УДК 511.17

В.М. Зюзьков

ПОСЛЕДОВАТЕЛЬНОСТЬ FIBONACCI(n) MOD n

Исследуется поведение последовательности Fibonacci(n) mod n. Рассматриваются некоторые подпоследовательности: n пробегает множество простых чисел и случаи, когда $n = q \times p$, где p пробегает множество простых чисел, а q – некоторое фиксированное натуральное число. Проводятся компьютерные исследования с помощью системы Mathematica, высказываются гипотезы, которые затем доказываются.

Ключевые слова: *последовательность чисел Фибоначчи*, *остатки от деления*, *сравнения*, *система Mathematica.*

Пусть $F(n)$ обозначает n-е число Фибоначчи. Последовательность $F(n) \bmod n$ (остаток от деления $F(n)$ на n) показывает замечательно сложное поведение. На рис. 1 изображен график первых двухсот чисел этой последовательности.

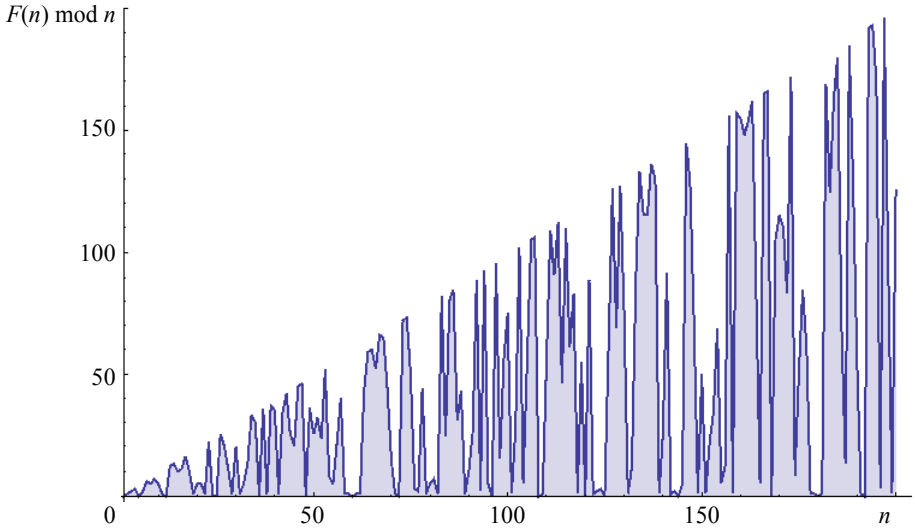

Рис. 1. График первых двухсот чисел последовательности $F(n) \bmod n$

Стивен Волфрам [1] полагает, что возможно провести полный анализ поведения этой последовательности, например представив значение $F(n) \bmod n$ в терминах стандартных теоретико-числовых функций от n, описать ее поведение простой примитивной рекурсией.

Последовательность $F(n) \bmod n$ представлена в on-line-энциклопедии Слоана последовательностью целых чисел [2], но там отсутствует анализ ее поведения. Автор исследует подпоследовательности вида $F(q \times p) \bmod q \times p$, где q – фиксированное натуральное число, а p пробегает простые числа. С помощью системы Mathematica вычисляются начальные отрезки подпоследовательностей, высказы-

ваются гипотезы, проводятся эксперименты для проверки. Доказаны достаточные условия на q, при которых значения последовательности $F(q\times p) \bmod q\times p$ лежат только на двух прямых. В частности, первые 13 значений q суть 1, 2, 5, 10, 12, 24, 25, 36, 48, 50, 60, 72, 96.

Когда в последовательности $F(n) \bmod n$ встречаются нули?

Перечислим известные факты.

1. Числа $F(5^k) \bmod 5^k$ равны нулю для натурального k [3].

2. Числа $F(4\times 3^k) \bmod 4\times 3^k$ равны нулю для любого положительного целого k [4].

Но не только для $n = 5^k$ или $n = 4\times 3^k$ числа $F(n) \bmod n$ равны 0. Были рассмотрены первые 250 тысяч чисел Фибоначчи. Отметим, что

$$F(250\ 000) = 36356117010939561826426164175798 4 \text{ <<52 180 цифр>>}$$
$$78569911024351647095730923104687 5.$$

Пусть R обозначает множество $\{F(n) \mid n \le 250\ 000, F(n) \bmod n = 0\}$. Оказывается, это множество состоит из 1406 чисел. Чисел вида $F(5^k)$ только восемь, $n = 1, 5, 25, 125, 625, 3125, 15625, 78125$. За исключением этих восьми чисел и числа $F(5^2\times 3001)$ все остальные числа в R имеют вид $F(12k)$. Чисел вида $F(4\times 3^k)$ только десять, $n = 12, 36, 108, 324, 972, 2916, 8748, 26244, 78732, 236196$. Три числа $F(24)$, $F(36)$ и $F(60)$ из R имеют вид $F(12p)$, где p – простое число. Остальные числа из R имеют вид $F(12k)$, где k – составное число. Но обратное неверно. Среди первых 250 000 чисел Фибоначчи имеется 17094 числа, которые не принадлежат R, хотя номера их имеют вид $12k$ и k – составное. Первые три таких числа $F(12\times 21)$, $F(12\times 22)$ и $F(12\times 26)$.

Подпоследовательность $F(p) \bmod p$, p – простое

Рассмотрим числа Фибоначчи с номерами, которые являются простыми числами. Отложим на оси *абсцисс* первые 200 простых чисел $P(n)$ ($n = 1, 2, \ldots, 200$), а на оси *ординат* соответствующие значения $F(P(n)) \bmod P(n)$. График полученных точек $(P(n), F(P(n)) \bmod P(n))$ изображен на рис. 2.

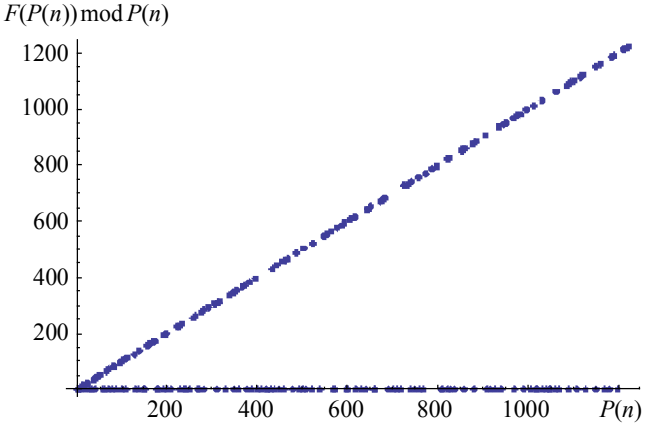

Рис. 2. График последовательности $P(n) \to F(P(n)) \bmod P(n)$

Изучение графика приводит к предположению, что $F(p) \bmod p$ может быть равно только 1 или $p-1$. Более детальный анализ с помощью системы Mathematica приводит к теореме.

Теорема 1.

a) Если простое p имеет вид $5t \pm 1$, то $F(p) \bmod p = 1$.

b) Если простое p имеет вид $5t \pm 2$, то $F(p) \bmod p = p - 1$.

Для доказательство теоремы нам потребуется лемма.

Лемма 1 [5, с. 53–54].

a) Если простое p имеет вид $5t \pm 1$, то p делит $5^{(p-1)/2} - 1$.

b) Если простое p имеет вид $5t \pm 2$, то p делит $5^{(p-1)/2} + 1$.

***Доказательство теоремы* 1**. Если $p = 2$, то $F(p) = F(2) = 1 \equiv -1 \pmod 2$. Поэтому в дальнейшем предполагаем, что p нечетно.

По формуле Бине имеем

$$F(p) = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^p - \left(\frac{1-\sqrt{5}}{2}\right)^p\right) =$$

$$= \frac{1}{\sqrt{5}}\frac{1}{2^p}\sum_{k=0}^{p}\left(C_p^k\left((\sqrt{5})^k - (-1)^k(\sqrt{5})^k\right)\right) =$$

$$= \frac{1}{\sqrt{5}}\frac{1}{2^p}\sum_{\substack{k=1,\\ k\ нечетно}}^{p}\left(2C_p^k\left((\sqrt{5})^k\right)\right) =$$

$$= \frac{1}{2^{p-1}}\sum_{\substack{k=1,\\ k\ нечетно}}^{p}\left(C_p^k\left((\sqrt{5})^{k-1}\right)\right) =$$

$$= \frac{1}{2^{p-1}}\sum_{\substack{k=1,\\ k\ нечетно}}^{p} C_p^k 5^{(k-1)/2} =$$

$$= \frac{1}{2^{p-1}}\left(C_p^1 + C_p^3 5 + C_p^5 5^2 + \ldots + C_p^{p-2}5^{(p-3)/2} + C_p^p 5^{(p-1)/2}\right).$$

Получаем

$$2^{p-1}F(n) = C_p^1 + C_p^3 5 + C_p^5 5^2 + \ldots + C_p^{p-2}5^{(p-3)/2} + C_p^p 5^{(p-1)/2}.$$

Так как

$$C_p^k = \frac{p!}{k(p-k)!}$$

и, если $0 < k < p$, то p в числителе C_p^k не сокращается. Поэтому все биномиальные коэффициенты в правой части, за исключением последнего, делятся на p, а $C_p^p = 1$. Отсюда имеем $2^{p-1}\ F(p) \equiv 5^{(p-1)/2} \pmod p$. По малой теореме Ферма $2^{p-1} \equiv 1 \pmod p$. Поэтому, используя лемму 1, получаем утверждение теоремы. ■

Подпоследовательности $F(q\times p) \bmod q\times p$, p – простое

Будем изучать подпоследовательности $F(q\times p) \bmod q\times p$, где q – фиксированное натуральное число, а p пробегает простые числа. Меняя q, имеем разное поведение подпоследовательностей. На рис. 3 – 8 видим типичные ситуации для некоторых небольших q. На оси *абцисс* размещаем числа $q\times P(n)$ ($P(n)$ – n-е простое число), а на оси *ординат* соответствующие значения $F(P(n)) \bmod P(n)$.

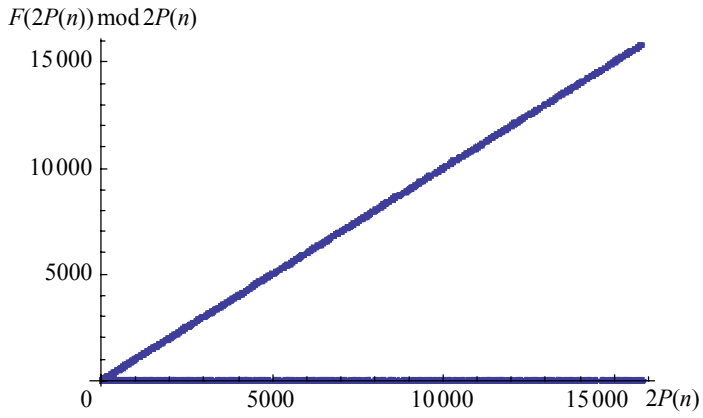

Рис. 3. График последовательности
$2P(n) \to F(2P(n)) \bmod 2P(n)$

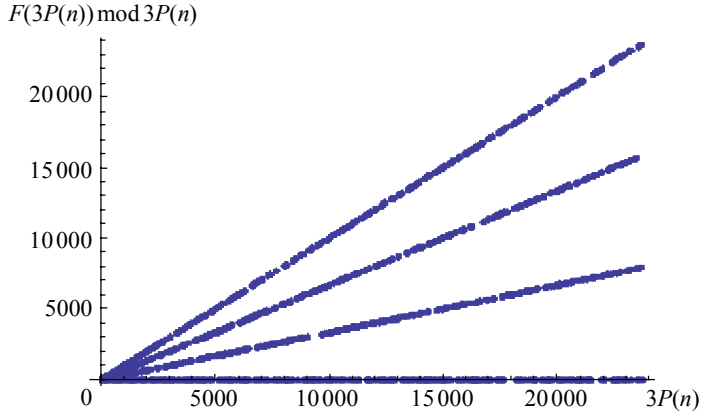

Рис. 4. График последовательности
$3P(n) \to F(3P(n)) \bmod 3P(n)$

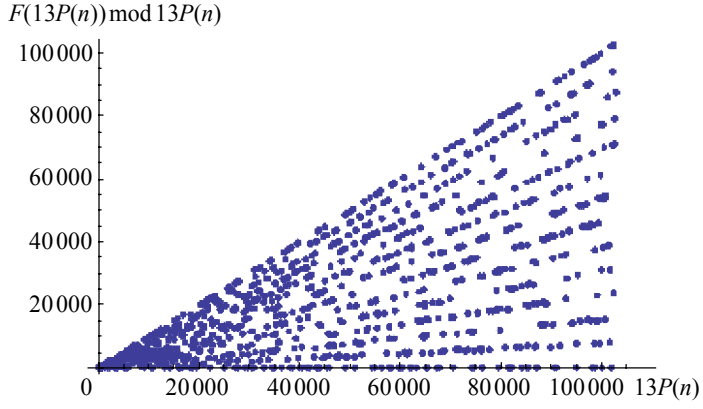

Рис. 5. График последовательности
$13P(n) \to F(13P(n)) \bmod 13P(n)$

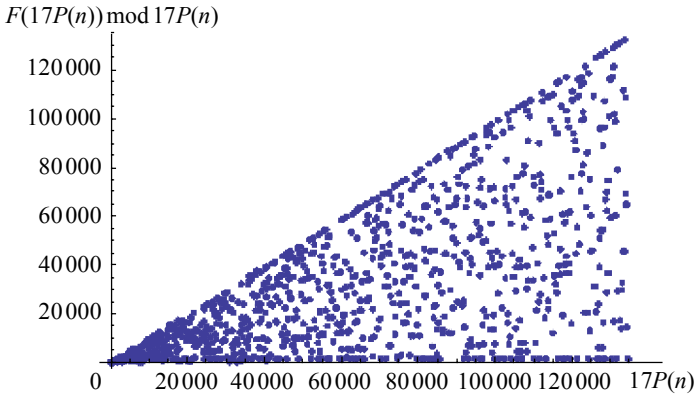

Рис. 6. График последовательности
$17P(n) \to F(17P(n)) \bmod 17P(n)$

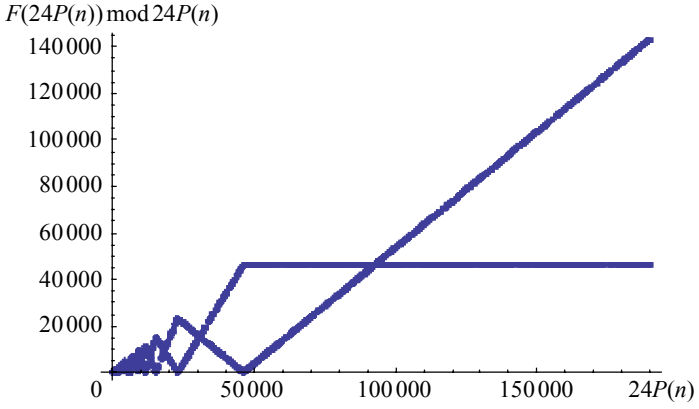

Рис. 7. График последовательности
$24P(n) \to F(24P(n)) \bmod 24P(n)$

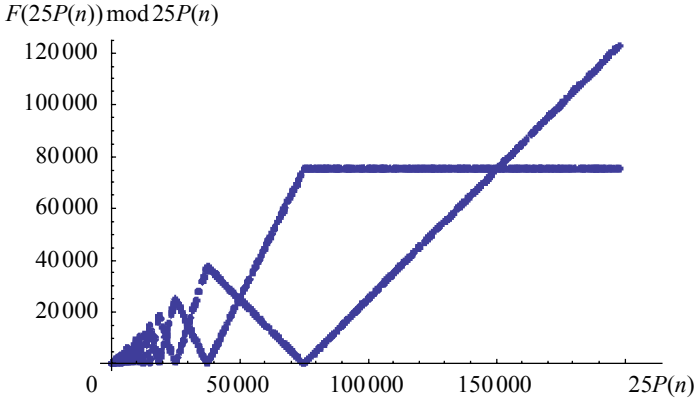

Рис. 8. График последовательности
$25P(n) \to F(25P(n)) \bmod 25P(n)$

На рис. 3, 7 и 8 значения ($q\times p$, $F(q\times p) \bmod q\times p$) находятся на двух прямых, начиная с некоторого $q\times p_0$. Такие случаи изучены. Для $n = 3p$ и $n = 4p$ высказаны только гипотезы без доказательств.

Ситуации, в которых поведение подпоследовательности $F(q\times p) \bmod q\times p$ описывается двумя прямыми, первоначально изучались по отдельности для разных значений q. Затем полученные результаты были обобщены. Мы же сейчас начнем с доказательства общих результатов, а потом приведем следствия.

Теорема 2. Пусть q – такое натуральное число, что выполнено условие

$$\forall p > \max(5, F(q)) \Rightarrow F(q\times p) \equiv \pm F(q) \bmod q. \qquad (1)$$

(Сравнение в (1) выполнено одновременно как для положительных, так и для отрицательных значений $F(q)$.)

Тогда

a) Если простое p имеет вид $5t \pm 1$, то $F(q\times p) \bmod q\times p = F(q)$.

b) Если простое p имеет вид $5t \pm 2$, то $F(q\times p) \bmod q\times p = q\times p - F(q)$.

Для доказательства теоремы 2 нам потребуется две леммы.

Лемма 2 (теорема Десмонда). Пусть p – простое число. Тогда для любого натурального n имеем

$$F(p\times n) \equiv F(n)\, F(p) \bmod p.$$

Оригинал изложен в [6]. Доступное доказательство см. в [3].

Лемма 3. Если сравнение $a \equiv b$ имеет место по нескольким разным модулям, то оно имеет место и по модулю, равному наименьшему общему кратному этих модулей.

Доказательство. Если $a \equiv b \pmod m$ и $a \equiv b \pmod n$, то $a - b$ делится на m и n и значит, что $a - b$ делится на наименьшее общее кратное m и n.

***Доказательство теоремы* 2**. Теорема Десмонда дает $F(q\times p) \equiv F(q)\, F(p) \bmod p$. Поэтому по теореме 1:

*a*1) Если простое p имеет вид $5t \pm 1$, то $F(q\times p) \equiv F(q) \bmod p$.

*b*1) Если простое p имеет вид $5t \pm 2$, то $F(q\times p) \equiv -F(q) \bmod p$.

Если $p > \max(5, F(q))$, то по условию (1) имеем

*a*2) Если простое p имеет вид $5t \pm 1$, то $F(q\times p) \equiv F(q) \bmod q$.

*b*2) Если простое p имеет вид $5t \pm 2$, то $F(q\times p) \equiv -F(q) \bmod q$.

Так как p – простое и $p > q$, то наименьшее общее кратное p и q равно qp. Поэтому по лемме 3 имеем

*a*3) Если простое p имеет вид $5t \pm 1$, то $F(q\times p) \equiv F(q) \bmod q\times p$.

*b*3) Если простое p имеет вид $5t \pm 2$, то $F(q\times p) \equiv -F(q) \bmod q\times p$.

Следовательно, для любого $p > \max(5, F(q))$ выполнено утверждение теоремы. ■

Чтобы получить следствие из теоремы, нам необходима следующая лемма.

Лемма 4. [5] Если $n > 2$, то $F(m)$ делится на $F(n)$ тогда и только тогда, когда m делится на n.

Следствие 1. Пусть $F(q) \bmod q = 0$. Тогда для каждого $p > \max(5, F(q))$ имеем

a) Если простое p имеет вид $5t \pm 1$, то $F(q\times p) \bmod q\times p = F(q)$.

b) Если простое p имеет вид $5t \pm 2$, то $F(q\times p) \bmod q\times p = q\times p - F(q)$.

Доказательство. Так как q делит $\pm F(q)$ и, по лемме 4, $F(q)$ делит $F(q\times p)$, то $F(q\times p) \equiv \pm F(q) \bmod q$. Получили условие (1). ■

Как мы знаем из введения, среди первых 250 000 значений q условие следствия 1 выполнено для 1406 значений q. Приведем несколько первых пар таких значений (q, $F(q)$); вторая компонента пары ограничивает снизу начальное значение p, начиная с которого поведение последовательности $F(q\times p) \bmod q\times p$ описывается двумя прямыми.

Первые значения q из следствия 1

q	$F(q)$
5	5
12	144
24	46368
25	75025
36	14930352
48	4807526976
60	1548008755920
72	498454011879264
96	51680708854858323072
108	16641027750620563662096

Следствие 2. Пусть $q = 2t$, причем t не делится на 3 и t – делитель $F(q)$. Тогда для каждого $p > \max(5, F(q))$ имеем

a) Если простое p имеет вид $5t \pm 1$, то $F(q\times p) \bmod q\times p = F(q)$.

b) Если простое p имеет вид $5t \pm 2$, то $F(q\times p) \bmod q\times p = q\times p - F(q)$.

Доказательство. Покажем, что $F(q)$ нечетно. Действительно, если $2 = F(3)$ делит $F(2t)$, то, по лемме 4, имеем 3 – делитель t, что невозможно. Следовательно, $F(q) \equiv \pm t \pmod q$. Так как p – простое и $p > q$, то pq не делится на 3. По лемме 4, $F(qp)$ нечетно, но $F(qp)$ делится на $F(q)$. Отсюда следует, что $F(qp)$ делится на t. Поэтому получаем $F(qp) \equiv \pm t \pmod q$. Так как $F(q) \equiv \pm t \pmod q$ и $F(qp) \equiv \pm t \pmod q$, то $F(q\times p) \equiv \pm F(q) \pmod q$. Получили условие (1). ■

Первые шесть значений q, для которых выполнено условие следствия 2, есть 2, 10, 50, 110, 250 и 550.

Предположения без доказательств

Теорема 2 вместе со следствиями дает достаточные условия того, когда поведение подпоследовательностей $F(q\times p) \bmod q\times p$ описывается двумя прямыми. В более сложных ситуациях (например, рис. 4 – рис. 6) удалось сформулировать только гипотезы, и то только в двух простейших случаях.

Рис. 9 показывает поведение последовательности $F(4p) \bmod 4p$.

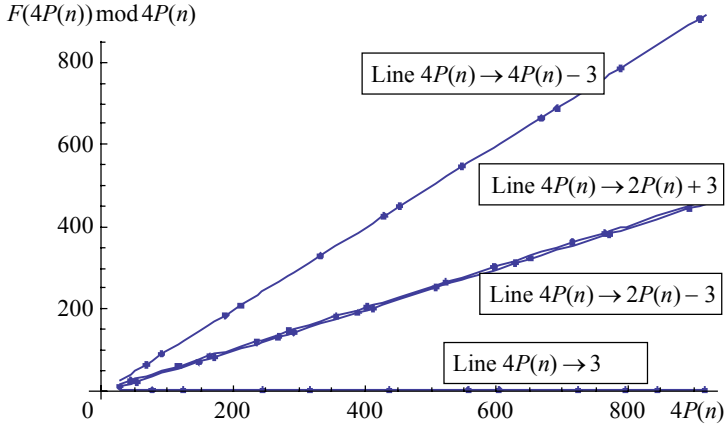

Рис. 9. График последовательности $4P(n) \to F(4P(n)) \bmod 4P(n)$

То, что точки $(4p,\ F(4p) \bmod 4p)$ последовательности $F(4p) \bmod 4p$ располагаются на четырех прямых обнаружено с помощью системы Mathematica. И с помощью Mathematica были высказаны гипотезы (проверены для первой тысячи простых чисел).

Возможно, для всех простых чисел справедливы следующие утверждения:

Гипотеза 1.

Если $p \equiv 1$ или $p \equiv 19$ по модулю 15, то $F(4p) \bmod 4p = 3$.
Если $p \equiv 7$ или $p \equiv 13$ по модулю 15, то $F(4p) \bmod 4p = 2p - 3$.
Если $p \equiv 2$ или $p \equiv 8$ по модулю 15, то $F(4p) \bmod 4p = 4p - 3$.
Если $p \equiv 11$ или $p \equiv 14$ по модулю 15, то $F(4p) \bmod 4p = 2p + 3$.

Гипотеза 2.

Если $p \equiv 1$ или $p \equiv 19$ по модулю 30, то $F(4p) \bmod 4p = 3$.
Если $p \equiv 7$ или $p \equiv 13$ по модулю 30, то $F(4p) \bmod 4p = 2p - 3$.
Если $p \equiv 17$ или $p \equiv 23$ по модулю 30, то $F(4p) \bmod 4p = 4p - 3$.
Если $p \equiv 11$ или $p \equiv 29$ по модулю 30, то $F(4p) \bmod 4p = 2p + 3$.

Поиск подходящего модуля m осуществлялся среди тех m, у которых значение функции Эйлера $\varphi(m)$ равно 4 или 8. Для $m \le 10\,000$ только два значения 15 и 30 оказались подходящими.

Изучалось также поведение последовательности $F(3p) \bmod 3p$ (см. рис. 10).

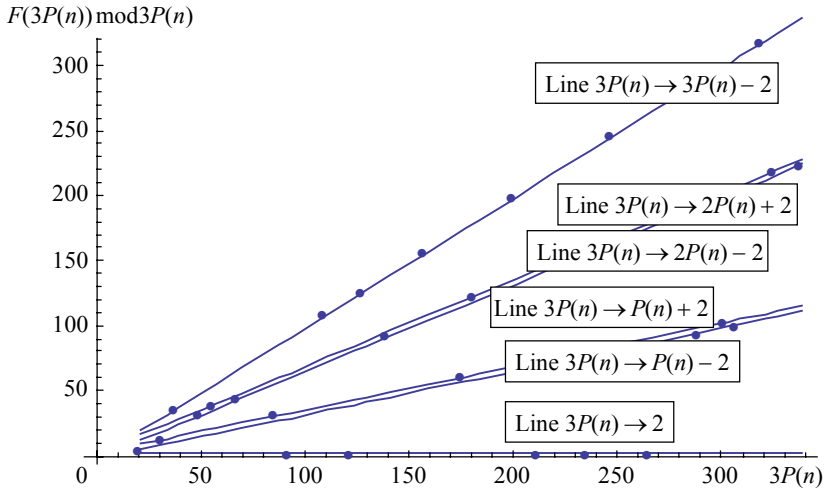

Рис. 10. График последовательности $3P(n) \to F(3P(n)) \bmod 3P(n)$

То, что точки $(3p,\ F(3p) \bmod 3p)$ последовательности $F(3p) \bmod 3p$ располагаются на шести прямых, обнаружено с помощью системы Mathematica (проверено для первой тысячи простых чисел).

Попытки сделать и в этом случае похожие предположения, как и в случае $q = 4$, оказались безуспешны. Поскольку прямых шесть, то подходящий модуль m отыскивался среди тех m, для которых функция Эйлера $\varphi(m)$ была бы кратна 6, точнее, $\varphi(m)$ должно быть равно 6, 12, 18 или 24. Были просмотрены все $m \le 10000$, но подходящий модуль m не найден.

ЛИТЕРАТУРА

1. *Wolfram S.* A New Kind of Science. Wolfram Media, 2002. 1197 p.
2. *Sloan's* On-Line Encyclopedia of Integer Sequences, http://oeis.org/
3. *Koshy T.* Fibonacci and Lucas Numbers with Applications. John Wiley & Sons, Inc, 2001.
4. *Kramer J. and V.E. Hoggatt*, *Jr.* Special cases of Fibonacci periodicity // The Fibonacci Quarterly. 1972. 10:5 (Nov.). P. 519–522.
5. *Воробьев Н.Н.* Числа Фибоначчи. М.: Наука, 1978. 144 с.
6. *Desmond J.E.* Problem B-182 // The Fibonacci Quarterly. 1970. 20:1 (Feb.). P. 96.

Статья поступила 11.03.2013 г.

Zyuz'kov V.M. FIBONACCI(N) MODULO N SEQUENCE.We study the behavior of the Fibonacci $(n) \bmod n$ sequence and pay attention to some subsequences: n runs through the set of prime numbers and the cases with $n = qp$, where p runs through the set of prime numbers and q is a fixed natural number. The behavior of the sequence is investigated using the Mathematica system. Some hypotheses are formulated and proved.

Keywords: Fibonacci sequence, remainders, congruence relation, Mathematica.

ZYUZ'KOV Valentin Mikhailovich (Tomsk State University)
E-mail: vmz@math.tsu.ru