

Select alternative format: [BibTeX](#) | [ASCII](#)**MR2182699 (Review)**[Liu, Yu-Ru \(3-WTRL-PM\)](#)**A prime analogue of the Erdős-Pomerance conjecture for elliptic curves. (English summary)***Comment. Math. Helv.* **80** (2005), *no. 4*, 755–769.[11N37 \(11G05 11G20\)](#)

Journal

Article

Doc
Delivery**[References: 23](#)****Reference Citations: 0****Review Citations: 0**

Let $\omega(n)$ denote the number of distinct prime factors of $n \in \mathbb{N}$, and let E/\mathbb{Q} be an elliptic curve of rank ≥ 1 , with $b \in E(\mathbb{Q})$ being a rational point of finite order. For a prime p^* of good reduction denote by (\bar{b}) the cyclic group generated by the reduction \bar{b} of b modulo p^* , and let $g_b(p^*)$ be its order. Assuming a certain Generalized Riemann Hypothesis (GRH), the two results proved in this paper are the following:

For all $x \geq 0$,

$$\sum_{p^* \leq x} (\omega(g_b(p^*)) - \log \log(p^*))^2 \ll \pi(x) \log \log x,$$

and, for any $\gamma \in \mathbb{R}$, as $x \rightarrow \infty$

$$\frac{\sqrt{2\pi}}{\pi(x)} \# \left\{ p^* \leq x: \frac{\omega(g_b(p^*)) - \log \log(p^*)}{\sqrt{\log \log(p^*)}} \leq \gamma \right\} \sim \int_{-\infty}^{\gamma} e^{-t^2/2} dt,$$

i.e., the distribution of the quantity in question is normal.

These results are elliptic curve analogues of results conjectured by P. Erdős and C. Pomerance [*Rocky Mountain J. Math.* **15** (1985), no. 2, 343–352; [MR0823246 \(87e:11112\)](#)], recently proved under the assumption of a GRH by the reviewer [*J. Ramanujan Math. Soc.* **17** (2002), no. 1, 19–33; [MR1906418 \(2003h:11119\)](#)], and M. R. Murty and the reviewer [*Canad. J. Math.* **56** (2004), no. 2, 356–372; [MR2040920 \(2005a:11114\)](#)] and the reviewer [*Arch. Math. (Basel)* **85** (2005), no. 4, 345–361; [MR2174232](#)], respectively.

Reviewed by [Filip Saidak](#)

[References]

Note: This list reflects references listed in the original paper as accurately as possible with no attempt to correct errors.

1. M. I. Bachmakov, Un théorème de finitude sur la cohomologie des courbes elliptiques. *C. R. Acad. Sci. Paris Sér. A-B* **270** (1970), A999–A1101. Zbl 0194.52303 MR 0269653 [MR0269653 \(42 #4548\)](#)
2. J. Coates and A. Wiles, On the conjecture of Birch and Swinnerton-Dyer. *Invent. Math.* **39** (1977), 223–251. Zbl 0359.14009 MR 0463176 [MR0463176 \(57 #3134\)](#)
3. P. D. T. A. Elliott, *Probabilistic number theory*. Vol. I and II, Grundlehren Math. Wiss. 239, 240, Springer-Verlag, New York, Berlin 1979. Zbl 0431.10029 MR 0551361 Zbl 0431.10030 MR 0560507 [MR0551361 \(82h:10002a\)](#)
4. P. Erdős, On the normal order of prime factors of $p - 1$ and some related problems concerning Euler's φ -functions. *Quart. J. Math. (Oxford)* **6** (1935), 205–213. Zbl 0012.14905
5. P. Erdős and M. Kac, The Gaussian law of errors in the theory of additive number theoretic functions. *Amer. J. Math.* **62** (1940), 738–742. JFM 66.0172.02 MR 0002374 [MR0002374 \(2,42c\)](#)
6. P. Erdős and C. Pomerance, On the normal number of prime factors of $\varphi(n)$. *Rocky Mountain J. Math.* **15** (1985), 343–352. Zbl 0617.10037 MR 0823246 [MR0823246 \(87e:11112\)](#)
7. R. Gupta and M. R. Murty, Primitive points on elliptic curves. *Compositio Math.* **58** (1986), 13–44. Zbl 0598.14018 MR 0834046 [MR0834046 \(87h:11050\)](#)
8. G. H. Hardy and S. Ramanujan, The normal number of prime factors of a number n . *Quart. J. Pure. Appl. Math.* **48** (1917), 76–97. JFM 46.0262.03
9. C. B. Haselgrove, *Some theorems in the analytic theory of numbers*, *J. London Math. Soc.* 26 (1951), 273–277. Zbl 0043.04704 MR 0044564 [MR0044564 \(13,438e\)](#)
10. J. Kubilius, *Probabilistic methods in the theory of numbers*. Transl. Math. Monogr. 11, Amer. Math. Soc., Providence, R.I., 1964. Zbl 0133.30203 MR 0160745 [MR0160745 \(28 #3956\)](#)
11. J. Lagarias and A. Odlyzko, Effective versions of the Chebotarev density theorem. In *Algebraic number fields* (A. Fröhlich, ed.), Academic Press, New York 1977, 409–464. Zbl 0362.12011 MR 0447191 [MR0447191 \(56 #5506\)](#)
12. S. Lang and H. Trotter, Primitive points on elliptic curves. *Bull. Amer. Math. Soc.* **83** (1977), 289–292. Zbl 0345.12008 MR 0427273 [MR0427273 \(55 #308\)](#)
13. S. Li and C. Pomerance, On generalizing Artin's conjecture on primitive roots to composite moduli. *J. Reine Angew. Math.* **556** (330), 205–224. Zbl 1022.11049 MR 1971146
14. Y.-R. Liu, Prime divisors of number of rational points on elliptic curves with complex multiplication. To appear in *Bull. London Math. Soc.* cf. [MR2164827](#)
15. Y.-R. Liu, Generalizations of the Turán and the Erdős-Kac theorems. Ph.D. thesis, Harvard 2003.
16. S. A. Miri and V. K. Murty, An application of sieve methods to elliptic curves. In *Progress in*

- Cryptology–INDOCRYPT*, Lecture Notes in Comput. Sci. 2247, Springer-Verlag, Berlin 2001, 91–98. Zbl 1011.94543 MR 1934487 [MR1934487 \(2003i:11137\)](#)
17. M. R. Murty and F. Saidak, Non-abelian generalizations of the Erdős-Kac theorem. *Canad. J. Math.* **56** (2004), 356–372. Zbl 1061.11052 MR 2040920 [MR2040920 \(2005a:11114\)](#)
 18. J.-P. Serre, Propriétés galoisiennes des points d’ordre fini des courbes elliptiques. *Invent. Math.* **15** (1972), 259–331. Zbl 0235.14012 MR 0387283 [MR0387283 \(52 #8126\)](#)
 19. J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, *Inst. Hautes Études Sci. Publ. Math.* **54** (1981), 123–201. Zbl 0496.12011 MR 0644559 [MR0644559 \(83k:12011\)](#)
 20. H. Shapiro, Distribution functions of additive arithmetic functions. *Proc. Nat. Acad. Sci. U.S.A.* **42** (1956), 426–430. Zbl 0071.04202 MR 0079609 [MR0079609 \(18,113c\)](#)
 21. J. H. Silverman, *The arithmetic of elliptic curves*. Grad. Texts in Math. 106, Springer-Verlag, New York 1986. Zbl 0585.14026 MR 1329092 [MR0817210 \(87g:11070\)](#)
 22. J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*. Grad. Texts in Math. 151, Springer-Verlag, New York 1994. Zbl 0911.14015 MR 1312368 [MR1312368 \(96b:11074\)](#)
 23. P. Turán, On a theorem of Hardy and Ramanujan. *J. London Math. Soc.* **9** (1934), 274–276. Zbl 0010.10401

© Copyright American Mathematical Society 2006