УДК 378.016:[519.6+004.43]
DOI:10.17853/2587-6910-2022-06-82-88

ЭКСПЕРИМЕНТАЛЬНАЯ МАТЕМАТИКА И ЯЗЫК JULIA — ЛОКАЛЬНОЕ РАСПРЕДЕЛЕНИЕ ПРОСТЫХ ЧИСЕЛ*

EXPERIMENTAL MATHEMATICS AND LANGUAGE JULIA – LOCAL DISTRIBUTION OF PRIME NUMBERS

Александр Викторович Рожков
доктор физико-математических наук, профессор
great.ros.marine2@gmail.com
ФГБОУ ВО «Кубанский государственный университет», Россия, Краснодар

Alexander Viktorovich Rozhkov
Kuban State University, Russia, Krasnodar

Александра Сергеевна Барсукова
магистрант факультета математики и компьютерных наук
great.ros.marine2@gmail.com
ФГБОУ ВО «Кубанский государственный университет», Россия, Краснодар

Alexandra Sergeevna Barsukova
Kuban State University, Russia, Krasnodar

Аннотация. *Научно-методическая инициатива по обучению математике и информатике, реализуемая в КубГУ с 2015 г. Поддержана Благотворительным фондом Владимира Потанина. В данной статье исследуется локальное распределение простых чисел.*

Abstract. *The scientific and methodical initiative of training in mathematics and informatics realized in KUBSU since 2015. Supported by the Vladimir Potanin Charitable Foundation. In this article, the local distribution of prime numbers is investigated.*

Ключевые слова: *Теория чисел, язык программирования Julia, функция Эйлера, локальное распределение простых чисел.*

Keywords: *Number theory, Julia programming language, Euler's function, local distribution of prime numbers.*

Цель проекта — проведение сочетание обучения математики и информатике на базе проведения разведочных вычислений в области нерешенных проблем алгебры и теории чисел. Частичные итоги проделанной работы представлены в [3]. В данной статье речь идет о локальном распределении простых чисел.

Введение

Формула для нахождения простых чисел до сих пор не найдена. Проблема глобального распределения простых чисел решена вполне удовлетворительно.

Пусть $\pi(\mathrm{n})$ — количество простых чисел, не превосходящих n, тогда

$$\pi(\mathrm{n}) \approx \frac{n}{\ln(\mathrm{n})}.$$

Гипотезу о распределении простых чисел К.Ф. Гаусс (1777–1855), опираясь на свои ручные вычисления, выдвинул в возрасте 17. Впервые строго доказал П. Л. Чебышев (1821–1894) в 1851 г.

Гаусс не чурался черновой вычислительной работы. В своём письме к астроному Энке Гаусс описывает, как он «очень часто употреблял свободные четверть часа, чтобы то там, то здесь просчитать хилиаду» (т. е. интервал в 1000 чисел), и так до тех пор, пока он не нашёл, наконец, все простые числа, меньшие трёх миллионов. Сегодня домашнему компьютеру на это требуется меньше секунды.

Найдем все простые числа до 3 млн. средствами языка Julia —официальный сайт https://julialang.org/. Язык свободно распространяемый, ориентирован на математические, в том числе параллельные и распределенные вычисления. Язык динамический, но компилируемый, и быстрый как C. Допускает подключение кода на языках C/C++, FORTRAN, Python, имеет 7 тыс. расширяющих пакетов, каждые сутки добавляется 3–4 новых пакета. Используется, как учебное средство, примерно в 2–тысячах университетов мира. В России в МГУ, МИФИ, КубГУ.

На рис. 1 приведен код программы на языке Julia по поиску простых чисел до 3 млн.

```
julia> using Nemo
Welcome to Nemo version
0.29.1
Nemo comes with absolutely no
warranty whatsoever
julia> function Ros(m,n)
          N = 1
             for i= m:n
                   if
isprobable_prime(ZZ(2*i+1))
                N+=1
          end
          end
               print(N)
          end
Ros (generic function with
1 method)
julia> @time Ros(1,15*10^5)
216816  0.521483 seconds
1.51 M allocations:
23.168 MiB
```

Рис. 1. Код программы поиска простых чисел до 3 млн

Мы подключили алгебраический пакет Nemo и использовали макрос `@time` для выяснения сколько времени и памяти займет вычисление. Итого простых чисел до 3 млн. 216816. Вычисления заняли примерно 0,5 сек. Памяти было занято 1,5 Мб. Гауссу, даже если он проверял на простоту тысячу чисел в час, при 8-часом рабочем дне потребовался бы целый год.

Обратим внимание на минималистичность синтаксиса языка Julia — нет знаков препинания и все циклы завершаются командой end.

Числа близнецы и их обобщения

Формула

$$\pi(n) \approx \frac{n}{\ln(n)}$$

дает распределение простых чисел в целом на числовой прямой, но не на конкретном отрезке или интервале. То есть формула ничего не говорит о локальном распределении простых

чисел. Однако именно локальное распределение важно для практики, в особенности для нужд криптографии. Сейчас в криптографии часто используются 1024 битные простые числа. Поскольку $2^{1024} \approx 10^{300}$, $\ln(10^{300}) = 300 \cdot \ln(10) \approx 700$, то это 300-значные числа в десятичной записи и простыми из них являются, в среднем, каждое 700-е число. Такое расположение простых чисел называется общим или стандартным. Именно оно является наилучшим для криптографических целей.

Однако, простые числа распложены на прямой очень неравномерно. Есть их сгущения, где их много и отрезки где простых чисел нет. Выясним вопрос каковы наиболее плотные скопления простых чисел.

Напомним некоторые общеизвестные определения.

Пары простых чисел вида *(p, p+2)* — называются ***близнецами***.

Тройки простых чисел *(p, p+2, p+6)* и *(p, p+4, p+6)* называются левыми и правыми ***триплетами*.**

Четверки простых чисел вида *(p, p+2, p+6, p+8)* называются ***сдвоенными близнецами.***

В пределах первых четырех тысяч натуральных чисел 10 сдвоенных близнецов:
(5, 7, 11, 13), (11, 13, 17, 19), (101, 103, 107, 109), (191, 193, 197, 199), (821, 823, 827, 829), (1481, 1483, 1487, 1489), (1871, 1873, 1877, 1879), (2081, 2083, 2087, 2089), (3251, 3253, 3257, 3259), (3461, 3463, 3467, 3469).

Пятерки и шестерки простых чисел и т. д.

Близнецы, триплеты и сдвоенные близнецы — это наиболее плотно расположенные двойки, тройки и четверки подряд идущих простых чисел.

Если расположить 4 числа на отрезке длины 6, то мы получим *(p, p+2, p+4,p+6)* . Здесь есть три подряд идущих нечетных числа, одно из них обязательно делится на 3, значит одно из чисел в четверке не будет простым. Это нам подсказывает идею как находить наиболее плотно расположенные, 5-ки, 6-ки и. т. д.

Пятерки простых чисел. Среди чисел *(p, p+2, p+4, p+6, p+8, p+10)* никакие пять чисел не могут быть простыми, т.к. какое бы число мы не выбросили среди оставшихся 5-ти будет три подряд идущих нечетных числа, а значит хотя бы одно из них обязательно будет делиться на 3.

Поэтому наименьший отрезок, который может содержать 5 подряд идущих простых чисел, имеет вид [*p, p+2, p+4, p+6, p+8, p+10, p+12*]. Составим таблицу 1.

Таблица 1

Остатков от деления на 3 чисел 0, 2, …, 12

	0	**2**	**4**	**6**	**8**	**10**	**12**
3	0	2	1	0	2	1	0

Поскольку границы отрезка — числа *p* и *p+12* обязательно входят в пятерку простых чисел, а их остатки от деления на 3 равны 0, то для того, чтобы три внутренних числа были простыми, нужно чтобы их остатки от деления принадлежали множеству {0, 2} или {0, 1}.

В первом случае получаем пятерку виду *(p, p+2, p+6, p+8, p+12)* .

Во втором случае получаем пятерку *(p, p+4, p+6, p+10, p+12)* .

Аналогично рассуждая получим единственную шестерку *(p, p+4, p+6, p+10, p+12, p+16*).

Семерки и т. д. Изложенный алгоритм универсален. Зная длину плотной n-ки начинаем увеличивать отрезок, в котором будет содержаться *(n+1)*-ка и проверяем остатки соответствующих чисел по простым модулям *3, 5, 7, …*

Нами была составлена программа для машинного вычисления и в течение несколько тысяч часов вычислены все плотные *n*-ки до *n=203* включительно.

Выяснилось, после настойчивого поиска в интернете, что гораздо ранее нас, используя суперкомпьютеры, американский профессор T. J. Engelsma еще в декабре 2009 г. вычислил структуру плотных *n*-к до $n = 4507$ включительно http://www.opertech.com/primes/k-tuples.html.

До $n = 203$ его и наши результаты полностью совпали.

Запись плотных *n*-к

Определение. *Множество из n подряд идущих простых чисел называется плотной n-кой, если они расположены на отрезке минимально возможной длины.*

Это определение не является оригинальным. Оно, независимо, формулировалось многими математиками. Сошлемся на известную работу, целиком посвященную плотным *n*-м, где они названы k-tuplet [1] и сайт https://primes.utm.edu/glossary/xpage/PrimeKTuplet.html.

Как люди селятся очень неравномерно — в мегаполисах, деревнях, хуторах, так и простые числа образуют разные уровни сгущения.

Мегаполисами простых чисел, с максимальной плотностью населения, являются плотные *n*-ки.

Условимся о некоторых обозначениях, упрощающих запись плотных n-к.

Поскольку четное число не может быть простым, то все четные числа внутри отрезка длины N внутри которого заключена плотная *n*-ка мы будем опускать. Если некоторое нечетное место занято простым числом, мы это пометим цифрой 1, а 0 будет означать отсутствие числа.

В этих обозначениях упомянутые выше близнецы, триплеты и сдвоенные близнецы примут вид (шаблон)

2-ки: (1,1).

3-ки: (1,1,0,1); (1,0,1,1).

4-ки: (1,1,0,1,1).

Приведем также вид плотных *n*-к до n=8 включительно.

5-ки: (1,1,0,1,1,0,1); (1,0,1,1,0,1,1).

6-ка: (1,0,1,1,0,1,1,0,1).

7-ки: (1,1,0,0,1,0,1,1,0,1,1); (1,1,0,1,1,0,1,0,0,1,1).

8-ки: (1,0,0,1,1,0,0,1,0,1,1,0,1,1);

(1,1,0,1,0,0,1,1,0,0,1,0,1,1);

(1,1,0,1,1,0,1,0,0,1,1,0,0,1).

Как мы видим плотные n-ки могут иметь несколько различных структур, например, при n = 105 разных структур 248.

Плотные *n*-ки важны для криптографии, а также могут помочь опровергнуть известную гипотезу.

Вторая гипотеза Харди-Литллвуда. *Пусть* $\pi(n)$ *— число простых чисел, не превосходящих n, тогда верно неравенство* $\pi(x + y) \leq \pi(x) + \pi(y)$.

Гипотеза утверждает, что чем дальше от начала координат, тем плотность распределения простых чисел меньше.

В настоящее время многие специалисты сомневаются в правильности этой гипотезы. Возможно есть где-то, очень далеко от начала координат, такой отрезок, на котором расположено больше простых чисел, чем на отрезке такой же длины в начале координат.

Профессор T. J. Engelsma в 2009 г. выяснил, что плотная 447-ка расположена на отрезке меньшей длины, чем отрезок, включающий первые 447 простых чисел.

Проблема в том, если подобная 447-ка из простых чисел и существует, то ее элементы являются примерно 900-значными числами в десятичной записи. До квантовых компьютеров их найти вряд ли получится, потому, что нужно перебирать все числа подряд.

Поиск плотных *n*-к

Поиск плотных *n*-к по шаблону вычислительно емкая задача. Как показала практика минимальные примеры *n*-к растут очень быстро. Увеличение *n* на 1 увеличивает минимальный пример *(n+1)*-ки примерно в 100 раз, на два порядка.

Отметим, что в настоящее время, январь 2022 г. http://www.pzktupel.de/ktuplets найдены всего пять 21-ки и ни одной 22-ки.

Программ поиска плотных *n*-к по шаблону *M* состоит из 3 подпрограмм: Rem, All, T.

В Rem мы выбираем вид чисел, которые претендуют на то, что они породят плотную *n*-ку. Это уменьшает число претендентов в тыс., млн., млрд., трлн. и т. д. число раз, в зависимости от n и от модуля, по которому производится отбор претендентов.

Программа All — проверяет координаты вектора-претендента на простоту.

Программа T, используя предыдущие программы, проверяет весь натуральный ряд на наличие плотных *n*-к с шаблоном M. На рис. 2 приведен код этих программ.

```
julia> using Mods
julia> using Nemo
Welcome to Nemo version 0.29.1
Nemo comes with absolutely no warranty whatsoever
julia> function Rem(M,m)
       l=1; K=[1];D=[];S=[];
       Pprime =
[2,3,5,7,11,13,17,19,23,29,31,37,41,47,53,59,61,67,71,7
3];
       for i=1:m
       l= l*Pprime[i]
       L= M.% Pprime[i+1]
       L=sort(unique(L))
       L= setdiff(0:Pprime[i+1]-1,L)
            for j in L
                for k in K
                   d=crt(ZZ(k),ZZ(l),ZZ(Pprime[i+1]-
j),ZZ(Pprime[i+1]))
                      D=vcat(D,d)
       end
          end
       K=sort(unique(D))
           D=[]
                end
       S= [K,length(K),l*Pprime[m+1]]
        return(S)
       end
Rem (generic function with 1 method)

julia> function All(M,p)
       j = true
       for i in M
           if isprobable_prime(ZZ(p+i))
        j=true
              else j=false
       break;
          end
       end
        return j
       end
All (generic function with 1 method)

julia> function T(S,M,m,n)
         L=[];
       for q in m:n
            for   s in S[1]
                      t= s +S[3]*q
                   if All(M,t)
                      println(t,",")
                      L=vcat(L,t)
                   end
             end
        end
        return(L)
       end
T (generic function with 1 method)
```

Рис. 2. Код трех программ по поиску плотных n-к

Как показали наши исследования. Для каждого n множество *n*-к симметрично, для каждой *n*-ки есть, симметричная ей.

Кроме того каждая *n*-ка содержит в себе по нескольку *m*-к при $m<n$.

Мы ниже, рис. 3, приводим пример графа вложений плотных n-к для $n<25$. Это граф частично упорядоченного множества, у которого соединены ребрами только соседние элементы.

Гипотеза. *Группа автоморфизмов графа вложений плотных n-к — это элементарная абелева 2-группа.*

В нашем случае группа имеет порядок 32, т. е. это Z_2^5.

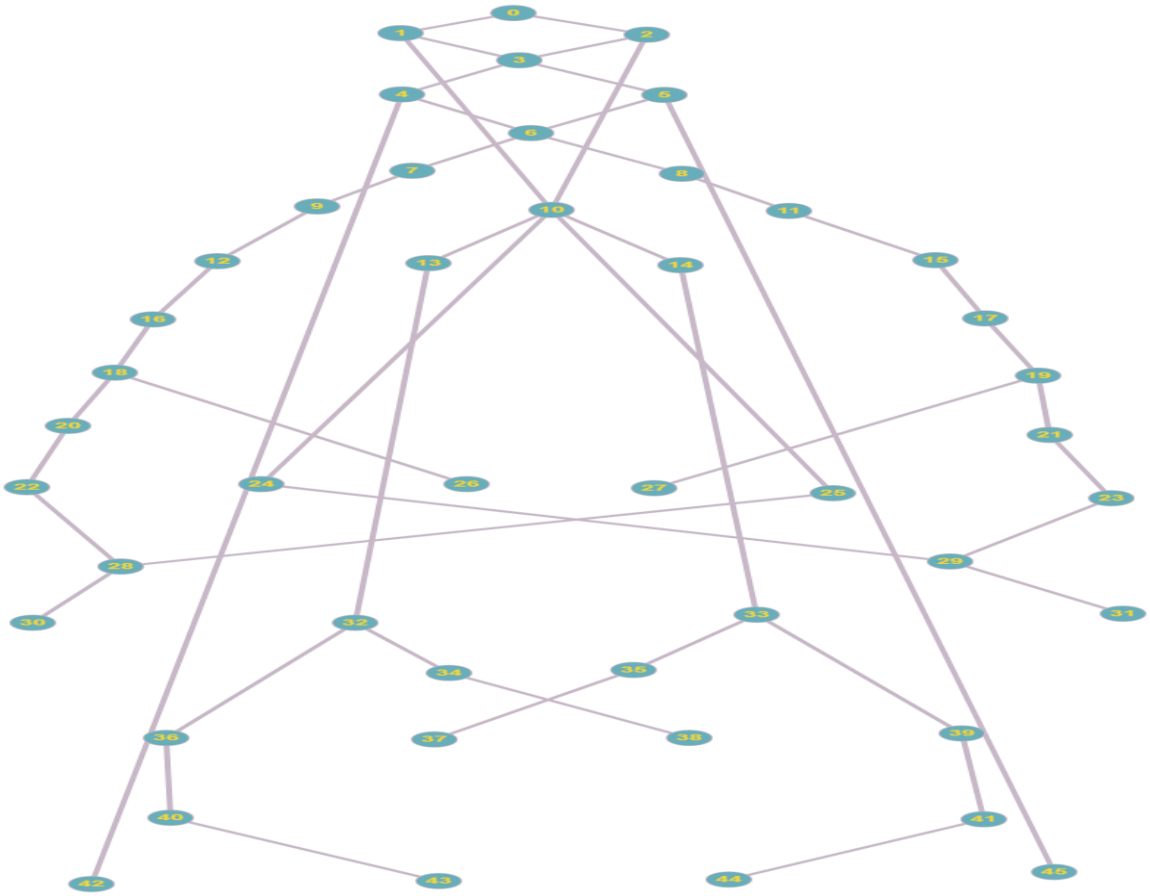

Рис. 3. Граф вложений плотных n-к для n<25

Исследование плотных n-к подсказывает как можно формализовать идею, что локально простые числа расположены «случайным образом». Один из вариантов формализации этого предположения следующая гипотеза.

Геленджикская гипотеза [2]. Пусть n — натуральное число, зафиксируем его. Пусть A — множество четных чисел, содержащее 0, из отрезка $[0, 2n]$, но не содержащее полной системы вычетов ни по какому нечетному простому модулю $q < 2n$.

Тогда существует бесконечно много простых чисел p, таких, что:

а) все числа $\{p+a \mid a \in A\}$, являются простыми (слабая гипотеза);

б) кроме того, все остальные числа отрезка $[p, p+2n]$ составные (сильная гипотеза).

Гипотеза обобщает много предположений на тему простых чисел. Она нетривиальна даже в случае, когда множество A одноэлементно.

Например, если $n = 0$ и $A = \{0\}$, то слабая гипотеза означает, что простых чисел бесконечно много, что, конечно, верно. Если $n > 0$ и $A = \{0\}$, то сильная гипотеза означает, что существует бесконечно много простых чисел правее которых расположено не менее $2n$ подряд идущих составных чисел.

Если A — это структура плотной n-ки, то сильная и слабая гипотеза совпадают и означают, что число плотных n-к любой структуры бесконечно, в частности не верна вторая гипотеза Харди-Литлвуда.

Планомерное изучение частных случаев этой гипотезы — одно из направлений исследований, проводимых в КубГУ в области экспериментальной теории чисел.

** Проект реализуется победителем Конкурса на предоставление грантов преподавателям магистратуры благотворительной программы «Стипендиальная программа Владимира Потанина» Благотворительного фонда Владимира Потанина*

Список литературы

1. *Forbes, T.* Prime clusters and Cunningham chains / Tony Forbes. Text: electronic // Mathtmatics of Computation. 1999. Vol. 68, iss. 228. P. 1739–1747. URL: https://www.ams.org/journals/mcom/1999-68-228/S0025-5718-99-01117-5/S0025-5718-99-01117-5.pdf.

2. *Рожков, А. В.* Автоморфизмы графа вложений сгущений простых чисел / А. В. Рожков, Н. В. Потапова. Текст: непосредственный // Теория групп и ее приложения: материалы XII международной школы конференции по теории групп, посвященной 65-летию А. А. Махнева. Краснодар: Кубан. гос. ун-т, 2018. С. 132–136.

3. *Рожков, А. В.* Экспериментальная математика в КубГУ – первые результаты чисел / А. В. Рожков. Текст: непосредственный // Наука. Информатизация. Технологии. Образование: материалы XIV международной научно-практической конференции, Екатеринбург, 1–5 марта 2021 г. Екатеринбург: Рос. гос. проф.-пед. ун-т, 2021. С. 163–172.