Упрощенное обоснование вероятностного теста Миллера-Рабина для проверки простоты чисел

С.Б.Гашков

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

$$s^{(m-1)2^{-i}} \bmod m,\ i = 0, 1, \dots, r,\ m - 1 = 2^r t,$$

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 Рабина. Множество всех свидетелей простоты составного числа m имеет мощность не более $\phi(m)/4$.

Доказательство.

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

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

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

Доказательство её основано на тождестве

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

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

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

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

Доказательство.

Если $a^{m-1} \bmod m \neq 1$, то $(as)^{m-1} \bmod m \neq s^{m-1} = 1$ при $s \in S$, значит $as \bmod m$ не принадлежит S.

Пусть теперь $a^{m-1} \bmod m = 1$ и при некотором простом делителе p числа m порядок числа a по $\bmod p$ равен $p-1$ и также $a^k \bmod m \neq -1$ при любом целом k. Если $a^{(m-1)2^{-i}} \bmod m = 1$, то $a^{(m-1)2^{-i}} \bmod p = 1$, значит $(m-1)2^{-i}$ делится на $p-1$, поэтому $i < r$, так как t — нечетно, а $p-1$ — четно, и значит $a^t \bmod m \neq 1$, и согласно малой теореме Ферма $s^{(m-1)2^{-j}} \bmod p = 1$, и, значит, $s^{(m-1)2^{-j}} \bmod m \neq -1$ при всех $j, 0 \leq j \leq i$, а так как $s \in S$, то из последнего утверждения следует, что $s^{(m-1)2^{-j}} \bmod m = 1, 0 \leq j \leq i$, и $s^{(m-1)2^{-i-1}} \bmod m = \pm 1$.

Можно выбрать $i \geq 0$ так, что $a^{(m-1)2^{-j}} \bmod m = 1$ при всех $j, 0 \leq j \leq i$, но $a^{(m-1)2^{-i-1}} \bmod m \neq 1$. Тогда имеем, что $(as)^{(m-1)2^{-j}} \bmod m = s^{(m-1)2^{-j}} \bmod m = 1$ при всех $j, 0 \leq j \leq i$, но $(as)^{(m-1)2^{-i-1}} \bmod m = \pm a^{(m-1)2^{-i-1}} \bmod m \neq \pm 1$ так как $a^{(m-1)2^{-i-1}} \bmod m \neq 1$ и $a^k \bmod m \neq -1$ при всех k. Доказанное означает, что $as \bmod m$ не является свидетелем.

Следующая алгебраическая лемма общеизвестна.

Лемма 3. Пусть $a \neq b \in \mathbf{Z}_m^*$. Тогда $Sa \cap Sb = \emptyset \Leftrightarrow S \cap Sab^{-1} = \emptyset$. 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 во множестве $\mathbf{Z}_m^*$

Действительно, если бы $c \in Sa \cap Sb$, то $cb^{-1} \bmod m \in Sab^{-1} \cap S$. 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 $\phi(m)/p$.

Доказательство.

Рассмотрим определенную в лемме 1 подгруппу G. Так как число p делит m, то оно не делит $m-1$, и значит согласно лемме 1 и элементарному утверждению теории групп для любого неединичного элемента $a \in G$ имеем $a^{m-1} \neq 1$, 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 $n \leq \phi(m)/p$.

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

Доказательство.

Применяя китайскую теорему об остатках и теорему о существовании первообразного корня, находим такие числа $a_i \in \mathbf{Z}_m^*$, что $a_i \bmod m/p_i = 1$ и порядок $a_i \bmod p_i$ равен $p_i - 1$, где p_i—делители числа $m, i = 1, 2$. Тогда при любом k имеем $a_i^k \bmod m/p_i = 1$ и, следовательно, $a_i^k \bmod m \neq -1$, 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 $a = a_1 a_2 \bmod m$ из равенства $a^k \bmod m = 1$ следует, что $a_1^k \bmod p_1 = 1$, 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 $a^{m-1} \bmod m \neq 1$, и поэтому a и ,аналогично, $b = a_1 a_2^{-1}$ — ещё два лжесвидетеля.

Если же m делится еще на третье простое число p_3, то $a_i \bmod p_3 = 1$, значит $a \bmod p_3 = 1$, $b \bmod p_3 = 1$, и $a^k \bmod p_3 = 1$, $b^k \bmod p_3 = 1$, поэтому $a^k \bmod m \neq -1, b^k \bmod m \neq -1$ при любом k, а также порядок чисел a и b по mod p_1 такой же как и у a_1, т.е. 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 $\phi(m)/4$.

Доказательство теоремы теперь непосредственно следует из последних лемм.

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта 96-01-068).

Литература

[1] Саломаа А. Криптография с открытым ключом. Изд.«Мир»,Москва, 1996.

[2] Miller G.L. Riemann's hypotesis and tests for primality. Journal of Computer and System Sciences v.13, 1976, pp. 300-317.

[3] Rabin M.O. Probabilistic algorithm for testing primality. Journal Number Theory,1980,v.12,No 1,pp.128-138.

[4] Knut D.E. The art of computer programming Vol. 2 Seminumerical Algorithms. Second Edition. Addison-Wesley Publishing Company, 1981.