Anatomy of random integers, permutations and polynomials

Kevin Ford

December 3, 2020

Random integers

How are the **prime factors** of a random positive integer $n \leqslant x$ distributed ?

Random permutations

How are the **cycle lengths** of a random permutation $\sigma \in \mathcal{S}_m$ distributed?

Random polynomials over a finite field

How are the **irreducible factor sizes** of a random polynomial $\in \mathbb{F}_q[x]$ of degree m distributed ?

Divisors

Random integers

How are the **divisors** of a random positive integer $n \leqslant x$ distributed ?

Random permutations

How are the **size of divisors** (divisor = product of cycles) of a random permutation $\sigma \in \mathcal{S}_m$ distributed ?

Random polynomials over a finite field

How are the **degree of divisors** (divisor = product of irreducible factors) of a random polynomial $\in \mathbb{F}_q[x]$ of degree m distributed ?

Examples

$n = 42$
Prime factors: 2, 3, 7
Divisors: 1, 2, 3, 6, 7, 14, 21, 42 $\longleftarrow$ **log(divisors)=subset sums of $\{\log 2, \log 3, \log 7\}$**

$\sigma = (126)(34)(5789) \in \mathcal{S}_9$
Cycle lengths : 2, 3, 4
Divisor lengths : 0, 2, 3, 4, 5, 6, 7, 9 $\longleftarrow$ **subset sums of $\{2,3,4\}$**

$x^9 + x^8 + x^6 + x + 1 = (x^2 + x + 1)(x^3 + x + 1)(x^4 + x + 1) \in \mathbb{F}_2[x]$.
Irreducible factor degrees: 2, 3, 4
Divisor degrees : 0, 2, 3, 4, 5, 6, 7, 9 $\longleftarrow$ **subset sums of $\{2,3,4\}$**

Let Poisson(λ) be a Poisson random variable with parameter λ.

(Erdős; Kubilius). Random integer $n \leqslant x$, $1 < a < b \leqslant x$. Then

$$\#\{p|n : a < p \leqslant b\} \approx \text{Poisson}(\log\log b - \log\log a)$$

and approx. independent for disjoint intervals $(a, b]$. Example:

$$\#\{p|n : e^k < p \leqslant e^{k+1}\} \approx \text{Poisson}(1/k).$$

Idea: $\forall$ prime p, $\mathbb{P}(p|n) \approx 1/p$. By Mertens,

probability

$$\sum_{a<p\leqslant b} \frac{1}{p} \approx \log\log b - \log\log a.$$

Let Poisson(λ) be a Poisson random variable with parameter λ.

(Arratia-Tavaré, 1992). Random permutation $\sigma \in \mathcal{S}_m$. Then

$$C_k = \#\{\text{cycles in } \sigma \text{ of size } k\} \approx \text{Poisson}(1/k),$$

with $C_1, C_2, \ldots, C_t$ approx. independent for $t = o(m)$.

Idea: Cauchy's formula ($r_1 + \cdots + r_m = m$):

$$\frac{1}{m!}\#\{\sigma \in \mathcal{S}_m : C_1 = r_1, \ldots, C_m = r_m\} = \prod_{j=1}^{m} \frac{(1/j)^{r_j}}{r_j!}.$$

over the rationals

I. (Chebotarev, 1922). Fix irreducible $f \in \mathbb{Z}[x]$, degree m. For prime p, let $g_j = g_j(p)$ be the number of degree j irred. factors of $f \mod p$. Then

$$\frac{\#\{p \leqslant x : g_1 = r_1, \ldots, g_m = r_m\}}{\pi(x)} \to \prod_{j=1}^{m} \frac{(1/j)^{r_j}}{r_j!}, \quad x \to \infty.$$

II. (Arratia-Barbour-Tavaré, 1993). Fix q. Random monic polynomial

$f \in \mathbb{F}_q[x]$, degree m (m large), and k large.

$$\#\{\text{irred. factors } g|f : \deg(g) = k\} \approx \text{Poisson}(1/k),$$

and quasi-independent for all $k = o(m)$.

Let $\text{Poisson}(\lambda)$ be a Poisson random variable with parameter λ.

$\#\{p|n : e^k < p \leqslant e^{k+1}\} \approx \text{Poisson}(1/k)$, quasi-indep. $k = o(\log x)$.

$C_k = \#\{\text{cycles } \tau|\sigma : |\tau| = k\} \approx \text{Poisson}(1/k)$, quasi-indep $k = o(m)$.

Polynomial $f \in \mathbb{F}_q[x]$ degree m, either f random or q random.

$$\#\{\text{irred. factors } g|f : \deg(g) = k\} \approx \text{Poisson}(1/k).$$

Quasi-independent for $k = o(m)$.

Common Poisson model

Let $Z_k = \text{Poisson}(1/k)$, $k = 1, 2, 3, \ldots$, with Z_j independent.
Then $(Z_1, Z_2, \ldots)$ models the factorization of random integers, permutations and polynomials over $\mathbb{F}_q[x]$.

Central Limit Theorems

Let $Z_k = \text{Poisson}(1/k)$, $k = 1, 2, 3, \ldots$, with Z_j independent.
The sum $Z_1 + Z_2 + \cdots + Z_n$ models the number of prime factors, the number of cycles, and the number of irreducible factors.

$$\begin{aligned} Z_1 + \cdots + Z_n &\stackrel{d}{=} \text{Poisson}(1 + 1/2 + \cdots + 1/n) \\ &\approx \text{Poisson}(\log n) \\ &\approx N(\log n, \log n), \end{aligned}$$

A normal random variable with mean and variance $\log n$.

Erdős-Kac, 1939. Let $\omega(n) = \#\{p : p|n\}$, $E(x) = \log\log x$. As $x \to \infty$

$$\frac{\#\{n \leqslant x : \omega(n) \leqslant E(x) + z\sqrt{E(x)}\}}{x} \to \Phi(z) := \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{z} e^{-\frac{1}{2}t^2}\, dt$$

Erdős-Kac, 1939. Let $\omega(n) = \#\{p : p|n\}$, $E(x) = \log\log x$. As $x \to \infty$

$$\frac{\#\{n \leqslant x : \omega(n) \leqslant E(x) + z\sqrt{E(x)}\}}{x} \to \Phi(z) := \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{z} e^{-\frac{1}{2}t^2}\, dt$$

Goncharav, 1944. Let $C(\sigma)$ be the number of cycles in the factorization of $\sigma \in \mathcal{S}_n$. For all $z \in \mathbb{R}$, as $n \to \infty$,

$$\frac{\#\{\sigma \in \mathcal{S}_n : C(\sigma) \leqslant \log n + z\sqrt{\log n}\}}{n!} \to \Phi(z)$$

Let $\omega(f)$ be the number of distinct irreducible factors of a polynomial $f \in \mathbb{F}_q[x]$. Then, for all $x \in \mathbb{R}$, as $n \to \infty$,

$$\frac{\#\{f \in \mathbb{F}_q[x] : \deg(f) = n, \omega(f) \leqslant \log n + z\sqrt{\log n}\}}{\#\{f \in \mathbb{F}_q[x] : \deg(f) = n\}} \to \Phi(z).$$

Divisors

Common Poisson model

Let $Z_k = \text{Poisson}(1/k)$, $k = 1, 2, 3, \ldots$, with Z_j independent.
Then $(Z_1, Z_2, \ldots)$ models the factorization of random integers, permutations and polynomials over $\mathbb{F}_q[x]$.

Let

subset sums of $\{\underbrace{1,\ldots,1}_{r_1},\underbrace{2,\ldots,2}_{r_2},\underbrace{3,\ldots,3}_{r_3},\ldots\}$

$$\mathcal{D}(r_1, r_2, \ldots, r_t) := \left\{ m_1 + 2m_2 + \cdots + tm_t : 0 \leqslant m_j \leqslant r_j \ (j \geqslant 1) \right\}.$$

Write $\mathcal{D} = \mathcal{D}(Z_1, Z_2, \ldots, Z_t)$

For integers n, $\quad k \in \mathcal{D} \quad \leftrightarrow \quad \exists\, d | n : d \approx e^k$.

For permutations $\sigma \in \mathcal{S}_m$, $k \in \mathcal{D} \quad \leftrightarrow \quad \exists\, \tau | \sigma : |\tau| = k$.

For polynomials $f \in \mathbb{F}_q[x]$, $k \in \mathcal{D} \quad \leftrightarrow \quad \exists\, g | f : \deg(g) = k$.

Common Poisson model of divisor sizes

Let $Z_k = \text{Poisson}(1/k)$, $k = 1, 2, 3, \ldots$, with Z_j independent.

$$\mathcal{D}(r_1, r_2, \ldots, r_t) := \Big\{ m_1 + 2m_2 + \cdots + tm_t : 0 \leqslant m_j \leqslant r_j \ (j \geqslant 1) \Big\},$$

Example: Suppose $r_1 = 2$, $r_2 = 0$, $r_3 = 0$, $r_4 = 1$.
Corresponds to 2 factors of size 1 and 1 factor or size 4, e.g.

$$\sigma = (1)(2563)(4) \in \mathcal{S}_6,$$
$$x^6 + 2x^4 + 2x^2 + 2x = x(x+1)(x^4 + 2x^3 + 2) \pmod 3.$$

Then

$$\mathcal{D}(2, 0, 0, 1) = \{0, 1, 2, 4, 5, 6\}$$

is the set of divisor sizes.

Theorem. (Eberhard, Ford, Green, 2015)

$$\mathbb{P}\Big(k \in \mathcal{D}(Z_1, Z_2, \dots, Z_k)\Big) \asymp \frac{1}{k^{\mathcal{E}}(1+\log k)^{3/2}} \quad (k \in \mathbb{N}),$$

where $\mathcal{E} = 1 - \frac{1+\log\log 2}{\log 2} = 0.08607\dots$.

OPEN PROBLEM: Asymptotic.

Theorem. (Ford, 2008)

Uniformly for $3 \leqslant y \leqslant \sqrt{x}$,

$$\#\{n \leqslant x : \exists\, d|n, y < d \leqslant 2y\} \asymp \frac{x}{(\log y)^{\mathcal{E}}(\log\log y)^{3/2}},$$

Corollary (Erdős' multiplication table problem):

$$\#\{ab : a \leqslant x, b \leqslant x\} \asymp \frac{x^2}{(\log x)^{\mathcal{E}}(\log\log x)^{3/2}}.$$

OPEN PROBLEM: Asymptotic formula. **maybe DNE (Pomerance)**

Theorem. (Eberhard, Ford, Green. 2015)

$\frac{1}{m!}\#\{\sigma \in \mathcal{S}_m : \exists\, \tau | \sigma : |\tau| = k\} \asymp \frac{1}{k^{\mathcal{E}}(1+\log k)^{3/2}} \quad (1 \leqslant k \leqslant n/2).$
If $m = 2n$, $k = n$ we have the probability

$$\frac{1}{(2n)!}\#\{\sigma \in \mathcal{S}_{2n} : \sigma = \tau_1\tau_2 \ \ , \ |\tau_1| = |\tau_2| = n\} \asymp \frac{1}{n^{\mathcal{E}}(\log n)^{3/2}}$$

that a random permutation in $\mathcal{S}_{2n}$ is *perfectly balanced*.

Corollary.

For $k \leqslant m/2$,

monic

$$\frac{1}{p^m}\#\{f \in \mathbb{F}_p[x] : \deg(f) \leqslant m, \exists\, g | f : \deg(g) = k\} \asymp \frac{1}{k^{\mathcal{E}}(1+\log k)^{3/2}}.$$

Theorem. (Ford, 2008)

$$\#\{ab : a \leqslant x, b \leqslant x\} \asymp \frac{x^2}{(\log x)^{\mathcal{E}} (\log \log x)^{3/2}}$$

Theorem. (Eberhard, Ford, Green. 2015)

$$\frac{1}{(2n)!} \#\{\sigma \in \mathcal{S}_{2n} : \sigma = \tau_1 \tau_2 \ , \ |\tau_1| = |\tau_2| = n\} \asymp \frac{1}{n^{\mathcal{E}} (\log n)^{3/2}}$$

Corollary.

monic

$$\frac{1}{p^{2n}} \#\{f \in \mathbb{F}_p[x] : \deg(f) = 2n, \exists\, g | f : \deg(g) = n\} \asymp \frac{1}{n^{\mathcal{E}} (\log n)^{3/2}}$$

Restricted multiplication table problems

For $\mathcal{A} \subset \mathbb{N}$, let

$$M(\mathcal{A};x) := \#\{ab : a \leqslant x, a \in \mathcal{A}, b \leqslant x, b \in \mathcal{A}\}$$
$$M^*(\mathcal{A};x) := \#\{ab : a \leqslant x, a \in \mathcal{A}, b \leqslant x\}$$

Examples.

- $\mathcal{A} = \{n \in \mathbb{N} : p|n \Rightarrow p > y\}$. Ford, 2019 for $M(\mathcal{A};x)$.
- $\mathcal{A} = \{n \in \mathbb{N} : p|n \Rightarrow p \leqslant y\}$; Mehdizadeh, 2020.
- (OPEN) $\mathcal{A} = \{n : p|n \Rightarrow p \in \mathcal{P}\}$ for a general set $\mathcal{P}$ of primes.

Permutation analogs to study (completely open)

$$\frac{1}{m!}\#\{\sigma \in \mathcal{S}_n : \exists\tau|\sigma, \tau \in \mathcal{B}\}$$
$$\frac{1}{m!}\#\{\sigma \in \mathcal{S}_n : \exists\sigma = \tau_1\tau_2, \tau_1 \in \mathcal{B}, \tau_2 \in \mathcal{B}\}$$

Another restricted divisor problem:

$$H(x,y;\mathcal{A}) = \#\{n \leqslant x, n \in \mathcal{A} : \exists\, d|n, y < d \leqslant 2y\}.$$

Examples

- $\mathcal{A} = \{p-1 : p \text{ prime }\}$; Ford 2008, Koukoulopoulos 2010.
- $\mathcal{A}_f := \{f(n) : n \in \mathbb{N}\}$, f a fixed polynomial. Erdős-Schinzel, 1990; Tenenbaum, 1990. Ford-Qian, 2019. Good results for $y \leqslant x^{1-\varepsilon}$, poorer results for $y \gg x$.

Erdős-Schinzel, 1990 (Chebyshev's problem). For any irreducible $f \in \mathbb{Z}[x]$ of degree g,

$$\max\left\{p : p \middle| \prod_{n \leqslant x} f(n)\right\} \gg x \exp\left\{\frac{\log x}{xg} H(x^g; x/2; \mathcal{A}_f)\right\}.$$

Tenenbaum: $H(x^g, x/2; \mathcal{A}_f) \gg x/(\log x)^{\log 4 - 1 + o(1)}$.
Unsolved: Is $H(x^g, x/2; \mathcal{A}_f) \gg x/(\log x)^{\mathcal{E}}$?
$\mathcal{E} = 0.086\ldots$ vs. $\log 4 - 1 = 0.386\ldots$.

The concentration of divisors

$$\Delta(n) := \max_u \#\{d|n : e^u < d \leqslant e^{u+1}\}.$$

Erdős Conjecture, 1948. $\Delta(n) \geqslant 2$ for almost all n.

Maier-Tenenbaum, 1984. Erdős' conjecture is true.

Maier-Tenenbaum, 2009. For almost all n,

$$(\log\log n)^{0.33827\ldots} \leqslant \Delta(n) \leqslant (\log\log n)^{\log 2 + o(1)}$$

The authors conjectured that the lower bound is the true normal order of $\Delta(n)$.

Hooley, Vaughan, ... Applications of $\Delta(n)$ to additive number theory.

Simplified model (F, Green, Koukoulopoulos; 2019)

Since Poisson($\mathbf{1/n}$) $\approx$ Bernouilli($\mathbf{1/n}$) for large n, consider a random subset $\mathcal{A}$ of $\{1, 2, \ldots, N\}$, where

$$\mathbb{P}(n \in \mathcal{A}) = 1/n$$

The biggest concentration of divisors in a short interval is modeled by the maximal concentration of subset sums

$$F(\mathcal{A}) := \max_k \# \left\{ \mathcal{B} \subset \mathcal{A} : \sum_{b \in \mathcal{B}} b = k \right\}$$

Example: $\mathcal{A} = \{1, 2, 4, 5, 7\}$. Then $F(\mathcal{A}) = 3$, corresponding to $k = 7$ or $k = 12$, e.g.

$$7 = 7 = 5 + 2 = 4 + 2 + 1.$$

(Setup) $\mathcal{A}$ is a random, harmonic weighted, subset of $\{1, \ldots, N\}$.

$$F(\mathcal{A}) := \max_k \#\Big\{\mathcal{B} \subset \mathcal{A} : \sum_{b \in \mathcal{B}} b = k\Big\}$$

Thm (FGK, 2020+). Let $\zeta = 0.3533227\ldots$ (a specific number). Then

$$F(\mathcal{A}) \geqslant (\log N)^{\zeta - o(1)} \text{ with prob. } \to 1 \text{ as } N \to \infty.$$

Corollaries (we believe these are best possible)

For almost all n, $\Delta(n) \geqslant (\log\log n)^{\zeta - o(1)}$. Conj: a.a. n, $\Delta(n) = (\log\log n)^{\zeta+o(1)}$

For most $\sigma \in \mathcal{S}_n$, $\max_r \#\{d|\sigma : \text{length}(d) = r\} \geqslant (\log n)^{\zeta - o(1)}$

Fix q. For most $f \in \mathbb{F}_q[x]$ of degree n,

$$\max_r \#\{g|f : \deg(g) = r\} \geqslant (\log n)^{\zeta - o(1)} \qquad (n \to \infty).$$

Theorem (FGK, 2020+). Let

$$\beta_k := \sup\left\{c : F\big(\mathcal{A} \cap [N^c, N]\big) \geqslant k \text{ with prob. } \to 1 \text{ as } N \to \infty\right\}.$$

Then

$$\limsup_{k\to\infty} \frac{\log k}{\log(1/\beta_k)} \geqslant \zeta = 0.3533\ldots$$

Maier-Tenenbaum, 1984: $\beta_2 = \frac{\log 3 - 1}{\log 3} = 0.08976\ldots$.

FGK, 2020+: $\beta_3 = 0.02616\ldots, \quad \beta_4 = 0.01295\ldots$

Thm: FGK, 2020+ For all k, and any $\alpha < \frac{\beta_k}{1-\beta_k}$, almost all integers n have k divisors in an interval of type

$$\left(y, y + \frac{y}{(\log y)^{\alpha}}\right].$$

This improves Tenenbaum, for all $k \geqslant 3$.