THE ERDŐS-KAC THEOREM AND ITS GENERALIZATIONS

WENTANG KUO AND YU-RU LIU

Abstract. We give a survey of the Erdő-Kac theorem and its various generalizations. In particular, we discuss an open conjecture of Erdős and Pomerance about the distribution of the number of distinct prime divisors of the order of a fixed integer in the multiplicative groups $(\mathbb{Z}/n\mathbb{Z})^*$. We also formulate a Carlitz module analogue of this conjecture and provide a sketch of its proof.

For $n \in \mathbb{N} := \{1, 2, 3, \cdots\}$, let $\nu(n)$ denote the number of distinct prime divisors of n. For $x \in \mathbb{R}$, a theorem of Turán [19] states that

$$\sum_{n \le x} \big(\nu(n) - \log\log x\big)^2 \ll x \log\log x;$$

from which we can derive an earlier result of Hardy and Ramanujan [6] that for any $\epsilon > 0$,

$$\#\Big\{n \,\Big|\, n \le x \text{ and } |\nu(n) - \log\log n| > \epsilon \log\log n\Big\} = o(x).$$

In other words, the normal order of $\nu(n)$ is $\log\log n$.

The idea behind Turán's proof is essentially probabilistic. Further development of probabilistic ideas led Erdős and Kac [3] to prove that the quantity

$$\frac{\nu(n) - \log\log x}{\sqrt{\log\log x}}$$

is distributed normally. More precisely, for $\gamma \in \mathbb{R}$, Erdős and Kac proved that

$$\lim_{x\to\infty} \frac{1}{x} \#\left\{n \,\middle|\, n \le x \text{ and } \frac{\nu(n) - \log\log x}{\sqrt{\log\log x}} \le \gamma\right\} = G(\gamma),$$

where

$$G(\gamma) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\gamma} e^{-t^2/2}\, dt$$

is the Gaussian normal distribution.

In their original proof, Erdős and Kac used the central limit theorem and the full force of Brun's sieve. By estimating the moments

$$\sum_{n \le x} (\nu(n) - \log\log x)^k$$

Date: September 24, 2023.

The research of the first author was supported by an NSERC discovery grant.

The research of the second author was supported by an NSERC discovery grant.

for all $k \in \mathbb{N}$, Halberstam [7] gave a more probabilistically natural approach to this problem. In 1969, by applying the concept of independent random variables, Billingsley [1] provided an elementary proof of the Erdős-Kac theorem. Recently, Granville and Soundararajan [5] further investigated this idea and obtained a relatively easy proof for the asymptotic formulas of the above moments. Their results hold uniformly in a wide range of k.

The celebrated theorem of Erdős and Kac opened a door to probabilistic number theory. In the 60s and 70s, the theory was refined by many authors, culminating in a generalized Erdős-Kac theorem, proved independently by Kubilius [10] and Shapiro [18]: let $f : \mathbb{N} \to \mathbb{R}$ be a strongly additive function, i.e., $f(n_1n_2) = f(n_1) + f(n_2)$ for $n_1, n_2 \in \mathbb{N}$ with $(n_1, n_2) = 1$, and $f(p^s) = f(p)$ for all primes p and $s \in \mathbb{N}$. Define

$$A(x) = \sum_{p \le x} \frac{f(p)}{p} \qquad \text{and} \qquad B(x) = \left(\sum_{p \le x} \frac{f^2(p)}{p} \right)^{\frac{1}{2}} \ge 0.$$

If for each fixed $\epsilon > 0$,

$$\lim_{x \to \infty} \frac{1}{B^2(x)} \sum_{\substack{p \le x \\ |f(p)| > \epsilon B(x)}} \frac{f^2(p)}{p} = 0,$$

then we have

$$\lim_{x \to \infty} \frac{1}{x} \# \left\{ n \,\middle|\, n \le x \text{ and } \frac{f(n) - A(x)}{B(x)} \le \gamma \right\} = G(\gamma).$$

In fact, the result of Kubilius and Shapiro is applicable to a more general class of distribution functions. One can find a comprehensive treatment of it in the monograph of Elliott [2, Chapter 12].

We can also consider functions that are not strongly additive, say Euler's φ-function. In this case, the result of Kubilius and Shapiro can not be applied directly. Using a nontrivial transform of $\varphi(n)$ into a strongly additive function, Erdős and Pomerance [4] showed that

$$\lim_{x \to \infty} \frac{1}{x} \# \left\{ n \,\middle|\, n \le x \text{ and } \frac{\nu(\varphi(n)) - \frac{1}{2}(\log\log x)^2}{\frac{1}{\sqrt{3}}(\log\log x)^{3/2}} \le \gamma \right\} = G(\gamma).$$

We remark here that the estimates of the number of prime divisors of $\varphi(n)$ involve the distributions of primes in an arithmetic progression. In other words, what is latent here is the distribution of primes in cyclotomic fields $\mathbb{Q}(\zeta_n)$, where, for each n, ζ_n is a primitive n-th root of unity. Each of these fields is an abelian extension of $\mathbb{Q}$.

One can also obtain a 'non-abelian' generalization of the Erdős-Kac theorem if we assume the Riemann Hypothesis for all Dedekind zeta functions of number fields (GRH). Let $\tau(n)$ be the Ramanujan τ-function. In [15], assuming the GRH and Lehmer's conjecture (i.e., $\tau(n)$ never vanishes [12]), R. Murty and K. Murty proved that

$$\lim_{x \to \infty} \frac{1}{x} \# \left\{ n \,\middle|\, n \le x \text{ and } \frac{\nu(\tau(n)) - \frac{1}{2}(\log\log x)^2}{\frac{1}{\sqrt{3}}(\log\log x)^{3/2}} \le \gamma \right\} = G(\gamma).$$

As shown in [15], their general theorem is applicable to a wider class of functions arising as Fourier coefficients of modular forms. One can also derive from it the result of Erdős and

Pomerance on $\nu(\varphi(n))$. What distinguishes this result from the classical theory is its 'non-abelian' nature. The divisibility properties of $\tau(n)$ are associated to the distribution of the Frobenius elements of trace 0 in certain l-adic representations, and their corresponding fields are GL_2-extensions of $\mathbb{Q}$.

In [4], Erdős and Pomerance proposed the following question. For $b \in \mathbb{Z}, n \in \mathbb{N}$ with $(b,n)=1$, let $l_b(n)$ be the multiplicative order of b modulo n. Thus $l_b(n)$ is a divisor of $\varphi(n)$. Based on the belief that the difference between $\nu(\varphi(n))$ and $\nu(l_b(n))$ is 'small on average', Erdős and Pomerance conjectured that if $|b|>1$, then the quantity

$$\frac{\nu(l_b(n)) - \frac{1}{2}(\log\log x)^2}{\frac{1}{\sqrt{3}}(\log\log x)^{3/2}}$$

is distributed normally. This conjecture remains open today. The first breakthrough on this problem was recently achieved by Murty and Saidak [16]. Under the GRH, they proved that

$$\lim_{x\to\infty}\frac{1}{x}\#\left\{n \,\middle|\, n\le x,\ (b,n)=1,\ \text{and}\ \frac{\nu(l_b(n)) - \frac{1}{2}(\log\log x)^2}{\frac{1}{\sqrt{3}}(\log\log x)^{3/2}} \le \gamma\right\} = \frac{\varphi(b)}{|b|}G(\gamma).$$

Li and Pomerance provided an alternative proof of this result in [13]. The difficulty of this conjecture lies in the role played by certain non-abelian extensions of $\mathbb{Q}$. More precisely, we need to bound the quantity $\sum \nu(i_b(n))$, where $i_b(n) = \varphi(n)/l_b(n)$, and this estimate involves the distribution of primes in the Kummer extensions $\mathbb{Q}(\zeta_n, \sqrt[n]{b})$, where $\sqrt[n]{b}$ is a n-th root of b.

Given a result involving the GRH, it is natural to ask if its polynomial analogue holds unconditionally. Let $A=\mathbb{F}_q[T]$ be the polynomial ring over the finite field $\mathbb{F}_q$. For $a \in A$, a monic polynomial $m \in A$ with $(a,m)=1$, let $l_{a,q}(m)$ be the multiplicative order of a modulo m. We can consider the distribution of $\nu(l_{a,q}(m))$. Let $\varphi_q(m)$ be the order of the multiplicative group $(A/mA)^*$, where mA is the ideal of A generated by m. Following the approach of Murty and Saidak, we seek to estimate the quantity $\sum \nu(i_{a,q}(m))$, where $i_{a,q}(m) = \varphi_q(m)/l_{a,q}(m)$. In this case, we obtain unconditionally the desired upper bound. Hence, the distribution of $\nu(l_{a,q}(m))$ is the same with the one of $\nu(\varphi_q(m))$, provided the latter exists. At this point, as the values of $\varphi_q(m)$ involve sums of q-powers, we encounter a difficulty to establish the existence of a normal distribution for $\nu(\varphi_q(m))$. More precisely, a heuristic argument shows that estimating $\nu(\varphi_q(m))$ involves an asymptotic formula for the sum

$$\sum_{w\le x}\frac{1}{l_q(w)},$$

where the sum is over primes w and each $l_q(w)$ is the multiplicative order of q modulo w. In [17], R. Murty and Srinvasan proved that if the above quantity is bounded by $O(x^{1/4})$, then the Artin primitive root conjecture holds for q. However, the conjecture remains unsolved. Moreover, since to estimate $\nu(\varphi_q(m))$, we require not just an upper bound for the above sum, but an asymptotic formula for it, this problem seems quite intractable.

Because of the above complication for polynomials, we consider the Erdős-Pomerance conjecture in a different formulation. From the point of view of class field theory, the

Carlitz module has properties remarkably similar to those of the multiplicative group $\mathbb{G}_{\mathrm{m}}$. Thus one may formulate a Carlitz module analogue of this problem. Let $A = \mathbb{F}_q[T]$ and τ the Frobenius element defined by $\tau(X) = X^q$. We denote by $A\{\tau\}$ the 'skew polynomial ring' whose multiplication is defined by

$$\tau f = f^q \tau, \qquad \forall\, f \in A.$$

The A-Carlitz module C is the $\mathbb{F}_q$-algebra homomorphism

$$C : A \longrightarrow A\{\tau\}, \qquad f \mapsto C_f,$$

given on the generator T by

$$C_T = T + \tau.$$

Let B be a commutative A-algebra and B_+ the additive group of B. We can view an element of $A\{\tau\}$ as an endomorphism of B_+ in the following way: let $b \in B$ and $\sum f_i \tau^i \in A\{\tau\}$ ($f_i \in A$), then

$$\Big(\sum f_i \tau^i\Big)(b) = \sum f_i b^{q^i}.$$

Using the A-Carlitz module C, we can define a new A-action on B as follows: for $f \in A$ and $b \in B$,

$$f \cdot b := C_f(b) \in B.$$

We denote B with this new A-module structure by $C(B)$.

For $g \in A$ and $m \in A$ a monic polynomial, let $\bar{g}$ be the reduction of g modulo mA. Consider $C(A/mA)$, the reduction of C modulo mA. For a fixed non-zero polynomial $a \in A$, consider the set

$$\big\{f \in A, C_f(\bar{a}) = \bar{0}\big\}$$

on $C(A/mA)$. This is an ideal of A because C is a ring homomorphism. Since A is a principle ideal domain, there exists a unique monic polynomial $f_a(m) \in A$ which generates the above ideal. Let $\omega(f_a(m))$ denote the number of distinct monic irreducible factors of $f_a(m)$. Then we have

Theorem 1. *Let $A = \mathbb{F}_q[T]$, C the A-Carlitz module, and $0 \neq a \in A$. For a monic polynomial $m \in A$, let $C(A/mA)$ and $\bar{a}$ be the reduction of C and a modulo mA respectively. Let $f_a(m)$ be the monic generator of the ideal $\{f \in A, C_f(\bar{a}) = \bar{0}\}$ on $C(A/mA)$. If $q \neq 2$, or $q = 2$ and $a \neq 1, T$, or $(1+T)$, then for $\gamma \in \mathbb{R}$, we have*

$$\lim_{\substack{x \in \mathbb{N} \\ x \to \infty}} \frac{1}{q^x} \#\left\{ m \;\middle|\; \deg m = x \text{ and } \frac{\omega(f_a(m)) - \frac{1}{2}(\log x)^2}{\frac{1}{\sqrt{3}}(\log x)^{3/2}} \leq \gamma \right\} = G(\gamma).$$

We recall that for $b \in \mathbb{Z}, n \in \mathbb{N}$ with $(b, n) = 1$, $l_b(n)$ is the multiplicative order of an integer b modulo n. Since it is the positive generator of the set $\{z \in \mathbb{Z},\, b^z \equiv 1 \,(\mathrm{mod}\, n)\}$, the above result can be viewed as an analogue of the Erdős-Pomerance conjecture for the Carlitz module. We remark here that the requirement $q \neq 2$ and $a \neq 0$, or $q = 2$ and $a \neq 0, 1, T$, or $(1+T)$ is analogous to the condition that an integer b satisfies $|b| > 1$ in the classical case. In the following, we will provide a sketch of a proof of Theorem 1. For a complete treatment of this result, we refer the reader to [11].

Proof: (Sketch) For $m \in A$, $0 \neq a \in A$, by the Chinese remainder theorem, we have

$$f_a(m) = \operatorname{lcm}\big\{f_a(p^\alpha),\, p^\alpha \| m\big\}.$$

Here each p is a monic irreducible polynomial in A, and for $\alpha \in \mathbb{N}$, $p^\alpha \| m$ denotes that $p^\alpha | m$ and $p^{\alpha+1} \nmid m$. Using the fact that $C_p(X)/X$ is an Eisenstein polynomial, one can show that [11, Lemma 8]

$$f_a(p^\alpha) = f_a(p)p^\beta \quad \text{for some } 0 \leq \beta \leq \alpha - 1. \tag{1}$$

Define

$$F_a(m) = \prod_{p^\alpha \| m} f_a(p^\alpha),$$

and let $\Omega(m)$ denote the total number of irreducible polynomials dividing m, counting with multiplicity. Then we have

$$\omega(F_a(m)) = \omega(f_a(m)) \leq \Omega(f_a(m)) \leq \Omega(F_a(m)).$$

Consider the difference

$$\Omega(F_a(m)) - \omega(f_a(m)) = \Omega(F_a(m)) - \omega(F_a(m)).$$

Since

$$F_a(m) \,\Big|\, \prod_{p^\alpha \| m} f_a(p)p^{\alpha-1},$$

if $l^2 | F_a(m)$, it implies that either (A) $l^2 | f_a(p)$ for some irreducible polynomial $p|m$, or (B) there exists two distinct irreducible polynomials p_1, p_2 such that $l | f_a(p_1)$, $l | f_a(p_2)$, and $p_1 p_2 | m$, or (C) $l | m$. By estimating the contributions in these three cases, it was proved in [11, Lemma 11] that

$$\sum_{\deg m = x} \Big(\Omega(F_a(m)) - \omega(f_a(m))\Big)^2 \ll q^x\,(\log x)^2.$$

As a direct consequence of the above inequality, for all but $o(q^x)$ monic polynomials $m \in A$ with $\deg m = x$, we have

$$\Omega(F_a(m)) - \omega(f_a(m)) = O\big((\log x)(\log\log x)\big) = o\big((\log x)^{3/2}\big).$$

Thus to prove Theorem 1, it suffices to show that for $\gamma \in \mathbb{R}$,

$$\lim_{\substack{x\in\mathbb{N}\\ x\to\infty}} \frac{1}{q^x} \#\left\{ m \,\Big|\, \deg m = x \text{ and } \frac{\Omega(F_a(m)) - \frac{1}{2}(\log x)^2}{\frac{1}{\sqrt{3}}(\log x)^{3/2}} \leq \gamma \right\} = G(\gamma). \tag{2}$$

One can see from (1) that

$$\sum_{p|m} \Omega(f_a(p)) \leq \Omega(F_a(m)) \leq \sum_{p|m} \Omega(f_a(p)) + \Omega(m).$$

It follows that

$$\Omega(F_a(m)) = \sum_{p|m} \Omega(f_a(p)) + O\big(\Omega(m)\big). \tag{3}$$

Since the normal order of $\Omega(m)$ is $\log m$, for all but $o(q^x)$ monic polynomials $m \in A$ with $\deg m = x$, we have

$$\Omega(m) = (1 + o(1)) \log x = o\big((\log x)^{3/2}\big). \tag{4}$$

Define

$$g(m) = \sum_{p|m} \Omega(f_a(p)),$$

Combining (2), (3), and (4), we see that to prove Theorem 1, it suffices to show that the quantity

$$\frac{g(m) - \frac{1}{2}(\log x)^2}{\frac{1}{\sqrt{3}}(\log x)^{3/2}}$$

is distributed normally.

We note that the function $g(m)$ is a strongly additive function on A, i.e., for $m_1, m_2 \in A$ with $(m_1, m_2) = 1$, an irreducible polynomial $p \in A$, and $s \in \mathbb{N}$,

$$g(m_1 m_2) = g(m_1) + g(m_2) \qquad \text{and} \qquad g(p^s) = g(p).$$

Let

$$A(x) = \sum_{\deg p \le x} \frac{g(p)}{q^{\deg p}} \qquad \text{and} \qquad B(x) = \left(\sum_{\deg p \le x} \frac{g^2(p)}{q^{\deg p}} \right)^{1/2} \ge 0.$$

Then a theorem of Zhang [20] on the function field analogue of the Kubilius-Shapiro theorem shows that if for each fixed $\epsilon > 0$,

$$\lim_{x \to \infty} \frac{1}{B^2(x)} \sum_{\substack{\deg p \le x \\ |g(p)| > \epsilon B(x)}} \frac{g^2(p)}{q^{\deg p}} = 0, \tag{5}$$

then the quantity

$$\frac{g(m) - A(x)}{B(x)}$$

is distributed normally.

Since $C(A/pA) \simeq A/(p-1)A$, we can write

$$p - 1 = f_a(p) \cdot i_a(p);$$

thus

$$\Omega(f_a(p)) = \Omega(p-1) - \Omega(i_a(p)). \tag{6}$$

It was shown in [8, Proposition 1.1] that if $q \neq 2$, or $q = 2$ and $a \neq 1$, T, or $(1 + T)$, the divisibility properties of $i_a(p)$ are associated to the distributions of primes in the fields obtained by adjoining roots of $C_m(X) = 0$ and $C_m(X) = a$ to $\mathbb{F}_q(T)$, the fraction field of A. Then by applying the Chebotarev density theorem for function fields [9], one can prove that [11, Lemma 7]

$$\sum_{\deg p = x} \Omega^2(i_a(p)) \ll \pi(x), \tag{7}$$

where $\pi(x)$ is the number of monic irreducible polynomials in A of degree x. Also, one can deduce from the estimates in [14, p 326] that

$$\sum_{\deg p=x} \Omega(p-1) = \pi(x)\log x + O(\log x). \tag{8}$$

and

$$\sum_{\deg p=x} \Omega^2(p-1) = \pi(x)(\log x)^2 + O\big((\log x)^2\big). \tag{9}$$

Combining (6), (7), (8), and (9), by partial summations, one can prove that

$$A(x) = \sum_{\deg p\le x} \frac{\Omega(f_a(p))}{q^{\deg p}} = \frac{1}{2}(\log x)^2 + O(\log x)$$

and

$$B^2(x) = \sum_{\deg p\le x} \frac{\Omega^2(f_a(p))}{q^{\deg p}} = \frac{1}{3}(\log x)^3 + O\big((\log x)^2\big).$$

Moreover, one can deduce from (8) and (9) that condition (5) is valid. Thus we have

$$\lim_{\substack{x\in\mathbb{N}\\ x\to\infty}} \frac{1}{q^x}\,\#\left\{m \;\middle|\; \deg m = x \text{ and } \frac{g(m)-A(x)}{B(x)} \le \gamma\right\} = G(\gamma).$$

This completes the proof of Theorem 1.

Acknowledgment
This work was first presented in the CRM workshop on Anatomy of Integers in Montreal. The second author would like to thank Prof. de Koninck and Prof. Granville for their kind invitation.

References

[1] P. Billingsley, *On the central limit theorem for the prime divisor functions*, Amer. Math. Monthly, 76 (1969), 132-139.
[2] P. D. T. A. Elliott, *Probabilistic number theory*, Vol. I. & II., Springer-Verlag (1979).
[3] P. Erdős & M. Kac, *The Gaussian law of errors in the theory of additive number theoretic functions*, Amer. J. Math. 62 (1940), 738-742.
[4] P. Erdős & C. Pomerance, *On the normal number of prime factors of $\varphi(n)$*, Rocky Mountain J. Math. 15 (1985), 343-352.
[5] A. Granville & K. Soundararajan, *Sieving and the Erdős-Kac theorem*, Proceedings, NATO-SMS ASI, Montreal 2005
[6] G. H. Hardy & S. Ramanujan, *The normal number of prime factors of a number n*, Quar. J. Pure. Appl. Math. 48 (1917), 76-97.
[7] H. Halberstam, *On the distribution of additive number theoretic functions (I)*, J. London Math. Soc. 30 (1955), 43-53.
[8] C.-N. Hsu, *On Artin's conjecture for the Carlitz module*, Comp. Math. 106 (1997), 247-266.
[9] M. Ishibashi, *Effective version of the Tschebotareff density theorem in function fields*, Bull. London Math. Soc. 24 (1992), 52-56.
[10] J. Kubilius, *Probabilistic methods in number theory*, Transl. Math. Monogr. 11, Rhode Island (1964).
[11] W. Kuo & Y.-R. Liu, *A Carlitz module analogue of a conjecture of Erdős and Pomerance*, to appear in Trans. Amer. Math. Soc., 22 pages.

[12] D. H. Lehmer, *Ramanujan's function $\tau(n)$*, Duke Math. J. 10 (1943), 483-492.
[13] S. Li & C. Pomerance, *On generalizing Artin's conjecture on primitive roots to composite moduli*, J. Reine Angew. Math. 556 (330), 205-224.
[14] Y.-R. Liu, *The Erdős theorem and the Halberstam theorem in function fields*, Acta. Arith. 114 (2004), 323-330.
[15] M. R. Murty & V. K. Murty, *An analogue of the Erdős-Kac theorem for Fourier coefficients of modular forms*, Indian J. Pure App. Math., 15 (1984), 1090-1101.
[16] M. R. Murty & F. Saidak, *Non-abelian generalizations of the Erdős-Kac theorem*, Canadian J. Math. 56 (2004), 356-372.
[17] M. R. Murty & S. Srinvasan, *Some remarks on Artin's conjecture*, Canad. Math. Bull. Vol. 30 (1987), 80-85.
[18] H. Shapiro, *Distribution functions of additive arithmetic functions*, Proc. Nat. Acad. Sci. USA 42 (1956), 426-430.
[19] P. Turán, *On a theorem of Hardy and Ramanujan*, J. London Math. Soc. 9 (1934), 274-276.
[20] W.-B. Zhang, *Probabilistic number theory in additive arithmetic semigroups*, In: Analytic Number Theory (B. C. Berndt et al. eds.) Prog. Math., Birkhäuser (1996), 839-884.

Department of Pure Mathematics, Faculty of Mathematics, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1

E-mail address: wtkuo@math.uwaterloo.ca

Department of Pure Mathematics, Faculty of Mathematics, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1

E-mail address: yrliu@math.uwaterloo.ca