CERIAS

The Center for Education and Research in Information Assurance and Security

Modular Prime Bias in Exponential Prime-Generating Functions

Arnold Spantzel

Brigham Young University

rspantzel@gmail.com

Abstract

Prime numbers play a crucial role in number theory, cryptography, and computational mathematics. This poster presents a computational analysis of modular biases in prime-generating functions of the form: $\boldsymbol{f(a,b,x,c)} = \frac{\boldsymbol{a^x+b}}{\boldsymbol{c}}$ where $(\boldsymbol{a},\boldsymbol{b},\boldsymbol{c})$ are integers, $\boldsymbol{x}$ is a positive integer exponent, and $\boldsymbol{f(a,b,x,c)}$ is tested for primality. Numerical experiments reveal a strong bias when $b \equiv 0\ mod\ 15$, indicating a structured influence of modular arithmetic on prime density. Applications include algorithmic number theory, prime-search heuristics, and cryptographic key generation.

Key Discovery

- Computational analysis shows a significant modular bias when $\mathrm{b} \equiv 0 \bmod 15$
- Functions with $\mathrm{b} \equiv 0 \bmod 15$ appear far more frequently among top prime-generating functions than expected.
- The effect is most pronounced at the highest-performing levels and diminishes as broader function sets are analyzed.

Empirical Findings

We carried out computational analysis to examine the distribution of high-performing prime generating functions in relation to $\mathrm{b} \equiv 0 \bmod 15$. The results showed the following:

Subset	Functions with $b \equiv 0 \bmod 15$	Likelihood Compared to Random (6.67%)
Top 50	30 (60%)	9× more likely
Top 100	57 (57%)	8.5× more likely
Top 1% (1125 functions)	230 (20.4%)	3× more likely
Top 5% (5625 functions)	854 (15.2%)	2.3× more likely
Top 20% (22,500 functions)	2040 (9.1%)	1.4× more likely
Top 50% (56,251 functions)	3554 (6.3%)	0.94× more likely

Observations

Density Comparison to Random Distribution

Since the dataset contains **112,503** prime-generating functions, the expected random occurrence of $\mathrm{b} \equiv 0 \bmod 15$ should be around

$$\frac{1}{15} \approx 6.67\%$$

Compared to this we see we see top 50 functions $\sim$ 9 times more likely than random, top 100 functions $\sim$ 8.5 times more likely etc.

Probability Decline with sample Set

The probability of $\mathrm{b} \equiv 0 \bmod 15$ influencing prime generation sharply declines as the sample size increases.

Discussion

This demonstrates that while the modular conditions greatly increases the chance of appearing in the top prime-generating functions, its influence diminishes as more functions are considered. The effected is highly concentrated at the extreme high-end but does not apply universally.

Significance and Applications

- **Number Theory:** Enhances understanding of prime distributions and modular properties.
- **Cryptography:** Structured biases in prime generation could impact key generation.
- **Computational Mathematics:** Optimized algorithms for prime searching.

Future Work

- Extend analysis to a broader range $\mathrm{b} \in [-5000,5000]$
- Investigate other modular conditions (e.g. $\mathrm{b} \equiv 0 \bmod 30$) to see if they exhibit similar biases.
- Develop a formal mathematical proof for the observed modular prime bias and understand why $\mathrm{b} \equiv 0 \bmod 15$ exhibits this effect.
- Further refining the dataset to confirm trends in prime generation bias across different modular conditions.

Conclusion

This research provides empirical evidence of a strong modular prime bias in exponential prime-generating functions, particularly when $\mathrm{b} \equiv 0 \bmod 15$. The findings suggest an underlying structure in modular arithmetic that influences prime formation. Future work will focus on formalizing theoretical justifications and expanding computational validation.

References

- L. Euler, "On an Ingenious Polynomial Prime Formula," 1772.
- G. H. Hardy & J. E. Littlewood, "Some Problems of 'Partitio Numerorum,'" Acta Mathematica, 1923.
- K. A. Ribet, "Galois Representations Attached to Modular Forms and the Conjectures of Serre," Inventiones Mathematicae, 1990.
- A. Granville, "It is Easy to Determine Whether a Given Integer is Prime," Bulletin of the American Mathematical Society, 2007.

PURDUE UNIVERSITY

CERIAS