является необходимым и достаточным условием для нётеровости оператора T (16). В силу (11), (8) и (5) условие (21) равносильно условию (18).

Далее, имея [1] для индекса χ оператора T формулу

$$\chi = \frac{1}{2\pi}\Delta\big|_{\partial G} \arg \frac{\det\left(\alpha^*(t) - i\pi\beta^*(t)\right)}{\det\left(\alpha^*(t) + i\pi\beta^*(t)\right)}$$

из (20) и (21), получаем (19). Теорема доказана.

Библиографический список

1. *Векуа Н. П.* Системы сингулярных интегральных уравнений и некоторые граничные задачи. 2-е изд. М. : Наука, 1970. 380 с.
2. *Кусковский Л. Н.* О краевой задаче типа Римана — Гильберта // Дифференциальные уравнения. 1975. Т. 11, № 3. С. 523—532.
3. *Люстерник Л. А., Соболев В. И.* Краткий курс функционального анализа. М. : Высш. шк., 1982. 271 с.
4. *Михлин С. Г.* Линейные уравнения в частных производных. М. : Высш. шк., 1977. 431 с.
5. *Мусхелишвили Н. И.* Сингулярные интегральные уравнения. 3-е изд. М. : Наука, 1968. 512 с.

УДК 513.64

С. И. Хашин, Ю. А. Хашина

СВОЙСТВА ЧИСЕЛ, ПСЕВДОПРОСТЫХ ПО ФРОБЕНИУСУ

Не существует чисел, меньших 2^{60}, псевдопростых по Фробениусу (FPP). Есть гипотеза, что их не существует вообще. Если эта гипотеза верна или хотя бы их нижняя граница будет существенно поднята, это позволит намного облегчить проверку чисел на простоту.

В работе доказываются некоторые свойства FPP-чисел.

Ключевые слова: псевдопростые числа, алгоритм Фробениуса.

There are no Frobenius pseudoprime numbers (FPP) less than 2^{60}. There is a hypothesis that they do not exist at all. If this hypothesis is true, or, at least, the lower bound will be substantially increased, this will make it much easier to check for prime numbers.

In the paper we prove some properties of the FPP numbers.

Key words: pseudoprime numbers, Frobenius algorithm.

1. Введение

Наиболее мощный среди элементарных вероятностных методов проверки чисел на простоту — тест Фробениуса [1—5].

Определение 1. Нечетное составное число \$n\$ называется псевдопростым по Фробениусу (Frobenius pseudoprimes, FPP), если оно не является полным квадратом и

$$(1+\sqrt{c})^n \equiv 1-\sqrt{c} \bmod n,$$

где c — наименьшее нечетное простое число такое, что символ Якоби $J(c/n)$ равен –1. Про такие числа будем говорить, что они принадлежат классу $FPP(c)$.

В работе [5] доказано, что не существует FPP, меньших 2^{60}. Есть гипотеза, что их не существует вообще. Если эта гипотеза верна или хотя бы их нижняя граница будет существенно поднята, это позволит сделать проверку чисел на простоту гораздо более эффективной.

Так как числа FPP(c) по определению являются составными, они раскладываются в произведение нескольких простых чисел. Символ Якоби $J(c/p)$ для каждого из сомножителей равен ±1. В [5] доказано, что сомножители, для которых $J(c/p) = +1$, должны обладать очень специальными свойствами, причем все такие числа не меньше 2^{34}, вполне вероятно, что таких чисел не существует вовсе. Здесь мы рассматриваем лишь разложение на множители p_i, для каждого из которых $J(c/p) = -1$.

Также получены некоторые ограничения на свойства таких сомножителей, что позволяет надеяться на существенное поднятие нижней границы FPP-чисел.

Основными результатами являются теоремы 3, 5, 6.

2. Свойства нечетных разложений FPP

В [5] доказано, что если n принадлежит классу FPP(c) и $n=pq$, где p — простое и $J(c/p) = -1$, то

$$(1+\sqrt{c})^{q-1} \equiv 1 \bmod p. \qquad (1)$$

Так как $J(c/p) = -1$, кольцо $\mathbf{Z}_p[\sqrt{c}]$ изоморфно полю Галуа $GF(p^2)$. Мультипликативная группа поля $GF(p^2)^*$ имеет мощность p^2-1, поэтому порядок любого элемента является делителем p^2-1.

Для простого числа p такого, что $J(c/p) = -1$, обозначим через $r(p)$ копорядок числа $z=1+\sqrt{c}$ в кольце $\mathbf{Z}_p[\sqrt{c}]$, т. е.

$$r(p) = \frac{p^2-1}{\operatorname{ord}(z,p)}.$$

Пусть n является произведением s простых: $n = p_1p_2...p_s$, и все символы Якоби $J(c/p_i)$ равны –1. Тогда согласно (1) будем иметь

$$z^{\frac{n}{p_i}-1} \equiv 1 \bmod p_i$$

при $i = 1, \ldots, s$, или

$$\frac{n}{p_i} \equiv 1 \bmod \operatorname{ord}(z,p_i).$$

Другими словами,

$$\frac{n}{p_i} - 1 = \alpha_i \frac{p_i^2-1}{r(p_i)}$$

для некоторых натуральных α_i. Такие разложения будем называть нечетными.

Определение 2. Набор рациональных чисел

$$\left(\frac{\alpha_1}{r(p_1)}, \dots, \frac{\alpha_s}{r(p_s)}\right)$$

будем называть типом разложения $n=p_1p_2...p_s$.

Теорема 3. Пусть $\left(\frac{\alpha_1}{r(p_1)}, \dots, \frac{\alpha_s}{r(p_s)}\right)$ — тип разложения $n=p_1p_2...p_s$. Тогда $\alpha_i \neq r(p_i)$ при всех i. Другими словами, тип разложения не может содержать единиц.

Доказательство. Если $\alpha_i = r(p_i)$, то $n/p_i - 1 = p_i^2 - 1$, или $n/p_i = p_i^2$ — противоречие.

Теорема 4. Пусть n является произведением 3 простых: $n = p_1p_2p_3$, причем все символы Якоби $J(c/p_i)$ равны –1 и

$$\left(\frac{\alpha_1}{r(p_1)}, \frac{\alpha_2}{r(p_2)}, \frac{\alpha_3}{r(p_3)}\right)$$

— тип разложения. Обозначим через R наименьшее из p_i. Тогда число

$$A = \frac{\alpha_1\alpha_2\alpha_3}{r(p_1)r(p_2)r(p_3)}$$

лежит в пределах от 1 до $R^2/(R^2-1)$.

Доказательство. Перемножив равенства

$$p_2p_3 - 1 = \alpha_1\frac{p_1^2-1}{r(p_1)}, \quad p_1p_3 - 1 = \alpha_2\frac{p_2^2-1}{r(p_2)}, \quad p_1p_2 - 1 = \alpha_3\frac{p_3^2-1}{r(p_3)},$$

получим

$$(p_2p_3 - 1)(p_1p_3 - 1)(p_1p_2 - 1) = A(p_1^2 - 1)(p_2^2 - 1)(p_3^2 - 1).$$

Если ввести обозначение $x_i = 1/p_i$, то будем иметь

$$(1 - x_1x_2)(1 - x_2x_3)(1 - x_1x_3) = A(1 - x_1^2)(1 - x_2^2)(1 - x_3^2),$$

или

$$A = \frac{(1 - x_1x_2)(1 - x_2x_3)(1 - x_1x_3)}{(1 - x_1^2)\,(1 - x_2^2)(1 - x_3^2)}.$$

Величину A можно представить в виде

$$A = 1 + \frac{(1 - x_3^2)(x_1 - x_2)^2 + (1 - x_2^2)(x_3 - x_1)^2 + (1 - x_1^2)(x_2 - x_3)^2}{2(1 - x_1^2)\,(1 - x_2^2)(1 - x_3^2)},$$

поэтому $A \geq 1$. При $0 < x_i \leq 1/R$ наибольшего значения функция A достигает, когда одна или две из переменных принимают значение $1/R$, а остальные (оставшаяся) — ноль, и это значение равно $1/(1 - 1/R^2)$. Отсюда и получаем требуемое.

Фактически мы доказали, что если n не имеет малых простых делителей и числа $r(p_i)$ не слишком велики, то $\alpha_1\alpha_2\alpha_3 = r(p_1)r(p_2)r(p_3)$.

Теорема 5. Пусть n является произведением 3 простых: $n=p_1p_2p_3$, причем все символы Якоби $J(c/p_i)$ равны –1. Тогда тип разложения не может содержать двух одинаковых чисел.

Доказательство. Предположим противное. Пусть, например, $\alpha_1/r(p_1) = \alpha_2/r(p_2) = s$. Имеем

$$p_2p_3 - 1 = s(p_1^2 - 1),\ p_1p_3 - 1 = s(p_2^2 - 1). \quad (2)$$

Из первого равенства получаем

$$p_3 = \frac{s(p_1^2 - 1) + 1}{p_2}.$$

Подставив это выражение во второе равенство из (2), получим

$$s(p_1^2 + p_1p_2 + p_2^2 - 1) + 1 = 0$$

— противоречие.

Теорема 6. Пусть n является произведением 3 простых: $n = p_1p_2p_3$, причем все символы Якоби $J(c/p_i)$ равны –1 и (s_1,s_2,s_3) — тип разложения. Тогда произведение $s_1s_2s_3$ не может равняться 1.

Доказательство. Пусть $s_1s_2s_3 = 1$. Мы имеем три уравнения:

$$\begin{aligned} f_1 &= p_2p_3 - 1 - s_1(p_1^2 - 1),\\ f_2 &= p_1p_3 - 1 - s_2(p_2^2 - 1),\\ f_3 &= p_1p_2 - 1 - s_3(p_3^2 - 1). \end{aligned}$$

Тогда

$$\begin{aligned} &\big((1 - s_3)p_3 - (1 - s_2)p_2\big)f_1 +\\ &+s_1\big((1 - s_3)p_1 - s_3(1 - s_2)p_3\big)f_2 +\\ &+s_1\big((1 - s_3)s_2p_2 - (1 - s_2)p_1\big)f_3 =\\ &= \frac{s_1^2s_2 + s_1s_2^2 - 3s_1s_2 + 1}{s_1s_2}(p_2 - p_3). \end{aligned}$$

Так как первый сомножитель отличен от нуля, получаем $p2 = p3$ — противоречие.

Следствие 7. В тех же обозначениях, если $p_1>p_2>p_3$, то

$$1 < s_1s_2s_3 < p_3^2/(p_3^2–1).$$

Теорема 8. В условиях теоремы 6, если $p_1 > p_2 > p_3$, то $p_3 > s_1p_1$.

Доказательство. Если бы $p_3 < s_1p_1$, то, т. к. $p_2p_3–1 = s_1\ (p_1^2–1)$, мы получили бы $p_2 > p_1$ — противоречие.

3. Заключение

Для разработки более эффективных методов проверки простоты чисел желательно либо найти пример FPP-чисел, либо доказать, что их не существует, либо значительно поднять их нижнюю границу. На сегодняшний день в криптографии используются простые числа размером до 2^{1000}, а доказанная нижняя граница FPP-чисел равна 2^{60}. Совместное использование теорем 4 и 6 позволит значительно поднять эту границу.

Библиографический список

1. *Хашин С. И.* Кратные множители псевдопростых чисел // Вестн. Иван. гос. ун-та. Сер.: Естественные, общественные науки. 2013. Вып. 2. С. 102—107.
2. *Crandall R. E., Pomerance C.* Prime Numbers : a Computational Perspective. 2nd ed. New York, etc. : Springer, 2005. 597 p.
3. *Damgard I. B., Frandsen G. S.* An extended quadratic Frobenius primality test with average- and worst-case error estimate // J. of Cryptology. 2006. Vol. 19, № 4. P. 489—520.
4. *Grantham J.* Frobenius pseudoprimes // Math. of Comp. 2000. Vol. 70, № 234. P. 873—891.
5. *Khashin S. I.* Counterexamples for Frobenius primality test // arXiv: abs/1307.7920.2013. URL: http://arxiv.org (дата обращения: 01.12.2013).

УДК: 512.544, 512.546, 512.582

Н. И. Яцкин

ФУНКТОРЫ ПОДГРУППОВОЙ ТОПОЛОГИЗАЦИИ ГРУПП

Рассматриваются функторы топологизации, действующие из категории групп в полную подкатегорию категории топологических групп, объектами которой служат группы, наделенные подгрупповыми топологиями, т. е. обладающие базисом окрестностей нейтрального элемента, составленным из нормальных подгрупп. Изучается соответствие между такими функторами и некоторыми абстрактными классами групп.

Ключевые слова: категория групп, подгрупповая топология, функтор подгрупповой топологизации, абстрактный класс групп, псевдомногообразие групп, радикальный класс групп, полупростой класс групп.

We consider the topologization functors acting from the category of groups into the full subcategory of the category of topological group whose objects are groups with subgroup topologies. We study the correspondence between such functors and some abstract classes of groups.

Key words: category of groups, topologization functor, abstract class of groups, pseudovariety of groups, radical class of groups, semisimple class of groups.

1. Введение. В теории *абелевых* групп значительный интерес, начиная с работы Б. Шарля [16] (1964), вызывают так называемые *функториальные топологии* (т. е. фактически — функторы из категории абелевых групп в категорию топологических абелевых групп, тождественные на морфизмах). Функторы такого типа определенным образом наделяют каждую из абелевых групп топологией, причем так, что все гомоморфизмы групп становятся непрерывными (в смысле введенных топологий). Понятие функториальной топологии упоминается в монографии Л. Фукса [19, § 7] (1970). Этапными в изучении функторов топологизации абелевых групп представляются работы [15, 18, 17] (1980, 1982, 2011).

В настоящей статье предпринимается попытка перенести некоторые из результатов, полученных в указанных выше (и других) работах, на категорию