# Groups and the Bateman–Horn Conjecture

Gareth A. Jones and Alexander K. Zvonkin

**Abstract.** A number of open problems, ranging from the twin primes conjecture to the classification of permutation groups of prime degree, depend on whether certain finite sets of polynomials in $\mathbb{Z}[t]$ can simultaneously take prime values for infinitely many $t \in \mathbb{N}$. The Bateman–Horn Conjecture (BHC) provides an estimate for the number of such $t \leq x$ for large $x \in \mathbb{R}$, and although it is unproved (except for the case of a single linear polynomial) these estimates agree closely with experimental evidence. We have applied the BHC to a number of problems in group theory (as well as other areas) to give strong evidence that various families of groups, such as permutation groups $\mathrm{PSL}_n(q)$ of prime degree $(q^n-1)/(q-1)$, are infinite.

## 1. Permutation groups of prime degree

Building on earlier work by Galois and Burnside, the classification of finite simple groups implies a classification of the transitive permutation groups of prime degree (a problem dating back to Lagrange). These groups are:

(a) subgroups of $\mathrm{AGL}_1(p)$ containing the translation group, for primes $p$;
(b) alternating and symmetric groups $\mathrm{A}_p$ and $\mathrm{S}_p$, for primes $p \geq 5$;
(c) $\mathrm{PSL}_2(11)$ and Mathieu groups $\mathrm{M}_{11}$ and $\mathrm{M}_{23}$, of degrees $11, 11$ and $23$;
(d) subgroups $G$ of $\mathrm{P\Gamma L}_n(q)$ containing $\mathrm{PSL}_n(q)$, in cases when the natural degree $d = (q^n-1)/(q-1)$ is prime.

It is unknown whether the degree $d$ in case (d) is prime for infinitely many pairs $(n, q)$. We met this problem in trying to extend the work of Klein on equations of degree 7 and 11 to all primes [5]. Such *projective primes*, as we call them, include the Fermat primes, of the form $q+1 = 2^{2^f}+1$, for $n = 2$ and the Mersenne primes, of the form $2^n - 1$, for $q = 2$. In investigating this problem (see [6] for details), to avoid these very difficult cases we restricted our attention to parameters $n, q \geq 3$.

If we write $q = p^e$, we are asking whether $p$ and

$$d := p^{(n-1)e} + p^{(n-2)e} + \cdots + p^e + 1. \tag{1}$$

can both be prime for infinitely many $p$. Clearly, this requires $n$ to be prime.

## 2. Prime values of polynomials

These problems are part of a more general number-theoretic problem concerning prime values of polynomials. In 1857 Bunyakovsky [2] conjectured that a polynomial $f(t) \in \mathbb{Z}[t]$ takes prime values for infinitely many $t \in \mathbb{N}$ if and only if it satisfies three obviously necessary conditions:

1. it has a positive leading coefficien,
2. it is irreducible, and
3. it is not identically zero modulo any prime.

For example, these conditions are satisfied by the polynomial $t^2+1$, the subject of the Euler–Landau Conjecture on primes of this form. The Bunyakovsky Conjecture has been proved only in the case $\deg f = 1$: this is Dirichlet's Theorem on primes in an arithmetic progression. Schinzel's Hypothesis [7] asserts that polynomials $f_1(t), \dots, f_k(t) \in \mathbb{Z}[t]$ simultaneously take prime values for infinitely many $t \in \mathbb{N}$ if and only if they satisfy the first two Bunyakovsky conditions and their product satisfies the third; again, this is proved only for a single linear polynomial.

In 1962 Bateman and Horn [1], extending earlier work by Hardy and Littlewood [4] on twin primes and related problems, conjectured that the number $Q(x)$ of $t \le x$ such that each $f_i(t)$ is prime is given asymptotically by the estimate

$$Q(x) \sim E(x) := C \int_a^x \frac{dt}{\prod_{i=}^k \ln f_i(t)} \quad \text{as} \quad x \to +\infty \tag{2}$$

where

$$C = C(f_1, \dots, f_k) := \prod_{r \text{ prime}} \left(1 - \frac{1}{r}\right)^{-k} \left(1 - \frac{\omega_f(r)}{r}\right), \tag{3}$$

$\omega_f(r)$ is the number of roots of $f := f_1 \dots f_k \bmod (r)$, and $a$ is chosen to avoid singularities of the integral, where some $f_i(t) = 1$. There are good heuristic arguments for these formulae, but no proof (again, apart from the case of the quantified version of Dirichlet's Theorem). If Schinzel's conditions are satisfied, the infinite product in (3) converges to a limit $C > 0$. Since the definite integral in (2) diverges to $+\infty$ as $x \to +\infty$, it follows that $E(x) \to +\infty$ and hence, if the BHC is true, $Q(x) \to +\infty$, proving that there are infinitely many $t \in \mathbb{N}$ with each $f_i(t)$ prime.

As simple examples, taking $f_i(t) = t$, $t+2$ or $t$, $2t+1$ gives the twin primes and Sophie Germain primes problems. Taking

$$f_i(t) = t, \quad t^{(n-1)e} + t^{(n-2)e} + \dots + t^e + 1 \tag{4}$$

for fixed $n$ and $e$ gives our projective primes problem.

## 3. Application to permutation groups

We concentrated on the simplest and most frequently arising case of the problem, where $n = 3$ and $e = 1$, so that

$$f_i(t) = t, \quad t^2 + t + 1. \tag{5}$$

Maple evaluates the definite integral in (2) almost instantly. The infinite product in (3) converges slowly, but taking the product over the first $10^9$ primes $r$ gives a good approximation to the limit. Table 1 compares the resulting estimates $E(x)$ with the actual numbers $Q(x)$ found by applying the Rabin–Miller primality test to the values $f_i(t)$ (this test is probabilistic, but the chances of an error are negligible).

| $x$ | $Q(x)$ | $E(x)$ | $E(x)/Q(x)$ |
|---|---|---|---|
| $10^{10}$ | 15 801 827 | $1.579642126 \times 10^7$ | 0.9996579044 |
| $2 \cdot 10^{10}$ | 29 684 763 | $2.968054227 \times 10^7$ | 0.9998578150 |
| $3 \cdot 10^{10}$ | 42 963 858 | $4.296235691 \times 10^7$ | 0.9999650617 |
| $4 \cdot 10^{10}$ | 55 877 571 | $5.587447496 \times 10^7$ | 0.9999445924 |
| $5 \cdot 10^{10}$ | 68 522 804 | $6.852175590 \times 10^7$ | 0.9999847043 |
| $6 \cdot 10^{10}$ | 80 962 422 | $8.096382889 \times 10^7$ | 1.0000173771 |
| $7 \cdot 10^{10}$ | 93 236 613 | $9.323905289 \times 10^7$ | 1.0000261688 |
| $8 \cdot 10^{10}$ | 105 372 725 | $1.053741048 \times 10^8$ | 1.0000130940 |
| $9 \cdot 10^{10}$ | 117 383 505 | $1.173885689 \times 10^8$ | 1.0000431394 |
| $10^{11}$ | 129 294 308 | $1.292974079 \times 10^8$ | 1.0000239757 |

TABLE 1. BHC estimates $E(x)$ and actual numbers $Q(x)$ of primes $p^2 + p + 1$ for primes $p \le x$.

The accuracy of the estimates is comparable to that in other applications of the BHC, such as to twin or Sophie Germain primes. The evidence for other pairs $(n, e)$, such as $(5, 1)$, is good but less convincing, simply because the primes involved increase so rapidly that only a much smaller number of them are within our computing range. Based on this evidence, we make the following conjecture:

**Conjecture 3.1.** *For each prime $n \ge 3$ there are infinitely many prime powers $q$ such that $(q^n - 1)/(q - 1)$ is prime .*

Of course this would imply that for each prime $n \ge 3$ there are infinitely many permutation groups $\mathrm{PSL}_n(q)$ of prime degree $(q^n - 1)/(q - 1)$.

## 4. Other applications to group theory

Similar problems and results arise in connection with extensions of the work in the 1890s of Burnside, Frobenius and Hölder on orders of simple groups, and the classification by Dixon and Zalesskii [3] of primitive linear groups of prime degree.

## 5. Conclusion

These results strongly suggest that various families of groups, appearing in major classification theorems, are all infinite. There are similar results based on the BHC, in our work and in that of others, in areas ranging from combinatorics to elliptic curves, and from error-correcting codes to fast integer multiplication. Their significance is not just that they demonstrate the existence of many examples (often millions) of various constructions and phenomena, but that the accuracy of the estimates obtained provides strong evidence for the validity of the BHC, and hence for the infinitude of these families. Such results also add further emphasis to the desirability of a proof of the BHC, a prospect which currently seems remote.

## References

[1] P. T. Bateman and R. A. Horn, A heuristic asymptotic formula concerning the distribution of prime numbers, *M*ath. Comp. 16 (1962), 220–228.

[2] V. Bouniakowsky, Sur les diviseurs numériques invariables des fonctions rationnelles entières, *M*ém. Acad. Sci. St. Péteresbourg, 6$^{e}$ série, vol. VI (1857), 305–329.

[3] J. D. Dixon and A. E. Zalesskii, Finite primitive linear groups of prime degree, *J.* London Math. Soc. (2) 57 (1998), 126–134; corrigendum *i*bid. 77 (2008), 808–812.

[4] G. H. Hardy and J. E. Littlewood, Some problems of 'Partitio numerorum'; III: On the expression of a number as a sum of primes, *A*cta Math. 114 (1923), 215–273.

[5] G. A. Jones and A. K. Zvonkin, Klein's ten planar dessins of degree 11, and beyond, arxiv.math:2104.12015, to appear.

[6] G. A. Jones. and A. K. Zvonkin, Groups of prime degree and the Bateman–Horn Conjecture, arxiv.math:2106.00346, to appear.

[7] A. Schinzel and W. Sierpiński, Sur certaines hypothèses concernant les nombres premiers, *A*cta Arith. 4 (1958), 185–298; erratum 5 (1958), 259.

Gareth A. Jones
School of Mathematics
University of Southampton
Southampton, UK
e-mail: `G.A.Jones@maths.soton.ac.uk`

Alexander K. Zvonkin
LaBRI
Université de Bordeaux
Bordeaux, France
e-mail: `zvonkin@labri.fr`