Trudy Instituta Matematiki i Mekhaniki UrO RAN

Vol. 29 No. 1 2023

MSC: 05B05, 11N32

DOI: 10.21538/0134-4889-2023-29-1-233-253

BLOCK DESIGNS, PERMUTATION GROUPS AND PRIME VALUES OF POLYNOMIALS [1,2]

Gareth A. Jones and Alexander K. Zvonkin

A recent construction by Amarra, Devillers and Praeger of block designs with specific parameters and large symmetry groups depends on certain quadratic polynomials, with integer coefficients, taking prime power values. Similarly, a recent construction by Hujdurović, Kutnar, Kuzma, Marušič, Miklavič and Orel of permutation groups with specific intersection densities depends on certain cyclotomic polynomials taking prime values. The Bunyakovsky Conjecture, if true, would imply that each of these polynomials takes infinitely many prime values, giving infinite families of block designs and permutation groups with the required properties. We have found large numbers of prime values of these polynomials, and the numbers found agree very closely with the estimates for them provided by Li's recent modification of the Bateman–Horn Conjecture. While this does not prove that these polynomials take infinitely many prime values, it provides strong evidence for this, and it also adds extra support for the validity of the Bunyakovsky and Bateman–Horn Conjectures.

Keywords: Block design, permutation group, intersection density, polynomial, prime number, Bateman–Horn Conjecture, Bunyakovsky Conjecture.

REFERENCES

1. Aletheia-Zomlefer S.L., Fukshansky L., and Garcia S.R. The Bateman–Horn conjecture: heuristics, history, and applications. *Expo. Math.*, 2020, vol. 38, pp. 430–479. Also available at `arXiv-math[NT]:1807.08899v4`.
2. Amarra C., Devillers A. and Praeger C.E. Delandsheer–Doyen parameters for block-transitive point-imprimitive block designs. *Designs, Codes and Cryptography*, 2022, vol. 90, pp. 2205–2221. doi: 10.1007/s10623-022-01015-5 . Also available at `arXiv-math[CO]:2009.00282`.
3. Banks W.D., Pappalardi F., and Shparlinski I.E. On group structures realized by elliptic curves over arbitrary finite fields. *Exp. Math.*, 2012, vol. 21, iss. 1, pp. 11–25. https://doi.org/10.1080/10586458.2011.606075
4. Bateman P.T. and Horn R.A. A heuristic asymptotic formula concerning the distribution of prime numbers. *Math. Comp.*, 1962, vol. 16, pp. 220–228. https://doi.org/10.1090/S0025-5718-1962-0148632-7
5. Belabas K., Cohen H. *Numerical Algorithms for Number Theory Using Pari/GP*, AMS, Mathematical Surveys and Monographs, vol. 254, 2021. All the programs used in the book may be downloaded via a link given on the page `https://www.math.u-bordeaux.fr/~kbelabas/Numerical_Algorithms/`.
6. Borevich Z.I. and Shafarevich I.R. *Number theory.* NY: Acad. Press, 1966.
7. Bouniakowsky V. Sur les diviseurs numériques invariables des fonctions rationnelles entières, *Mém. Acad. Sci. St. Péteresbourg*, 6$^{\text{e}}$ série, 1857, vol. VI, pp. 305–329.[3]

---

[1]This paper is based on the results of the 2021 Conference of International Mathematical Centers “Groups and Graphs, Semigroups and Synchronization”.

[2]Alexander Zvonkin was partially supported by the ANR project Combiné (ANR-19-CE48-0011).

[3]Numerous publications give the following wrong title for Bunyakovsky's paper: “Nouveaux théorèmes relatifs à la distinction des nombres premiers et à la décomposition des entiers en facteurs”. According to the French Wikipedia (see [9]), an article with this title does indeed exist, but it was published in 1840 and not in 1857, and it does not discuss the conjecture in question. The reader may also consult the original paper reproduced in the Google archive.

8. Boxall J. and Gruenewald D. Heuristics on pairing-friendly abelian varieties. *LMS J. Comput. Math.*, 2015, vol. 18, iss. 1, pp. 419–443. https://doi.org/10.1112/S1461157015000091
9. Bunyakovsky conjecture: *Wikipedia* [e-resource]. `https://en.wikipedia.org/wiki/Bunyakovsky_conjecture`
10. Carmichael numbers: *Wikipedia* [e-resource]. `https://en.wikipedia.org/wiki/Carmichael_number`
11. Cohen H. *High-precision computation of Hardy–Littlewood constants* [e-resource]. Preprint. Available at `https://oeis.org/A221712/a221712.pdf` .
12. Cook J.D. Distribution of prime powers [e-resource]. *John D. Cook's blog.* `https://www.johndcook.com/blog/2018/09/03/counting-prime-powers`
13. Covanov S. and Thomé E. Fast integer multiplication using generalized Fermat primes. *Math. Comp.* 2019, vol. 8, pp. 1449–1477. https://doi.org/10.1090/mcom/3367
14. David C. and Smith E. A Cohen–Lenstra phenomenon for elliptic curves. *J. London Math. Soc. (2)*, 2014, vol. 89, no. 1, pp. 24–44. https://doi.org/10.1112/jlms/jdt036
15. Delandtsheer A. and Doyen J. Most block-transitive t-designs are point-primitive. *Geom. Dedicata*, 1989, vol. 29, pp. 307–310. https://doi.org/10.1007/BF00572446
16. Ellis D., Kalai G., and Narayanan B. On symmetric intersecting families. *European J. Combin.*, 2020, vol. 86, article no. 103094. https://doi.org/10.1016/j.ejc.2020.103094
17. Erdős P., Ko C., and Rado R. Intersection theorems for systems of finite sets. *Q. J. Math.*, 1961, vol. 12, pp. 313–320.
18. Euler L. Letter to Goldbach, 28th October 1752 (letter CXLIX). Available at `http://eulerarchive.maa.org/correspondence/letters/OO0877.pdf` . See also De numeris primis valde magnis, *Novi Commentarii academiae scientiarum Petropolitanae*, 1760, vol. 9, pp. 99–153; reprinted in *Commentat. Arith.*, 1849, vol. 1, pp. 356–378, and in *Opera Omnia*: Ser. 1, vol. 3, pp. 1–45.
19. Fernández-Alcober G.A., Kwashira R., and Martínez L. Cyclotomy over products of finite fields and combinatorial applications. *Europ. J. Comb.*, 2010, vol. 31, pp. 1520–1538.
20. Hardy G.H. and Littlewood J.E. Some problems of 'Partitio numerorum'; III: On the expression of a number as a sum of primes. *Acta Math.*, 1923, vol. 114, pp. 215–273.
21. Hujdurović A., Kutnar K., Kuzma B., Marušič D., Miklavič Š., and M. Orel On intersection density of transitive groups of degree a product of two odd primes. *Finite Fields Appl.*, 2022, vol. 78, article no. 101975. Also available at `arXiv.math:2107.09327[CO]` .
22. Jacobson M.J., Jr. and Williams H.G. New quadratic polynomials with high densities of prime values. *Math. Comp.*, 2002, vol. 72, no. 241, pp. 499–519.
23. Jones G.A. and Jones J.M. *Elementary Number Theory.* NY: Springer, 1998.
24. Jones G.A. and Zvonkin A.K. *Klein's ten planar dessins of degree 11, and beyond* [e-resource]. Available at `https://arxiv.org/pdf/2104.12015.pdf` .
25. Jones G.A. and Zvonkin A.K. *Groups of prime degree and the Bateman–Horn Conjecture. Expo. Math.*, 2022. Available at `https://doi.org/10.1016/j.exmath.2022.11.002` .
26. Kim D. Nonexistence of perfect 2-error-correcting Lee codes in certain dimensions. *European J. Combin.*, 2017, vol. 63, pp. 1–5.
27. Li W. A note on the Bateman–Horn conjecture, *J. Number Theory*, 2020, vol. 208, pp. 390–399. Also available at `https://arxiv.org/pdf/1906.03370.pdf` .
28. McEliece R.J. Irreducible cyclic codes and Gauss sums. In: *Combinatorics (Proc. NATO Advanced Study Inst., Breukelen, 1974), Part I: Theory of designs, finite geometry and coding theory*, pp. 179–196, Math. Centre Tracts 55, Math. Centrum, Amsterdam, 1974.
29. Meagher K., Razafimahatratra A.S., and Spiga P. On triangles in derangement graphs. *J. Combin. Theory*, Ser. A, 2021, vol. 180, article no. 105390. Also available at `https://arxiv.org/pdf/2009.01086.pdf` .
30. Mertens F. Ein Beitrag zur analytischen Zahlentheorie. *J. reine angew. Math.*, 1874, vol. 78, pp. 46–62.
31. *The Online Encyclopedia of Integer Sequences* [e-resource]: `https://oeis.org`.
32. Rivin I. *Some experiments on Bateman–Horn.* 2015. Available at `https://arxiv.org/pdf/1508.07821` .
33. RSA numbers: *Wikipedia* [e-resource]: `https://en.wikipedia.org/wiki/RSA_numbers` .
34. Scholl T. Isolated elliptic curves and the MOV attack. *J. Math. Cryptol.*, 2017, vol. 11, pp. 131–146.
35. Scholl T. Super-isolated elliptic curves and abelian surfaces in cryptography. *Exp. Math.*, 2019, vol. 28, pp. 385–397.
36. Sha M. Heuristics of the Cocks–Pinch method. *Adv. Math. Commun.*, 2014, vol. 8, pp. 103–118.

37. Shanks D. and Lal M. Bateman's constant reconsidered and the distribution of cubic residues. *Math. Comp.*, 1972, vol. 26, no. 117, pp. 265–285.

Received September 30, 2021
Revised December 8, 2022
Accepted December 9, 2022

Funding Agency: Alexander Zvonkin was partially supported by the ANR project Combiné (ANR-19-CE48-0011).

Gareth A. Jones, Emeritus Professor, School of Mathematical Sciences, University of Southampton, Southampton SO17 1BJ, UK, e-mail: G.A.Jones@maths.soton.ac.uk .

Alexander K. Zvonkin, Emeritus Professor, LaBRI, Université de Bordeaux, 351 Cours de la Libération, F-33405 Talence Cedex, France, e-mail: zvonkin@labri.fr .

Cite this article as: Gareth A. Jones and Alexander K. Zvonkin. Block Designs, Permutation Groups and Prime Values of Polynomials. *Trudy Instituta Matematiki i Mekhaniki UrO RAN*, 2023, vol. 29, no. 1, pp. 233–253.