УДК 519.688, 511.174

СТРУКТУРА ПЛОТНЫХ N-К И ЕЕ 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 — $(p, p+2, p+6, p+8)$. Дальнейшее построение плотных n-к нужно производить по индукции.

Алгоритм построения плотных n-к.

Пусть плотные n-ки уже построены построим $(n+1)$-ки. Допустим плотные n-ки разместились на отрезке $[p, p+2, \cdot, p+2k]$ длины $k+1$.

Рассматриваем отрезок $[p, p+2, \ldots, p+2k, p+2(k+1)]$ длины $k+2$.

Этап делителя 3. Рассматриваем числа $0, 2, 4, \ldots, 2(k+1)$ по модулю 3. Тут возможны два варианта. Число $k+1$ делится на 3.

Тогда у нас два подварианта. Из серединных чисел от 2 до $2k$ оставляем те, чей остаток от деления на 3 равен 1. Из серединных чисел оставляем те, что имеют остаток 2.

Если число $k+1$ не делится 3, то из серединных чисел оставляем те, что имеют остаток от деления на 3 равный 0 или $k+1$. На этом этап тройки завершен. Оставшиеся числа не образуют полную систему вычетов по модулю 3, и при правильном выборе начального числа p ни одно из них не будет делиться на 3.

Этап делителя 5. Получившиеся на предыдущем этапе числа рассматриваем по модулю 5. Пусть $S = \{0, 1, 2, 3, 4\} \backslash \{0, k+1 \mod 5\}$. Берем s из S и вычеркиваем все числа, имеющие остаток s, а остальные не трогаем. Так у нас возникнет 3 или 4 варианта. Этот этап нам гарантирует, что числа не будут делиться на 5, при соответствующем выборе числа p.

Этап делителя 7. К каждому варианту предыдущего этапа применяем тот же метод, что и на этапе делителя 5, только заменяем 5 на 7 и т.д. Вычеркивания производим до тех пор, пока у нас не останется ровно $n+1$ число, а последним этапом делителя будет максимальное простое число, не превосходящее число $n+1$. При

этом на некотором этапе может оказаться, что все оставшиеся числа делятся на текущий делитель. Тогда мы переходим к отрезку длины $k+3$ и повторяем процедуру. **Алгоритм** завершен.

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 образую 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

Вложение плотных n-к друг в друга

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/

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 близницы, триплеты и сдвоенные близнецы примут вид

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=15 включительно. Отметим, что в настоящее время, октябрь 2017 г. найдены всего три 21-ки и ни одной 22-ки.

```
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).
9-ки:       (1,0,1,0,0,1,1,0,0,1,0,1,1,0,1,1);
            (1,1,0,1,1,0,1,0,0,1,1,0,0,1,0,1);
            (1,0,1,1,0,1,0,0,1,1,0,0,1,0,1,1);
            (1,1,0,1,0,0,1,1,0,0,1,0,1,1,0,1).
10-ка:      (1,0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0,1).
11-ки:      (1,0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0,1,1);
            (1,1,0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0,1).
12-ки:      (1,0,0,1,0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0,1,1);
            (1,1,0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0,1,0,0,1).
13-ки:      (1,1,0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0,1,0,0,1,0,0,1);
            (1,0,0,1,0,0,1,0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0,1,1);
            (1,1,0,0,0,0,1,1,0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0,1);
            (1,0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0,1,1,0,0,0,0,1,1);
            (1,1,0,0,1,0,0,1,0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0,1);
```

```
            (1,0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0,1,0,0,1,0,0,1,1).
14-ки:      (1,1,0,0,1,0,0,1,0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0,1,1);
            (1,1,0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0,1,0,0,1,0,0,1,1)
15-ки:      (1,0,0,1,1,0,0,1,0,0,1,0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0,1,1);
            (1,1,0,1,0,0,1,1,0,0,1,0,0,1,0,1,1,0,1,0,0,1,1,0,0,1,0,1,1);
            (1,1,0,1,0,0,1,1,0,0,1,0,1,1,0,1,0,0,1,0,0,1,1,0,0,1,0,1,1);
            (1,1,0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0,1,0,0,1,0,0,1,1,0,0,1).
```

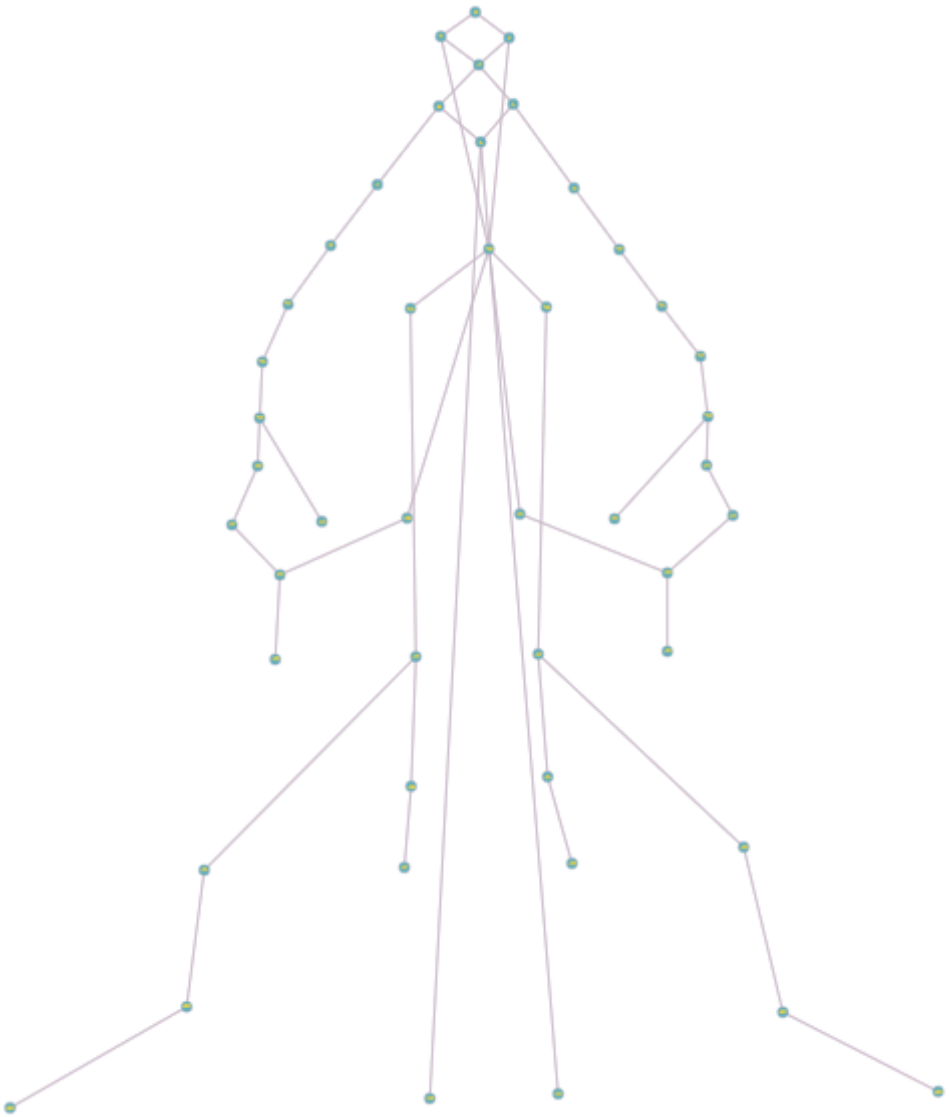

Рис. 1. Граф вложений плотных n-к до n < 20

Вычисление структуры плотной n-ки. Данные вычисления плохо поддаются распараллеливанию, поскольку чтобы вычислить структуру n-ки нужно знать структуру $(n-1)$-к. Затратив несколько сотен часов машинного времени нам удалось в 2013 г. вычислить структуру всех n-к до $n = 203$ включительно. В то же время, используя суперкомпьютеры, американский профессор из г. Мичиган Thomas J Engelsma со своей командой еще в декабре 2009 г. нашли 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. Следует отметить, что для данного n плотные n-ки могут иметь несколько различных структур, например, при $n = 105$ разных структур 105-к ровно 248.

Некоторые обобщения и выводы

Структура плотных n-к весьма интересна. Прежде всего для каждого n множество n-к симметрично, для каждой n-ки есть симметричная ей относительно середины отрезка, внутри которого она заключена.

Кроме того каждая n-ка содержит в себе по нескольку m-к при $m < n$. Подобное вложение имеет и большой практический смысл. Если мы нашли n-к для малых значений n, то для больших значений можно искать среди уже найденных. Мы приводим пример графа вложений плотных n-к для $n < 20$.

Точнее — это граф частично упорядоченного множества, у которого соединены ребрами только соседние элементы, в смысле упорядочения, а транзитивность — это движение по путям в графе. Сделано это для того, чтобы не перегружать граф ребрами. Но и даже в таком облегченном виде граф. на Рис. 1 выглядит весьма живописно. Обратим внимание, что его группа автоморфизмов элементарная абелева порядка 16.

Этот граф построен вручную. Следующая наша задача составить программу для построения графа вложений плотных n-к хотя бы до $n = 204$ — структур таких плотных n-к около 5 тыс.

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.

STRUCTURE OF DENSE K-TUPLES AND ITS CALCULATION

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

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

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