Probability and Number Theory: an Overview of the Erdős-Kac Theorem

Alex Beckwith

December 12, 2012

Probabilistic number theory?

Pick $n \in \mathbb{N}$ with $n \leq 10,000,000$ at random.

- How likely is it to be prime?
- How many prime divisors will it have?

The prime divisor counting function ω

Definition

The function $\omega : \mathbb{N} \to \mathbb{N}$ defined by

$$\omega(n) := \sum_{\{p : p \mid n\}} 1$$

is called the **prime divisor counting function**; $\omega(n)$ yields the number of distinct prime divisors of n.

The prime divisor counting function ω

Definition

The function $\omega : \mathbb{N} \to \mathbb{N}$ defined by

$$\omega(n) := \sum_{\{p : p|n\}} 1$$

is called the **prime divisor counting function**; $\omega(n)$ yields the number of distinct prime divisors of n.

n	prime factorization	$\omega(n)$
6		
30		
1872		
2012		

The prime divisor counting function ω

Definition

The function $\omega : \mathbb{N} \to \mathbb{N}$ defined by

$$\omega(n) := \sum_{\{p: p|n\}} 1$$

is called the **prime divisor counting function**; $\omega(n)$ yields the number of distinct prime divisors of n.

n	prime factorization	$\omega(n)$
6	$2 \cdot 3$	
30		
1872		
2012		

The prime divisor counting function ω

Definition

The function $\omega : \mathbb{N} \to \mathbb{N}$ defined by

$$\omega(n) := \sum_{\{p : p | n\}} 1$$

is called the **prime divisor counting function**; $\omega(n)$ yields the number of distinct prime divisors of n.

n	prime factorization	$\omega(n)$
6	$2 \cdot 3$	2
30		
1872		
2012		

The prime divisor counting function ω

Definition

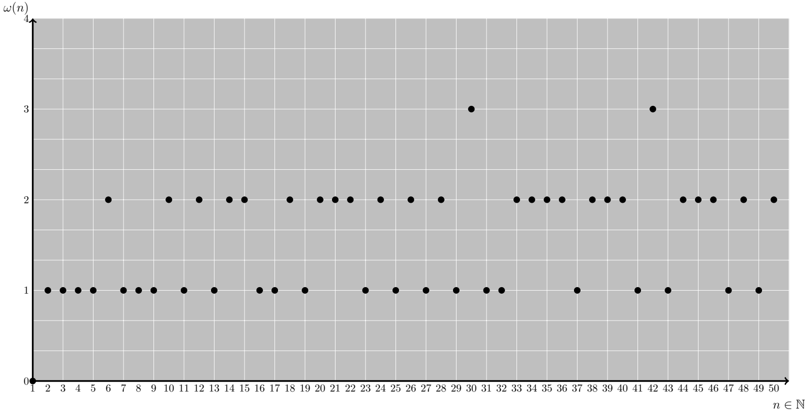
The function $\omega : \mathbb{N} \to \mathbb{N}$ defined by

$$\omega(n) := \sum_{\{p : p | n\}} 1$$

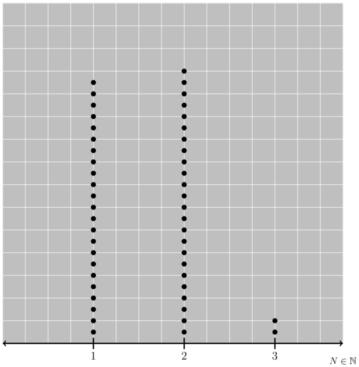
is called the **prime divisor counting function**; $\omega(n)$ yields the number of distinct prime divisors of n.

n	prime factorization	$\omega(n)$
6	$2 \cdot 3$	2
30	$2 \cdot 3 \cdot 5$	3
1872	$2^4 \cdot 3^2 \cdot 13$	3
2012	$2^2 \cdot 503$	2

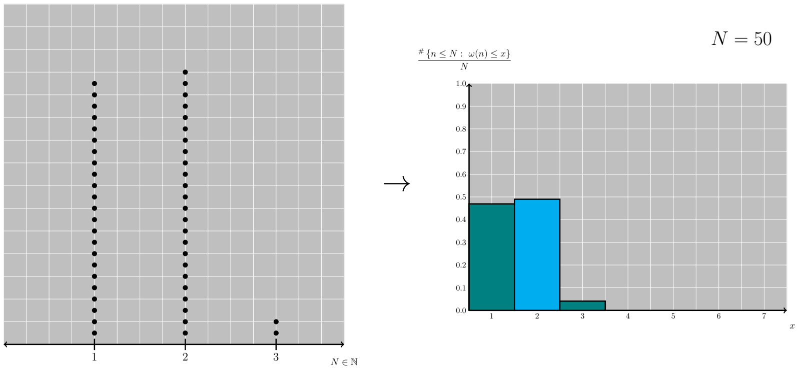
An Illustration



An Illustration



An Illustration



The Erdős-Kac Theorem

Theorem

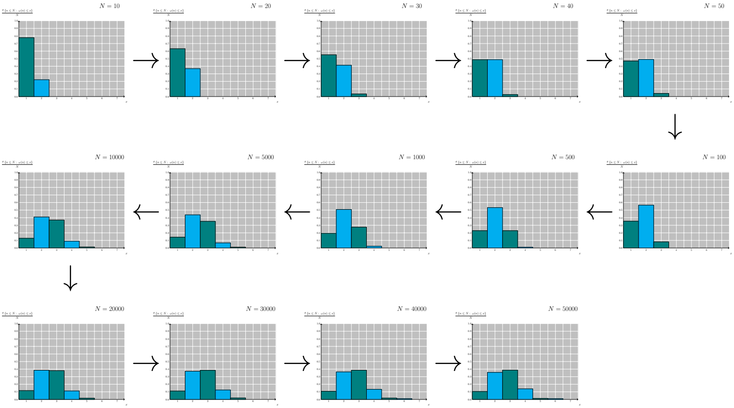
Let $N \in \mathbb{N}$. Then as $N \to \infty$,

$$\nu_N \left\{ n \leq N : \frac{\omega(n) - \log \log N}{\sqrt{\log \log N}} \leq x \right\} = \Phi(x).$$

That is, the limit distribution of the prime-divisor counting function $\omega(n)$ is the normal distribution with mean $\log \log N$ and variance $\log \log N$.

An Illustration

An Illustration



The Erdős-Kac Theorem

Heuristically:

1. Most numbers near a fixed $N \in \mathbb{N}$ have $\log \log N$ prime factors (Hardy and Ramanujan, Turán).

The Erdős-Kac Theorem

Heuristically:

1. Most numbers near a fixed $N \in \mathbb{N}$ have $\log \log N$ prime factors (Hardy and Ramanujan, Turán).
2. Most prime factors of most numbers near N are small.

The Erdős-Kac Theorem

Heuristically:

1. Most numbers near a fixed $N \in \mathbb{N}$ have $\log \log N$ prime factors (Hardy and Ramanujan, Turán).
2. Most prime factors of most numbers near N are small.
3. The events "p divides n, with p a small prime, are roughly independent (Brun sieve).

The Erdős-Kac Theorem

Heuristically:

1. Most numbers near a fixed $N \in \mathbb{N}$ have $\log \log N$ prime factors (Hardy and Ramanujan, Turán).
2. Most prime factors of most numbers near N are small.
3. The events "p divides n, with p a small prime, are roughly independent (Brun sieve).
4. If the events were exactly independent, a normal distribution would result.

Erdős-Kac vs. Central Limit Theorem

Theorem

Let $X_1, X_2, \dots$ be a sequence of independent and identically distributed random variables, each having mean μ and variance σ^2. Then the distribution of

$$\frac{X_1 + \cdots + X_n - n\mu}{\sigma\sqrt{n}}$$

tends to the standard normal as $n \to \infty$.

Uniform probability law

By ν_N we denote the probability law of the uniform distribution with weight $\frac{1}{N}$ on $\{1, 2, \dots, N\}$. That is, for $A \subset \mathbb{N}$,

$$\nu_N A = \sum_{n \in A} \lambda_n \quad \text{with} \quad \lambda_N = \begin{cases} \frac{1}{N} & n \leq N \\ 0 & n > N. \end{cases}$$

Weak convergence

We say that a sequence $\{F_n\}$ of distribution functions **converges weakly** to a function F if

$$\lim_{n\to\infty} F_n(x) = F(x)$$

for all points where F is continuous.

Limiting distributions

Let f be an arithmetic function. Let $N \in \mathbb{N}$. Define

$$F_N(z) := \nu_N\{n : f(n) \leq z\} = \frac{1}{N}\#\{n \leq N : f(n) \leq z\}.$$

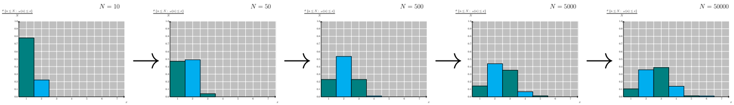
We say that f possess a **limiting distribution function** F if the sequence F_N converges weakly to a limit F that is a distribution function.

Limiting distributions

Let f be an arithmetic function. Let $N \in \mathbb{N}$. Define

$$F_N(z) := \nu_N\{n : f(n) \leq z\} = \frac{1}{N}\#\{n \leq N : f(n) \leq z\}.$$

We say that f possess a **limiting distribution function** F if the sequence F_N converges weakly to a limit F that is a distribution function.



Characteristic functions

Definition

Let F be a distribution function. Then its characteristic function is given by

$$\varphi_F(\tau) := \int_{-\infty}^{\infty} \exp(i\tau z) dF(z).$$

The characteristic function is uniformly continuous on the real line.

Characteristic functions

Definition

Let F be a distribution function. Then its characteristic function is given by

$$\varphi_F(\tau) := \int_{-\infty}^{\infty} \exp(i\tau z) dF(z).$$

The characteristic function is uniformly continuous on the real line.

Fact: A distribution function is completely characterized by its characteristic function.

Characteristic functions

Definition

Let F be a distribution function. Then its characteristic function is given by

$$\varphi_F(\tau) := \int_{-\infty}^{\infty} \exp(i\tau z) dF(z).$$

The characteristic function is uniformly continuous on the real line.

Fact: A distribution function is completely characterized by its characteristic function.

Lemma

The characteristic function of the standard normal distribution Φ is given by

$$\varphi_\Phi(\tau) = \exp\left(-\frac{\tau^2}{2}\right).$$

Levy's continuity theorem

Theorem

Let $\{F_n\}$ be a sequence of distribution functions and $\{\varphi_{F_n}\}$ be the corresponding sequence of their characteristic functions. Then $\{F_n\}$ converges weakly to a distribution function F if and only if φ_{F_n} converges pointwise on $\mathbb{R}$ to a function φ that is continuous at 0. Additionally, in this case, φ is the characteristic function of F.

The Erdős-Kac Theorem

Theorem

Let $N \in \mathbb{N}$. *Then as* $N \to \infty$,

$$\nu_N \left\{ n \leq N : \frac{\omega(n) - \log\log N}{\sqrt{\log\log N}} \leq x \right\} = \Phi(x).$$

That is, the limit distribution of the prime-divisor counting function $\omega(n)$ *is the normal distribution with mean* $\log\log N$ *and variance* $\log\log N$.

A proof sketch

The atomic distribution function for $N \in \mathbb{N}$ is

$$F_N(x) = \nu_N \left\{ n \leq N : \frac{\omega(n) - \log\log N}{\sqrt{\log\log N}} \leq x \right\}$$
$$= \frac{1}{N} \# \left\{ n \leq N : \frac{\omega(n) - \log\log N}{\sqrt{\log\log N}} \leq x \right\}.$$

We denote by $\varphi_{F_N}(\tau)$ the characteristic function of F_N. We have

$$\varphi_{F_N}(\tau) = \int_{-\infty}^{\infty} e^{i\tau z} dF_N(z)$$

Let $P = \{\cdots < x_{-1} < x_0 < x_1 < \cdots < x_i \cdots\}$ be a partition of $\mathbb{R}$. Then we have $\varphi_{F_N}(\tau)$ equal to

A proof sketch continued

$$
\begin{aligned}
&= \int_{-\infty}^{\infty} e^{i\tau z} dF_N(z) \\
&= \lim_{\text{mesh}(P)\to 0} \sum_k e^{i\tau z} \left(F_N(x_k) - F_N(x_{k-1})\right) \\
&= \lim_{\text{mesh}(P)\to 0} \sum_k e^{i\tau z} \left(\frac{1}{N}\# \{n \le N : f(n) \le x_k\} - \frac{1}{N}\# \{n \le N : f(n) \le x_{k-1}\}\right) \\
&= \frac{1}{N}\left[\lim_{\text{mesh}(P)\to 0} \sum_k e^{i\tau z} \left(\# \{n \le N : f(n) \le x_k\} - \# \{n \le N : f(n) \le x_{k-1}\}\right)\right] \\
&= \frac{1}{N} \sum_{k=0}^{\max\{\omega(n): n \le N\}} e^{i\tau f(n)} \\
&= \frac{1}{N} \sum_{n \le N} e^{i\tau f(n)}
\end{aligned}
$$

A proof sketch continued

Next, we find some bounds for $\varphi_{F_N}(\tau)$:

$$\varphi_{F_N}(\tau) = \exp\left(-\frac{\tau^2}{2}\right)\left(1 + O\left(\frac{|\tau| + |\tau|^3}{\sqrt{\log\log N}}\right)\right) + O\left(\frac{1}{\log N}\right).$$

(Informally, we write $f(x) = O(g(x))$ when there exists a positive function g such that f does not grow faster than g.)

A proof sketch continued

Next, we find some bounds for $\varphi_{F_N}(\tau)$:

$$\varphi_{F_N}(\tau) = \exp\left(-\frac{\tau^2}{2}\right)\left(1 + O\left(\frac{|\tau| + |\tau|^3}{\sqrt{\log\log N}}\right)\right) + O\left(\frac{1}{\log N}\right).$$

(Informally, we write $f(x) = O(g(x))$ when there exists a positive function g such that f does not grow faster than g.)
Take the limit as $N \to \infty$:

$$\varphi_{F_N}(\tau) \to \exp\left(-\frac{\tau^2}{2}\right) = \varphi_\Phi(\tau).$$

A proof sketch continued

In other words, the sequence of characteristic functions φ_{F_N} converges pointwise to the characteristic function of the normal distribution.

A proof sketch continued

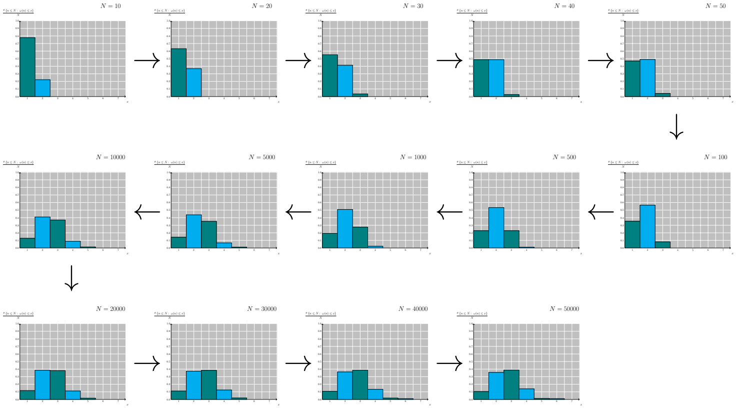
In other words, the sequence of characteristic functions φ_{F_N} converges pointwise to the characteristic function of the normal distribution.

Apply Levy's continuity theorem:

$$\nu_N \left\{ n \leq N : \frac{\omega(n) - \log\log N}{\sqrt{\log\log N}} \leq x \right\} = \Phi(x).$$

Thus, the limit distribution of the prime-divisor counting function $\omega(n)$ is the normal distribution with mean $\log\log N$ and variance $\log\log N$. This completes the proof.

An Illustration



References

Steuding, J. *Probabilistic Number Theory* 2002.

Gowers, T. *The Importance of Mathematics*.