А.Н.Рудаков

Числа Фибоначчи и простота числа $2^{127}-1$

1. Введение

Число $M = 2^{127}-1$ долгое время было в списке рекордов, оно являлось самым большим известным простым числом с 1877 г. по 1951 г. Простота $2^{127}-1$ была установлена Э. Лукасом (É. Lucas). Им был найден замечательный способ доказательства простоты, потребовавший для $M = 2^{127}-1$ около ста часов вычислений, но никаких делений на меньшие простые числа. Я собираюсь изложить математическую часть алгоритма Лукаса, обсудив заодно некоторые изящные результаты из конечной арифметики. Сами вычисления мы проводить не будем.

Мне лично этот сюжет кажется очень хорошим примером того, что для построения хорошего алгоритма нужна хорошая теория. Впрочем, существуют изложения результата Лукаса, привлекающие значительно меньше «теории», чем мое изложение здесь (см. [R] и [B]).

Подробное историческое исследование работ Э. Лукаса и нахождения простых чисел см. в [W].

2. Числа Фибоначчи и основная теорема

Как известно, последовательность чисел Фибоначчи получается следующим образом: мы определяем $u_1 = 1$, $u_2 = 1$ и находим каждое следующее число по формуле $u_{n+1} = u_n + u_{n-1}$. У чисел Фибоначчи

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots$$

немало замечательных свойств. Например, сначала идут два нечетных числа, потом четное, а потом опять два нечетных и т. д. Это легко увидеть, если рассматривать числа Фибоначчи по модулю 2. Если мы знаем u_{n-1} и u_n по модулю 2, то u_{n+1} будет их «суммой по модулю 2». Следовательно, мы имеем последовательность:

$$\begin{aligned} u_3 &\equiv 1+1 \equiv 0 \pmod 2 \\ u_4 &\equiv 0+1 \equiv 1 \pmod 2 \\ u_5 &\equiv 1+0 \equiv 1 \pmod 2 \\ &\ldots\ldots\ldots \end{aligned}$$

или $1, 1, 0, 1, 1, 0, 1, 1, 0, \ldots$ Это и означает, что каждое третье число четно, а числа перед ним и после него нечетны и т. д.

Можно заметить и что каждое пятое число делится на 5. Для этого надо только вычислить числа Фибоначчи по модулю 5. Это будет последовательность чисел

$$1, 1, 2, 3, 0, 3, 3, 6, 9 \equiv -1, 0, -1, -1, -2, -3, 0, -3, -3, \ldots$$

После 20-го члена все начнет повторяться, и регулярно, через четыре места на пятом идут нули.

Задача 1. *Покажите, что каждое четвертое число Фибоначчи делится на 3.*

Задача 2. *Покажите, что если m делит u_k, то m делит u_{2k}, u_{3k}, u_{4k}, ...*

Можно получить также формулу для чисел Фибоначчи. Она очень известна, но позвольте мне напомнить, как мы рассуждаем. Если мы отвлечемся от «начальных данных», $u_1 = 1$, $u_2 = 1$, а рассмотрим только уравнение перехода

$$x_{n+1} = x_n + x_{n-1}, \tag{1}$$

то, конечно, есть много последовательностей, удовлетворяющих этому уравнению. Одна из них, называемая иногда *числами Лукаса*, это:

$$v_1 = 1,\ v_2 = 3,\ v_3 = 4,\ \ldots,\ v_{n+1} = v_n + v_{n-1}.$$

Есть и еще, при этом если $\{a_n\}$ и $\{b_n\}$ — две такие последовательности, то можно построить третью, взяв их линейную комбинацию с некоторыми коэффициентами, например, $c_n = 2a_n + 3b_n$. Тут стоят коэффициенты 2 и 3, но они могут быть любыми. В частности, если

$$\alpha = \frac{1+\sqrt{5}}{2} \quad \text{и} \quad \beta = \frac{1-\sqrt{5}}{2},$$

т. е. α и β — корни уравнения $x^2 = x+1$, то последовательности $a_n = \alpha^n$ и $b_n = \beta^n$ удовлетворяют уравнению перехода (1), а значит, и любая их линейная комбинация обладает этим свойством. Так как $\alpha + \beta = 1$, $\alpha^2 + \beta^2 = 3$, то сумма этих последовательностей дает числа Лукаса

$$\alpha^2 + \beta^2 = v_n. \tag{2}$$

Для чисел Фибоначчи надо более искусно подобрать коэффициенты. В результате получится

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}. \tag{3}$$

В частности, из этого следует, что $u_{2n} = u_n \cdot v_n$.

Мне бы хотелось сейчас сформулировать нашу основную теорему, которая есть по существу теорема Лукаса (1886), хотя она не была сформулирована им в такой форме. Современное изложение исторических деталей есть в [W].

Теорема 1. *Пусть q — простое число вида $4k+3$ и $M = 2^q - 1$. Тогда M простое если и только если $v_{\frac{M+1}{2}} \equiv 0 \pmod{M}$.*

Этот результат является основой алгоритма, позволяющего установить простоту числа $2^{127} - 1$, однако надо еще добавить «быстрый» способ вычисления $v_{\frac{M+1}{2}}$. Мы это обсудим позже.

3. Комплексные числа в конечной арифметике

Давайте немножко изменим способ выражения: вместо того чтобы говорить a сравнимо с b по модулю m, $a \equiv b \pmod{m}$, будем говорить a равно b в «арифметике по модулю m», $a =_{(m)} b$. Формально это ничего не меняет, чуть-чуть другие слова, но можно начать представлять себе, что есть некие числа «арифметики по модулю m», которые просто обозначаются целыми числами, а сами по себе есть нечто другое. Например, 6 и -1 это два обозначения для одного и того же числа «арифметики по модулю 7».

При таком подходе почти сразу возникает вопрос, а нельзя ли увеличить область чисел, рассмотрев, например, «комплексные числа». Ведь комплексные числа — это пары действительных, а пары можно рассматривать и здесь. Давайте рассмотрим «комплексные числа по модулю 7». Определим такое комплексное число z как пару $z = (a, b)$, где a и b — «числа по модулю 7». Сложение задается обычным образом:

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2,\ b_1 + b_2);$$

умножение тоже:

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2 - b_1 b_2,\ a_1 b_2 + a_2 b_1).$$

Довольно просто убедиться, что это хорошее определение: есть нуль, единица, ассоциативность, коммутативность... Можно вычислить и обратный элемент: если $z = (a, b)$, то

$$z^{-1} = \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right).$$

Однако может оказаться, что $a^2+b^2 =_{(7)} 0$ и обратный элемент не определен.

Мы можем это явно проверить, так как 7 — очень небольшое число. Всевозможные элементы по модулю 7 легко выписываются, это:

$$0, 1, 2, 3, 4, 5, 6.$$

Квадратами будут $0, 1, 4, 2$, и все! Суммы двух квадратов получаются такие:

$$0, 1, 4, 2; \quad 1, 2, 5, 3; \quad 4, 5, 3, 6; \quad 2, 3, 6, 4.$$

То есть 0 встречается только один раз как $0 = 0^2 + 0^2$, все остальные суммы ненулевые. Значит, у ненулевого комплексного числа есть обратный элемент. Получилась хорошая арифметика со всеми четырьмя операциями, или то, что иначе называют полем, а точнее, квадратичным расширением простого поля из 7 элементов.

Кстати, 7 нельзя заменить на 5, поскольку $1^2 + 2^2 =_{(5)} 0$ в арифметике по модулю 5. Проблема, собственно, в том, какие числа в арифметике по модулю p надо считать отрицательными.

Вспомним, для построения обычных комплексных чисел мы берем -1, т.е. отрицательное число, для которого не существует квадратного корня, и «добавляем» этот квадратный корень формально, т.е. пишем $z = a + bi$, где $i^2 = -1$. Далее правила операций возникают сами собой, из раскрытия скобок:

$$(a_1 + b_1 i) + (a_2 + b_2 i) = (a_1 + a_2) + (b_1 + b_2) i,$$

$$(a_1 + b_1 i) \cdot (a_2 + b_2 i) = (a_1 a_2 + b_1 b_2 (-1)) + (a_1 b_2 + a_2 b_1) i.$$

Можно взять и другое отрицательное число, например -2, и рассмотреть комплексные числа в виде $z = a + bj$, где $j^2 = -2$. Получится все то же самое, в частности, операции тоже возникают сами собой, из раскрытия скобок:

$$(a_1 + b_1 j) + (a_2 + b_2 j) = (a_1 + a_2) + (b_1 + b_2) j,$$

$$(a_1 + b_1 j) \cdot (a_2 + b_2 j) = (a_1 a_2 + b_1 b_2 (-2)) + (a_1 b_2 + a_2 b_1) j.$$

Отличие возникает только в одном месте, где приходится считать j^2.
Формулой для обратного элемента будет

$$(a+bj)^{-1} = \frac{a}{a^2+2b^2} + \frac{-b}{a^2+2b^2}\,j,$$

и так как $a^2+2b^2 \neq 0$ как только $(a,b) \neq (0,0)$, то никаких проблем не возникает.

Задача 3. *Проверьте, что можно построить квадратичное расширение простого поля из 5 элементов, рассматривая числа $a+bj$, где $j^2=-2$. Все четыре действия арифметики будут корректно определены.*

Давайте будем использовать такое определение: скажем, что элемент a является отрицательным в «арифметике по модулю p», где p — простое число, если уравнение $x^2 =_{(p)} a$ не имеет решений, и положительным в противном случае (если при этом $a \neq_{(p)} 0$). Например, по модулю 5 числа 1 и 4 положительные, а 2 и 3 — отрицательные. Так как $-1 =_{(5)} 4$, то число -1 тоже положительное, так уж получается. Зато по модулю 7 числа 1, 2, 4 положительные, а -1, -2 и -4, или 6, 5 и 3, отрицательные. То, что нам естественно назвать «знаком элемента», исторически называется символом Лежандра $\left(\dfrac{a}{p}\right)$. По определению

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & \text{если } a \text{ положительно по модулю } p; \\ -1, & \text{если } a \text{ отрицательно по модулю } p; \\ 0, & \text{если } a =_{(p)} 0. \end{cases}$$

Можно проверить, что для нечетного простого числа p ровно половина $\left(\text{т. е. } \dfrac{p-1}{2}\right)$ ненулевых чисел по модулю p положительна и ровно половина отрицательна, и что произведение двух отрицательных всегда положительно.

Задача 4. *Докажите, что если $\left(\dfrac{a}{p}\right)=-1$ и $\left(\dfrac{b}{p}\right)=-1$, то $\left(\dfrac{ab}{p}\right)=+1$.*

Задача 5. *Проверьте, что если t отрицательно по модулю p, то числа $a+bj$, где $j^2=t$, определяют квадратичное расширение простого поля из p элементов (где все четыре действия арифметики корректно определены).*

Главное приложение вышесказанного для нас в следующем. Пусть p — простое число и число 5 отрицательно по модулю p. Тогда числа $\alpha = \dfrac{1+\sqrt{5}}{2}$ и $\beta = \dfrac{1-\sqrt{5}}{2}$ определены как комплексные числа по модулю p (как элементы квадратичного расширения) и формулы (2) и (3) для чисел Лукаса и Фибоначчи сохраняют смысл в комплексных числах по модулю p.

4. Комплексное сопряжение для чисел по модулю p

Существенной составляющей структуры обычных комплексных чисел является операция комплексного сопряжения: если $z=a+bi$, то $\bar{z}=a-bi$. Мы знаем, что сопряженное суммы есть сумма сопряженных и то же для произведения:

$$\overline{(z_1+z_2)}=\bar{z}_1+\bar{z}_2, \quad \overline{(z_1\cdot z_2)}=\bar{z}_1\cdot\bar{z}_2.$$

Отсюда легко заключить, что если α есть комплексный корень уравнения с действительными коэффициентами:

$$x^2+ax+b=0,$$

то $\bar{\alpha}$ тоже будет корнем этого уравнения.

Мы можем определить сопряжение и в квадратичном расширении поля из p элементов формулой

$$\overline{(a+b\cdot j)}:=a-b\cdot j.$$

Ясно, что сопряженное суммы есть сумма сопряженных, сопряженное произведения есть произведение сопряженных. Кроме того, имеет место следующая замечательная формула.

Пусть p — простое число и t отрицательно по модулю p, т. е. $\left(\frac{t}{p}\right)=-1$. Построим комплексные числа как числа вида $a+b\cdot j$, где a и b рассматриваются по модулю p и $j^2=t$.

Предложение 1. *В этих условиях если $z=a+bj$ и $\bar{z}=a-bj$, то*

$$\bar{z}=z^p. \tag{1}$$

В частности, $z^{p+1}=z\bar{z}=a^2-tb^2$, т. е. $(p+1)$-я степень «комплексного» числа обязательно будет «действительным» числом.

Для доказательства формулы (1) давайте вспомним, что для наших чисел

$$(x+y)^p=_{(p)}x^p+y^p.$$

Это следует из того, что коэффициенты бинома Ньютона, $\binom{p}{i}=\frac{p!}{i!(p-i)!}$, являются целыми числами, делящимися на p при $0<i<p$. Тогда мы можем написать

$$(a+b\cdot j)^p=_{(p)}a^p+b^p\cdot j^p.$$

Используя малую теорему Ферма, мы заключаем, что $a^p =_{(p)} a$, $b^p =_{(p)} b$. Остается вычислить j^p. Конечно,

$$j^p = j^{p-1} \cdot j = t^{(p-1)/2} \cdot j.$$

Нам нужно показать, что для отрицательного элемента t выполняется равенство $t^{(p-1)/2} =_{(p)} -1$. Отметим, что число $(p-1)/2$ целое, и если s является положительным элементом, то $s = a^2$ и

$$s^{(p-1)/2} =_{(p)} a^{p-1} =_{(p)} 1,$$

где последнее равенство следует из теоремы Ферма. Тем самым положительные элементы предоставляют нам $(p-1)/2$ корней полиномиального уравнения

$$x^{(p-1)/2} = 1$$

в поле «элементов по модулю p». Полиномиальное уравнение, по теореме Безу, не может иметь больше корней, чем его степень, и тем самым для отрицательного элемента t имеем

$$t^{(p-1)/2} \neq_{(p)} 1.$$

В то же время $t^{p-1} =_{(p)} 1$, и так как

$$t^{p-1} - 1 =_{(p)} (t^{(p-1)/2} - 1)(t^{(p-1)/2} + 1),$$

то остается единственная возможность: $t^{(p-1)/2} =_{(p)} -1$. Это завершает доказательство формулы.

Следствие. *Пусть p простое и 5 отрицательно по модулю p. Тогда для $\alpha = \dfrac{1+\sqrt{5}}{2}$ и $\beta = \dfrac{1-\sqrt{5}}{2}$ имеем:*
1) $\alpha^p =_{(p)} \beta, \quad \beta^p =_{(p)} \alpha;$
2) $\alpha^{p+1} =_{(p)} \beta^{p+1} =_{(p)} \alpha \cdot \beta =_{(p)} -1.$

Мы можем применить этот результат к числам Фибоначчи и Лукаса. В этих условиях получаем:

$$u_{p+1} = \frac{\alpha^{p+1} - \beta^{p+1}}{\alpha - \beta} \equiv 0 \pmod{p};$$
$$v_p = \alpha^p + \beta^p \equiv \alpha + \beta \equiv 1 \pmod{p}.$$

Чтобы пользоваться этими сравнениями, нам надо уметь определять, для каких p «5» будет положительным и для каких отрицательным. Сейчас мы попробуем в этом разобраться.

5. Квадратный корень из 5 по модулю p

Свойство, которое я хочу сейчас сформулировать, легко следует из более общих и довольно глубоких результатов о символе Лежандра, которые объединяются под названием квадратичного закона взаимности. Нам нужен только частный случай этого общего закона, обнаруженного Эйлером и Лежандром, доказанного Гауссом, и являющегося одной из жемчужин «элементарной» теории чисел.

Предложение 2.

$$\left(\frac{5}{p}\right) = \begin{cases} +1, & \textit{если } p \equiv \pm 1 \pmod 5; \\ -1, & \textit{если } p \equiv \pm 2 \pmod 5. \end{cases}$$

Сначала две общих леммы.

Лемма 1 (Лежандр).

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod p.$$

Фактически это значит, что для положительных a, $(p-1)/2$-я степень равна $+1$, а для отрицательных равна -1 по модулю p. Это мы разобрали в предыдущем пункте.

Заметим, что любое ненулевое число по модулю p равно с точностью до знака одному из чисел $1, 2, \ldots, (p-1)/2$. Если обозначить через $\mathscr{P}$ множество этих чисел:

$$\mathscr{P} = \{1, 2, \ldots, (p-1)/2\},$$

то для любого ненулевого x по модулю p либо $x \in \mathscr{P}$, либо $-x \in \mathscr{P}$. Фиксируем p и некоторое $a \neq_{(p)} 0$.

Лемма 2 (Гаусс). *Пусть для $k = 1, 2, \ldots, (p-1)/2$ число ϵ_k равно $+1$ или -1 и выбрано так, что $a \cdot k \cdot \epsilon_k \in \mathscr{P}$ по модулю p. Тогда*

$$\left(\frac{a}{p}\right) = \prod_{k=1}^{(p-1)/2} \epsilon_k.$$

Действительно, во-первых заметим, что если числа k' и k'' различны, то произведения $a \cdot k' \cdot \epsilon_{k'}$ и $a \cdot k'' \cdot \epsilon_{k''}$ тоже будут различны. Они могли бы совпадать только если $a \cdot k' =_{(p)} a \cdot k''$ или $a \cdot k' =_{(p)} -a \cdot k''$, но и первое и второе невозможно. Тогда, когда k пробегает все множество $\mathscr{P}$, то и произведение $a \cdot k \cdot \epsilon_k$ пробегает все $\mathscr{P}$. Пусть K есть произведение всех элементов из $\mathscr{P}$. Мы имеем:

$$K = \prod_{k=1}^{(p-1)/2} a \cdot k \cdot \epsilon_k =_{(p)} a^{(p-1)/2} \cdot K \cdot \prod_{k=1}^{(p-1)/2} \epsilon_k.$$

Сокращая на K, получаем, что $1 =_{(p)} a^{(p-1)/2} \cdot \prod\limits_{k=1}^{(p-1)/2} \epsilon_k$, что с учетом леммы Лежандра доказывает лемму Гаусса.

Замечание 1. Можно сказать, что мы здесь моделируем одно из известных доказательств малой теоремы Ферма.

Теперь мы можем обратиться к нашему предложению. У нас будет $a = 5$. Для нечетного p

$$\begin{aligned} p &\equiv \pm 1 \pmod 5 \iff p = 10n+1 \quad \text{или} \quad p = 10n+9, \\ p &\equiv \pm 2 \pmod 5 \iff p = 10n+3 \quad \text{или} \quad p = 10n+7. \end{aligned}$$

Давайте применим лемму Гаусса для $p = 10n+1$. Здесь $(p-1)/2 = 5n$, и нам нужны $k = 1, 2, \ldots, 5n$.

При $k = 1, 2, \ldots, n$:

$$5k = 5, 10, \ldots, 5n \quad \text{и} \quad \epsilon_k = +1.$$

При $k = n+1, \ldots, 2n$:

$$5k = 5n+1, \ldots, 10n \quad \text{и} \quad \epsilon_k = -1.$$

При $k = 2n+1, \ldots, 3n$:

$$5k = (10n+1)+4, \ldots, (10n+1)+5(n-1)+4 \quad \text{и} \quad \epsilon_k = +1.$$

При $k = 3n+1, \ldots, 4n$ аналогичным образом $\epsilon_k = -1$, и при $k = 4n+1, \ldots, 5n$ снова $\epsilon_k = +1$.

Тем самым -1 встречается $2n$ раз и $\prod \epsilon_k = +1$. То есть если $p = 10n+1$, то $\left(\frac{5}{p}\right) = +1$.

Для случая $p = 10n+3$ можно рассуждать совершенно аналогично. Здесь $(p-1)/2 = 5n+1$.

При $k = 1, \ldots, n \quad \epsilon_k = +1$.

При $k = n+1, \ldots, 2n \quad \epsilon_k = -1$.

При $k = 2n+1, \ldots, 3n \quad \epsilon_k = +1$.

При $k = 3n+1, \ldots, 4n \quad \epsilon_k = -1$.

Теперь при $k=4n+1$, $5k=20n+5=(10n+3)+(10n+2)$, что дает $\epsilon_k=-1$.

При $k=4n+2,\dots,5n+1 \quad \epsilon_k=+1$.

В результате мы получаем на один элемент «-1» больше, всего $2n+1$ «минус единиц», а значит, $\left(\frac{5}{p}\right)=-1$ в этом случае. Мы предоставляем читателям самостоятельно проверить два оставшихся случая и будем считать предложение 2 доказанным.

6. Доказательство основной теоремы

Возвращаясь к доказательству основной теоремы, сформулированной в конце раздела 2, заметим прежде всего, что мы можем вычислить значение $M \pmod 5$. Мы знаем, что $2^4\equiv 1 \pmod 5$ и что

$$M=2^q-1=2^{4k+3}-1\equiv 2^3-1\equiv 2 \pmod 5.$$

Запомним это: в условиях теоремы $M\equiv 2 \pmod 5$.

Предположим теперь, что M — простое число. Тогда $\left(\frac{5}{M}\right)=-1$ и мы можем применить лемму и следствие из пункта 4. В частности,

$$\alpha^{M+1}\equiv\beta^{M+1}\equiv -1 \pmod M,$$

а значит, $v_{M+1}\equiv -2 \pmod M$.

Пусть $N=2^{q-1}=\frac{M+1}{2}$, т.е. $M+1=2N$. Заметим, что

$$(v_N)^2=(\alpha^N+\beta^N)^2=\alpha^{2N}+\beta^{2N}+2(\alpha\beta)^N=v_{2N}+2\cdot(-1)^N. \qquad (1)$$

Мы знаем, что N четно, значит,

$$(v_N)^2=v_{2N}+2\equiv -2+2\equiv 0 \pmod M.$$

Тем самым мы получили утверждение теоремы в этом случае.

Обратно, пусть известно, что $v_N\equiv 0 \pmod M$. Надо доказать, что число M простое. Во всяком случае, мы можем утверждать (поскольку $M\equiv 2 \pmod 5$), что не все простые делители p числа M имеют вид $p\equiv\pm 1 \pmod 5$; найдется простой делитель p числа M, для которого $p\equiv \pm 2 \pmod 5$, и тем самым $\left(\frac{5}{p}\right)=-1$, поэтому число 5 отрицательно по модулю p и мы можем использовать результаты пункта 4. В частности, $\alpha^{p+1}=_{(p)}\beta^{p+1}=_{(p)}-1$. Раз p делит M и $v_M\equiv 0 \pmod M$, значит,

$$v_N=\alpha^N+\beta^N=_{(p)}0.$$

Пусть $\epsilon = \alpha/\beta$. Тогда мы получим, с одной стороны,

$$\epsilon^N =_{(p)} -1, \tag{2}$$

а с другой стороны, $\epsilon^{p+1} =_{(p)} 1$. Из этих двух равенств следует, что $p+1 = 2N$, т.е. $p = M$.

Действительно, из равенства (2) следует, что $\epsilon^{2N} = \epsilon^{2^q} =_{(p)} +1$.

Лемма 3. *Пусть $\epsilon^a = 1$ и $\epsilon^b = 1$. Используя деление с остатком, запишем $a = b \cdot c + r$. Тогда $\epsilon^r = 1$.*

Действительно, $1 = \epsilon^a = (\epsilon^b)^c \cdot \epsilon^r = 1 \cdot \epsilon^r = \epsilon^r$. Пусть d минимальное положительное число, для которого $\epsilon^d =_{(p)} 1$. Тогда, ввиду леммы, d делит $2N$ (значит $d = 2^s$) и d делит $p+1$. Если $s = q$, то $p+1 = 2^q$. Иначе $s < q$, тогда d делит $N = 2^{q-1}$, значит, $\epsilon^N = (\epsilon^d)^{N/d} =_{(p)} 1$, что противоречит равенству (2). Теорема доказана.

Таким образом, простота числа $M = 2^q - 1$ зависит от значения числа $v_{2^{q-1}}$ по модулю M.

Замечательным образом мы можем использовать формулу (1) для вычисления чисел v_{2^i}. Обозначим $r_i = v_{2^i}$. Тогда $r_0 = v_1 = 1$. Теперь из формулы (1) имеем: $r_1 = r_0^2 + 2 = 3$ (здесь N нечетно). При $i \geqslant 1$ мы применяем формулу (1) с четным N:

$$r_{i+1} = r_i^2 - 2, \quad r_1 = 3.$$

И наш основной результат принимает следующий вид.

Теорема 2. *Если q — простое число вида $4k+3$, то число $M = 2^q - 1$ простое если и только если $r_{q-1} \equiv 0 \pmod{M}$.*

7. Организация вычислений. Примеры

Вычисление r_i удобно производить в двоичной записи: $r_1 = 11$ (в двоичной системе).

Для r_2 получаем:

$$\begin{array}{rccc}
 & \times & 1 & 1 \\
 & & 1 & 1 \\
\hline
+ & & 1 & 1 \\
 & 1 & 1 & \\
\hdashline
- & & 1 & 0 \\
\hline
r_2 = & 1 & 1 & 1
\end{array}$$

Таким образом, $r_2 = 111$, т.е. 7 в десятичной системе.

Для r_3:

$$
\begin{array}{r@{\;}cccccc}
\times & & & & 1 & 1 & 1 \\
 & & & & 1 & 1 & 1 \\
\hline
 & & & & 1 & 1 & 1 \\
 & & & 1 & 1 & 1 & \\
 & & 1 & 1 & 1 & & \\
 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
- & & & & & 1 & 0 \\
\hline
r_3 = & 1 & 0 & 1 & 1 & 1 & 1
\end{array}
$$

Итак, $r_3 = 101111$, т. е. 47 в десятичной системе.

Здесь мы уже видим один случай нашей теоремы: при $q=3$, $M=7$ — простое, и как раз $r_2 = 7 \equiv 0 \pmod 7$.

Следующим q будет $q=7$, $M=2^7-1=127$. Конечно, можно использовать обычные деления для анализа простоты числа 127, но посмотрим, как работает алгоритм.

Нам надо посчитать r_4, r_5 и $r_6 \pmod{127}$. Приятно заметить, что мы можем производить редукцию по модулю 127 уже в процессе вычислений, и она соответствует «сдвигу двоичной записи» на 7 единиц:

$$2^7 \equiv 1 \pmod{2^7-1}, \quad \text{значит,} \quad 2^{7+k} \equiv 2^k \pmod{2^7-1}.$$

Тем самым r_4 по модулю 127 можно считать следующим образом:

$$
\begin{array}{ccccccccccccc}
 & & & & & : & & 1 & 0 & 1 & 1 & 1 & 1 \\
 & & & & & : & 1 & 0 & 1 & 1 & 1 & 1 & \\
+ & & & & 1 & : & 0 & 1 & 1 & 1 & 1 & & \\
 & & & 1 & 0 & : & 1 & 1 & 1 & 1 & & & \\
 & 1 & 0 & 1 & 1 & : & 1 & 1 & & & & & \\
\hline
- & & & & & & & & & & & 1 & 0
\end{array}
$$

После переноса получаем

$$
\begin{array}{cccccccc}
: & & 1 & 0 & 1 & 1 & 1 & 1 \\
: & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\
: & 0 & 1 & 1 & 1 & 1 & 0 & \mathbf{1} \\
: & 1 & 1 & 1 & 1 & 0 & \mathbf{1} & \mathbf{0} \\
: & 1 & 1 & 0 & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{1} \\
\hline
- & & & & & & 1 & 0
\end{array}
$$

Теперь мы должны считать «циклически» — перенося любую вылезающую влево за 7 разрядов единичку направо. Получаем:

$$\begin{array}{r} 1\,0\,1\,1\,0\,1 \\ 1\,0\,1\,1\,1\,1\,0 \\ +\;0\,1\,1\,1\,1\,0\,1 \\ 1\,1\,1\,1\,0\,1\,0 \\ 1\,1\,0\,1\,0\,1\,1 \\ \hline 0\,1\,1\,0\,0\,0\,0 \end{array}$$

Таким образом, $r_4 \equiv 0110000 \pmod{127}$.

Теперь для r_5:

$$\begin{array}{r} 0\,0\,0\,0\,1\,1\,0 \\ +\;0\,0\,0\,1\,1\,0\,0 \\ \hline 0\,0\,1\,0\,0\,0\,0 \end{array}$$

То есть $r_5 \equiv 2^4 \pmod{127}$. Теперь $r_6 \equiv 2^8 - 2 \equiv 2 - 2 \equiv 0 \pmod{127}$. Тем самым 127 — простое число.

Аналогичным образом было посчитано, что число $M = 2^{127} - 1$ простое. Только тут надо было осуществлять циклические сложения двоичных чисел длины 127. Как объясняет Вильямс [W], Лукас сделал себе шахматную доску и записывал числа по линиям этой доски, расставляя ладьи на местах единиц и оставляя пустыми клетки нулей. Циклические сложения можно тогда осуществлять как «игру», следуя нескольким простым правилам. Потребовалось примерно 100 часов такой игры, чтобы вычислить r_{127} по модулю $2^{127} - 1$.

Литература

[B] J. M. Bruce. A really trivial proof of the Lucas—Lehmer test // Amer. Math. Monthly **100** (1993), P. 370—371.

[R] M. I. Rosen. A proof of the Lucas—Lehmer test // Amer. Math. Monthly **95** (1988), P. 855—856.

[W] H. C. Williams. Édouard Lucas and primality testing, Canadian Math. Soc. Monographs **22**, John Wiley & Sons, N. Y., 1998.