МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ

УДК 510.52 DOI 10.17223/20710410/62/9

О ГЕНЕРИЧЕСКОЙ СЛОЖНОСТИ ПРОБЛЕМЫ ИЗВЛЕЧЕНИЯ КВАДРАТНОГО КОРНЯ ПО ПРОСТОМУ МОДУЛЮ[1]

А. Н. Рыбалов

Институт математики им. С. Л. Соболева СО РАН, г. Омск, Россия

E-mail: alexander.rybalov@gmail.com

Изучается генерическая сложность проблемы извлечения квадратного корня по простому модулю. Вопрос о вычислительной сложности этой проблемы до сих пор открыт. Однако известны алгоритмы (например, алгоритм Чиполлы), которые являются полиномиальными при условии истинности расширенной гипотезы Римана. Доказывается, что проблема является генерически разрешимой за полиномиальное время. Фактически это означает, что алгоритм Чиполлы работает за полиномиальное время для «почти всех» входов. Понятие «почти все» формализуется введением асимптотической плотности на множестве входных данных.

Ключевые слова: *генерическая сложность, квадратный корень по простому модулю.*

ON THE GENERIC COMPLEXITY OF THE SQUARE ROOT MODULO PRIME PROBLEM

A. N. Rybalov

Sobolev Institute of Mathematics, Omsk, Russia

We study the generic complexity of the problem of finding a square root modulo a prime number. The question about the computational complexity of this problem is still open. However, there are known algorithms (e.g. Cipolla's algorithm) which are polynomial if the extended Riemann hypothesis holds. We prove that this problem is generically decidable in polynomial time. In fact, this means that Cipolla's algorithm runs in polynomial time for "almost all" inputs. The notion "almost all" is formalized by introducing the asymptotic density on a set of input data.

Keywords: *generic complexity, square root modulo prime.*

Введение

Проблема нахождения квадратного корня по простому модулю является классической алгоритмической проблемой теории чисел, восходящей ещё к Эйлеру и Гауссу. В отличие от других классических проблем, таких, как проблема факторизации целых

[1]Работа поддержана грантом Российского научного фонда № 22-11-20019.

чисел или проблема дискретного логарифма, известны алгоритмы, которые решают её за полиномиальное время при условии истинности некоторых гипотез теории чисел. Например, алгоритм Чиполлы [1] является полиномиальным при условии истинности расширенной гипотезы Римана [2]. Проблема распознавания существования квадратного корня по простому модулю значительно проще — для неё известен эффективный критерий Эйлера.

Генерический подход [3] — это один из подходов к изучению алгоритмических проблем для «почти всех» входов. В рамках этого подхода алгоритмическая проблема рассматривается не на всём множестве входов, а на некотором подмножестве «почти всех» входов. Такие входы образуют так называемое генерическое множество. Понятие «почти все» формализуется введением естественной меры на множестве входных данных. С точки зрения практики алгоритмы, решающие быстро проблему на генерическом множестве, так же хороши, как и быстрые алгоритмы для всех входов.

В данной работе изучается генерическая сложность проблемы извлечения квадратного корня по простому модулю. Доказывается, что эта проблема генерически разрешима за полиномиальное время. Отметим, что для составного модуля неизвестно полиномиального алгоритма даже для распознавания существования квадратного корня [4]. Для данной проблемы получен результат об отсутствии полиномиальных генерических алгоритмов [5].

1. Предварительные сведения

Пусть p — простое число. Натуральное число $a < p$ называется *квадратичным вычетом*, если существует такое натуральное $x < p$, что $x^2 = a \pmod p$. В противном случае a называется *квадратичным невычетом*. Есть эффективный критерий проверки, является ли натуральное число квадратичным вычетом по простому модулю.

Теорема 1 (Эйлер). Пусть p — нечётное простое число. Натуральное число a является квадратичным вычетом по модулю p тогда и только тогда, когда

$$a^{(p-1)/2} = 1 \pmod p.$$

Из этой теоремы следует, что проблема распознавания квадратичных вычетов по простому модулю разрешима за полиномиальное время.

Проблема извлечения квадратного корня по простому модулю состоит в следующем. Даны простое число p и натуральное число $a < p$, записанные в двоичной системе. Необходимо найти натуральное число $x < p$, такое, что $x^2 = a \pmod p$, если это возможно, либо выдать ответ -1.

В отличие от проблемы распознавания квадратичных вычетов, для извлечения квадратного корня не доказана разрешимость за полиномиальное время [4]. Однако существует алгоритм Чиполлы [1], который решает эту задачу за полиномиальное время при условии знания какого-нибудь квадратичного невычета b по модулю p.

Алгоритм Чиполлы:

1) Вход: p, a и квадратичный невычет b.
2) Квадратный корень получается вычислением по формуле $x = \left(a + \sqrt{b}\right)^{(p+1)/2}$ в поле $\mathbb{F}_{p^2} = \mathbb{F}_p(\sqrt{b})$ — квадратичном расширении поля $\mathbf{F}_p$.

Обозначим через $\eta(p)$ наименьший квадратичный невычет по модулю p. Н. Анкени доказал [2], что в предположении истинности расширенной гипотезы Римана существует константа C, такая, что для любого простого p имеет место $\eta(p) < C(\log p)^2$. Здесь

и далее под $\log p$ понимается логарифм по основанию 2. Таким образом, в предположении истинности расширенной гипотезы Римана квадратичный невычет может быть найден за полиномиальное время и алгоритм Чиполлы становится полиномиальным.

2. Основной результат

Определение генерического полиномиального алгоритма можно найти в [3, 5].

Множество входов проблемы извлечения квадратного корня по простому модулю есть

$$I = \{(p, a) : p \text{ простое}, \ 0 < a < p\}.$$

Под размером входа (p, a) будем понимать длину двоичной записи числа p. Таким образом, множество входов размера n есть

$$I_n = \{(p, a) : (p, a) \in I, \ 2^n < p < 2^{n+1}\}.$$

Для конечного множества A через $|A|$ обозначается число его элементов; функция $\pi(x)$ задаёт количество простых чисел, не превосходящих x.

Лемма 1. Для достаточно больших n имеет место

$$\frac{2^{2n}}{n} < |I_n| < \frac{2^{2(n+1)}}{n}.$$

Доказательство. Заметим, что

$$|I_n| = \sum_{2^n < p < 2^{n+1}} p,$$

где суммирование идёт по простым числам. Отсюда

$$2^n(\pi(2^{n+1}) - \pi(2^n)) < |I_n| < 2^{n+1}(\pi(2^{n+1}) - \pi(2^n)). \tag{1}$$

Из асимптотического закона распределения простых чисел следует, что для достаточно больших n имеет место

$$\frac{0{,}9 \cdot 2^n}{n \ln 2} < \pi(2^n) < \frac{1{,}1 \cdot 2^n}{n \ln 2},$$

а также

$$\frac{0{,}9 \cdot 2^{n+1}}{(n+1) \ln 2} < \pi(2^{n+1}) < \frac{1{,}1 \cdot 2^{n+1}}{(n+1) \ln 2}.$$

Поэтому

$$\frac{0{,}9 \cdot 2^{n+1}}{(n+1) \ln 2} - \frac{1{,}1 \cdot 2^n}{n \ln 2} < \pi(2^{n+1}) - \pi(2^n) < \frac{1{,}1 \cdot 2^{n+1}}{(n+1) \ln 2} - \frac{0{,}9 \cdot 2^n}{n \ln 2}.$$

Отсюда получаем

$$\frac{2^n}{n} < \pi(2^{n+1}) - \pi(2^n) < \frac{2^{n+1}}{n},$$

что вместе с (1) даёт нужную оценку. ■

Рассмотрим следующее множество входов проблемы извлечения корня:

$$\mathcal{S} = \{(p, a) : (p, a) \in I, \ \eta(p) > 21 \log p\}.$$

Лемма 2. Для достаточно больших n имеет место

$$\frac{|\mathcal{S} \cap I_n|}{|I_n|} < \frac{1}{n}.$$

Доказательство. П. Эрдеш доказал [6], что существует константа C, $3 < C < 4$, такая, что

$$\lim_{k\to\infty} \frac{\sum\limits_{p\leqslant k} \eta(p)}{\pi(k)} = C.$$

Здесь суммирование берётся по простым p. Отсюда следует, что для достаточно больших k имеет место

$$3\pi(k) < \sum_{p\leqslant k} \eta(p) < 4\pi(k).$$

Используя это неравенство, оценим сумму

$$\sum_{2^n<p<2^{n+1}} \eta(p) = \sum_{p<2^{n+1}} \eta(p) - \sum_{p<2^n} \eta(p)$$

следующим образом:

$$3\pi(2^{n+1}) - 4\pi(2^n) < \sum_{2^n<p<2^{n+1}} \eta(p) < 4\pi(2^{n+1}) - 3\pi(2^n).$$

Используя асимптотический закон распределения простых чисел, для достаточно больших n получаем

$$\frac{2^{n+1}}{n} < \sum_{2^n<p<2^{n+1}} \eta(p) < \frac{10\cdot 2^n}{n}.$$

Из этих неравенств следует, что

$$\sum_{2^n<p<2^{n+1}} \eta(p)\, p < 2^{n+1} \sum_{2^n<p<2^{n+1}} \eta(p) < \frac{20\cdot 2^{2n}}{n}. \tag{2}$$

Допустим теперь, что лемма неверна, то есть существуют сколь угодно большие n, такие, что

$$\frac{|\mathcal{S} \cap I_n|}{|I_n|} > \frac{1}{n},$$

то есть

$$|\mathcal{S} \cap I_n| > \frac{|I_n|}{n}.$$

Заметим, что

$$|\mathcal{S} \cap I_n| = \sum_{\substack{2^n<p<2^{n+1},\\ \eta(p)>21n}} p.$$

Тогда

$$\sum_{2^n<p<2^{n+1}} \eta(p)\, p = \sum_{\substack{2^n<p<2^{n+1},\\ \eta(p)>21n}} \eta(p)\, p + \sum_{\substack{2^n<p<2^{n+1},\\ \eta(p)\leqslant 21n}} \eta(p)\, p \geqslant$$

$$\geqslant 21n \sum_{\substack{2^n<p<2^{n+1},\\ \eta(p)>21n}} p > 21n\, \frac{|I_n|}{n} = 21|I_n| > \frac{21\cdot 2^{2n}}{n}.$$

Последняя оценка следует из леммы 1. Но это противоречит оценке сверху (2). ■

Теорема 2. Проблема извлечения квадратного корня по простому модулю генерически разрешима за полиномиальное время.

Доказательство. Полиномиальный генерический алгоритм работает на входе (p, a) размера n следующим образом:

1) С помощью критерия Эйлера проверяет, является ли a квадратичным вычетом по модулю p. Если не является, выдаёт -1. Иначе переходит к следующему шагу.
2) Ищет среди чисел от 2 до $21n$ квадратичный невычет с помощью критерия Эйлера.
3) Если квадратичный невычет не найден, то выдаёт ответ «НЕ ЗНАЮ».
4) Если найден квадратичный невычет, то с его помощью по алгоритму Чиполлы находится квадратный корень из a по модулю p.

Генеричность этого алгоритма следует из того, что множество входов, на которых алгоритм выдаёт ответ «НЕ ЗНАЮ», является пренебрежимым, согласно лемме 2. ■

ЛИТЕРАТУРА

1. *Cipolla M.* Un metodo per la risoluzione della congruenza di secondo grado // Rendiconto dell' Accademia delle Scienze Fisiche e Matematiche. Napoli, 1904. V. 10. No. 3. P. 144–150. (in Italian)
2. *Ankeny N. C.* The least quadratic non residue // Ann. Math. 1952. V. 55. P. 65–72.
3. *Kapovich I., Miasnikov A., Schupp P., and Shpilrain V.* Generic-case complexity, decision problems in group theory and random walks // J. Algebra. 2003. V. 264. No. 2. P. 665–694.
4. *Adleman L. M. and McCurley K. S.* Open problems in number theoretic complexity, II // LNCS. 1994. V. 877. P. 291–322.
5. *Рыбалов А. Н.* О генерической сложности проблемы распознавания квадратичных вычетов // Прикладная дискретная математика. 2015. № 2(28). С. 54–58.
6. *Erdos P.* Remarks on number theory I // Mat. Lapok. 1961. V. 12. P. 10–17.

REFERENCES

1. *Cipolla M.* Un metodo per la risoluzione della congruenza di secondo grado. Rendiconto dell' Accademia delle Scienze Fisiche e Matematiche. Napoli, 1904, vol. 10, no. 3, pp. 144–150. (in Italian)
2. *Ankeny N. C.* The least quadratic non residue. Ann. Math., 1952, vol. 55, pp. 65–72.
3. *Kapovich I., Miasnikov A., Schupp P., and Shpilrain V.* Generic-case complexity, decision problems in group theory and random walks. J. Algebra, 2003, vol. 264, no. 2, pp. 665–694.
4. *Adleman L. M. and McCurley K. S.* Open problems in number theoretic complexity, II. LNCS, 1994, vol. 877, pp. 291–322.
5. *Rybalov A. N.* O genericheskoy slozhnosti problemy raspoznavaniya kvadratichnykh vychetov [On generic complexity of the quadratic residuosity problem]. Prikladnaya Diskretnaya Matematika, 2015, no. 2(28), pp. 54–58. (in Russian)
6. *Erdos P.* Remarks on number theory I. Mat. Lapok., 1961, vol. 12, pp. 10–17.