Rozkład liczb na czynniki pierwsze a rozkład permutacji na cykle

Rafał Bystrzycki

Uniwersytet im. Adama Mickiewicza w Poznaniu

rafbys@amu.edu.pl

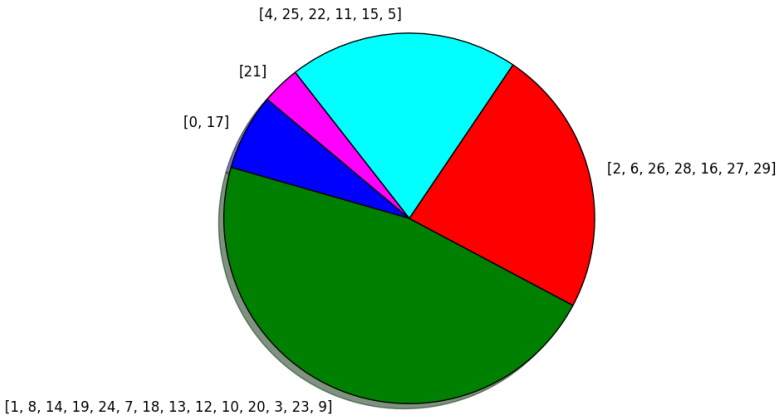
Wola Ducka, 25 sierpnia 2018

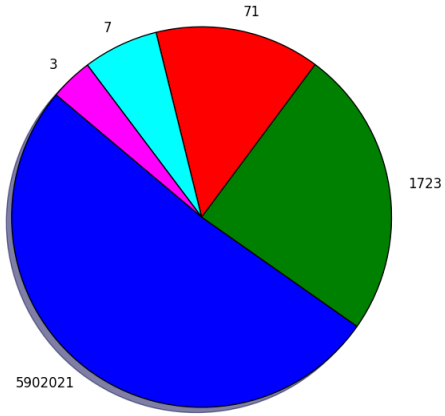
Dwa doświadczenia

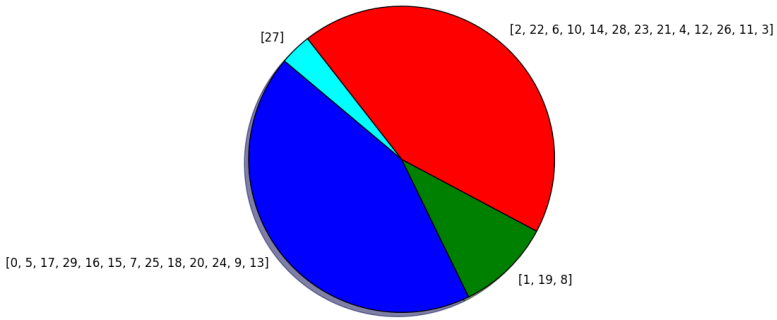
- Losujemy permutację zbioru N-elementowego i rozpatrujemy jej rozkład na cykle

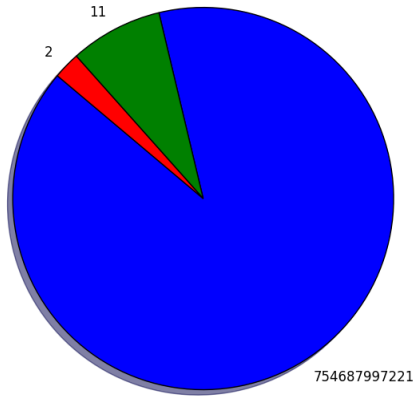
- Losujemy liczbę naturalną z przedziału $[x, 2x]$ i rozpatrujemy jej rozkład na czynniki pierwsze

Przykłady


[4, 25, 22, 11, 15, 5]
[21]
[0, 17]
[2, 6, 26, 28, 16, 27, 29]
[1, 8, 14, 19, 24, 7, 18, 13, 12, 10, 20, 3, 23, 9]


71
7
3
1723
5902021


[27]
[2, 22, 6, 10, 14, 28, 23, 21, 4, 12, 26, 11, 3]
[0, 5, 17, 29, 16, 15, 7, 25, 18, 20, 24, 9, 13]
[1, 19, 8]


11
2
754687997221

Większe próbki

1000 losowych permutacji zbioru $\{0, 1, \ldots, 29\}$.

1000 losowych liczb z przedziału $[e^{30}, 2e^{30}]$

Oczywiste podobieństwa

- każda permutacja $\sigma \in S_N$ może być jednoznacznie przedstawiona jako złożenie parami rozłacznych cykli

$$\sigma = C_1 \cdots C_k$$

- każda liczba może być jednoznacznie przedstawiona jako iloczyn (niekoniecznie różnych) liczb pierwszych

$$n = p_1 \cdots p_k$$

Oczywiste podobieństwa

- każda permutacja $\sigma \in S_N$ może być jednoznacznie przedstawiona jako złożenie parami rozłacznych cykli

$$\sigma = C_1 \cdots C_k$$

- długości cykli tworzą podział wielkości permutowanego zbioru

$$N = |C_1| + \cdots + |C_k|$$

- każda liczba może być jednoznacznie przedstawiona jako iloczyn (niekoniecznie różnych) liczb pierwszych

$$n = p_1 \cdots p_k$$

- logarytmy czynników tworzą podział logarytmu liczby

$$\log n = \log p_1 + \cdots + \log p_k$$

Mniej oczywiste

- prawdopodobieństwo, że losowo wybrana permutacja zbioru N-elementowego jest cyklem wynosi $\frac{1}{N}$
- prawdopodobieństwo, że losowo wybrana liczba z przedziału $[x, 2x]$ jest pierwsza wynosi $\approx \frac{1}{\log x}$

Oczywiste różnice

- właściwym parametrem jest N
- właściwym parametrem jest $\log x$

Oczywiste różnice

- właściwym parametrem jest N
- możliwe rozmiary składników to $1, 2, 3, \ldots$

- właściwym parametrem jest $\log x$
- możliwe rozmiary składników to $\log 2, \log 3, \log 5, \ldots$

Oczywiste różnice

- właściwym parametrem jest N
- możliwe rozmiary składników to $1, 2, 3, \ldots$
- jest wiele elementów o tych samych rozmiarach składników

- właściwym parametrem jest $\log x$
- możliwe rozmiary składników to $\log 2, \log 3, \log 5, \ldots$
- wielkości składników wyznaczają badany element

Liczba części

- średnia liczba cykli to $\log N$ (folklor?)
- średnia liczba czynników pierwszych liczby to $\log \log x$ (Hardy-Ramanujan, 1917)

Liczba części

- średnia liczba cykli to $\log N$ (folklor?)
- średnia liczba czynników pierwszych liczby to $\log\log x$ (Hardy-Ramanujan, 1917)

Twierdzenie (Gonczarow, 1942)

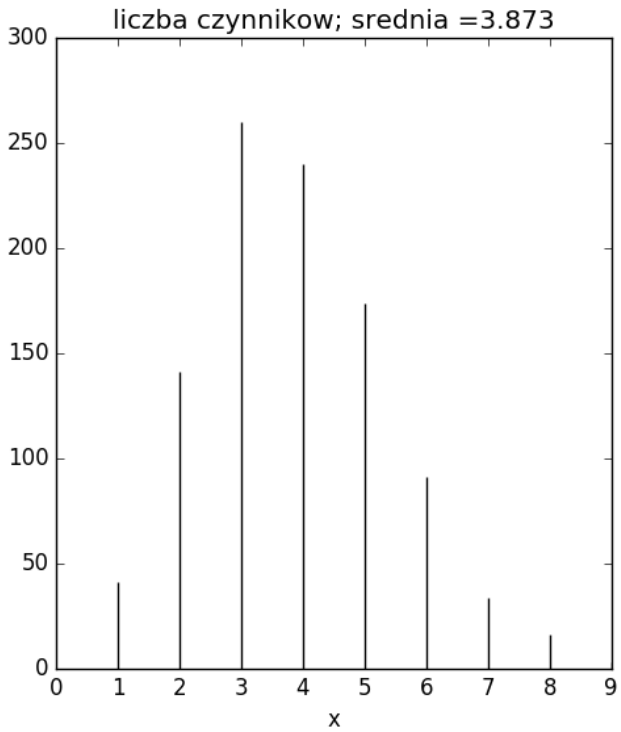
Rozkład prawdopodobieństwa zbiega do rozkładu normalnego o średniej i wariancji $\log N$.

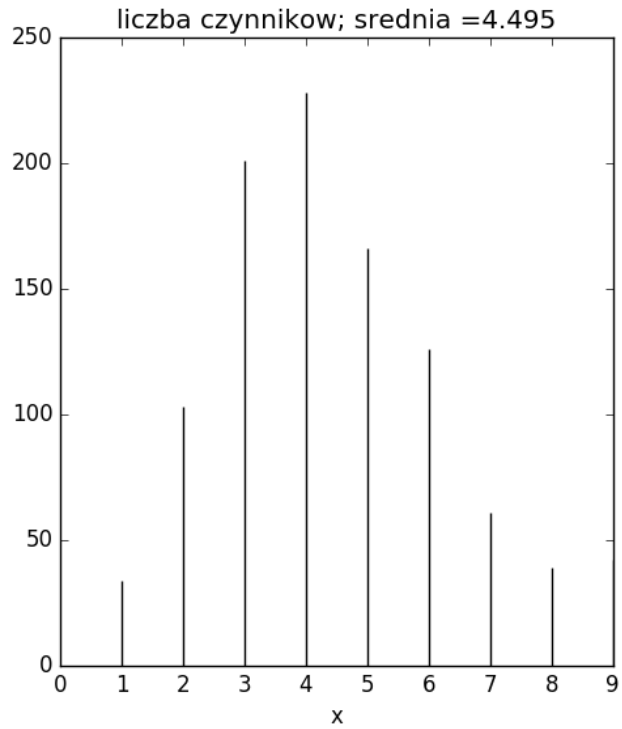
Twierdzenie (Erdős-Kac, 1940)

Rozkład prawdopodobieństwa zbiega do rozkładu normalnego o średniej i wariancji $\log\log x$.

W przykładach

$$\log 30 = 3,4011973816621555$$





Największe części

Twierdzenie (Gonczarow, 1944)

Prawdopodobieństwo tego, że najdłuższy cykl losowo wybranej permutacji $\sigma \in S_N$ ma mniej niż $\frac{N}{u}$ elementów wynosi około $\rho(u)$

Twierdzenie (deBruijn, 1930)

Prawdopodobieństwo tego, że największy czynnik pierwszy losowo wybranej liczby $n \leqslant x$ jest mniejszy niż $x^{\frac{1}{u}}$ wynosi około $\rho(u)$

Funkcja Dickmana-deBruijna i stała Golomba-Dickmana

Funkcja ρ jest zdefiniowana przez:

- $\rho(u) = 1$ dla $u \in [0, 1]$.
- dla $u \geqslant 1$:

$$\rho(u) = \frac{1}{u} \int_{u-1}^{u} \rho(t)dt$$

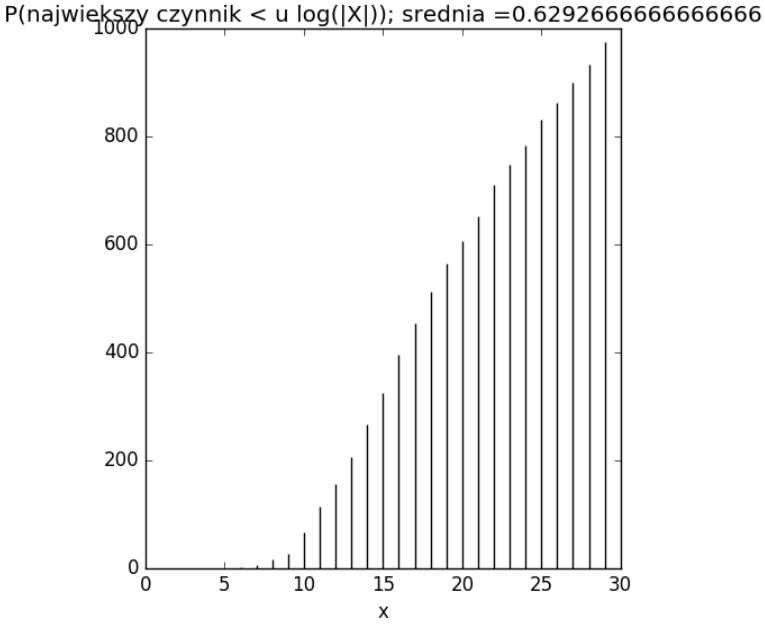
Stała Golomba-Dickmana:

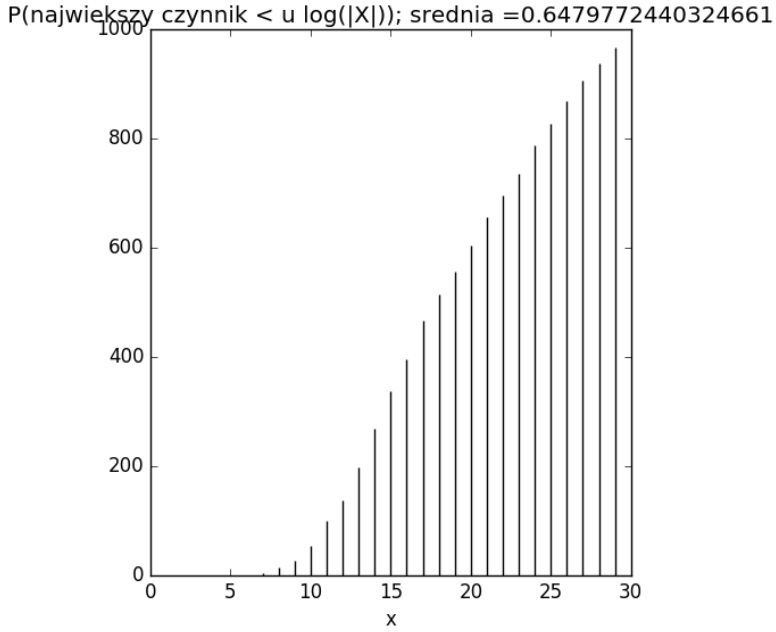
$$\lambda = 0,624329988543550 87$$

to wartość średnia $\frac{|C_{max}|}{N}$ i $\frac{\log P_{max}}{\log x}$.

W przykładach

$\lambda = 0,62432998854355087$





Najmniejsze części

Twierdzenie

Liczba permutacji $\sigma \in S_N$ bez cykli długości $\leqslant M$ wynosi około

$$\frac{e^{-\gamma}}{M} N!$$

Twierdzenie (Mertens?)

Liczba liczb całkowitych $n \leqslant x$ bez dzielników pierwszych $\leqslant y$ wynosi około

$$\frac{e^{-\gamma}}{\log y} x$$

Stała Eulera-Mascheroniego

- Stała Eulera-Mascheroniego $\gamma = 0,5772156649015328 6$
- $e^{-\gamma} = 0,561459483566885 1$

Dowód

Twierdzenie

Liczba permutacji $\sigma \in S_N$ bez cykli długości $\leqslant M$ wynosi około

$$\frac{e^{-\gamma}}{M} N!$$

Dowód

Twierdzenie

Liczba permutacji $\sigma \in S_N$ bez cykli długości $\leqslant M$ wynosi około

$$\frac{e^{-\gamma}}{M} N!$$

- wzór włączeń i wyłączeń

Dowód

Twierdzenie

Liczba permutacji $\sigma \in S_N$ bez cykli długości $\leqslant M$ wynosi około

$$\frac{e^{-\gamma}}{M} N!$$

- wzór włączeń i wyłączeń
- średnia liczba cykli długości j to $\frac{1}{j}$,
- średnia liczba par cykli o długościach j_1, j_2 to

$$\frac{1}{j_1 j_2} \,\mathrm{dla}\, j_1 \neq j_2 \qquad \frac{1}{2j_1^2} \,\mathrm{dla}\, j_1 = j_2, \ldots$$

Dowód

Twierdzenie

Liczba permutacji $\sigma \in S_N$ bez cykli długości $\leqslant M$ wynosi około

$$\frac{e^{-\gamma}}{M} N!$$

- wzór włączeń i wyłączeń
- średnia liczba cykli długości j to $\frac{1}{j}$,
- średnia liczba par cykli o długościach j_1, j_2 to

$$\frac{1}{j_1 j_2} \,\mathrm{dla}\, j_1 \neq j_2 \qquad \frac{1}{2j_1^2} \,\mathrm{dla}\, j_1 = j_2, \ldots$$

$$\underbrace{N!}_{\text{wszystkie}} - \underbrace{\sum_{j=1}^{M} \frac{1}{j} N!}_{\text{zawrające dany cykl}} + \underbrace{\frac{1}{2} \sum_{j_1=1}^{M} \sum_{j_2=1}^{M} \frac{1}{j_1 j_2} N!}_{\text{zawrające daną parę cykli}} - \ldots$$

Dowód

Twierdzenie

Liczba permutacji $\sigma \in S_N$ bez cykli długości $\leqslant M$ wynosi około

$$\frac{e^{-\gamma}}{M} N!$$

Dowód

Twierdzenie

Liczba permutacji $\sigma \in S_N$ bez cykli długości $\leqslant M$ wynosi około

$$\frac{e^{-\gamma}}{M} N!$$

- niech $\mu_M := \sum_{j=1}^{M} \frac{1}{j}$, wtedy mamy

$$N! \sum_{r \geqslant 0} (-1)^r \frac{\mu_M^r}{r!}$$

Dowód

Twierdzenie

Liczba permutacji $\sigma \in S_N$ bez cykli długości $\leqslant M$ wynosi około

$$\frac{e^{-\gamma}}{M} N!$$

- niech $\mu_M := \sum_{j=1}^{M} \frac{1}{j}$, wtedy mamy

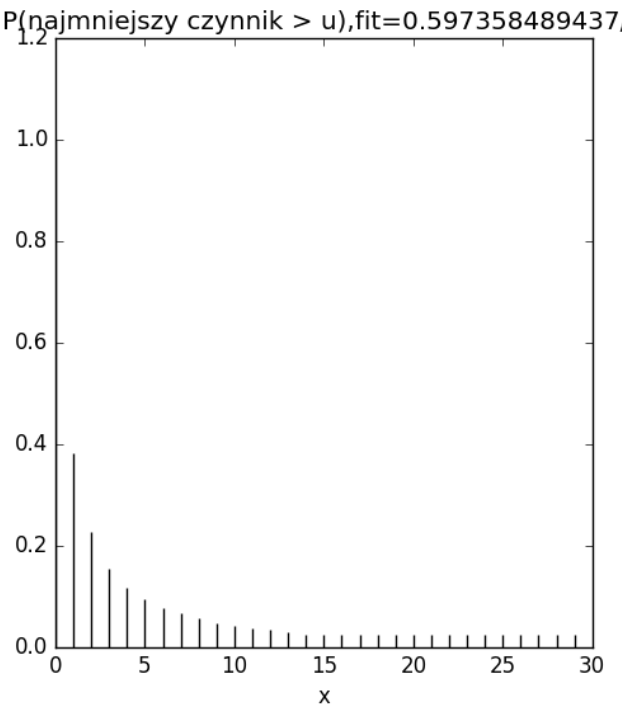
$$N! \sum_{r \geqslant 0} (-1)^r \frac{\mu_M^r}{r!}$$

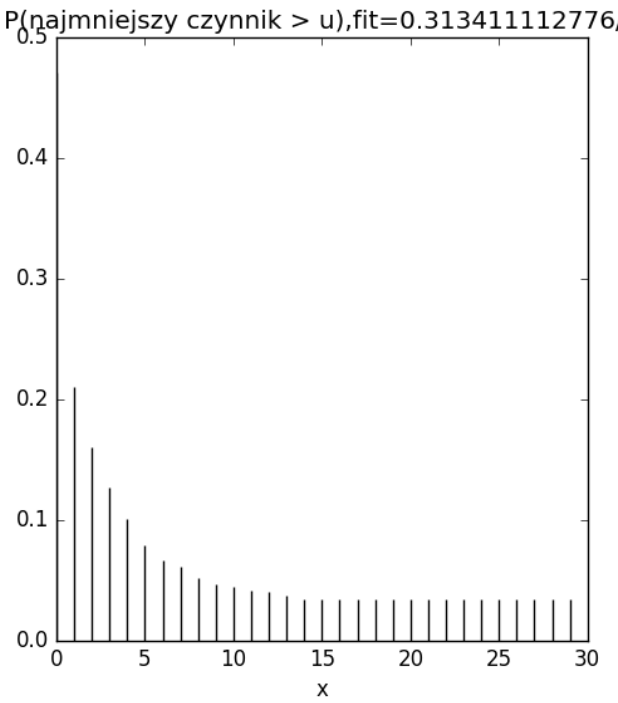
- z wzoru Taylora i definicji γ, to około

$$N! e^{-\mu_M} = N! e^{-\gamma} e^{-\log M} = e^{-\gamma} \frac{N!}{M}$$

W przykładach

$$e^{-\gamma} = 0,561459483566885 1$$





Dana liczby części

Twierdzenie (Jordan, 1947)

Dla danej liczby całkowitej l frakcja permutacji z S_N o dokładnie l cyklach to około

$$\frac{1}{N}\frac{(\log N)^{l-1}}{(l-1)!}$$

Twierdzenie (Landau, 1909)

Dla danej liczby całkowitej l frakcja liczb $\leqslant x$ o dokładnie l czynnikach pierwszych to około

$$\frac{1}{\log x}\frac{(\log\log x)^{l-1}}{(l-1)!}$$

Dana liczby części

Twierdzenie (Jordan, 1947)

Dla danej liczby całkowitej l frakcja permutacji z S_N o dokładnie l cyklach to około

$$\frac{1}{N}\frac{(\log N)^{l-1}}{(l-1)!}$$

Dla $l \sim \log N$, pomnożyć przez

$$\frac{1}{\Gamma(r+1)},$$

gdzie $r = \frac{l-1}{\log N}$.

Twierdzenie (Landau, 1909)

Dla danej liczby całkowitej l frakcja liczb $\leqslant x$ o dokładnie l czynnikach pierwszych to około

$$\frac{1}{\log x}\frac{(\log\log x)^{l-1}}{(l-1)!}$$

Dla $l \sim \log\log x$, pomnożyć przez

$$\frac{1}{\Gamma(r+1)}\prod_p (1+\frac{r}{p-1})(1-\frac{1}{p}),$$

gdzie $r = \frac{l-1}{\log\log x}$.

Przypadek?

Przypadek?

Nie sądzę...

Wielomiany

Wielomiany

- każdy wielomian moniczny $f \in F_q[X]$ rozkłada się jednoznacznie na iloczyn wielomianów monicznych

$$f = P_1 \cdots P_k$$

Wielomiany

- każdy wielomian moniczny $f \in F_q[X]$ rozkłada się jednoznacznie na iloczyn wielomianów monicznych

$$f = P_1 \cdots P_k$$

- $deg(f) = deg(P_1) + \ldots + deg(P_k)$

Wielomiany

- każdy wielomian moniczny $f \in F_q[X]$ rozkłada się jednoznacznie na iloczyn wielomianów monicznych

$$f = P_1 \cdots P_k$$

- $deg(f) = deg(P_1) + \ldots + deg(P_k)$
- losowo wybrany wielomian moniczny stopnia n jest nierozkładalny z prawdopodobieństwem $\approx \frac{1}{n}$

Wielomiany

- każdy wielomian moniczny $f \in F_q[X]$ rozkłada się jednoznacznie na iloczyn wielomianów monicznych

$$f = P_1 \cdots P_k$$

- $deg(f) = deg(P_1) + \ldots + deg(P_k)$
- losowo wybrany wielomian moniczny stopnia n jest nierozkładalny z prawdopodobieństwem $\approx \frac{1}{n}$
- punkty $\{\log deg(P_1), \ldots, \log deg(P_k)\}$ są rozłożone poissonowsko w przedziale $[0, \log n]$.

Przejścia graniczne

Przejścia graniczne

- granica $n \to \infty$ (zwykle łączone z $\mathbb{Z}$)

Przejścia graniczne

- granica $n \to \infty$ (zwykle łączone z $\mathbb{Z}$)
- granica $q \to \infty$ (tego będziemy używać)

Idea

Powiązać struktury:

Idea

Powiązać struktury:

- permutacji z działaniem składania,

Idea

Powiązać struktury:

- permutacji z działaniem składania,
- wielomianów z działaniem mnożenia.

Istotne różnice

- nieprzemienne

- przemienne

Istotne różnice

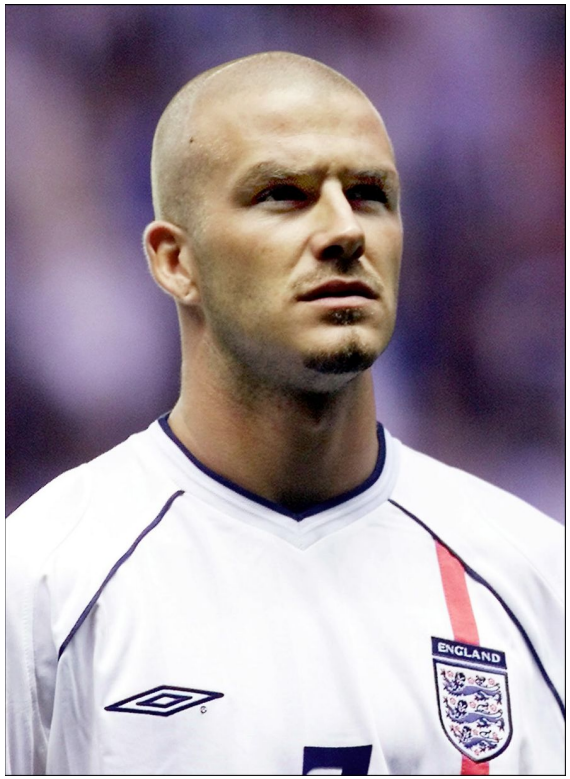
- nieprzemienne
- odwracalne

- przemienne
- nieodwracalne

Istotne różnice

- nieprzemienne
- odwracalne

- przemienne
- nieodwracalne



Wspólne środowisko

- dziedzina X; elementy stanowią częściowe permutacje, czyli pary (S, σ), gdzie $S \subset X$, σ - permutacja elementów S.

Wspólne środowisko

- dziedzina X; elementy stanowią częściowe permutacje, czyli pary (S, σ), gdzie $S \subset X$, σ - permutacja elementów S.
- „mnożenie” to rozłączna suma zbiorów S_1, S_2.

Wspólne środowisko

- dziedzina X; elementy stanowią częściowe permutacje, czyli pary (S, σ), gdzie $S \subset X$, σ - permutacja elementów S.
- „mnożenie" to rozłączna suma zbiorów S_1, S_2.
- „liczby pierwsze" $\mathcal{P}$ to pewien zbiór częściowych cykli.

Wspólne środowisko

- dziedzina X; elementy stanowią częściowe permutacje, czyli pary (S, σ), gdzie $S \subset X$, σ - permutacja elementów S.
- „mnożenie" to rozłączna suma zbiorów S_1, S_2.
- „liczby pierwsze" $\mathcal{P}$ to pewien zbiór częściowych cykli.
- „liczby naturalne" $\mathcal{N}$ to zbiór częściowych permutacji generowanych z $\mathcal{P}$ za pomocą mnożenia.

Uogólnione pojęcia

- $X = \{1, 2, \ldots, q\}$
- $X = \overline{\mathbb{F}_q}$

Uogólnione pojęcia

- $X = \{1, 2, \ldots, q\}$
- $\mathcal{P}$ - wszystkie częściowe cykle

- $X = \overline{\mathbb{F}_q}$
- $\mathcal{P}$ - obcięcia automorfizmu Frobeniusa $x \mapsto x^q$ do pojedynczych orbit (pierwiastki wielomianów nierozkładalnych nad $\mathbb{F}_q$).

Uogólnione pojęcia

- $X = \{1, 2, \ldots, q\}$
- $\mathcal{P}$ - wszystkie częściowe cykle
- $\mathcal{N}$ - wszystkie częsciowe permutacje

- $X = \overline{\mathbb{F}_q}$
- $\mathcal{P}$ - obcięcia automorfizmu Frobeniusa $x \mapsto x^q$ do pojedynczych orbit (pierwiastki wielomianów nierozkładalnych nad $\mathbb{F}_q$).
- $\mathcal{N}$ - obcięcia automorfizmu Frobeniusa $x \mapsto x^q$ do zbiorów niezmienniczych (pierwiastki wielomianów bezkwadratowych nad $\mathbb{F}_q$).

Uniwersalność

Twierdzenie

Niech $\mathcal{P}, \mathcal{N}$ będą rodzinami odpowiednio uogólnionych liczb pierwszych i naturalnych określonych na dziedzinie X (wszystko zależy od parametru q zbiegającego do nieskończoności). Przypuśćmy, że:

Uniwersalność

Twierdzenie

Niech $\mathcal{P}, \mathcal{N}$ będą rodzinami odpowiednio uogólnionych liczb pierwszych i naturalnych określonych na dziedzinie X (wszystko zależy od parametru q zbiegającego do nieskończoności). Przypuśćmy, że:

- *dla dowolnych m, n (przy $q \to \infty$) zbiory $\mathcal{N}_m, \mathcal{N}_n, \mathcal{N}_{m+n}$ są niepuste i*

$$|\mathcal{N}_{m+n}| = (1 + o(1))|\mathcal{N}_m||\mathcal{N}_n|.$$

Uniwersalność

Twierdzenie

Niech $\mathcal{P}, \mathcal{N}$ będą rodzinami odpowiednio uogólnionych liczb pierwszych i naturalnych określonych na dziedzinie X (wszystko zależy od parametru q zbiegającego do nieskończoności). Przypuśćmy, że:

- *dla dowolnych m, n (przy $q \to \infty$) zbiory $\mathcal{N}_m, \mathcal{N}_n, \mathcal{N}_{m+n}$ są niepuste i*

$$|\mathcal{N}_{m+n}| = (1 + o(1))|\mathcal{N}_m||\mathcal{N}_n|.$$

- *tylko $o(|\mathcal{N}_m||\mathcal{N}_n|)$ par $(\sigma_1, \sigma_2) \in \mathcal{N}_m \times \mathcal{N}_n$ ma przecinające się nośniki.*

Uniwersalność

Twierdzenie

Niech $\mathcal{P}, \mathcal{N}$ będą rodzinami odpowiednio uogólnionych liczb pierwszych i naturalnych określonych na dziedzinie X (wszystko zależy od parametru q zbiegającego do nieskończoności). Przypuśćmy, że:

- *dla dowolnych m, n (przy $q \to \infty$) zbiory $\mathcal{N}_m, \mathcal{N}_n, \mathcal{N}_{m+n}$ są niepuste i*

$$|\mathcal{N}_{m+n}| = (1 + o(1))|\mathcal{N}_m||\mathcal{N}_n|.$$

- *tylko $o(|\mathcal{N}_m||\mathcal{N}_n|)$ par $(\sigma_1, \sigma_2) \in \mathcal{N}_m \times \mathcal{N}_n$ ma przecinające się nośniki.*

Wówczas istnieje uniwersalna granica (niezależna od $\mathcal{P}, \mathcal{N}, X$), do której dla $q \to \infty$ zbiega rozkład podziałów losowej uogólnionej liczby całkowitej z $\mathcal{N}_n$.

Wielomiany względnie pierwsze

Twierdzenie

- *Losowy wielomian* $f \in \mathbb{F}_q[T]$ *stopnia* n *jest bezkwadratowy z prawdopodobieństwem* $1 - o(1)$ *(dla* $q \to \infty$*).*
- *Losowe wielomiany* $f, g \in \mathbb{F}_q[T]$ *stopni* m, n *są względnie pierwsze z prawdopodobieństwem* $1 - o(1)$ *(dla* $q \to \infty$*).*

Dlaczego nie można powtórzyć tego rozumowania dla $\mathbb{Z}$?

Dlaczego nie można powtórzyć tego rozumowania dla $\mathbb{Z}$?

Potrzebowaliśmy

- granicy $q \to \infty$,
- automorfizmu Frobeniusa,

które nie mają odpowiedników w ciałach liczbowych.

Hipoteza Riemanna

Twierdzenie

Liczba permutacji $\sigma \in S_n$, *które są cyklami*

$$\frac{1}{n} n!$$

Twierdzenie

Liczba monicznych wielomianów nierozkładalnych $f \in \mathbb{F}_{p^n}$ *stopnia* d

$$\frac{1}{n} p^n + O(p^{\frac{n}{2}})$$

Hipoteza

Liczba liczb pierwszych mniejszych niż x

$$Li(x) + O(\sqrt{x} \log x)$$

Nowe wyniki

Twierdzenie (Arratia--Barbour-Tavaré, 1992)

Można wskazać zmienną losową $(\vec{C}, \vec{Z})$ *o tej własności, że pierwsza współrzędna ma rozkład odpowiadający liczbom cykli o danych długościach w rozkładzie na cykle losowej permutacji, druga współrzędna ma rozkład odpowiadający n niezależnym zmiennym o rozkładach Poissona z parametrami* $\frac{1}{i}$ $(i = 1, \ldots, n)$ *oraz średnia odległość pomiędzy współrzędnymi to* $2 + o(1)$.

Twierdzenie (Arratia,2013)

Można wskazać zmienną losową $(\vec{C}, \vec{Z})$ *o tej własności, że piewsza współrzędna ma rozkład odpowiadający krotnościom liczb pierwszych w rozkładzie losowej liczby całkowitej, druga współrzędna ma rozkład odpowiadający niezależnym zmiennym o rozkładach Poissona z parametrami* $\frac{1}{p}$ $(p \leqslant n$ *pierwsze) oraz średnia odległość pomiędzy współrzędnymi to* $2 + o(1)$.

Nowe wyniki

Twierdzenie (Eberhard-Ford-Green, 2015)

Losowa permutacja $\sigma \in S_n$ ma zbiór niezmienniczy wielkości k z prawdopodobieństwem $\asymp k^{-\delta}(1+\log k)^{-\frac{3}{2}}$, gdzie $\delta = 1 - \frac{1+\log\log 2}{\log 2}$.

Twierdzenie (Ford, 2008)

Losowa liczba z przedziału $[e^n, e^{n+1}]$ ma dzielnik w przedziale $[e^k, e^{k+1}]$ z prawdopodobieństwem $\asymp k^{-\delta}(1+\log k)^{-\frac{3}{2}}$, gdzie $\delta = 1 - \frac{1+\log\log 2}{\log 2}$.

Źródła

T. Tao, Cycles of a random permutation, and irreducible factors of a random polynomial, *What's new* https://terrytao.wordpress.com.

What's new

Updates on my research and expository papers, discussion of open problems, and other maths-related topics. By Terence Tao

Subscribe to feed | Home | About | Career advice | On writing | Books | Applets

RECENT COMMENTS

adityaguharoy on IMO 2009 Q6 mini-polymath proj...

KM on Polymath15, ninth thread: goin...

Anonymous on 1% quasimorphisms and group...

Allan van Hulst on 1% quasimorphisms and group...

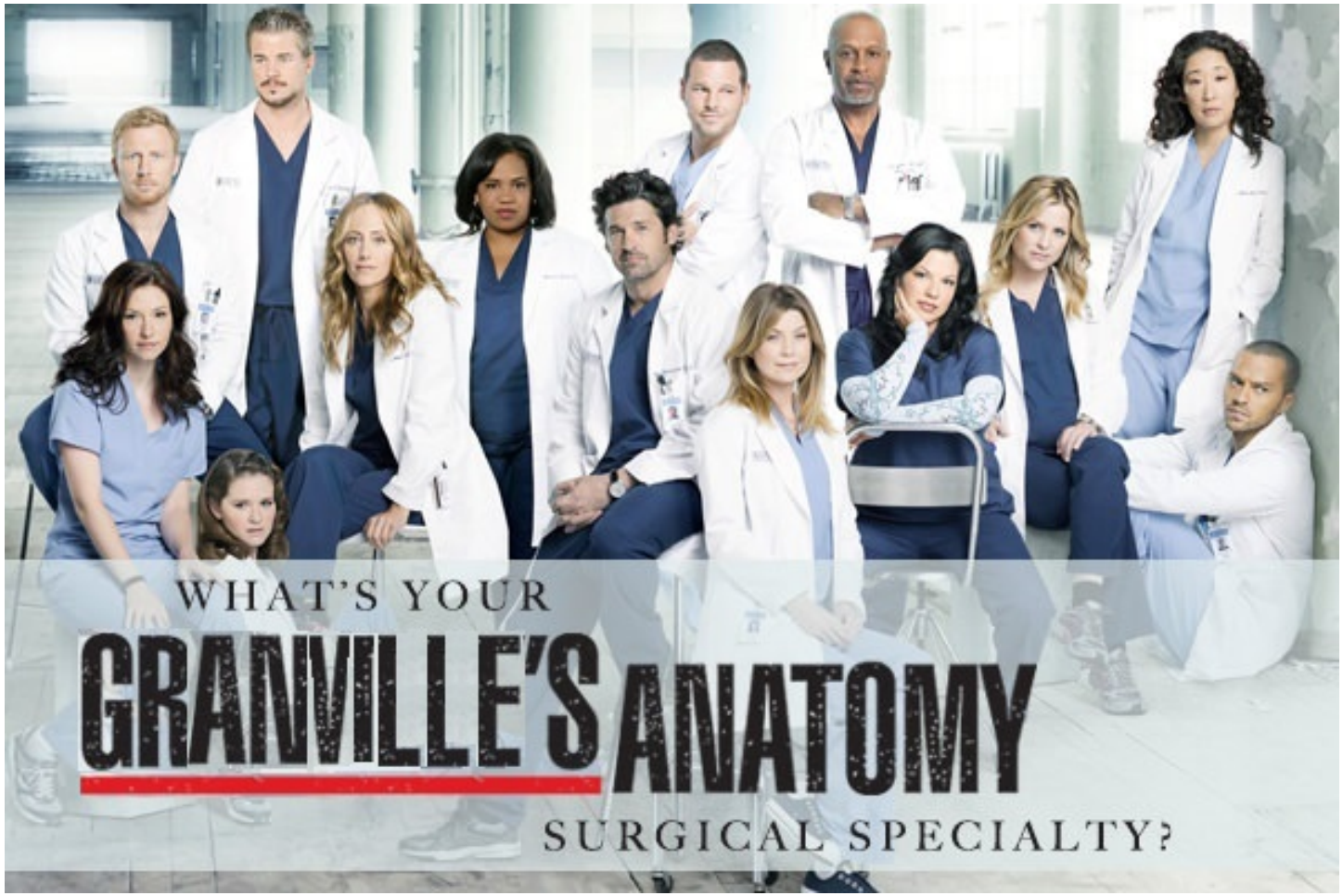
Cycles of a random permutation, and irreducible factors of a random polynomial

15 July, 2015 in expository, math.CO, math.NT, math.PR | Tags: finite fields, permutations, prime number theorem

In analytic number theory, there is a well known analogy between the prime factorisation of a large integer, and the cycle decomposition of a large permutation; this analogy is central to the topic of "anatomy of the integers", as discussed for instance in this survey article of Granville. Consider for instance the following two parallel lists of facts (stated somewhat informally). Firstly, some

Źródła

A. Granville, The Anatomy of Integers and Permutations, preprint.



Dziękuję za uwagę.