Оценка вероятности ошибки теста Миллера-Рабина на полупростых числах

Жуманиёзов Алишер Равшонбекович

Аспирант

ИВМиИТ К(П)ФУ, Казань, Россия

E-mail: ASZhumaniezov@kpfu.ru

Научный руководитель *— Ишмухаметов Шамиль Талгатович*

Одной из главных проблем криптографии является поиск простых чисел. Для её решения были разработаны различные алгоритмы проверки на простоту. Одним из наиболее известных и эффективных способов является тест Миллера-Рабина, который основан на теореме Эйлера [1]:

$$a^{n-1} \equiv 1 (mod\ n), \text{где } n - \text{простое} \tag{1}$$

Тест Миллера-Рабина вероятностный. Это означает, что он может выдавать ошибочный результат. Оценка вероятности ошибочного определения играет ключевую роль в оценки эффективности всего алгоритма.

Один из подходов к оценке распределения вероятности ошибки — через количество свидетелей простоты для произвольного числа n [3]. Для этого вводятся следующие определения:

Определение 1. *Пусть n представимо в виде $n = 2^s \cdot u$, где u — нечётное. Тогда введём следующие функции: $bin(n) = s$, $odd(n) = u$*

Определение 2. *Число a называют свидетелем простоты числа n, если тест Миллера-Рабина по этому основанию выносит вердикт "вероятно простое". Само n в свою очередь называют строго псевдопростым по основанию a.*

Верхняя граница для $Fr(n)$ — вероятности выбрать свидетеля простоты достигается на бесконечно большом множестве чисел. Поэтому для оценки используют среднее значение на отрезке $[1, X]$. В настоящий момент получена оценка только для класса полупростых чисел $n = pq$ при фиксированном p [2]:

$$AvgFr(X) = \frac{2p}{X} \ln(X) \ln(\ln(X)) \tag{2}$$

В данной работе представлен другой подход к оценке вероятности ошибки. Он основывается на следующей теореме [4]:

Теорема 1. *Пусть число $n = kp_t$, где p_t - простое, тогда, чтобы a был свидетелем простоты для n, необходимо, чтобы p_t делило без остатка число $h(a,k)$, где $h(a,k)$ вычисляется следующим образом:*

$$h(a,k) = \begin{cases} a^{odd(k-1)} - 1 & \text{если } bin(ord_k(a)) = 0 \\ a^{odd(k-1)\cdot 2^{c-1}} + 1 & \text{если } bin(ord_k(a)) = c > 0 \end{cases} \quad (3)$$

Теперь рассмотрим случай полупростых чисел $n = pq$. Поскольку p — нечётно и простое, то $bin(p-1) \geq bin(ord_p(a)) \geq 1$, применяя данное неравенство к функции $h(a,k)$ из теоремы 1 получаем:

$$h(a,p) \leq a^{odd(k-1)\cdot 2^{bin(p-1)-1}} + 1 \leq a^{\frac{p-1}{2}} + 1 \quad (4)$$

Теперь оценим количество делителей $h(a,p)$:

$$|\{p_t - \text{кандидат для строго пссевдопростого } n\}| \leq \ln(2)\frac{\ln(h(a,p))}{\ln(\ln(h(a,p)))} \approx \frac{\ln(2) ln(a)(p-1)}{2\ln(p-1)} \quad (5)$$

Просуммировав выражение (5) по всем p, получим количество полупростых и строго псевдопростых по основанию a чисел на отрезке $[1, X]$:

$$|\{n = pq - \text{строго псевдопростое по основанию } a\}| \leq \frac{\ln(2)\ln(a)}{2} \sum_{p \leq \sqrt{X}} \frac{p-1}{\ln(p-1)} \approx \frac{\ln(2)\ln(a)}{2} \frac{\left(\frac{\sqrt{X}}{\ln(\sqrt{X})}\right)^2}{2} = \frac{\ln(2)\ln(a)X}{(\ln(X))^2} \quad (6)$$

Таким образом мы находим оценку вероятности события, что число n на отрезке $[1, X]$ — полупростое и строго псевдопростое по основанию a:

$$P(n = pq - \text{строго псевдопростое по основанию } a) \leq \frac{\ln(2)\ln(a)}{(\ln(X))^2} \quad (7)$$

Таким образом мы получили верхнюю границу для оценки вероятности ошибки теста Миллера-Рабина для полупростых чисел. Однако данную оценку можно улучшить по нескольким направлением:

1. Использование нескольких оснований для теста. Поскольку p_t должен делить $h(a,k)$ для всех a, то для набора оснований необхо-

димо, чтобы p_t делило НОД этих значений. Это приводит к уменьшению значения, как показано на рис. 1, а также к приближению к линейной функции как показано на рис. 2.

Иллюстрации

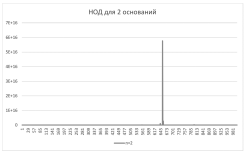

Рис. 1. НОД функции для 2 оснований

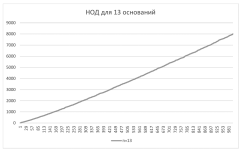

Рис. 2. НОД функции для 13 оснований

2. Количество делителей. Функция $h(a, k)$ возвращает в качестве результата не произвольное чисо, а определённого вида. Это можно использовать для уменьшения оценки количества делителей.

Литература

1. Винберг Э. Б. Малая теорема Ферма и ее обобщения // Матем. просв. — М.: МЦНМО, 2008. Т. 12, С. 43–53.
2. Мубараков Б. Г. Эффективная оценка теста простоты Миллера-Рабина натуральных чисел // Материалы XIX Всероссийской молодежной научной школы-конференции, Казань, 2020, Т. 59. С. 106-109.
3. Ishmukhametov S. T., Mubarakov B. G., Rubtsova R. G. On the Number of Witnesses in the Miller-Rabin Primality Test. Symmetry 2020, V.12, № 6. P. 890.
4. Sorenson J., Webster J. Strong Pseudoprimes to Twelve Prime Bases, Mathematics of Computation 2017, V.86, № 304. P. 985-1003.