С. Б. Гашков, Упрощенное обоснование вероятностного теста Миллера–Рабина для проверки простоты чисел, *Дискрет. матем.*, 1998, том 10, выпуск 4, 35–38

DOI: 10.4213/dm442

Дискретная математика

том 10 выпуск 4 * 1998

УДК 519.7

Упрощенное обоснование вероятностного теста Миллера–Рабина для проверки простоты чисел

© 1998 г. С. Б. Гашков

Пусть m — положительное целое число, $\mathbf{Z}_m^*$ — множество всех положительных целых чисел, взаимно простых с m, не превосходящих m. Число $s \in \mathbf{Z}_m^*$ называется свидетелем простоты числа m, если последовательность степеней

$$s^{(m-1)2^{-i}} \pmod m, \quad i = 0, 1, \ldots, r, \quad m - 1 = 2^r t,$$

где t нечетно, состоит только из единиц, либо с них начинается, после чего продолжается минус единицей, и может быть, другими числами. В статье приводится простое доказательство следующего известного утверждения, лежащего в основе вероятностного алгоритма Миллера–Рабина распознавания простоты чисел.

Множество всех свидетелей простоты составного числа m имеет мощность, не большую $\varphi(m)/4$, где $\varphi(m)$ — функция Эйлера.

Работа выполнена при поддержке Российского фонда фундаментальных исследований, проект 96–01–068.

Пусть m — число, простоту которого мы хотим распознать. Рассмотрим множество $\mathbf{Z}_m^*$, состоящее из всех целых чисел, взаимно простых с m и лежащих в пределах от 1 до m. Как известно, оно имеет мощность $\varphi(m)$, где φ — функция Эйлера, и образует группу относительно умножения по модулю m. Число $s \in \mathbf{Z}_m^*$ называется свидетелем простоты числа m, если последовательность степеней

$$s^{(m-1)2^{-i}} \pmod m, \quad i = 0, 1, \ldots, r, \quad m - 1 = 2^r t,$$

где t нечетно, состоит только из единиц, либо с них начинается, после чего продолжается минус единицей, и может быть, другими числами. Множество всех свидетелей простоты числа m обозначим S.

Докажем следующую теорему, лежащую в основе вероятностного алгоритма Миллера–Рабина распознавания простоты ([2, 3, 4]).

Теорема 1 (Теорема Рабина). *Множество всех свидетелей простоты составного числа m имеет мощность, не большую $\varphi(m)/4$.*

Будем предполагать, что m не кратно трем и обозначать буквами p, с индексами или без них, простые числа. Справедлива следующая известная лемма.

Лемма 1. *Пусть m делится на p^2. Тогда множество чисел*

$$1 + km/p, \qquad k = 0, 1, \ldots, p-1,$$

образует подгруппу $\mathbf{Z}_m^*$ порядка p и все ее неединичные элементы имеют порядок p.

Доказательство. Доказательство основано на тождестве

$$(1 + km/p)(1 + k'm/p) \pmod m = 1 + ((k + k') \pmod p)m/p \pmod m,$$

из которого вытекает изоморфизм этой группы с циклической группой порядка p.

Назовем лжесвидетелем любое число a из множества $\mathbf{Z}_m^*$ такое, что либо $a^{m-1} \pmod m \neq 1$, либо $a^k \pmod m \neq -1$ для любого целого k и для некоторого простого делителя p числа m порядок $a \pmod p$ равен $p-1$ (порядок — это наименьшая натуральная степень k такая, что $a^k = 1 \pmod m$). Обозначим через A множество всех лжесвидетелей. Основой доказательства теоремы является следующая лемма.

Лемма 2. *Произведение лжесвидетеля и свидетеля не является свидетелем. Другими словами, если $a \in A$, а $s \in S$, то $as \pmod m$ не принадлежит S, то есть $S \cap aS = \varnothing$.*

Доказательство. Если $a^{m-1} \pmod m \neq 1$, то при $s \in S$

$$(as)^{m-1} \pmod m \neq s^{m-1} = 1,$$

значит $as \pmod m$ не принадлежит S.

Пусть теперь $a^{m-1} \pmod m = 1$ и при некотором простом делителе p числа m порядок числа a по модулю p равен $p-1$ и также $a^k \pmod m \neq -1$ при любом целом k.

Если $a^{(m-1)2^{-i}} \pmod m = 1$, то

$$a^{(m-1)2^{-i}} \pmod p = 1,$$

значит, $(m-1)2^{-i}$ делится на $p-1$, поэтому $i < r$, так как t нечетно, а $p-1$ четно, и, значит, $a^t \pmod m \neq 1$, и согласно малой теореме Ферма

$$s^{(m-1)2^{-j}} \pmod p = 1,$$

и, значит, $s^{(m-1)2^{-j}} \pmod m \neq -1$ при всех j, $0 \leqslant j \leqslant i$, а так как $s \in S$, из последнего утверждения следует, что

$$s^{(m-1)2^{-j}} \pmod m = 1, \qquad 0 \leqslant j \leqslant i,$$

и $s^{(m-1)2^{-i-1}} \pmod m = \pm 1$.

Можно выбрать $i \geqslant 0$ так, что $a^{(m-1)2^{-j}} \pmod m = 1$ при всех $j, 0 \leqslant j \leqslant i$, но $a^{(m-1)2^{-i-1}} \pmod m \neq 1$. Тогда

$$(as)^{(m-1)2^{-j}} \pmod m = s^{(m-1)2^{-j}} \pmod m = 1$$

при всех j, $0 \leqslant j \leqslant i$, но

$$(as)^{(m-1)2^{-i-1}} \pmod m = \pm a^{(m-1)2^{-i-1}} \pmod m \neq \pm 1$$

так как $a^{(m-1)2^{-i-1}} \pmod m \neq 1$ и $a^k \pmod m \neq -1$ при всех k. Доказанное означает, что $as \pmod m$ не является свидетелем.

Следующая алгебраическая лемма общеизвестна.

Лемма 3. *Пусть* $a \neq b \in \mathbf{Z}_m^*$. *Тогда*

$$Sa \cap Sb = \varnothing \iff S \cap Sab^{-1} = \varnothing.$$

В частности, для любой подгруппы G *группы* $\mathbf{Z}_m^*$ *множества* Sg, *где* $g \in G$, *попарно не пересекаются тогда и только тогда, когда не пересекаются множества* S *и* Sg *для любого неединичного элемента* $g \in G$. *Множества* S *и* Sa *при любом* $a \in \mathbf{Z}_m^*$ *равномощны и целиком содержатся в множестве* $\mathbf{Z}_m^*$.

Действительно, если бы $c \in Sa \cap Sb$, то $cb^{-1} \pmod m \in Sab^{-1} \cap S$. Отображение $x \to xa$ задает взаимно однозначное соответствие между S и Sa. Остальное очевидно.

Лемма 4. *Пусть число* m *делится на* p^2. *Тогда мощность множества* S *не превосходит* $\varphi(m)/p$.

Доказательство. Рассмотрим определенную в лемме 1 подгруппу G. Так как число p делит m, оно не делит $m-1$, и, значит, согласно лемме 1 и элементарному утверждению теории групп, для любого неединичного элемента $a \in G$ справедливо неравенство $a^{m-1} \neq 1$ и, значит, a — лжесвидетель и согласно лемме 2 множество $S \cap Sa$ пусто. Применяя лемму 3, выводим отсюда, что все множества Sg, где $g \in G$, попарно не пересекаются, и поэтому мощность их объединения равна pn, где n — мощность S, а так как оно содержится во множестве $\mathbf{Z}_m^*$, то $n \leqslant \varphi(m)/p$.

Лемма 5. *Пусть* m *свободно от квадратов. Тогда мощность множества* S *не превосходит* $\varphi(m)/4$.

Доказательство. Применяя китайскую теорему об остатках и теорему о существовании первообразного корня, находим такие числа $a_i \in \mathbf{Z}_m^*$, что $a_i \pmod{m/p_i} = 1$ и порядок $a_i \pmod{p_i}$ равен $p_i - 1$, где p_i — делители числа m, $i = 1, 2$. Тогда при любом k

$$a_i^k \pmod{m/p_i} = 1$$

и, следовательно, $a_i^k \pmod m \neq -1$, поэтому a_i и $a_i^{-1}, i = 1, 2$, — четыре лжесвидетеля.

Предположим, что $m = p_1 p_2$, $p_1 > p_2$, и заметим, что для $a = a_1 a_2 \pmod m$ из равенства $a^k \pmod m = 1$ следует, что $a_1^k \pmod{p_1} = 1$, и поэтому k делится на $p_1 - 1$. Но $m - 1 = p_2(p_1 - 1) + p_2 - 1$ не делится на $p_1 - 1$, так как $1 < p_2 < p_1$, значит, $a^{m-1} \pmod m \neq 1$, и поэтому a и, аналогично, $b = a_1 a_2^{-1}$ — еще два лжесвидетеля.

Если же m делится еще на третье простое число p_3, то $a_i \pmod{p_3} = 1$, значит,

$$a \pmod{p_3} = 1, \qquad b \pmod{p_3} = 1,$$

и

$$a^k \pmod{p_3} = 1, \qquad b^k \pmod{p_3} = 1,$$

поэтому при любом k

$$a^k \pmod m \neq -1, \qquad b^k \pmod m \neq -1,$$

а также порядок чисел a и b по модулю p_1 такой же, как и у a_1, то есть равен $p_1 - 1$. Следовательно, и в этом случае a, b — лжесвидетели.

Применяя лемму 3 к множествам S, Sa_1, Sa_2, Sa, замечаем, что они попарно не пересекаются и равномощны, значит, каждое из них имеет мощность не более $\varphi(m)/4$.

Доказательство теоремы теперь непосредственно следует из последних лемм.

Список литературы

1. Саломаа А. *Криптография с открытым ключом.* Мир, Москва, 1996.
2. Miller G. L. Riemann's hypothesis and tests for primality. *J. Comp. System Sci.* (1976) **13**, 300–317.
3. Rabin M. O. Probabilistic algorithm for testing primality. *J. Number Theory* (1980) **12**, №1, 128–138.
4. Knuth D. *The Art of Computer Programming. V.* 2. *Seminumerical Algorithms.* Addison–Wesley, Reading, Mass., 1981.

Статья поступила 02.02.1998.