DOI: 10.24143/2072-9502-2017-3-48-64
УДК 511.1:004.056

С. И. Чермидов

РАСПРЕДЕЛЕНИЕ ПРОСТЫХ И СОСТАВНЫХ ЧИСЕЛ И ИХ АЛГОРИТМИЧЕСКИЕ ПРИЛОЖЕНИЯ

На базе множества чисел вида $\Theta = \{6k \pm 1 \,/\, k \in N\}$, где N – множество всех натуральных чисел, являющихся полугруппой относительно операции умножения, приводятся методы определения и распределения простых чисел, составных чисел, простых чисел близнецов и составных чисел близнецов, не имеющих делителей 2 и 3 в N. Дано вычисление точного числа простых чисел в заданном интервале. Предложен способ получения простых чисел по их порядковым номерам n во множестве простых чисел $p \geq 5$, а также новый алгоритм нахождения и распределения простых чисел на базе замкнутости множества Θ. Показано, что любое составное число $n \in \Theta$ представимо в виде произведения $(6x \pm 1)\,(6y \pm 1)$, где x, $y \in N$ являются натуральными решениями одного из четырех диофантовых уравнений: $P(x, y, \lambda) = 0$: $6xy \pm x \pm y - \lambda = 0$. Доказано, что если λ есть параметр простых чисел близнецов, то ни одно из диофантовых уравнений $P(x, y, \lambda) = 0$ не имеет решения. Приводится новый универсальный, детерминированный, полиномиальный и независимый тест, позволяющий проверить, являются ли числа вида $6 \cdot k \pm 1$ простыми. Приведены алгоритмы распределения параметров простых чисел близнецов и параметров составных чисел близнецов, не делящихся на 2 и 3, даны варианты доказательств их бесконечного количества.

Ключевые слова: простые и составные числа, параметры простых чисел, диофантовы уравнения, простые числа близнецы, тест на простоту, алгоритм распределения параметров.

Введение

В последние десятилетия интерес к законам распределения простых чисел [1] из теоретической сферы все больше смещается в практическую. Особо важным примером является их использование в криптографии [2], и именно поэтому любые результаты, уточняющие отдельные особенности законов распределения простых чисел, немедленно становятся предметом изучения специалистов в области криптографии. Особый интерес применительно к криптографии в системе с открытыми ключами (в частности, в системе шифрования RSA) вызывает вопрос о том, является ли данное конкретное (большое) число простым или нет.

Цель работы – исследование законов распределения простых чисел (PN), составных чисел (CN), простых чисел близнецов (Tw) и составных чисел близнецов $(TwCN)$, не имеющих делителей 2 и 3 в N [3].

1. Метод выделения простых чисел

При поиске простых чисел в натуральном ряду большая потеря времени приходится на числа, делящиеся на 2 и 3. Если произвести факторизацию множества N по основанию 6, то можно упростить поиск простых чисел и исследование их свойств. Разобьем множество натуральных чисел на 2 непересекающихся подмножества H и Θ, т. е. $N = H \cup \Theta$, $H \cap \Theta = \varnothing$. Пусть H включает 1 и натуральные числа, которые при делении на 6 дают остатки 0, 2, 3, 4. Очевидно, что множество H включает два простых числа – 2 и 3. Множество Θ содержит числа, которые при делении на 6 дают остатки 1 и 5, т. е. числа вида $\Theta = \{6 \cdot k \pm 1 / k \in N\}$, т. к. выражение $6m + 5 = 6 \cdot (m + 1) - 1$. Числа с остатками 0, 2, 3, 4 являются составными, т. к. делятся на 2 или на 3. Следовательно, $P \subset \Theta \subset N$. Непосредственной проверкой нетрудно убедиться, что множество $\Theta = \{6 \cdot k \pm 1 / k \in N\}$ – полугруппа относительно бинарной операции умножения. При этом выполняются следующие соотношения:

$$
\begin{aligned}
&1.\ n=(6x-1)(6y-1)=6\ (6xy-x-y)+1.\\
&2.\ n=(6x+1)(6y+1)=6\ (6xy+x+y)+1.\\
&3.\ n=(6x+1)(6y-1)=6\ (6xy-x+y)-1.\\
&4.\ n=(6x-1)(6y+1)=6\ (6xy+x-y)-1,
\end{aligned}
\tag{1}
$$

т. е. произведения чисел вида $(6x\pm1)$ и $(6y\pm1)$ выражаются числами вида $6xy\pm x\pm y$.

Определение 1. Для числа *n* значения числовых функций $\lambda(x,y)=6xy\pm x\pm y$, $x,\ y\in N$, представленные в (1), назовём *параметрами числа* $n\in\Theta$.

Отметим, что проблема однозначного соответствия между числами *n* и их параметрами $\lambda(x, y)$ остается открытой, т. е. одному и тому же числу *n* могут соответствовать несколько различных параметрических функций $\lambda(x, y)$. Однако, с точки зрения последующих исследований, данный факт не является существенным. Заметим, что форма $6\cdot\lambda-1$ при умножении может перейти в другую форму (см. (1)). Так как множество Θ есть полугруппа относительно бинарной операции умножения, то все его составные элементы будут

$$
\theta=(6\lambda_1\pm1)\cdot(6\lambda_2\pm1)\cdot(6\lambda_3\pm1)\cdot\ldots\cdot(6\lambda_i\pm1),\ \ \forall i,\lambda_i\in N.
\tag{2}
$$

Во множестве Θ есть элементы $\theta=6\cdot\lambda\ \pm\ 1,$ у которых число множителей в (2) равно 1, т. е. они не разлагаются в произведения других чисел из Θ, эти числа являются примитивными элементами Θ, т. е. простыми числами $p\geq5$ во множестве натуральных чисел. Для каждого из выражений (1) введем свой параметр $\lambda=6xy\pm x\pm y$. Тогда из (1) имеем

$$
\lambda=(n\pm1)/6,
\tag{3}
$$

т. е. получаем диофантовы уравнения $P(x,y,\lambda)=0,$ связывающие числа *x*, *y* и λ:

$$
\begin{aligned}
&1.\ 6x\cdot y-x-y-\lambda=0:P_1(x,y,\lambda)=0.\\
&2.\ 6x\cdot y+x+y-\lambda=0:P_2(x,y,\lambda)=0.\\
&3.\ 6x\cdot y-x+y-\lambda=0:P_3(x,y,\lambda)=0.\\
&4.\ 6x\cdot y+x-y-\lambda=0:P_4(x,y,\lambda)=0.
\end{aligned}
\tag{4}
$$

Если хотя бы одно из уравнений в (4) имеет одно решение, то число *n* составное, если ни одно из уравнений в (1) не имеет решений, число *n* является простым.

2. Распределение составных чисел множества Θ

Нетрудно заметить, что составные числа множества Θ формируются значениями из нижеследующих функций $\forall\ x,y\in N:$:

$$
\begin{aligned}
&1.\ \lambda_1=f_{11}(x,y)=6\cdot xy-x-y=x(6y-1)-y.\\
&2.\ \lambda_2=f_{12}(x,y)=6\cdot xy+x+y=x(6y+1)+y.\\
&3.\ \lambda_3=f_{21}(x,y)=6\cdot xy-x+y=x(6y-1)+y.\\
&4.\ \lambda_4=f_{22}(x,y)=6\cdot xy+x-y=x(6y+1)-y.
\end{aligned}
\tag{5}
$$

Составные числа множества Θ вида $6\cdot\lambda+1$ (обозначим их CN^+) в силу (1) порождаются значениями не взаимно однозначных функций): $f_{11}(x,y)=6xy-x-y$ и $f_{12}(x,y)=6xy+x+y$, ибо при неравных значениях аргументов $(x_1,y_1)\neq(x_2,y_2)$ значения функций могут быть равными: $f_{11}(x_1,y_1)=f_{11}(x_2,y_2)$ и $f_{12}(x_1,y_1)=f_{12}(x_2,y_2)$. Заметим, с учетом (1), что числа вида $\theta_1=6\cdot\lambda_1+1$ и $\theta_2=6\cdot\lambda_2+1$ составные и $(\theta_1,\ \theta_2)\in CN^+$.Составные числа множества Θ вида

$6\cdot\lambda-1$ (обозначим их CN^-), в силу (1), порождаются значениями функций) $f_{21}(x,\ y)=6xy-x+y$ и $f_{22}(x,\ y)=6xy+x-y$. Из (1) также следует, что числа вида $\theta_3=6\ \cdot\lambda_3-1$ и $\theta_4=6\ \cdot\lambda_4-1$ составные и $(\theta_3,\ \theta_4)\in CN^-$. Так как числа $(\theta_1,\ \theta_2)$ – составные, то значения переменных $(x,\ y)$ являются решениями соответствующих диофантовых уравнений $P_1(x,y,\lambda)=0$ или $P_2(x,y,\lambda)=0$. И точно так же для составных чисел $(\theta_3,\ \theta_4)$ значения переменных $(x,\ y)$ являются решениями диофантовых уравнений $P_3(x,y,\lambda)=0$ или $P_4(x,y,\lambda)=0$.

Таким образом, множество всех составных чисел множества Θ состоит из объединения $CN=CN^+\cup CN^-$.

Заметим также, что для факторизации составного числа $n\in\Theta$ наиболее результативный и наилучший способ – воспользоваться выражением (2), т. е. число $n\in\Theta$ поделить на числа вида $(6\lambda\ \pm\ 1)$, где $\lambda=1,\ 2,\ 3,\ \ldots$, [4]. Из (4) нетрудно вывести, что множество параметров всех четырех типов чисел (простых и составных) Θ в натуральном ряду чисел бесконечно.

Действительно, например, если функция $f_{11}(x,\ y)$ из (5) определена как множество $M_{x,y}=\{6xy-x-y\}$, то для любого натурального n, при $y=n$, число $(6n\ -\ 1)x\ -\ n\}\to\infty$. Аналогично рассматриваются и другие функции $f_{i\ j}(x,y)$, приведенные в (5). Таким образом, множества $M_{x,y}=M_{x1}\cup M_{x2}\cup M_{x3}\cup\ldots\cup M_{xn}$ во всех функциях (5) являются бесконечными как объединения бесконечных множеств. Введем обозначения для множества параметров составных чисел Θ вида $6\lambda+1: FN^+=\mathrm{Im}\ f_{11}(x,\ y)\cup\mathrm{Im}\ f_{12}(x,\ y)$ и множества параметров составных чисел вида $6\lambda-1: FN^-=\mathrm{Im}\ f_{21}(x,\ y)\cup\mathrm{Im}\ f_{22}(x,\ y)$. Тогда множество всех параметров составных чисел Θ будет представлять собой объединение $FN=FN^+\cup FN^-$.

Очевидно, что множества FN^-, FN^+, FN бесконечны как объединения бесконечных множеств. Для определения и исследования параметров простых и составных чисел множества Θ нужно будет найти все параметрические решения диофантовых уравнений (4). Однако решения диофантовых уравнений – проблема сложная, поэтому для решения уравнений (4) можно построить таблицу значений функции $\lambda(x,y)$ или функций (5). Тогда числу λ в таблице соответствует число n составное, иначе число n простое.

Для исследования параметров простых и составных чисел множества Θ зададим любые значения $x,\ y\in N$ для значений функций (5) от 1 до $s\in N$, где s – заданный размер таблицы. Построим таблицу (табл. 1) с размерностью $s\times s$, со структурой $f_{1,1}(x,y)\,|\,f_{1,2}(x,y)\,|\,f_{2,1}(x,y)\,|\,f_{2,2}(x,y)$.

Заметим, что при одних и тех же значениях $x,y\in N$ в каждой строке $(x,\ y)$ табл. 1 имеем возрастающую последовательность функций:

$$f_{1,\ 1}(x,y)<f_{2,\ 2}(x,y)\le f_{2,\ 1}(x,y)<f_{1,\ 2}(x,y). \tag{6}$$

Формирование строк $(x,\ y)$ и поиск значений функций (5) осуществляются по принципу $\overset{s}{\underset{x=1}{|}}\ \overset{s}{\underset{y=x}{|}}\ f_{ij}(x,y)\quad i<2, j<2.$ Выберем для демонстрации описываемых ниже алгоритмов значение s = 10, но описываемые ниже построения могут быть реализованы для любого s. Найдем значения функций $f_{11}(x,\ y),\ f_{12}(x,\ y),\ f_{21}(x,\ y),\ f_{22}(x,\ y),$ где $6\cdot f_{11}(x,\ y)+1,\ 6\cdot f_{12}(x,\ y)+1$ и $6\cdot f_{21}(x,\ y)-1,\ \ 6\cdot f_{22}(x,\ y)-1$ – составные числа, ибо значения переменных x и y известны как заранее заданные решения диофантовых уравнений (4). Пусть $x=n\in N,$ тогда значения функций (5) в последующей строке $(x,\ y+1)$ отличаются от значений предыдущей строки $(x,\ y)$ на следующие величины: для $f_{11}(x,y)$ – на $6x-1$; для $f_{12}(x,y)$ – на $6x+1$; для $f_{21}(x,y)$ – на $6x+1$; для $f_{22}(x,y)$ – на $6x-1$.

Таблица 1

Формирование параметров составных чисел во множестве Θ

x	y	$f_{11}(x, y)$	$f_{12}(x, y)$	$f_{21}(x, y)$	$f_{22}(x, y)$
1	1	4	8	6	6
	2	9	15	13	11
	3	14	22	20	16
	4	19	29	27	21
	5	24	36	34	26
	6	29	43	41	31
	7	34	50	48	36
	8	39	57	55	41
	9	44	64	62	46
	10	49	71	69	51
2	2	20	28		24
	3	31	41	37	35
	4	42	54	50	46
	5	53	67	63	57
	6	64	80	76	68
	7	75	93	89	79
	8	86	106	102	90
	9	97	119	115	101
	10	108	132	128	112
3	3	48	60	54	54
	4	65	79	73	71
	5	82	98	92	88
	6	99	117	111	105
	7	116	136	130	122
	8	133	155	149	139
	9	150	174	168	156
	10	167	193	187	173

x	y	$f_{11}(x, y)$	$f_{12}(x, y)$	$f_{21}(x, y)$	$f_{22}(x, y)$
4	4	88	104	96	96
	5	111	129	121	119
	6	134	154	146	142
	7	157	179	171	165
	8	180	204	196	188
	9	203	229	221	211
	10	226	254	246	234
5	5	140	160	150	150
	6	169	191	181	179
	7	198	222	212	208
	8	227	253	243	237
	9	256	284	274	266
	10	285	315	305	295
6	6	204	228	216	216
	7	239	265	253	251
	8	274	302	290	286
	9	309	339	327	321
	10	344	376	364	356
7	7	280	308	294	294
	8	321	351	337	335
	9	362	394	380	376
	10	403	437	423	417
8	8	368	400	384	384
	9	415	449	433	431
	10	462	498	482	478
9	9	468	504	486	486
	10	521	559	541	539
10	10	580	620	600	600

Пример 1. Найти составные числа множества Θ в интервале от 1 до $N=155$. Вычислим в заданном интервале максимальный параметр: $\lambda_{\max}=[N/6]=26$ и из табл. 1 выпишем параметры составных чисел $\le\lambda_{\max}$. В результате имеем:

$$P_{CN}=\{4^{+}, 6^{-}, 8^{+}, 9^{+}, 11^{-}, 13^{-}, 14^{+}, 15^{+}, 16^{-}, 19^{+}, 20^{-}, 21^{-}, 22^{+}, 24^{+}, 26^{-}\}\le\lambda_{\max}.$$

Опираясь на определение параметров составных чисел множества Θ, найдём их значения:

$CN^{+}: 6\cdot4+1=25,\ \ 6\cdot8+1=49,\ \ 6\cdot9+1=55,\ \ 6\cdot14+1=85,\ \ 6\cdot15+1=91,\ \ 6\cdot19+1=115,$ $6\cdot20+1=121,\ 6\cdot22+1=133,\ 6\cdot24+1=145;$

$CN^{-}: 6\cdot6-1=35,\ \ 6\cdot11-1=65,\ \ 6\cdot13-1=77,\ \ 6\cdot16-1=95,\ \ 6\cdot20-1=119,\ \ 6\cdot21-1=125,$ $6\cdot24-1=143,\ 6\cdot26-1=155.$

Значит, полная последовательность составных чисел множества Θ в интервале $1\div n=155$ будет

$$CN=CN^{+}\cup CN^{-}=\{25,\ 35,\ 49,\ 55,\ 65,\ 77,\ 85,\ 91,\ 95,\ 115,\ 119,\ 121,\ 125,\ 133,\ 145,\ 155\}.$$

3. Распределение параметров простых и составных чисел Θ в *N*

Распределение параметров простых и составных чисел множества Θ есть проаналог распределения простых чисел $p\ge5$ и составных чисел, не имеющих делителей 2 и 3 в *N*. Нужно будет найти все простые и составные числа Θ вида $6\lambda\pm1$. Опишем алгоритмы построения этих чисел. Пусть в интервале от 1 до *n* даны записи в файле по следующей структуре: $R_{\pi}=DCPN(id\cdot[F_1]\cdot[F_2])$, где параметры (реквизиты) *id* – серийные номера записей и поля F_1

и F_2 принимают значения «+» или «–». Перед началом алгоритмов 3.1 и 3.2 (см. ниже) в интервале $1 \div [n/6]$ построчно в поля F_1 и F_2 вводятся символы «+».

3.1. ***Алгоритм распределения простых чисел множества Θ вида 6λ – 1***

Пусть $x,\ y = 1,\ 2,\ 3,\ ...$ меняются по принципу табл. 1. Тогда по значениям параметров $\lambda = 6 \cdot xy - x + y$ и $\lambda = 6 \cdot xy + x - y$ составных чисел вида $(6 \cdot \lambda - 1) \in \Theta$ из файла R_π по прямому доступу достаются записи $id = \lambda$ и в поле F_1 знак «+» меняется на знак «–». Оставшиеся записи в конце алгоритма в поле F_1 = «+» говорят о наличии простых чисел типа $(6 \cdot id - 1) \in PN^-$. Введем обозначения: $\Xi_1 = N \setminus Jm\ f_{21}(x,\ y)$, $\Xi_1' = N \setminus Jm\ f_{22}(x,\ y)$, $K_{-1} = \Xi_1 \cup \Xi_1'$. Тогда $PN^- = \{6 \cdot \lambda - 1 / \lambda \in K_{-1}\}$.

3.2. ***Алгоритм распределения простых чисел множества Θ вида 6λ + 1***

Пусть $x,\ y = 1,\ 2,\ 3,\ ...$ меняются по принципу табл. 1, тогда по значениям параметров $\lambda = 6xy - x - y$ и $\lambda = 6xy + x + y$ составных чисел вида $(6 \cdot \lambda + 1) \in \Theta$ из файла R_π по прямому доступу достаются записи с номерами $id = \lambda$ и в поле F_2 знак «+» меняется на знак «–». Оставшиеся записи в конце алгоритма в поле F_2 = «+» говорят о наличии простых чисел типа $(6 \cdot id + 1) \in PN^+$. Пусть $\Xi_2 = N \setminus Jm\ f_{11}(x,\ y)$, $\Xi_2' = N \setminus Jm\ f_{12}(x,\ y)$, $K_{+1} = \Xi_2 \cup \Xi_2'$. Тогда $PN^+ = \{6 \cdot \lambda + 1 / \lambda \in K_{+1}\}$.

Итак, простые числа состоят из объединения двух множеств: $P = PN^- \cup PN^+$. Таким образом, получено распределение параметров $id \in N$ простых и составных чисел Θ в N. Объединив алгоритмы 3.1 и 3.2 в один, получим алгоритм Pr*Nb* – алгоритм распределения параметров простых и составных чисел Θ в N. Параметры *id* с приписанными полями F_1 и F_2 со значением «+», согласно 3.1 и 3.2, являются параметрами простых чисел, а со значением «–» – параметрами составных чисел.

Теорема 1. ***Диофантовы уравнения (4) имеют решения тогда, когда числа вида*** $\mathbf{6 \cdot \lambda \pm 1}$ ***– составные.***

Необходимость. Пусть числа вида $n = 6\lambda \pm 1$ составные, значит, они являются произведениями по крайней мере двух элементов: $\theta_1 = 6x \pm 1$ и $\theta_2 = 6y \pm 1$, $(\theta_1,\ \theta_2) \in \Theta$, $x \in N$, $y \in N$. Согласно (1), число n может быть представлено одним из произведений – $(6 \cdot x \pm 1)(6 \cdot y \pm 1) = 6\ (6 \cdot xy \pm x \pm y) \pm 1$ и может быть сопоставлено с одним из диофантовых уравнений $6xy \pm x \pm y - \lambda = 0$, где $\lambda \in N$, т. к. $x \in N$, $y \in N$. Тогда найдутся тройки чисел, $(\lambda,\ x,\ y) \in N$, которые являются решениями хотя бы одного из диофантовых уравнений (4). Если числа вида $n = 6\lambda \pm 1$ являются простыми числами, то решений не будет, ибо из единственности представления простых чисел имеем $n = 1 \cdot n = (6 \cdot 0 \pm 1)(6 \cdot \lambda \pm 1)$, откуда следует, что элемент $(6 \cdot 0 \pm 1) \notin \Theta$.

*Достаточность***.** Пусть одно из диофантовых уравнений (4) имеет решение, т. е. существует тройка чисел $(\lambda, x, y) \in N$ таких, что справедливо $\lambda = 6xy \pm x \pm y$. Тогда, с учетом (3), имеем: $(n \pm 1) / 6 = 6xy \pm x \pm y \rightarrow n = 6 \cdot (6xy \pm x \pm y) \pm 1 = (6x \pm 1)(6y \pm 1)$, откуда n – составное число.

Пример 2. Пусть $x = 11,\ y = 2$ – решение уравнения $P_1(x, y, \lambda) = 0$. Тогда $\lambda = 6xy - x - y = 119$. С учетом (3) имеем $(n-1) / 6 = 119$ или $n = 6 \cdot 119 + 1 = 715$, и из (1) следует, что $715 = (6 \cdot 11 - 1)(6 \cdot 2 - 1)$, т. е. $n = 6 \cdot 119 + 1$ – составное число.

При решении диофантовых уравнений (4) нужно проверить числа вида $n_1 = 6 \cdot \lambda + 1$ и $n_2 = 6 \cdot \lambda - 1$ на простоту. При простых значениях n_1 и n_2 диофантовы уравнения $P_1(x, y, \lambda) = 0$, $P_2(x, y, \lambda) = 0$ и $P_3(x, y, \lambda) = 0$, $P_4(x, y, \lambda) = 0$ соответственно не имеют решений. Приведем примеры.

I. Пусть $\lambda = 16$, тогда число $n = 6 \cdot 16 + 1 = 97$ – простое, значит, уравнения $P_1(x, y, \lambda) = 0$ и $P_2(x, y, \lambda) = 0$ не имеют решений. Если $\lambda = 15$, то число $n = 6 \cdot 15 - 1 = 89$ – простое и уравнения $P_3(x, y, \lambda) = 0$ и $P_4(x, y, \lambda) = 0$ не имеют решений.

II. Пусть $\lambda = 7589$, тогда число $n = 6 \cdot 7589 + 1 = 45535 = 5 \cdot 9107 \to n$ – составное и диофантовы уравнения $P_1(x, y, \lambda) = 0$ и $P_2(x, y, \lambda) = 0$ имеют натуральные решения, т. е.:

1. $6xy - x - y = 7589$. Решения следуют из выражения $n = (6x - 1)(6y - 1)$ (см. (1)).

$y = \bigvee_{x=1}^{[\lambda/6]} \alpha = 6x - 1,\ [\frac{n + \alpha}{6\alpha}]$. Решения: $(\lambda, x_1, y_1) = (7589,\ 1,\ 1518)$ и $(\lambda, x_2, y_2) = (7589,\ 6,\ 217)$.

2. $6xy + x + y = 7589$. Решения следуют из выражения $n = (6x + 1)(6y + 1)$ (см. (1)).

$y = \bigvee_{x=1}^{[\lambda/6]} \alpha = 6x + 1,\ [\frac{n - \alpha}{6\alpha}]$, если $y \in N$ стремится к решению (7589, 1, 1084).

III. Пусть $\lambda = 63$, тогда $n = 6 \cdot 63 - 1 = 377 = 13 \cdot 29$ – составное число. $P_3(x, y, \lambda) = 0$, и $P_4(x, y, \lambda) = 0$ имеют следующие решения:

3. $6xy - x + y = 63$, $y = \bigvee_{x=1}^{[\lambda/6]} \alpha = 6x + 1,\ [\frac{n + \alpha}{6\alpha}]$; если $y \in N$ стремится к решению (63, 2, 5).

4. $6xy + x - y = 63$, $y = \bigvee_{x=1}^{[\lambda/6]} \alpha = 6x - 1,\ [\frac{n - \alpha}{6\alpha}]$; если $y \in N$ стремится к решению (63, 5. 2).

Следствие 1. Для любого простого $\lambda \in PN^+$ не существует никакой тройки чисел $(\lambda,\ x,\ y) \in N$, которые были бы решением диофантовых уравнений $P_1(x, y, \lambda) = 0$ и $P_2(x, y, \lambda) = 0$.

Следствие 2. Для любого простого $\lambda \in PN^-$ не существует никакой тройки чисел $(\lambda,\ x,\ y) \in N$, которые были бы решением диофантовых уравнений $P_3(x, y, \lambda) = 0$ и $P_4(x, y, \lambda) = 0$.

Рассмотрим взаимосвязь диофантовых уравнений (4) с простыми числами близнецами. Из определения чисел близнецов известно, что это числа $p_1,\ p_2 \in P$ и $p_2 - p_1 = 2$. Заметим, что разность чисел $\theta_\lambda^+ - \theta_\lambda^- = (6 \cdot \lambda + 1) - (6 \cdot \lambda - 1) = 2$, и если при одном и том же значении параметра λ числа $\theta_\lambda{}^+ \in PN^+$ и $\theta_\lambda{}^- \in PN^-$ простые, то числа вида $(6 \cdot \lambda \pm 1)$ будут простыми числами близнецами.

Теорема 2. ***Для того чтобы $\lambda \in N$ было параметром простых чисел близнецов, необходимо и достаточно, чтобы ни одно из диофантовых уравнений (4) при одном и том же λ не имело решений.***

Необходимость. Пусть при одном и том же $\lambda \in N$ все диофантовы уравнения (4) не имеют решений. Тогда, по Теореме 1, из $P_1(x, y, \lambda) = 0$ и $P_2(x, y, \lambda) = 0$ следует, что $\theta_\lambda{}^+ = 6 \cdot \lambda + 1$ – простое число, и из уравнений $P_3(x, y, \lambda) = 0$ и $P_4(x, y, \lambda) = 0$ – что $\theta_\lambda{}^- = 6 \cdot \lambda - 1$ – простое число. Так как разность чисел $(\theta_\lambda{}^+ - \theta_\lambda{}^-) = 2$, то по определению простых чисел близнецов $(\theta_\lambda{}^+,\ \theta_\lambda{}^-) \in Tw$, где Tw – множество пар простых чисел близнецов. А это значит, что λ есть параметр простых чисел близнецов.

Достаточность. Пусть λ есть параметр простых чисел близнецов, т. е. $p_2 = 6 \cdot \lambda + 1$ и $p_1 = 6 \cdot \lambda - 1$ – простые числа в силу определения чисел близнецов $(p_2, p_1) \in P$ и $p_2 - p_1 = 2$. Значит, из Следствия 1, для простого числа $p_2 = 6 \cdot \lambda + 1$ следует, что диофантовы уравнения $P_1(x, y, \lambda) = 0$ и $P_2(x, y, \lambda) = 0$ не имеют решений, и, точно так же, из Следствия 2, не имеют решений диофантовы уравнения $P_3(x, y, \lambda) = 0$ и $P_4(x, y, \lambda) = 0$ для простого $p_1 = 6 \cdot \lambda - 1$. Итак, ни одно из диофантовых уравнений (4) не имеет решений.

Приписывая к серийным номерам записей $id \in N$ знаки «+» или «–», в полях F_1 и F_2 можно сформировать таблицу знаков (табл. 2), и с помощью алгоритмов 3.1 и 3.2 натуральный ряд чисел разбивается на подмножества чисел согласно сочетаниям знаков «+» и «–».

Таблица 2

Распределение параметров простых и составных чисел Θ в *N*

Id	F_1	F_2												
1	+	+	41	–	–	81	–	+	121	–	+	161	–	+
2	+	+	42	+	–	82	+	–	122	–	+	162	+	–
3	+	+	43	+	–	83	–	+	123	–	+	163	+	–
4	+	–	44	+	–	84	+	–	124	+	–	164	+	–
5	+	+	45	+	+	85	+	–	125	–	+	165	–	+
6	–	+	46	–	+	86	–	–	126	–	+	166	–	+
7	+	+	47	+	+	87	+	+	127	+	–	167	–	–
8	+	–	48	–	–	88	–	–	128	–	+	168	–	+
9	+	–	49	+	–	89	–	–	129	+	–	169	+	–
10	+	+	50	–	–	90	–	+	130	–	–	170	+	+
11	–	+	51	–	+	91	–	+	131	–	+	171	–	–
12	+	+	52	+	+	92	–	–	132	–	–	172	+	+
13	–	+	53	+	–	93	+100	–	133	+	–	173	–	+
14	+	–	54	–	–	94	+	–	134	–	–	174	–	–
15	+	–	55	–	+	95	+	+	135	+	+	175	+	+
16	–	+	56	–	+	96	–	+	136	–	–	176	–	–
17	+	+	57	–	–	97	–	–	137	+	+	177	+	+
18	+	+	58	+	+	98	+	–	138	+	+	178	–	+
19	+	–	59	+	–	99	+	–	139	–	–	179	–	–
20	–	–	60	+	–	100	+	+	140	+	–	180	–	–
21	–	+	61	–	+	101	–	+	141	–	–	181	–	+
22	+	–	62	–	+	102	–	+	142	–	+	182	+	+
23	+	+	63	–	+	103	+	+	143	+	+	183	+	–
24	–	–	64	+	–	104	–	–	144	+	–	184	+	–
25	+	+	65	+	–	105	–	+	145	–	–	185	+	–
26	–	+	66	–	+	106	–	–	146	–	+	186	–	+
27	–	+	67	+	–	107	+	+	147	+150	+	187	–	+
28	+	–	68	–	+	108	+	–	148	+	–	188	–	+
29	+	–	69	–	–	109	+	–	149	–	–	189	–	–
30	+	+	70	+	+	110	+	+	150	–	–	190	–	–
31	–	–	71	–	–	111	–	–	151	–	+	191	–	–
32	+	+	72	+	+	112	–	+	152	+	–	192	+	+
33	+	+	73	–	+	113	+	–	153	–	+	193	–	–
34	–	–	74	+	–	114	+	–	154	–	–	194	+	–
35	–	+	75	+	–	115	–	+	155	+	–	195	–	+
36	–	–	76	–	+	116	–	–	156	–	+	196	–	–
37	–	+	77	+	+	117	+	–	157	+	–	197	+	–
38	+	+	78	+	–	118	–	+	158	+	–	198	+	–
39	+	–	79	–	–	119	–	–	159	+	–	199	+	–
40	+50	+	80	+	–	120	+	–	160	–	–	200	–	+

Очевидно, что эти подмножества чисел в натуральном ряду являются параметрами соответствующих подмножеств множества Θ:

Множество составных чисел $CN = \{6 \cdot id - 1 / id \in FN^-\} \cup \{6 \cdot id + 1 / id \in FN^+\}$, где FN^- – множество значений параметров, представимо в виде

$$\{\lambda_3(x,y) = 6xy - x + y\} \cup \{\lambda_4(x,y) = 6xy + x - y\} \quad \forall (xy) \in N; \tag{8}$$

где FN^+ – множество значений параметров $\{\lambda_1(x,y)=6xy-x-y\}\bigcup\{\lambda_2(x,y)=6xy+x+y\}$, $P_{CN}=FN^+\cup FN^-$.

Составные числа близнецы

$$Tw_{CN}=\{6\cdot id\pm1/\,id\in P_{Tw_{CN}}\},\ id:"-","-",\ (6\cdot id+1)-(6\cdot id-1)=2, \tag{9}$$

параметры P_{TwCN} лежат на непустых пересечениях значений функций (4).

Параметрами простых чисел (часть 1)

$$PN=\{6\cdot id-1/\,id\in FN^+\setminus P_{Tw_{CN}}\}\bigcup\{6\cdot id+1/\,id\in FN^-\setminus P_{Tw_{CN}}\} \tag{10}$$

будут $P_{PN}=FN^+\setminus P_{Tw_{CN}}\cup FN^-\setminus P_{Tw_{CN}}$, т. к. множество параметров FN^- не являются решениями диофантовых уравнений $P_1(x,y,\lambda)=0$ и $P_2(x,y,\lambda)=0$ и множество параметров FN^+ не являются решениями диофантовых уравнений $P_3(x,y,\lambda)=0$ и $P_4(x,y,\lambda)=0$.

Параметрами простых чисел близнецов (часть 2)

$$Tw=\{6\cdot id\pm1/\,id\in P_{Tw}\},\quad (6\cdot id+1)-(6\cdot id-1)=2 \tag{11}$$

будут $P_{Tw}\in Ch=N\setminus FN$. Тогда параметры всех простых чисел – $P_P=P_{PN}\bigcup P_{Tw}$.

4. Определение простых чисел по их порядковым номерам во множестве простых чисел $p\geq5$. Формула нахождения π(*x*) в интервале от 1 до *N*

Из таблицы распределения параметров простых и составных чисел Θ в *N* (табл. 2) нетрудно заметить, что между порядковыми номерами *n* простых чисел в табл. 3 и параметрами (*id*) простых чисел $p\geq5$, приведенными в табл. 2, существуют зависимости.

Таблица 3

Множество простых чисел *P* ($p\geq5$)

		• 5	7	11	13	17	19	23	29	31	37	41
43	**47**	**53**	**59**	**61**	**67**	**71**	**73**	**79**	**83**	**89**	**97**	**101**
103	**107**	**109**	**113**	**127**	**131**	**137**	**139**	**149**	**151**	**157**	**163**	**167**
173	**179**	**181**	**191**	**193**	**197**	**199**	**211**	**223**	**227**	**229**	**233**	**239**
241	**251**	**257**	**263**	**269**	**271**	**277**	**281**	**283**	**293**	**307**	**311**	**313**
317	**331**	**337**	**347**	**349**	**353**	**359**	**367**	**373**	**379**	**383**	**389**	**397**
401	**409**	**419**	**421**	**431**	**433**	**439**	**443**	**449**	**457**	**461**	**463**	**467**
479	**487**	**491**	**499**	**503**	**509**	**521**	**523**	**541**	**547**	**557**	**563**	**569**
571	**577**	**587**	**593**	**599**	**601**	**607**	**613**	**617**	**619**	**631**	**641**	**643**
647	**653**	**659**	**661**	**673**	**677**	**683**	**691**	**701**	**709**	**719**	**727**	**733**
739	**743**	**751**	**757**	**761**	**769**	**773**	**787**	**797**	**809**	**811**	**821**	**823**
827	**829**	**839**	**853**	**857**	**859**	**863**	**877**	**881**	**883**	**887**	**907**	**911**
919	**929**	**937**	**941**	**947**	**953**	**967**	**971**	**977**	**983**	**991**	**997**	**. . .**

Пусть *n* – порядковый номер числа $p\geq5$ во множестве простых чисел *P*. Соответствующий параметр к простому числу в табл. 2 будет: $id=\sum_{i=1}^{n}S_1+S_2$, где

$S_1=(0:F_1=\text{«–»},\ 1:F_1=\text{«+»}),\qquad S_2=(0:F_2=\text{«–»},\ 1:\ F_2=\text{«+»}),\qquad P(n)=\begin{cases}1.\ \ 6\cdot id-1/\,\psi(n)=1.\\ 2.\ \ 6\cdot id+1/\,\psi(n)=2.\end{cases}$.

Подсчет знаков «+» ведётся по следующему принципу просмотра строк: $\begin{matrix}F_1\to F_2\to\\ \to\ F_1\to F_2\to\downarrow\ ...,\end{matrix}$ (12)

$\psi\ (n)$ – индекс поля $F_{\psi(n)}$, где заканчивается счет. Для достоверности полученное простое число $P(n)$ можно сверить с числом, которое лежит над порядковым номером n в любой таблице простых чисел $p\geq5$.

Пример 3. Пусть n – порядковый номер простого числа $p \geq 5$, тогда из табл. 2 имеем:

1. При $n = 1 \to id = 1,\ \psi(n) = 1 \to P(1) = 6 \cdot 1 - 1 = 5.$

2. При $n = 15 \to id = 10,\ \psi(n) = 1 \to P(15) = 6 \cdot 10 - 1 = 59.$

Число простых чисел $\pi(x)$ в интервале $1 \div N$ найдём на основе табл. 2 по типу $\pi(x) = 2 + \sum_{id=1}^{m} S_1 + S_2$, где верхняя граница $m = [N/6]$. Подсчет знаков «+» в табл. 2 в полях F_1 и F_2 ведется аналогично (12).

Пример 4. Определить количество простых чисел $\pi(x)$ в интервале $1 \div N$.

1. $1 \div N = 100 \to 1 \div m = [N/6] = 16,\ \sum_{i=1}^{m} S_1 = 12,\ \sum_{i=1}^{m} S_2 = 11,$ тогда $\pi(x) = 2 + 12 + 11 = 25.$

2. $1 \div N = 217 \to 1 \div m = [N/6] = 36,\ \sum_{i=1}^{m} S_1 = 23,\ \sum_{i=1}^{m} S_2 = 22,$ тогда $\pi(x) = 2 + 23 + 22 = 47.$

5. Алгоритм распределения простых чисел $p \geq 5$ в интервале $1 \div n$

Так как множество простых чисел $P \subset \Theta \subset N$, то очевидно, что поиск простых чисел будет идти быстрее во множестве Θ, чем в натуральном ряду чисел N. Наиболее естественный способ удаления составных чисел множества Θ в интервале $1 \div n$ – это использование свойства замкнутости по умножению. Именно поэтому, умножая числа вида $6 \cdot i \pm 1$ поэлементно на элементы множества Θ, где $i \in (1 \div [n/6])$, можно легко и просто достичь поставленной цели. Вначале построчно вводятся натуральные числа в файл $\Theta' = \Pr mNub\ 1\ (id \cdot [N])$, однако места чисел, делящихся на 2 и 3, заполняются символом «» – символом пустоты. Затем, на основе следующего алгоритма – *RasPrm* (рис. 1), удаляются все те элементы файла Θ', которые являются поэлементными произведениями чисел Θ' на числа вида $\theta_i = 6 \cdot i - 1,$ и, аналогично, для чисел вида $\theta_i = 6 \cdot i + 1,$ где i = 1, 2, 3, … (см. ниже пример 5). Каждый последующий новый элемент θ_i возводится в квадрат, чтобы избежать повторения операции умножения, и затем поэлементно перемножается на последующие числа файла Θ'.

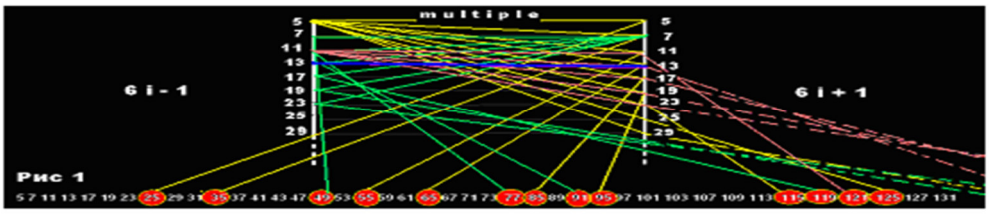

Рис. 1. Окно программы, реализующей алгоритм *RasPrm*

Процесс удаления продолжается до тех пор, пока $\theta_i^2 \leq n$. Если произведения чисел θ_i на последующие числа Θ' больше, чем n, то осуществляется переход к следующему элементу $\theta_{i=i+1}$ и повторяется вышеописанная процедура.

Описанный метод отсеивания составных чисел из множества Θ с числами вида $\theta_i = 6 \cdot i \pm 1$ прост в использовании, алгоритм работает эффективнее и быстрее таких известных алгоритмов, как решето Эратосфена, решето Сунтарами и решето Аткина, поскольку во всех этих алгоритмах областью функционирования является множество натуральных чисел. Метод отсеивания составных чисел из множества Θ числами вида $6 \cdot i \pm 1$ позволяет получить те же результаты, что и вышеперечисленные алгоритмы, но при существенно меньшем числе операций умножения.

Пример 5. Найти все простые числа множества Θ в интервале $1 \div N = 1 \div 133$.

С помощью чисел вида $\theta_i = 6 \cdot i \pm 1,$ где $i \in (1 \div [133/6] = 22),$ сформируем элементы файла Θ':

{5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47, 49, 53,
55, 59, 61, 65, 67, 71, 73, 77, 79, 83, 85, 89, 91, 95, 97,
101, 103, 107, 109, 113, 115, 119, 121, 125, 127, 131, 133, ...}.

1. Удаление составных чисел файла Θ', имеющих вид $\theta_i = 6 \cdot i - 1$**.** Пусть $i = 1,$ тогда $\theta_1 = 5.$ Возведём θ_1 в квадрат как новый элемент: $\theta_1^2 = 5 \cdot 5 = 25,$ и если $id = 25 \le 133,$ то из файла Θ' по прямому доступу достаётся номер записи $id = 25$ и удаляется значение поля $[N] = 25.$ Затем θ_1 поэлементно умножается на последующие числа файла Θ' и также удаляются числа с номерами записей $id = 5 \cdot 7 = 35;$ $id = 5 \cdot 11 = 55;$ $id = 5 \cdot 13 = 65;$ $id = 5 \cdot 17 = 85;$ $id = 5 \cdot 19 = 95;$ $id = 5 \cdot 23 = 115;$ $id = 5 \cdot 25 = 125$. Так как $id = 5 \cdot 29 = 145,$ осуществляется переход на следующий шаг, ибо $145 > 133,$ т. е. $i = i + 1 = 2,$ $\theta_2 = 6 \cdot 2 - 1 = 11$ – новый элемент, $id = 11^2 = 121 < 133$, и удаляется запись *id* = 121 из поля [*N*]. Когда $id = 11 \cdot 13 = 143,$ вновь осуществляется переход на следующий шаг, т. к. $143 > 133,$ $i = i + 1 = 2 + 1,$ т. е. $\theta_3 = 6 \cdot 3 - 1 = 17$ – новый элемент, $id = 17^2 = 289 \ge 133$, и прекращается удаление при появлении чисел вида $6 \cdot i - 1$.

2. Удаление составных чисел файла Θ', имеющих вид $\theta_i = 6 \cdot i + 1$**.** Пусть $i = 1 \to \theta_1 = 7,$ θ_1 – новый элемент; возводится в квадрат $id = 7^2 = 49 < 133,$ и удаляется аналогично, как и в предыдущих примерах. По прямому доступу достаются номера записей $id = 7 \cdot 11 = 77,$ $id = 7 \cdot 13 = 91,$ $id = 7 \cdot 17 = 119$ и удаляются числа. Так как $id = 7 \cdot 19 = 133 \ge 133,$ то осуществляется переход на шаг $i = i + 1 = 1 + 1 = 2,.$ Тогда $\theta_2 = 6 \cdot 2 + 1 = 13,$ поскольку $id = 13^{\cdot 2} = 169 > 133.$ ***Конец алгоритма.***

6. Простые числа близнецы

Область определения простых чисел близнецов. Так как простые числа множества *P* есть объединение множеств просто простых чисел (*PN*) и простых чисел близнецов (*Tw*), то этот факт рассмотрим на уровне их параметров $P_P = P_{PN} \cup P_{Tw}.$ Обозначим и исследуем разности между функциями (5): $\delta^1{}_{x,y} = f_{22}(x,\ y) - f_{11}(x,\ y) = 2x,$ $\delta^2{}_{x,y} = f_{21}(x,\ y) - f_{22}(x,\ y) = 2 \cdot (y - x)$ и $\delta^3{}_{x,y} = f_{12}(x,\ y) - f_{21}(x,\ y) = 2x.$ Заметим, что $\delta_{x,y}{}^1 = \delta_{x,y}{}^3 = 2x \to \infty$ и $\delta_{x,y}{}^2 \to \infty$ при $x \in N,$ $y \to \infty,$ т. к. $x,\ y \in N,$ $\delta_{x,y}{}^1 > 0,$ $\delta_{x,y}{}^3 > 0$ и $y > x \to \delta^2_{x,y} > 0.$ Значит, между значениями функций (4) в строках (*x*, *y*) табл. 1 существуют интервальные последовательности чисел $(\{\sigma^1_{x,y}\}, \{\sigma^2_{x,y}\}, \{\sigma^3_{x,y}\})$, число элементов в которых соответственно равно: $K\delta^j{}_{x,y} = (\delta^1{}_{x,y}\colon 2x - 1,\ \delta^2{}_{x,y}\colon 2(y - x) - 1,\ \delta^3{}_{x,y}\colon 2x - 1).$

Определение 2. Объединение $\sigma_{x,y} = \{\sigma^1{}_{x,y}\} \cup \{\sigma^2{}_{x,y}\} \cup \{\sigma^3{}_{x,y}\}$ интервальных последовательностей в строке (*x*, *y*) назовём $\sigma_{x,y}$-последовательностью.

Число элементов в $\sigma_{x,y}$-последовательности равно: $K\sigma_{x,y} = 2(x + y) - 3.$ Число элементов в приводимых далее последовательностях стремится к бесконечности: $(\{\delta^1{}_{x,y},\ \delta^2{}_{x,y}\},\ \{\delta^3{}_{x,y}\}) \to \infty,$ и потому стремятся к бесконечности интервальные последовательности $(\{\sigma^1{}_{x,y}\},\ \{\sigma^2{}_{x,y}\},\ \{\sigma^3{}_{x,y}\}) \to \infty$ Пусть множество $\Delta = \bigcup_{x,y} \sigma_{x,y},$ тогда $\Delta \to \infty.$ В силу (6) $\sigma_{x,y}$-последовательности являются упорядоченными и возрастающими.

Итак, табл. 1 состоит из двух частей: из множеств параметров составных чисел FN^- и FN^+, которые являются параметрами составных чисел P_{CN} и, параллельно, – простых чисел P_{PN} вида $6\lambda \pm 1$ (8)–(11)), и из явно невидимого множества Δ, которое содержит параметры простых чисел близнецов $P_{Tw} \in \Delta$ как 2-ю часть параметров всех простых чисел P_P. Так как часть параметров множества простых чисел $P_{PN} = FN^+ \setminus P_{TwCN} \bigcup FN^- \setminus P_{TwCN} \notin \Delta$ и $P_{Tw} \in \Delta,$ то элемен-

тами $\sigma_{x,y}$ -последовательностей будут α – параметры P_{Tw} простых чисел близнецов и β – параметры P_{CN} составных чисел множества Θ, т. е.

$$\{\sigma_{x,y}\} = P_{Tw} \cup P_{CN} \tag{13}$$

Пример 6. Найти обычную построчную $\sigma_{x,y}$-последовательность чисел в строке (1, 5), табл. 1.

1. $\delta^1_{1,5} : f_{22}(x,y) = 6xy + x - y = 26,\ f_{11}(x,y) = 6xy - x - y = 24,\ K\delta^1_{1,5} = 2\cdot 1 - 1 = 1,\ \sigma^1_{1,5} = \{25\}.$
2. $\delta^2_{1,5} : f_{21}(x,y) = 6xy - x + y = 34,\ f_{22}(x,y) = 6xy + x - y = 26,\ K\delta^2_{1,5} = 2\cdot(5-1) - 1 = 7,\ \sigma^2_{1,5} = \{27,\ ...,\ 33\}.$
3. $\delta^3_{1,5} : f_{12}(x,y) = 6xy + x + y = 36,\ f_{21}(x,y) = 6xy - x + y = 34,\ K\delta^3_{1,5} = 2\cdot 1 - 1 = 1,\ \sigma^3_{1,5} = \{35\}.$

Значит, $\sigma_{1,5} = \{\ 25,\ 27,\ 28,\ 29,\ 30,\ 31,\ 32,\ 33,\ 35\ \}$ и число элементов $K\sigma_{1,5} = 9$. Заметим, что в построчных $\sigma_{1,y}$-последовательностях начальная граница $= 5y$, а конечная $= 7y$.

Рассмотрим представление элементов $\sigma_{x,y}$-последовательности (табл. 4):

Таблица 4

Представление элементов $\sigma_{x,y}$-последовательности

$\lambda(x, y)/\sigma_{1,5}$	25	27	28	29	30	31	32	33	35
$6xy - x - y$	–	–		6–1	–	3–2	–	–	–
$6xy + x + y$	–	–	2–2	4–1	–	–	–	–	–
$6xy - x + y$	–	1–4	–	–	–	6–1	–	–	3–2
$6xy + x - y$	–	–	–	–	–	1–6	–	–	2–3

Числа 25, 30, 32, 33 не представимы ни одним из уравнений (4), т. е. являются параметрами простых чисел близнецов. Остальные числа представимы, например: $27 = 6xy - x + y = 6\cdot 1\cdot 4 - 1 + 4$, $29 = 6xy - x - y = 6\cdot 6\cdot 1 - 6 - 1$, $28 = 6xy + x + y = 6\cdot 2\cdot 2 + 2 + 2$, $35 = 6xy + x - y = 6\cdot 2\cdot 3 + 2 - 3$.

С увеличением значений *id* (см. табл. 2) рост параметров простых чисел близнецов заметно уменьшается, поэтому с обычными $\sigma_{1,y}$-последовательностями табл. 1 строгого доказательства проблемы о бесконечности простых чисел близнецов не найти. Очевидно, в $\sigma_{1,y}$-последовательностях начальной границей будет 1, а конечную необходимо непрерывно расширять, связав со строкой *y*. Число элементов в построчных $\sigma_{1,y}$-последовательностях находится по типу $K\sigma_{1,y} = 2\,(1 + y) - 3 = 2y - 1$. Тогда конечная граница $\sigma_{1,y}$-последовательности будет равна:

$$M_{1,y} = 7y + y(2y - 1) = 2y^2 + 6y = 2y(y + 3). \tag{13'}$$

При таком характере роста параметров в последующих $\sigma_{1,y}$-последовательностях будут присутствовать и параметры простых чисел близнецов предыдущих $\sigma_{1,y}$-последовательностей.

***Алгоритм простых чисел близнецов*:**

A. *Описание программы* N. В поле $[N]$ файла T = PrmNub1 (id.[prm1].[prm2]) построчно вводятся натуральные числа от 1 до *n*.

B. *Описание программы* Tws. Для того чтобы извлечь параметры простых чисел близнецов из множества $\Delta \subset N$ в интервале $1 \div n,$, нужно будет удалять из него параметры составных чисел, т. е. $P_{Tw} = N \setminus FN$. Определяется максимальный интервал для пробега переменных $(i, j) \in 1 \div [n/3]$. Программа стартует с $j = i,$ и параметры составных чисел P_{CN} удаляются с помощью значений функций (5) $id = f_{p,q}(i,\ j)$, где $p \le 2,\ q \le 2$. Если $id \le n,$ то по прямому доступу из T достаются записи с номерами id и удаляются числа в поле $[N]$.

Если $j \ge [n/3],$ увеличиваем значение шага $i = i + 1$, и повторяем процедуру. Процесс удаления продолжается, пока не будет $i > [n \setminus 3]$. Непустые значения поля [*N*] говорят о наличии параметров чисел близнецов вида $6\lambda \pm 1$. Если $\lambda = [N] = \varnothing,$ значит, алгоритмом были удалены

числа как параметры составных чисел. Например, параметр $\lambda = 10,$ не удаляется из файла, ибо $6\lambda + 1 = 61 \in PN^{+}$ и $6\lambda - 1 = 59 \in PN^{-}$ – простые числа.

Если параметр $\lambda = 11,$ то имеем $6\lambda + 1 = 67 \in PN^{+}$ и $6\lambda - 1 = 65 \notin PN^{-},$ и тогда параметр $\lambda = 11$ удаляется как параметр составного числа. Значит, когда $\lambda = [N] \neq \varnothing,$ имеем простые числа $6\lambda \pm 1 \in P$ и значения полей $[prm\ 1] = 6 \cdot [N] - 1$ и $[prm\ 2] = 6 \cdot [N] + 1$ в паре образуют множество простых чисел близнецов: $Ch = \{\lambda \in N / (6\lambda \pm 1) \in P,\ (6 \cdot \lambda + 1) - (6 \cdot \lambda - 1) = 2\}.$

Пример 7. Пусть $n = 100,$ тогда интервал параметров чисел близнецов $1 \div N = [n / 6] = 16.$ Из табл. 1 выпишем параметры составных чисел $FN = (4,\ 6,\ 8,\ 9,\ 11,\ 13,\ 14,\ 15,\ 16\},$ имеем:

$$P_{Tw} = Ch = N \setminus FN = \{1,\ 2,\ 3,\ 5,\ 7,\ 10,\ 12\} \rightarrow \quad tw_{\,1} = \{\ p_1 = 6 \cdot 1 - 1 = 5, \quad p_2 = 6 \cdot 1 + 1 = 7\},$$
$$tw_2 = \{p_1 = 6 \cdot 2 - 1 = 11,\ p_2 = 6 \cdot 2 + 1 = 13\}, \quad tw_{\,3} = \{\ p_1 = 6 \cdot 3 - 1 = 17, \quad p_2 = 6 \cdot 3 + 1 = 19\},$$
$$tw_4 = \{p_1 = 6 \cdot 5 - 1 = 29,\ p_2 = 6 \cdot 5 + 1 = 31\}, \quad tw_{\,5} = \{\ p_1 = 6 \cdot 7 - 1 = 41, \quad p_2 = 6 \cdot 7 + 1 = 43\},$$
$$tw_6 = \{p_1 = 6 \cdot 10 - 1 = 59,\ p_2 = 6 \cdot 10 + 1 = 61\}, \quad tw_{\,7} = \{\ p_1 = 6 \cdot 12 - 1 = 71,\ p_2 = 6 \cdot 12 + 1 = 73\}.$$

Теорема 3. ***В последующих $\sigma_{1,y}$-последовательностях всегда существуют параметры простых чисел близнецов, отличные от параметров простых чисел близнецов предыдущих $\sigma_{1,y}$-последовательностей.***

Пусть $M_{1,y}$ – число элементов в $\sigma_{1,y}$-последовательности, определенное типом (13'). Обозначим в $\sigma_{1,\,y}$-последовательностях число параметров составных чисел как $\mathrm{KPCN}_{\mathbf{1},\,y}$ и число параметров простых чисел близнецов как $\mathrm{KPTW}_{\mathbf{1},\,y}$, тогда число $\mathrm{KPTW}_{\mathbf{1},\,y} = M_{1,\,y} - \mathrm{KPCN}_{\mathbf{1},\,y}$ в силу (13). Если $\mathrm{KPCN}_{\mathbf{1},y} < M_{1,y}$, то очевидно, что $\sigma_{x,y}$-последовательность содержит параметры простых чисел близнецов. Так как в табл. 1 формируются параметры составных чисел множества Θ и в каждой ее строке по четыре $\mathrm{KPCN}_{\mathbf{1},y}$, то, чтобы сосчитать число параметров составных чисел $\mathrm{KPCN}_{\mathbf{1},y}$ в $\sigma_{1,y}$-последовательности, нужно найти по значениям $M_{1,y}$, где y – номер строки в табл. 1.

Так как в строке $(1, y)$ функция $f_{12}(1, y)$ наибольшая в силу (6) и со значением $\approx 7y,$ то соответствующая строка $y \approx 1 / 7 * \boldsymbol{M_{1,y}}$. Тогда, в $\sigma_{1,y}$-последовательности число параметров составных чисел равно $\mathrm{KPCN}_{1,\,y} \approx 4 / 7 * M_{1,\,y}$, откуда следует, что $\mathrm{KPCN}_{\mathbf{1},\,y} < M_{1,\,y}$. Значит, $\sigma_{1,y}$-последовательности всегда содержат параметры простых чисел близнецов, число которых равно $\mathrm{KPTW}_{\mathbf{1},\,y} = M_{1,\,y} - 4 / 7 * M_{1,\,y} \approx 3 / 7 * M_{1,\,y}$. Для того чтобы убедиться в достоверности распределения параметров простых чисел близнецов, рассмотрим несколько примеров. Так как каждой $M_{1,\,y}$ соответствует своя $\sigma_{1,y}$-последовательность, то очевидно, что при удалении в строках $(1, y)$ табл. 1 параметров составных чисел в ней, в силу (13), останутся параметры простых чисел близнецов:

1. $(1;\ 1),\ M_{1,\,1} = 8 \rightarrow f_{11}(x, y) = \{4\},\ f_{12}(x, y) = \{8\},\ f_{21}(x, y) = \{6\},\ f_{22}(x, y) = \{6\} \rightarrow$
$FN_{1,\,1} = \{4,\ 6,\ 8\},$ тогда $Ch_{1,\,1} = M_{1,\,1} \setminus FN_{1,\,1} = \{1,\ 2,\ 3,\ 5,\ 7\}$ и пусть $A_{1,\,1} = Ch_{1,\,1}$

2. $(1;\ 2),\ M_{1,\,2} = 20 \rightarrow f_{11}(x, y) = \{4,\ 9,\ 14,\ 19\},\ f_{12}(x, y) = \{8,\ 15\},\ f_{21}(x, y) = \{6,\ 13,\ 20\},$
$f_{22}(x, y) = \{6,\ 11,\ 16\},\ FN_{1,\,2} = \{4,\ 6,\ 8,\ 9,\ 11,\ 13,\ 14,\ 15,\ 16,\ 19,\ 20\},$ тогда
$Ch_{1,\,2} = M_{1,\,2} \setminus FN_{1,\,2} = \{1,\ 2,\ 3,\ 5,\ 7,\ 10,\ 12,\ 17,\ 18\},\ A_{1,\,2} = Ch_{1,\,2} \setminus Ch_{1,\,1} = \{10,\ 12,\ 17,\ 18\}.$

3. $(1;\ 3),\ M_{1,\,3} = 36 \rightarrow f_{11}(x, y) = \{4,\ 9,\ 14,\ 19,\ 20,\ 24,\ 29,\ 31,\ 34\},$
$f_{12}(x, y) = \{8,\ 15,\ 22,\ 28,\ 29,\ 36\},\ f_{21}(x, y) = \{6,\ 13,\ 20,\ 24,\ 27,\ 34\},$
$f_{22}(x, y) = \{6,\ 11,\ 16,\ 21,\ 26,\ 31,\ 35,\ 36\},$
$FN_{1,\,3} = \{4,\ 6,\ 8,\ 9,\ 11,\ 13,\ 14,\ 15,\ 16,\ 19,\ 20,\ 21,\ 22,\ 24,\ 26,\ 27,\ 28,\ 29,\ 31,\ 34,\ 35,\ 36\},$
$Ch_{1,\,3} = M_{1,\,3} \setminus FN_{1,\,3} = \{1,\ 2,\ 3,\ 5,\ 7,\ 10,\ 12,\ 17,\ 18,\ 23,\ 25,\ 30,\ 32,\ 33\},$
$A_{1,\,3} = Ch_{1,\,3} \setminus Ch_{1,\,2} = \{23,\ 25,\ 30,\ 32,\ 33\}.$

Пусть $^{*}\mathrm{KPTW}_{\mathbf{1},\ y}$ – число параметров простых чисел близнецов в последующей $\sigma_{1,y}$-последовательности. Тогда разность с числом параметров простых чисел близнецов в предыдущей $\sigma_{1,y}$-последовательности $^{*}\mathrm{KPTW}_{1,\,y} - \mathrm{KPTW}_{1,\,y} = [3 / 7(^{*}M_{1,\,y} - M_{1,\,y})]$, что

показывает число новых параметров простых чисел близнецов. Так как $*M_{1,y} - M_{1,y} = 2(y+1) * *((y+1)+3) - 2y(y+3) = 4y+8$ и всегда > 7 при любом $y \in N$, то в последующих $\sigma_{1,y}$-последовательностях всегда имеются параметры простых чисел близнецов, отличные от параметров простых чисел близнецов предыдущих $\sigma_{1,y}$-последовательностей.

Теорема 4. ***Множество простых чисел близнецов бесконечно.***

Функции (5) бесконечные и возрастающие, т. к. разности

$m_1 > 0, m_2 > 0, m_3 > 0, m_4 > 0 \forall x \in N$, где $m_1 = f_{11}(x, y+1) - f_{11}(x, y) = 6x - 1$,

$m_2 = f_{22}(x, y+1) - f_{22}(x, y) = 6x - 1$, $m_3 = f_{21}(x, y+1) - f_{21}(x, y) = 6x + 1$,

$m_4 = f_{12}(x, y+1) - f_{12}(x, y) = 6x + 1$

и зависят от двух переменных. Тогда их значения могут быть и равными, хотя это не влияет на процесс роста параметров простых чисел близнецов, ибо в объединениях $FN_{1,y}$-последователь ностей одинаковые элементы отсеиваются, а сами элементы занимают свои места в них, не нарушая рост параметров простых чисел близнецов $Ch_{1,y} = M_{1,y} \setminus FN_{1,y}$. Параметры простых чисел близнецов в последовательностях $A_{1,y} = Ch_{1,y+1} \setminus Ch_{1,y}$ всегда останутся различными, потому что элементы $\sigma_{1,y}$-последовательностей упорядоченные и различные. Пусть процесс получения параметров простых чисел близнецов применим и к числам с номером $A_{1,n}$. И пусть на шаге $n+1$ процесс получения параметров простых чисел близнецов разрывается, т. е. $A_{1,n+1} = \varnothing$. Но по Теореме 3 в последующих $\sigma_{1,y}$-последовательностях всегда существуют параметры чисел близнецов, отличные от параметров чисел близнецов предыдущих $\sigma_{1,y}$-последовательностей, что противоречит допущению. Значит, $A_{1,n+1} \neq \varnothing$. Таким образом, построено счетное множество последовательностей параметров простых чисел близнецов $\bigcup_{i=1}^{n} A_{1,i}$. И т. к. счетное множество равномощно к $\boldsymbol{N}$, то бесконечны и параметры, и сами простые числа близнецы.

Таблица 5

Параметры простых чисел близнецов ($P_{Tw} = Ch$) от 1 до 6300

1, 2, 3, 5, 7, 10, 12, 17, 18, 23, 25, 30, 32, 33, 38, 40, 45, 47, 52, 58, 70, 72, 77, 87, 95, 100, 103, 107, 110, 135, 137, 138, 143, 147, 170, 172, 175, 177, 182, 192, 205, 213, 215, 217, 220, 238, 242, 247, 248, 268. 270, 278, 283, 287, 298, 312, 313, 322, 325, 333, 338, 347, 348, 352, 355, 357, 373, 378, 385, 390, 397, 425, 432, 443, 448, 452, 455, 465, 467, 495, 500, 520, 528, 542, 543, 550, 555, 560, 562, 565, 577, 578, 588, 590, 593, 597, 612, 628, 637, 642, 653, 655, 667, 670, 675, 682, 688, 693, 703, 705, 707, 710, 712, 723, 737, 747, 753, 758, 773, 775, 787, 798, 800, 822, 828, 835, 837, 850, 872, 880, 903, 907, 913, 917, 920, 940, 942, 943, 957, 975, 978, 980,1015, 1022,1033,1045, ...

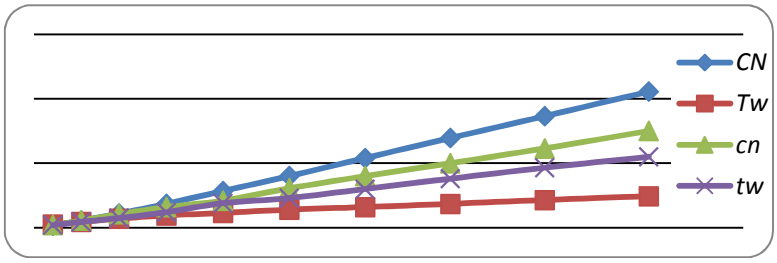

Рис. 2. Диаграмма роста количества простых чисел близнецов в интервале 1 – $M_{1,y}$: *CN* – составных чисел фактических; *Tw* – простых чисел близнецов фактических; *cn* – составных чисел теоретических, *tw* – простых чисел близнецов теоретических

7. Составные числа близнецы

Из табл. 1 легко заметить, что параметры составных чисел близнецов лежат на пересечениях значений функций (5). Рассмотрим несколько параметров составных чисел близнецов, лежащих на пересечениях значений функций (5): $P_{TwCN} = \{20, 24, 36, 41, 54, 57\}$. Тогда соответствующие им составные числа близнецы: $TwCN_{20} = (119; 121)$, $TwCN_{24} = (143; 145)$, $TwCN_{36} = (215, 217)$, $TwCN_{41} = (245, 247)$, $TwCN_{54} = (323, 325)$, $TwCN_{57} = (341, 343)$, $TwCN_n = \{6n \pm 1 / n \in P_{TwCN}\}$.

Алгоритм составных чисел близнецов:

A. *Описание программы N.* Так же, как и в параграфе 6 ***A***.

B. *Описание программы TwCN.* Проверяются на простоту числа вида $\theta_1 = 6 \cdot id - 1$ и $\theta_2 = 6 \cdot id + 1,$ где id – номера записей в файле T. Если хоть одно из чисел θ_1 или θ_2 простое, то удаляется соответствующее значение поля $[N]$.

C. *Описание программы DisTwCN*. Если $\lambda = [N] \neq \varnothing,$ то значения полей $[prm\ 1] = 6 \cdot [N] - 1$ и $[prm\ 2] = 6 \cdot [N] + 1$ в паре образуют множество.

Теорема 5. ***Составные числа близнецы во множестве* Θ *бесконечны.***

Рассмотрим множества X_i и A_i, состоящие из объединений и пересечений параметров P_{CN}.

1. $X_1 = FN^+ = 4,\ 8,\ 9,\ 14,\ 15,\ 19,\ 22,\ 24,\ 29,\ 34,\ 36,\ 39,\ 43,\ 44,\ 49,\ 50,\ 57,\ 64,\ 71\},$ и пусть $A_0 = X_1$;

$FN^- = \{6,\ 11,\ 13,\ 16,\ 20,\ 21,\ 26,\ 27,\ 31,\ 34,\ 36,\ 41,\ 46,\ 48,\ 51,\ 55,\ 62,\ 69$

$$X_2 = \{FN^+ = \{20, 28, 31, 41, 42, 53, 54, 64, 67, 75, 80, 86, 93, 97, 106, 108, 119, 132\},$$
$$FN^- = \{24,\ 35,\ 37,\ 46,\ 50,\ 57,\ 63\ 68,\ 76,\ 79,\ 89,\ 90,\ 101,\ 102,\ 112,\ 115,\ 128\}$$

$$\beta_1 = X_2 \cap A_0 = \{20, 24,\ 31,\ \ 34,\ 36,\ 41,\ 50,\ 57\}$$

$$A_1 = A_0 \cup X_2 = FN^+ = 4,\ 8,\ 9,\ 14, 15, 19,\ 22,\ 24,\ 29, 34,\ 36, 39,\ 43,\ 44,\ 48,\ 49, 50, 57,\ 64, 71,$$
$$20,\ 28,\ 31,\ 41,\ 42,\ 53,\ 54,\ 64,\ 67,\ 75,\ 80,\ 86,\ 93,\ 97,\ 106,\ 108,\ 119,\ 132,$$
$$FN^- = 6,\ 11,\ 13,\ 16,\ 20,\ 21,\ 26,\ 27,\ 31,\ 34,\ 36,\ 41,\ 46,\ 48,\ 51,\ 55,\ 62,\ 69$$
$$24,\ 35,\ 37,\ 46,\ 50,\ 57,\ 63,\ 68,\ 76,\ 79,\ 89,\ 90,\ 101,\ 102,\ 112,\ 115,\ 128$$

2. $X_3 = FN^+ = 48, 60, 65, 79, 82, 98, 99, 116, 117, 133, 136, 150, 155, 167, 174, 193$

$FN^- = 54,\ 71,\ 73,\ 88,\ 92,\ 105,\ 111,\ 122,\ 130,\ 139,\ 149,\ 156,\ 168,\ 173,\ 187$

$$\beta_2 = X_3 \cap A_1 = \{48,\ 71, 79\}$$

$$A_2 = A_1 \cup X_3 = FN^+ = 4,\ 8,\ 9,\ 14,\ 15,\ 19,\ 22,\ 24,\ 29,\ 34, 36,\ 39,\ 43,\ 44,\ 48,\ 49,\ 50, 57, 64, 71,$$
$$20, 28, 31, 41, 42, 53, 54, 64, 67, 75, 80, 86, 93,\ 97,\ 106, 108, 119,\ 132, 48,$$
$$60, 65, 79, 82, 98, 99, 116, 117, 133, 136, 150, 155, 167, 174, 193$$
$$FN^- = 6,\ 11,\ 13,\ 16,\ 20,\ 21,\ 26,\ 27,\ 31,\ 34,\ 36,\ 41,\ 46,\ 48,\ 51,\ 55,\ 62,\ 69$$
$$24,\ 35,\ 37,\ 46,\ 50,\ 57,\ 63,\ 68,\ 76,\ 79,\ 89,\ 90,\ 101,\ 102,\ 112,\ 115,\ 128$$

3. $X_4 = FN^+ =\ 88, 104, 111, 129, 134, 154, 157, 179, 180, 203, 204, 226,\ 229,\ 254$

$FN^- =\ 96,\ 119,\ 121,\ 142,\ 146,\ 165,\ 171,\ 188,\ 196,\ 211,\ 221,\ 234,\ 246$

$$\beta_3 = X_4 \cap A_2 = \{88,\ \ 111, 119\}\ \ .\ .\ .$$

Пусть утверждение верно и с номером β_n. Докажем, что вышеизложенный процесс получения параметров составных чисел близнецов не разрывается со следующим шагом $n = n + 1$. Допустим, что процесс разрывается, т. е. $\beta_n = \varnothing,$ тогда элементы $\beta_{n+1} = X_{n+2} \cap A_n = \varnothing,$ откуда следует, что функции (5) ограниченные. Это приводит к противоречию, ибо ранее было доказано, что функции (5) бесконечные. Тогда из противоречия следует, что $\beta_{n+1} \neq \varnothing.$ Таким образом, построено счетное множество последовательностей параметров составных чисел близнецов. Пусть $B = \bigcup_{i=1}^{m} \beta_i$, где $m \in N.$ Так как параметры составных чисел близнецов P_{TwCN} при формировании множеств FN^+ и FN^- являются различными (в силу операции объединения), то различными будут и сами составные числа близнецы $TwCN$. Так как счетное множество с различными элементами – бесконечное множество, то параметры составных чисел близнецов P_{TwCN} бесконечны, а значит, бесконечны и сами числа $TwCN$ (табл. 6). ***Теорема доказана.***

Таблица 6

Параметры составных чисел близнецов множества Θ (P_{TwCN}) от 1 до 2 500

20, 24, 31, 34, 36, 41, 48, 50, 54, 57, 69, 71, 79, 86, 88, 89, 92, 97, 104, 106, 111, 116, 119, 130, 132, 134, 136, 139, 141, 145, 149, 150, 154, 160, 167, 171, 174, 176, 179, 180, 189, 190, 191, 193, 196, 201, 207, 209, 211, 212, 219, 222, 223, 224, 225, 226, 231, 232, 234, 236, 244, 246, 251, 253, 256, 265, 272, 274, 275, 279, 280, 281, 284, 286, 288, 294, 295, 299, 301, 303, 306, 307, 309, 314, 316, 320, 321, 323, 324, 326, 327, 328, 337, 339, 341, 343, 345, 349, 351, 353, 354, 358, 361, 362, 364, 365, 366, 371, 372, 376, 377, 384, 386, 387, 388, 394, 401, 405, 409, 414, 415, 416, 418, ...

8. Тест *Primality* – проверка чисел вида 6*k* ± 1 на простоту

Существуют 2 вида проверок (тестов) чисел на простоту: истинные и вероятностные. Одним из истинных является тест Люка – Лемера. Недостаток этого теста заключается в том, что его можно применять только к рядам определенного вида. Вычислительная сложность $\approx O(q^2 \cdot \log q \cdot \log\log q)$. Ограничения имеет и тест Пепина, использующийся для проверки на простоту чисел Ферма. Тест Аггавала – Каяла – Саксены (тест AKS) считается универсальным, полиномиальным и детерминированным: если $\exists\, r \in Z$ и $\alpha_r(\nu) > \log^2 n,$, и $\forall\, a$ от 1 до $[\sqrt{\varphi(r)} \cdot \log n]$ выполняется $(x+a)^n \equiv (x^n + a) \pmod{x^r - 1, n}$, то n либо простое число, либо степень простого числа. Вычислительная сложность теста $\approx O(\log^6 n)$, если предположения верности гипотезы Артина верны, иначе $\approx O\ (\log^{10.5} n)$.

При проверке на простоту натуральных чисел вида $n = 6\lambda \pm 1$ исследуются их параметры **λ**.

Определяются типы множеств, к которым принадлежат параметры **λ**. Тогда с точностью устанавливается тип числа (составное или простое). Тест является независимым, универсальным, детерминированным и полиномиальным. Вычислительная сложность $\approx O\ (n/2)$.

Пусть число n = 557 = 6 · 93 – 1. Тогда параметр $\lambda = 93$, и, по методу определения простых чисел по их порядковым номерам, имеем: $R_n(93) = "+"$, и, значит, $557 \in P$. Однако этот же результат можно получить и по тесту *Primality* $6\lambda \pm 1$, т. к. параметр $93 = 6 \cdot 2 \cdot 7 + 2 + 7$ может быть представлен в виде функции $(6xy + x + y) \in FN^+$, и, значит, $557 \in P$. Пусть n = 4 294 967 297 = 6 715 827 883 – 1. Тогда параметр λ = 715827883. Из-за ограниченного размера табл. 2 трудно определить методом вычисления простых чисел по их порядковым номерам $R_n(\lambda)$ соответствующий знак, поэтому воспользуемся тестом *Primality* $6\lambda \pm 1$. При значениях x = 107, y = 116 736 параметр $\lambda = 715827883 = 6 \cdot 107 \cdot 1116736 + 107 - 1\ 116736$, т. е. $\lambda \in FN^-$, значит, по (8) число составное и n = 641 · 6700417. Пусть число n = 197297 = 6 32883 – – 1. Тогда параметр $\lambda = 32883 \in Tw$, т. е. не представим ни одной из функций (5), значит, $197297 \in P$. Примеры с использованием больших чисел: n = 18 446744073709551617 = = 6 · 3074457345618258603 – 1 → λ = 3074457345618258603 при $x = 45696$, y=11213403551787, $\lambda = 6 \cdot 11\ 213\ 403\ 551\ 787 \cdot 45\ 696 - 45\ 696 + 11\ 213\ 403\ 551\ 787$, т. е. $\lambda \in FN^-$, по (8) является составным: $n = 18446744073709551617 = 274177 \cdot 67280421310721$.

Пусть число $n = 1471 = 6 \cdot 245 + 1$, тогда параметр $\lambda = 245$ не представим ни одной из функций (5), т. е. по (11) является параметром простых чисел близнецов, поэтому $1471 \in P$. Пусть число $n = 524287 = 6 \cdot 87381 + 1$, тогда параметр $\lambda = 87381$, $\lambda = 6 \cdot 4 \cdot 3799 + 4 - 3799$, т. е. $\lambda \in FN^-$, следовательно, по (10) число $524287 \in P$. Число $n = 536870911 = 6 \cdot 89478485 + 1$, тогда параметр $\lambda = 89478485$, по тесту *Primality* $6\lambda \pm 1$ найдём соответствующую функцию (5). При числовых значениях $x = 39$, $y = 384028$, параметр $\lambda = 89478485 == 6 \cdot 39 \cdot 384028 - -39 - 384028$, т. е. $\lambda \in FN^+$, значит, по (8), число составное: $n = 536870911 = 233 \cdot 2304167$.

Ниже приводится исходный текст использованной программы:

```
Private Sub Primality_Click() Dim i, m, m1, m2, m3, m4, t1, t2 As String
ora 1 = Time() ora 2 = "" t1 = 0  t2 = 0  m = sl4  m3 = dln(m, 6, ss)
If IsNull(m) Or m = "" Or m = " " Or m = 0 Then  П4 = " Вводите число или сделайте клик над числом "
```

```
Else ππ = 6 * m – 1,  πχ = 6 * m + 1, pol6 = sl4 πχ 1 = "FN – :  6xy – x + y :"   πχ 2 ="FN + :  6xy – x –
y : " πχ 3 = "FN – : 6xy + x – y :"    πχ 4 = "FN + :  6xy + x + y : "
For i = 1 To m3
m1 = slg(m, i, ss)  m2 = vich(umn(i, 6, ss), 1, ss) If OST(m1, m2, ss) = 0 Then
 t1 = i  t2 = dln(m1, m2, ss)    m4 = vich(vich(umn(umn(t1, t2, ss), 6, ss), t1, ss), t2, ss)
  If m = m4 Then πχ 2 = πχ 2 & "    x= " & t1 & "  y= " & t2
Else
End If
m1 = vich(m, i, ss)   m2 = slg(umn(i, 6, ss), 1, ss) If OST(m1, m2, ss) = 0 Then
 t1 = i    t2 = dln(m1, m2, ss)  m4 = slg(slg(umn(umn(t1, t2, ss), 6, ss), t1, ss), t2, ss)
 If m = m4 Then πχ 4 = πχ 4 & "    x= " & t1 & "  y= " & t2
Else
End If
m1 = slg(m, i, ss)     m2 = slg(umn(i, 6, ss), 1, ss) If OST(m1, m2, ss) = 0 Then
t1 = i  t2 = dln(m1, m2, ss)    m4 = slg(vich(umn(umn(t1, t÷2, ss), 6, ss), t1, ss), t2, ss)
If m = m4 Then πχ 1 = πχ 1 & "    x = " & t1 & "  y = " & t2
Else
End If
m1 = vich(m, i, ss)     m2 = vich(umn(i, 6, ss), 1, ss) If OST(m1, m2, ss) = 0 Then
t1 = i  t2 = dln(m1, m2, ss)    m4 = vich(slg(umn(umn(t1, t2, ss), 6, ss), t1, ss), t2, ss)
If m = m4 Then πχ 3 = πχ 3  & "    x = " & t1 & "  y = " & t2
End If              // slg(m, i, ss)  –  сложение больших чисел vich(m, i, ss)  –  вычитание больших
чисел
Next I              umn(πχ1, πχ2, ss) –  умножение больших чисел  dln(m1, m2, ss)  –  деление
больших чисел
 ora 2 = Time()     OST(m1, m2, ss)      –  остаток при делении больших чисел
End If   End Sub
```

Заключение

Комплексное исследование проблемы нахождения и распределения простых и составных чисел, простых чисел близнецов и составных чисел близнецов, включающее теоретическое исследование, его программное обеспечение и численный анализ, позволило получить следующие результаты:

– предложен новый алгоритм нахождения и распределения простых чисел;

– приведено вычисление точного числа простых чисел $\pi(x)$ в интервале $1 \div x$;

– предложен способ получения простых чисел $P(n)$ по их порядковым номерам n во множестве простых чисел $p \geq 5$;

– предложен алгоритм проверки на простоту чисел вида $6\lambda \pm 1$;

– получен метод распределения параметров простых и составных чисел;

– доказано, что любое составное $n \in \Theta$ может быть представлено одним из произведений $(6x \pm 1) \cdot (6y \pm 1)$, где x и y являются решениями одного из четырех диофантовых уравнений $6xy \pm x \pm y = \lambda$;

– приведены алгоритмы нахождения простых чисел близнецов и составных чисел близнецов, даны варианты доказательств их бесконечного количества.

СПИСОК ЛИТЕРАТУРЫ

1. *Прахар К.* Распределение простых чисел. М.: Мир, 1967. 511 с.

2. *Крэндалл Р., Померанс К.* Простые числа. Криптографические и вычислительные аспекты. М.: УРСС: Книжный дом «Либроком», 2011. 664 с.

3. *Гельфанд А. О., Линник Ю. В.* Элементарные методы в аналитической теории чисел. М.: Физматгиз, 1962. 131 с.

4. *Чермидов С. И.* О факторизации натуральных чисел // Диалоги о науке. 2011. № 2. С. 68–70.

Статья поступила в редакцию 29.05.2017,
в окончательном варианте – 14.07.2017

ИНФОРМАЦИЯ ОБ АВТОРЕ

Чермидов Сергей Иванович – Россия, 350040, Краснодар; Кубанский государственный университет; соискатель кафедры прикладной математики; chermidov.sergei@mail.ru.

S. I. Chermidov

DISTRIBUTION OF PRIME AND COMPOSITE NUMBERS AND THEIR ALGORHYTHMIC APPENDICES

Abstract. The article focuses on methods defining and distributing the composite numbers, prime numbers, twins of prime numbers and composite numbers of twins that do not have divisors 2 and 3 in N, based on the set of numbers of type $\Theta = \{6k \pm 1 \,/\, k \in N\}$ where N is the set of all natural numbers, which is a semigroup with respect to multiplication. The calculation the exact quantity of primes in a given interval is given. A method for obtaining prime numbers $p \geq 5$ by their ordinal numbers in a set of primes $p \geq 5$ is proposed, as well as a new algorithm for finding and distributing prime numbers on the basis of the closeness of the set Θ. The article shows that any composite number $n \in \Theta$ is representable as products $(6x \pm 1)\,(6y \pm 1)$, where $x, y \in N$ are the natural solutions of one of the four Diophantine equations $P(x, y, \lambda) = 0 : 6 \cdot xy \pm x \pm y - \lambda = 0$. It has been proved that if there is a parameter λ of twins of prime numbers, then none of the Diophantine $P(x, y, \lambda) = 0$ equations has any solutions. A new universal, deterministic, polynomial and independent verification test is provided for the simplicity of the numbers of a species $6 \cdot k \pm 1$. Algorithms of distributions of parameters of twins of prime numbers and parameters composite numbers of twins are given, they are not divisible by 2 and 3, and variants of proofs for their infinite number are given.

Key words: simple and composite numbers, parameters of prime numbers, Diophantine equations, twins of prime numbers, test for simplicity testing, algorithm for parameter distribution.

REFERENCES

1. Prashar K. *Primzahlverteilung*. Springer, Berlin, 1957. 527 p. (Russ. ed.: Prakhar K. Raspredelenie prostykh chisel. Moscow, Mir Publ., 1967. 511 p.).

2. Crandall R., Pomerance C. *Prime Numbers: A Computational Perspective*. New York: Springer-Verlag, 2001. 545 p. (Russ. ed.: Krendall R., Pomerans K. Prostye chisla. Kriptograficheskie i vychislitel'nye aspekty. Moscow, URSS: Knizhnyi dom «Librokom», 2011. 664 p.).

3. Gel'fand A. O., Linnik Iu. V. *Elementarnye metody v analiticheskoi teorii chisel* [Elementary methods in analytical number theory]. Moscow, Fizmatgiz, 1962. 131 p.

4. Chermidov S. I. O faktorizatsii natural'nykh chisel [On factorization of natural numbers]. *Dialogi o nauke*, 2011, no. 2, pp. 68-70.

The article submitted to the editors 29.05.2017,
in the final version – 14.07.2017

INFORMATION ABOUT THE AUTHOR

Chermidov Sergey Ivanovich – Russia, 350040, Krasnodar, Kuban State University, Competitor for a Scientific Degree of the Department of Applied Mathematics; chermidov.sergei@mail.ru.