УДК 519.688, 511.174

ПЛОТНЫЕ N-КИ И ИХ ВЫЧИСЛЕНИЕ

А. Большаков[1], А. Тимофеев[2], А.В. Рожков[3]

1 *aleksiosroller@mail.ru*; Кубанский государственный университет
2 *caesar147@mail.ru*; Кубанский государственный университет
3 *ros.seminar@bk.ru*; Кубанский государственный университет

Изучаются сгущения простых чисел — их количество, расположение на прямой, указываются их приложения для теории чисел и криптографии.

Ключевые слова: теория чисел, пакеты компьютерной алгебры, числа близнецы, простые числа.

Введение

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

Определение независимо введено в работах [1], [2]. Возможно это не единственные и не первые работы, где это очень естественное понятие определено. Плотная n-ка - это обобщение хорошо известных близнецов, т.е. простых чисел вида $(p, p+2)$, триплетов — простых чисел вида $(p, p+2, p+6)$ и $(p, p+4, p+6)$, сдвоенных близнецов — $(p, p+2, p+6, p+8)$.

Таким образом плотная n-ка или k-tuples [1] — это n чисел по модулю N (N — длина отрезка, внутри которого эти n чисел расположены), которые не образуют полной системы вычетов ни по одному простому числу $p \leq N$.

В силу того, что вычисления приходится вести по все возрастающему числу простых модулей — нахождение структуры n-к весьма трудоемкая задача

Следует отметить, что зная структуру плотной n-ки мы знаем только то, что если она существует, то имеет именно такой вид, но существование “живой” n-ки не гарантировано.

Ниже мы перечисляем некоторые плотные n-ки и указываем минимальное значение p, с которых эти n-ки начинаются. Условимся в записи n-ки символ p писать только вначале.

```
5-ки:    (p,2,6,8,12),                      p = 1481;
         (p,4,6,10,12),                     p = 1867.
6-ка:    (p,4,6,10,12,16),                  p = 97.
7-ки:    (p, 2,8,12,14,18,20),              p = 5 639;
         (p, 2,6,8,12,18,20),               p = 165 701.
8-ки:    (p,6,8,14,18,20,24,26),            p = 88 793;
         (p,2,6,12,14,20,24,26),            p = 1 277;
         (p,2,6,8,12,18,20,26),             p=  15 760 091.
9-ки:    (p,4,10,12,18,22,24,28,30),        p = 74 266 249;
         (p,2,6,8,12,18,20,26,30),          p = 226 449 521;
         (p,4,6,10,16,18,24,28,30),         p = 113 143;
         (p,2,6,12,14,20,24,26,30),         p = 113 147.
```

Нахождение плотных n-к

В процессе вычислений были использованы идеи и методология, изложенная в работах [1], [2]. Вычисления производились с использованием пакета компьютерной алгебры gap 4.8.8. официальный адрес http://www.gap-system.org/

Зная структуру n-ки трудной задачей является непосредственное нахождение "живой n-ки" данной структуры. Эта задача легко поддается распараллеливанию - натуральный ряд разбивается на отрезки и на каждом из них ищется n-ка данной структуры. Используя около 20 компьютеров в 2013 г. нам удалось найти первую 14-ку, она оказалась 17-ти значной. Наименьшая 15-ка имеет 19 знаков, 16-ка - 21 знак, 17-ка 23 знака, 18-ка 25 знаков, 19-ка 27 знаков, 20-ка 29 знаков, первая 20-ка была найдена только в 2015 г. и самая маленькая 21-ка имеет тоже 29 знаков. В настоящее время 21-к найдено всего 3 штуки. В тоже время 22-к еще не найдено ни одной! Ознакомиться с последними достижениями в этой области можно по адресу https://sites.google.com/site/anthonydforbes/ktuplets.htm?attredirects=0

Вот основная программа по вычислению "живой" n-ки. Здесь две вспомогательные подпрограммы:

Rem — находит всех претендентов на число p — начало плотной n-ки, имеющей структуру M и претенденты выбраны по модулю — произведения всех первых m простых чисел.

All — проверяет, что все элементы n-ки со структурой M состоит из простых чисел.

Основная программа $T(S, M, m, n)$ использует эти программы на разных промежутках натурального ряда, а именно на промежутке (m, n).

```
Rem:=function(M,m)
local i,j,k,l,d,D,K,L,S;
l:=1; L:=[]; K:=[1]; D:=[]; S:=[];
for i in [1..m] do
l:= l*Primes[i];
L:= M mod Primes[i+1];
L:= Set(L);
L:= Difference([0..Primes[i+1]-1],L);
    for j in L do
        for k in K do
           d:=ChineseRem([l,Primes[i+1]],[k,Primes[i+1]-j]);
           Add(D,d);
od;
   od;
K:=Set(D);D:=[];
od;
S[1]:=K;
S[2]:=Length(K);
S[3]:=l*Primes[m+1];
 return(S);
end;
S:=Rem(M,m);;
```

```
All:=function(M,p)
local i,j,l;
for i in M do
    if IsProbablyPrimeInt(p+i) then  j:=true;
       else j:=false; break;
    fi;
od;
 return j;
end;

T:=function(S,M,m,n)
local t,q,s,l,L;
L:=[];
for  q in [m..n] do
    for  s in S[1] do t:= s +S[3]*q;
       if All(M,t) then
           Print(t,"\n");
           Add(L,t);
       fi;
   od;
od;

   return(L);
end;
```

Простые числа вездесущи в математике, особенно в криптографии [3]. Почти любой криптографический алгоритм начинается словами: “Пусть p – случайное простое число”. Число должно быть случайным и очень желательно расположенным в “общем положении”. Но если простое число оказалось принадлежащим, например, плотной 10-ке, то его положение окажется совсем не общим. В самом деле, рассмотрим типичное “криптографическое число”, содержащее 300 десятичных знаков. Согласно закону распределения простых чисел в районе 300-х значных чисел простым будет примерно каждое 700-е число. В тоже время в плотной 10-ке простым будет каждое 4-е число! Поэтому если мы случайно выбрали простое число из плотной n-ки, то его криптографическая ценность становится сомнительной.

Приложение из области абстрактной математики. Хорошо известна гипотеза Харди-Литлвуда, о том, что с удалением от начала координат локальная (а не только глобальная по закону П.Л. Чебышева) плотность распределения простых чисел уменьшается. Тем не менее, в плотной 447-ке плотность расположения простых чисел выше, чем в начале координат (см. http://www.opertech.com/primes/k-tuples.html). Проблема в том, что если плотная 447-ка и существует, то минимальный элемент в ней, возможно, имеет не менее 900 знаков в десятичной записи, поэтому нахождение ее до изобретения квантовых компьютеров весьма сомнительно.

Выводы

Даже не имея суперкомпьютеров исследовать плотные n-ки имеет смысл, и, более того, необходимо. Упомянутые выше вычислители занимаются рекордами, ищут все более и более многозначные n-ки, не интересуясь устройством этих сгущений простых чисел $\frac{n}{n!}$. показали, что даже в пределах до 10^{12} плотных 6-к примерно в 20 раз больше, чем предсказывает глобальный закон распределения простых чисел. Плотных 7-к в 100 раз больше, плотных 8-к в 1000 раз, плотных 9-к в 4000 раз больше, плотных 10-к в 5 тыс. раз и т.д.

Следует отметить, что пропорции количества реальных n-к к предсказанных глобальным законом распределения сохраняется на всех интервалах, которые нам удалось проверить от 10^6 до 10^{15} это рождает надежду, что подобное отношение является законом, а не эффектом начала координат.

Распределение плотных n-к – неких городов для простых чисел, может быть ключом для понимания законов локального распределения простых чисел, что очень важно и для теории чисел и для криптографии.

Литература

1. Forbes T. *Prime clusters and Cunningham chains* // Math. Comp. – 1999. – V. 68, tom 228. – P. 1739–1747.

2. Рожков А.В., Рожкова М.В. *Локальная плотность множества простых чисел и апериодические коды* // Наука ЮУрГУ: Материалы 64-й научной конф. Секция техн. наук. – Челябинск: Изд-во ЮурГУ, 2012. – С. 86-90.

3. Рожков А.В. *Стратегия DPS - Debian-Python-Sage: Проблемно-ориентированные вычислительные среды на открытом коде* // Труды V междунар. науч.-практич. Конф. «Информационные технологии в образовании и науке» (ИТОН – 2016). – Казань: КФУ, 2016. – С. 172–179.

4. Рожков А.В., Рожкова М.В. *Экспериментальная (вычислительная) теория чисел* // Новые информационные технологии в образовании и науке: Материалы X межд. науч.-практ. конф., Екатеринбург, 27 февраля – 3 марта 2017 г. ФГАОУ ВО «Рос. гос. проф.-пед. ун-т». – Екатеринбург, 2017. – С. 413–417.

5. Рожков А.В., Ниссельбаум О.В. *Теоретико-числовые методы в криптографии*. – Тюмень: ТюмГУ, 2007. – 160 с.

DENSE K-TUPLES AND THEIR CALCULATION

A. Bolchakov, A. Timofeev, A.V. Rozhkov

Condensations of prime numbers — their quantity, the arrangement on the straight line are studied, their appendices for the number theory and cryptography are specified.

Keywords: number theory, packages of computer algebra, number twins, prime numbers.