to know $\omega_f(p)$ which is the number of solutions of the equation $f(t) = 0 \mod (p)$.

- $p = 2$: $\quad 32t^2 + 20t + 1 = 0 \;\Leftrightarrow\; 1 = 0$: $\quad$ no solutions.

- $p \neq 2$: multiply $f(t)$ by 8:

  $$256t^2 + 80t + 8 = 256t^2 + 80t + 25 - 17 = (16t + 5)^2 - 17,$$

  so finally we have

  $$(16t + 5)^2 = 17 \mod (p).$$

- $p = 17$: unique solution: $16t + 5 = 0$, hence $t = 5$.

- $p \neq 2, 17$: the equality $(16t + 5)^2 = 17 \mod p$ means that 17 is a *quadratic residue* modulo p.

To verify, for each p, if 17 is a quadratic residue, is a dull and time-consuming occupation.

The magic wand: The Gauss law of quadratic reciprocity!

Quadratic residues

We consider remainders modulo some number. Quadratic residues are those which are squares (except zero).

Modulo a composite number they do not have much interest. For example, $1^2 = 5^2 = 7^2 = 11^2 = 1 \mod (12)$.

Modulo a prime p there are exactly $(p - 1)/2$ quadratic residues and the same number of quadratic non-residues. To find out if a given $y \in \mathbb{Z}_p$ is a quadratic residue or not is a difficult question.

Notation: the **Legendre symbol**:

$$\left(\frac{m}{p}\right) = \begin{cases} 0 & \text{if } m \equiv 0 \bmod p, \\ 1 & \text{if } m \text{ is a quadratic residue mod } p, \\ -1 & \text{otherwise.} \end{cases}$$

The Legendre symbol is multiplicative:

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right) \cdot \left(\frac{n}{p}\right).$$

Also, the following equalities are often useful:

$$\left(\frac{2}{p}\right) = 1 \text{ or } -1 \text{ as } p \equiv \pm 1 \text{ or } \pm 3 \bmod (8)$$

and

$$\left(\frac{-1}{p}\right) = 1 \text{ or } -1 \text{ as } p \equiv 1 \text{ or } -1 \bmod (4).$$

The Quadratic Reciprocity Law

Theorem: Let $p, q \neq 2$ be two primes. Then

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \quad \text{if one or both } p, q \equiv 1 \bmod (4),$$
$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right) \quad \text{if both } p, q \equiv -1 \bmod (4).$$

Gauss was so impressed by this property that he published six (!) different proofs of this result, and two more proofs were found in his papers after his death.

In our case, $17 \equiv 1 \bmod (4)$. Therefore, instead of verifying if 17 is a quadratic residue modulo p, we may verify if p is a quadratic residue modulo 17.

Quadratic residues modulo 17 are: $1, 2, 4, 8, 9, 13, 15, 16$, or, if you prefer, $\pm 1, \pm 2, \pm 4, \pm 8$.

To conclude: for $f(t) = 32t^2 + 20t + 1$ we have the number $\omega_f(p)$ of solutions of $f(t) = 0$ in $\mathbb{Z}_p$ equal to the following:

$$\omega_f(p) = \begin{cases} 0 & p = 2, \\ 1 & p = 17, \\ 2 & p \equiv 1, 2, 4, 8, 9, 13, 15, 16 \text{ mod } (17), p \neq 2, \\ 0 & \text{otherwise.} \end{cases}$$

Computing the product below over $p \leq 10^8$ we get

$$C(f) = \prod_p \left(1 - \frac{1}{p}\right)^{-1} \left(1 - \frac{\omega_f(p)}{p}\right) = 4.721240276.$$

Finally, the estimation of the number of prime values of $f(t)$ for $t \leq x$ is

$$E(x) = C(f) \int_2^x \frac{dt}{\ln(f(t))}.$$

The results are summarized in the table below:

segment	#(prime $f(t)$)	$E(x)$	relative error
$t \leq 10^3$	326	314.49	-3.53%
$t \leq 10^4$	2421	2404.86	-0.67%
$t \leq 10^5$	19 394	19 438.26	0.23%
$t \leq 10^6$	162 877	163 182.75	0.19%
$t \leq 10^7$	1 405 448	1 406 630.14	0.084%
$t \leq 10^8$	12 357 532	12 362 961.06	0.044%

Beautiful !

At the same time, the above considerations demonstrate that the computation of the constant factor $C(f)$ may be an intricate matter. It depends on the nature of f.

For example: what to do with cubic polynomials?

(There exists a "cubic reciprocity law" but it is much more difficult to apply. And a cubic equation cannot, in general, be reduced to the form $(at + b)^3 = c$.)

Back to groups and "projective primes"

Reminder: a projective prime is a prime m of the form

$$m = 1 + q + q^2 + \cdots + q^{n-1}$$

where q is a prime power: $q = p^e$, $e \geq 1$. The exponent n must itself be prime, otherwise the polynomial $1 + t + \cdots + t^{n-1}$ would be reducible, like $1 + t + t^2 + t^3 + t^4 + t^5 = (1 + t)(1 + t^2 + t^4)$.

Jean Bétréma, using the program Julia, computed all projective primes $m \leq 10^{18}$. There are 1 974 311 of them.

Among them, there are:

- 1 974 010 numbers of the form $1 + p + p^2$ with p prime, and
- 301 projective primes of other types.

Taking $f_1 = t$ and $f_2 = 1 + t + t^2$ and computing the integral over $t \leq 10^9$ we get the Bateman–Horn estimate for the first number: 1 973 868. The relative error is 0.0072%.

Why there are so few projective primes of other types?

Let us take, for example, $m = 1 + p + p^2 + p^3 + p^4$, p prime. In order to have $m \leq 10^{18}$ **we must take the integral over** $t \leq 10^{18/4}$ **instead of** $t \leq 10^{18/2}$ as in the previous case.

The number of primes of this form is 252, the estimate gives 246.72.

Another example: the number of primes $m \leq 10^{18}$ of the form $m = 1+p^3+p^6$ is 10; the integral is taken over $[2, 10^{18/6}] = [2, 10^3]$; the "asymptotic estimate" of this number is 12.06.

There is a single projective prime $m \leq 10^{18}$ for p prime and $n = 31$: it is $1+2+2^2+\cdots+2^{30}$. We look for $p \leq 10^{18/30} = 3.98$; thus, the only other candidate is $1 + 3 + 3^2 + \cdots + 3^{30}$, but it is composite. We did not try to get an asymptotic estimate of the number 1.

The constant factor

In order to compute the constant factor we need the following lemma.

Lemma. Let $f = t(1 + t + \cdots + t^{n-1})$, and consider the equation

$$f(t) = 0 \mod p.$$

Then:

$$\omega_f(p) = \begin{cases} 2, & p = n \text{ (namely, } t = 0 \text{ and } t = 1), \\ n, & p \equiv 1 \mod n \text{ (namely, } t = 0 \text{ and } n-1 \text{ primitive} \\ & \text{roots of unity of degree } n \text{ modulo } p), \\ 1, & \text{otherwise (there is always the root } t = 0). \end{cases}$$

For example, take $n = 7$, so that

$$f = t(1 + t + t^2 + t^3 + t^4 + t^5 + t^6),$$

and let $p = 43 \equiv 1 \mod 7$. Then we have seven roots of f in $\mathbb{Z}_{43}$:

$$0; \quad 4,\ 4^2 = 16,\ 4^3 = 21,\ 4^4 = 41,\ 4^5 = 35,\ 4^6 = 11 \quad (4^7 = 1).$$

Conclusion

At the beginning of the talk, I cited a review paper by Aletheia-Zomlefer, Fukshansky and Garcia on the Bateman–Horn conjecture. The first version of this paper was called

One conjecture to rule them all: Bateman–Horn

(An allusion to Tolkien: "One Ring to rule them all".)

And, indeed, we may continue indefinitely, inventing new and new conjectures *ad infinitum*.

Just two examples:

Our conjecture about projective primes (that there are infinitely many of them) does not figure in any known list of corollaries of the BH-conjecture. The same for polynomials coming from block designs.

Another remarkable feature of this conjecture is an **incredible accuracy** with which it predicts the number of "solutions", i. e., of prime values of polynomials, in all kinds of problems which fall into its framework.

Other topics to which the Bateman–Horn conjecture applies:

– Linear groups
– Orders of elements in groups
– Difference sets
– Elliptic curves
– Cryptography
– Error-correcting codes
– Fast multiplication
– Ramanujan graphs

Every problem in which there is a polynomial, or there are several polynomials, which must take prime values, is a potential area of applications of this conjecture.

L'arithmétique

Tapestry (around 1520) – Musée Cluny, Paris

The Latin inscription at the bottom:

Monstrat ars numeris que virtus possit habere

Explico pernumeru(m) que sit proportio rerum

The art of the number shows what virtue it may have:
I explain by the number which is the proportion of things

Thank you!