Об одной комбинации вероятностных тестов простоты

Антонов Николай Андреевич

Аспирант 3 курса

Институт ВМиИТ(ВМК) КФУ, Казань, Россия

E-mail: nikoljaany@mail.ru

Научный руководитель *— Ишмухаметов Шамиль Талгатович*

Эффективная проверка натурального числа на простоту является важной задачей теории чисел и её приложений в криптографии. Детерминированный тест простоты AKS обладает полиномиальной, но сравнительно высокой сложностью $\mathbf{O}(\log^6 n)$ [1], поэтому в практических приложениях чаще используются вероятностные тесты простоты или их комбинации. Исследования показывают, что комбинация теста простоты LMR [2] и теста Миллера-Рабина, усиленного эвристическим поиском пробных баз, демонстрирует высокую эффективность проверки натурального числа на простоту.

Тест простоты LMR. Данный тест является расширением теста простоты Лукаса. В последнем используется ряд Фибоначчи $\{F_n\}_n$, а именно, проверяется условие $F_{n-e(n)} \equiv 0 \pmod{n}$, где $e(n) = \binom{n}{5}$ - символ Лежандра. Тест простоты LMR обладает большей точностью [2] и основан на следующих утверждениях:

Определение 1. *Пусть $n > 5$ - нечётное целое число, $e(n) = L(n, 5)$ - символ Лежандра, $n - e(n) = t \cdot 2^s$, причём t нечётно. Число n называется LMR-простым числом, если выполнено одно из следующих условий:*

1. $F_t \equiv 0 \pmod{n}$,
2. $(\exists\, i)\ \ 0 \le i < s,\ F_{m-1} + F_{m+1} \equiv 0 \pmod{n}$, *где* $m = t \cdot 2^i$.

Теорема 1. *Простое число $p > 5$ является LMR-простым числом.*

Эвристический выбор пробных чисел в тесте Миллера-Рабина. Сформулируем марковский процесс решений, состояние которого задано вектором параметов $(\alpha_1, \alpha_2, ..., \alpha_k)$, зависящим от проверяемого на простоту числа n. Действием будем считать выбор для итерации теста Миллера-Рабина пробного числа $a \in [2; 2\ln^2 n]$, либо сообщение о том, что n является простым числом. Если n простое, то оптимальная π^* сообщает об этом и завершает работу. Если n составное число, тогда π^*, исходя из текущего состояния $(\alpha_1, \alpha_2, ..., \alpha_k)$

	Mean	*Std*	*Median*	*Mode*
SEQ	15.879	15.341	12	12
RAND	4.010	8.690	2	1
RL	**1.509**	**1.088**	**1**	**1**

Таблица 1: Анализ количества использованных пробных чисел в зависимости от стратегии: последовательный выбор (SEQ) начиная с двойки, случайный выбор (RAND) и выбор на основе обучения с подкреплением (RL)

возвращает такое пробное число $a \in [2; 2\ln^2 n]$, что итерация теста Миллера-Рабина с ним наиболее вероятно (по сравнению с другими пробными числами) покажет, что n составное. Число a также называют *базой*. Подробные результаты исследования эвристического поиска баз для усиления теста Миллера-Рабина опубликованы в нашей статье [3], краткое резюме представлено в таблице 1. Поиск оптимальной политики π^* осуществляется при помощи алгоритма обучения с подкреплением PPO [4]. Тестирование стратегий проведено на выборке составных чисел $n \in [10^{24}; 10^{36}]$, имеющих высокую долю ложных свидетелей простоты [5].

Комбинация тестов. Практические эксперименты на числах $n \leq 10^{36}$ показывают, что последовательное применение теста простоты LMR и теста Миллера-Рабина, усиленного эвристическим поиском баз, позволяет безошибочно определить простоту числа.

Литература

1. M, Agrawal, N. Kayal, N. Saxena (2004). *PRIMES is in P.* Annals of Mathematics. 160 (2): 781-793.
2. S. Ishmukhametov, R. Rubtsova, R. Khusnutdinov. On a primality test of natural numbers, Russian Mathematics (rus), v.2, p.83-87 (2022)
3. N. Antonov, Sh. Ishmukhametov. An Intelligent Choice of Witnesses in the Miller–Rabin Primality Test. Reinforcement Learning Approach. Accepted for publication in LJM. DOI:10.1134/S1995080222150045
4. Schulman, J., Wolski, F., Dhariwal, P., Radford, A. Klimov, O. (2017). Proximal Policy Optimization Algorithms.. CoRR, abs/1707.06347.
5. Z. Zhang, Two kinds of strong pseudoprimes up to 10^{36}, Math. Comput., 76 (260):2095-2107, 2007.