

СЛОЖНОСТЬ ВЫЧИСЛЕНИЙ

# Вероятностная проверка на простоту без ошибок

Чернис Константин, группа 694

# Содержание

<b>1</b>	<b>Введение в сложностные классы</b>	<b>2</b>
<b>2</b>	<b>Сертификаты</b>	<b>3</b>
<b>3</b>	<b>Алгоритм Миллера-Рабина</b>	<b>3</b>
3.1	Описание алгоритма . . . . .	3
3.2	Доказательство оценки на число свидетелей . . . . .	4
3.3	Сертификат . . . . .	6
<b>4</b>	<b>Алгоритм Эдельмана-Хуана</b>	<b>7</b>
4.1	Пример . . . . .	7
4.2	Алгоритм Гольдвассер-Килиана . . . . .	8
4.3	Алгоритм Эдельмана-Хуана . . . . .	9
4.4	Сертификат . . . . .	10
<b>5</b>	<b>Алгоритм ЕСРР</b>	<b>10</b>
5.1	Описание . . . . .	10
5.2	Сертификат . . . . .	11
5.3	Время работы . . . . .	11
<b>6</b>	<b>Практика</b>	<b>11</b>
<b>7</b>	<b>Список литературы</b>	<b>11</b>

В данном проекте доказываются избранные факты вероятностной проверки чисел на простоту, а также проводятся некоторые эксперименты.

## 1. Введение в сложностные классы

Для начала опишем сложностные классы, затрагиваемые данной задачей:

**Определение 1.1.** Вероятностной машиной Тьюринга называется детерминированная машина Тьюринга  $M$  с двумя аргументами  $x$  (аргумент вероятностной машины) и  $r$  (случайные биты), где длина  $r$  есть некоторая функция от длины  $x$ . Результатом работы  $M$  на входе  $x$  будет вероятностное распределение, индуцированное данным  $x$  и равномерным на всех значениях  $r$ . Временем работы  $M$  на данном  $x$  будем считать максимальное время работы  $M(x, r)$  для всех  $r$  указанной длины. Так же определяется и использованная память.

**Определение 1.2.** Классом **RP** называется класс языков  $A$ , для которых существует полиномиальный в худшем случае вероятностный алгоритм  $V$ , такой что:

- если  $x \in A$ , то  $P_r[V(x, r) = 1] \geq \frac{1}{2}$ ;
- если  $x \notin A$ , то  $P_r[V(x, r) = 1] = 0$ .

**Определение 1.3.** Классом **coRP** называется класс языков  $A$ , для которых существует полиномиальный в худшем случае вероятностный алгоритм  $V$ , такой что:

- если  $x \in A$ , то  $P_r[V(x, r) = 1] = 1$ ;
- если  $x \notin A$ , то  $P_r[V(x, r) = 1] \leq \frac{1}{2}$ .

**Определение 1.4.** Классом **ZPP** называется класс языков  $A$ , для которых существует вероятностный алгоритм  $A$ , такой что

$$x \in A \iff \forall r V(x, r) = 1,$$

а для каждого  $x$  ожидаемое по  $r$  время работы полиномиально.

Обозначение **ZPP** расшифровывается как "zero-error probabistic polynomial".

**Утверждение 1.1.**  $\mathbf{ZPP} = \mathbf{RP} \cap \mathbf{coRP}$ .

Таким образом, для вероятностной проверки чисел на простоту достаточно предоставить алгоритмы проверки чисел на простоту из **RP** и **coRP**, после чего запускать их по очереди до тех пор, пока один из алгоритмов не выдаст ответ, в котором он уверен. Вероятность отсутствия ответа будет уменьшаться минимум в 4 раза после каждой итерации цикла проверки, так что за полиномиальное число шагов вероятность станет экспоненциально малой и можно будет применить детерминированный экспоненциальный алгоритм.

## 2. Сертификаты

### Утверждение 2.1. $\mathbf{RP} \subset \mathbf{NP}$

**Доказательство.** Действительно, любое значение  $r$ , при котором  $V(x, r) = 1$ , будет доказательством того, что  $x \in A$ . ■

### Следствие 2.1. $\mathbf{coRP} \subset \mathbf{coNP}$

Таким образом, в силу того, что язык простых чисел, как будет показано далее, лежит в  $\mathbf{ZPP}$ , для любого  $n \in \mathbb{Z}$  существует либо сертификат простоты, либо сертификат того, что  $n$  составное, проверяемый за полиномиальное время. Таким образом, единожды проверив число на простоту за вероятностно полиномиальное время, в дальнейшем можно снова доказать корректность проверки уже за детерминированный полином. Эти сертификаты будут указаны для каждого описанного ниже алгоритма соответственно.

В следующей секции будет описан алгоритм из  $\mathbf{coRP}$ , а в секции 4 — из  $\mathbf{RP}$ .

## 3. Алгоритм Миллера-Рабина

Большинство алгоритмов вероятностной проверки на простоту из  $\mathbf{coRP}$  опираются на какое-либо свойство простых чисел, то есть проверяют необходимое условие. Наиболее популярным среди них является алгоритм Миллера-Рабина, который гарантирует, что для нечётного составного минимум 75% чисел от 1 до  $n - 1$  позволяют определить его непростоту.

Говоря в терминах Определения 1.3,  $A$  — множество простых чисел, и для  $x \notin A$   $P_r[V(x, r) = 1] \leq \frac{1}{4}$ , где  $r \in \overline{1, n-1}$ . Кроме того, как будет показано ниже, проверяемое условие действительно является необходимым, то есть для  $x \in A$   $P_r[V(x, r) = 1] = 1$ , то есть алгоритм Миллера-Рабина лежит в  $\mathbf{coNP}$ .

### 3.1 Описание алгоритма

Заданное нечётное целое число  $n > 1$  можно представить в виде  $n - 1 = 2^e k$ , где  $e \geq 1$  (т.к.  $n$  нечётно) и  $k$  нечётное. Применяя к  $x^{n-1} - 1 = x^{2^e k} - 1$  формулу разности квадратов, получаем:

$$\begin{aligned} x^{2^e k} - 1 &= \left( x^{2^{e-1} k} \right)^2 - 1 \\ &= \left( x^{2^{e-1} k} - 1 \right) \left( x^{2^{e-1} k} + 1 \right) \\ &= \left( x^{2^{e-2} k} - 1 \right) \left( x^{2^{e-2} k} + 1 \right) \left( x^{2^{e-1} k} + 1 \right) \\ &\vdots \\ &= \left( x^k - 1 \right) \left( x^k + 1 \right) \left( x^{2k} + 1 \right) \left( x^{4k} + 1 \right) \dots \left( x^{2^{e-1} k} + 1 \right) \end{aligned}$$

Если  $n$  простое и  $a \in \overline{1, n-1}$ , то по малой теореме Ферма  $a^{n-1} - 1 \equiv 0 \pmod n$ . Используя разложение, полученное выше, имеем

$$(x^k - 1)(x^k + 1)(x^{2k} + 1)(x^{4k} + 1) \dots (x^{2^{e-1}k} + 1) \equiv 0 \pmod n$$

Таким образом, для простого  $n$  один из множителей должен делиться на  $n$ , то есть необходимым условием, нарушение которого означает, что число составное, является

$$a^k \equiv 1 \pmod n \text{ или } a^{2^i k} \equiv -1 \pmod n \text{ для некоторого } i \in \overline{0, e-1}.$$

**Определение 3.1.** Представим нечётное  $n > 1$  в виде  $n - 1 = 2^e k$ , где  $e$  нечётно и выберем  $a \in \overline{1, n-1}$ . Тогда  $a$  называется свидетелем для числа  $n$ , если не выполнено необходимое условие, то есть

$$a^k \not\equiv 1 \pmod n \text{ и } a^{2^i k} \not\equiv -1 \pmod n \forall i \in \overline{0, e-1}.$$

Если же необходимое условие выполнено, то есть

$$a^k \equiv 1 \pmod n \text{ или } a^{2^i k} \equiv -1 \pmod n \text{ для некоторого } i \in \overline{0, e-1},$$

то  $a$  не является свидетелем для  $n$ .

Отметим, что уже сейчас можно построить вероятностный алгоритм проверки на простоту со сколь угодно малой вероятностью ошибки:

**Data:** проверяемое число  $n$ , количество итераций  $t$

**Result:** является ли число  $n$  простым

**for**  $i \in \overline{1, t}$  **do**

выбрать случайное  $a$  из  $\overline{1, n-1}$ ;  
**if**  $a$  является свидетелем для  $n$  **then**  
    | **return** "n составное";  
**end**

**end**

**return** "n простое с вероятностью минимум  $1 - 1/4^t$ ";

## 3.2 Доказательство оценки на число свидетелей

Для начала покажем, что оценка 75% неумлучшаема:

**Утверждение 3.1.** Доля свидетелей для  $n = 9$  составляет  $3/4$ .

**Доказательство.**  $n - 1 = 8 = 2^3$ , так что  $e = 3$  и  $k = 1$ , и для проверки необходимого условия надо перебрать  $(a, a^2, a^3)$ . Из приведённой ниже таблицы видно, что свидетелями среди  $\overline{1, 8}$  являются 2, 3, 4, 5, 6, 7, что составляет  $6/8 = 3/4$ , что и требовалось.

$a \pmod 9$	1	2	3	4	5	6	7	8
$a^2 \pmod 9$	1	4	0	7	7	0	4	1
$a^3 \pmod 9$	1	7	0	4	4	0	7	1

Существует также доказательство неулучшаемости оценки при  $n \rightarrow \infty$ , оно приведено в [3]. ■

**Теорема 3.1.** Пусть  $n > 1$  нечётное составное.

Доля целых чисел среди  $\overline{1, n-1}$ , являющихся свидетелями числа  $n$ , превышает 75%, за исключением  $n = 9$ , для которого доля составляет 75%.

Другими словами, доля целых чисел среди  $\overline{1, n-1}$ , не являющихся свидетелями числа  $n$ , меньше 25%, за исключением  $n = 9$ , для которого доля составляет 25%.

Докажем более слабое утверждение:

**Теорема 3.2.** Если  $n > 1$  нечётное и составное, то доля свидетелей числа  $n$  превышает 50%. Другими словами, больше 50% из  $a \in \overline{1, n-1}$  удовлетворяют  $a^k \not\equiv 1 \pmod n$  и  $a^{2^i k} \not\equiv -1 \pmod n \forall i \in \overline{0, e-1}$ .

**Доказательство.** Докажем, что доля не свидетелей для  $n$  меньше 50%, показав, что они образуют собственную подгруппу группы обратимых чисел  $\pmod n$ . В силу того, что порядок собственной подгруппы составляет максимум половину от порядка группы, множество свидетелей числа  $n$  содержит минимум половину обратимых чисел  $\pmod n$  и все необратимые числа  $\pmod n$  среди  $\overline{1, n-1}$  (множество необратимых непусто в силу того, что  $n$  составное). Таким образом, доля свидетелей для числа  $n$  превышает 50%.

**Случай 1:**  $n$  является степенью простого числа, то есть  $n = p^\alpha$ , где  $p$  — нечётное простое и  $\alpha \geq 2$ .

**Утверждение 3.2.** Если  $n = p^\alpha$  для простого  $p$  и  $\alpha \geq 1$ , то не свидетели для  $n$  являются корнями уравнения  $a^{p-1} \equiv 1 \pmod{p^\alpha}$ , которые образуют группу по умножению  $\pmod n$ .

**Доказательство.** Обоснование приведено в [2]. ■

Согласно Утверждению 2.2 свидетели непростоты образуют группу по умножению  $\pmod n$ . Порядок числа  $a$ , являющегося решением уравнения  $a^{p-1} \equiv 1 \pmod n$ , делит  $p-1$ , так что он не делится на  $p$ . В то же время существуют обратимые  $\pmod n$  числа, порядок которых делится на  $p$ : примером такого числа является  $1+p$ , чей порядок  $\pmod{p^\alpha}$  составляет  $p^{\alpha-1}$  (этот факт можно показать индукцией по  $r$ : база  $-1+kp \equiv 1 \pmod p$ , переход  $-(1+kp^r)^p \equiv 1 \pmod{p^{r+1}}$ ). Таким образом, не свидетели  $\pmod n$  образуют собственную подгруппу в группе обратимых чисел  $\pmod n$ , что заканчивает доказательство этого случая.

**Случай 2:**  $n$  не является степенью простого. Пусть  $i_0 \in \overline{0, e-1}$  — максимальное число, такое что  $\exists a_0 \in \mathbb{Z}$  такой что  $a_0^{2^{i_0}} \equiv -1 \pmod n$ . (В силу того, что  $(-1)^{2^0} = -1$ , требуемый  $i_0$  существует, причём  $a_0$  взаимно прост с  $n$ ).

Множество

$$G_n = \{ a \in \overline{1, n-1} \mid a^{2^{i_0} k} \equiv \pm 1 \pmod n \}$$

является группой по умножению  $\pmod n$  и содержит все  $a$ , удовлетворяющие одному из двух условий:

$$(1) \ a^k \equiv 1 \pmod n,$$

(2)  $a^{2^i k} \equiv 1 \pmod n$  для одного из  $i \in \overline{0, e-1}$ .

Если  $a^k \equiv 1 \pmod n$ , то  $a^{2^{i_0} k} \equiv 1 \pmod n$ . Если же  $a^{2^i k} \equiv 1 \pmod n$  для некоторого  $i \in \overline{0, e-1}$ , то  $(2^k)^{2^i} \equiv -1 \pmod n$ , причём  $i \leq i_0$  в силу максимальнойности  $i_0$ . Таким образом,  $a^{2^{i_0}} \equiv -1 \pmod n$ , если  $i = i_0$ , и  $a^{2^{i_0}} \equiv 1 \pmod n$ , если  $i < i_0$ . Отсюда все  $a \in \overline{1, n-1}$ , удовлетворяющие (1) или (2), лежат в  $G_n$ .

Покажем, что  $G_n$  является собственной подгруппой обратимых чисел  $\pmod n$ , для чего найдём обратимое число, не лежащее в  $G_n$ . Пусть  $p$  — простой делитель  $n$ , тогда представим  $n$  в виде  $n = p^\alpha n'$ , где  $\alpha \geq 1$  и  $p \nmid n'$ .  $p^\alpha$  и  $n'$  нечётные и не равны 1 (в силу того, что  $n$  не является степенью простого)  $\implies p^\alpha, n' \geq 3$ .

Согласно китайской теореме об остатках,  $\exists a \in \overline{1, n-1}$ , удовлетворяющий следующим двум уравнениям:

$$a \equiv a_0 \pmod{p^\alpha}, \quad a \equiv 1 \pmod{n'}.$$

Выше показали, что  $(a_0, n) = 1 \implies (a, n) = 1$  (т.к.  $(a, n') = 1$ ), то есть  $a$  является обратимым  $\pmod n$ . Тогда для доказательства того, что подгруппа  $G_n$  не является собственной, остаётся показать, что  $a \notin G_n$ .

$$a^{2^{i_0} k} \equiv a_0^{2^{i_0} k} \equiv (-1)^k \equiv -1 \pmod{p^\alpha} \implies a^{2^{i_0} k} \not\equiv 1 \pmod n$$

в силу того, что  $-1 \not\equiv 1 \pmod{p^\alpha}$  (т.к.  $p^\alpha \geq 3$ ). Кроме того,

$$a^{2^{i_0} k} \equiv 1 \pmod{n'} \implies a^{2^{i_0} k} \not\equiv -1 \pmod n$$

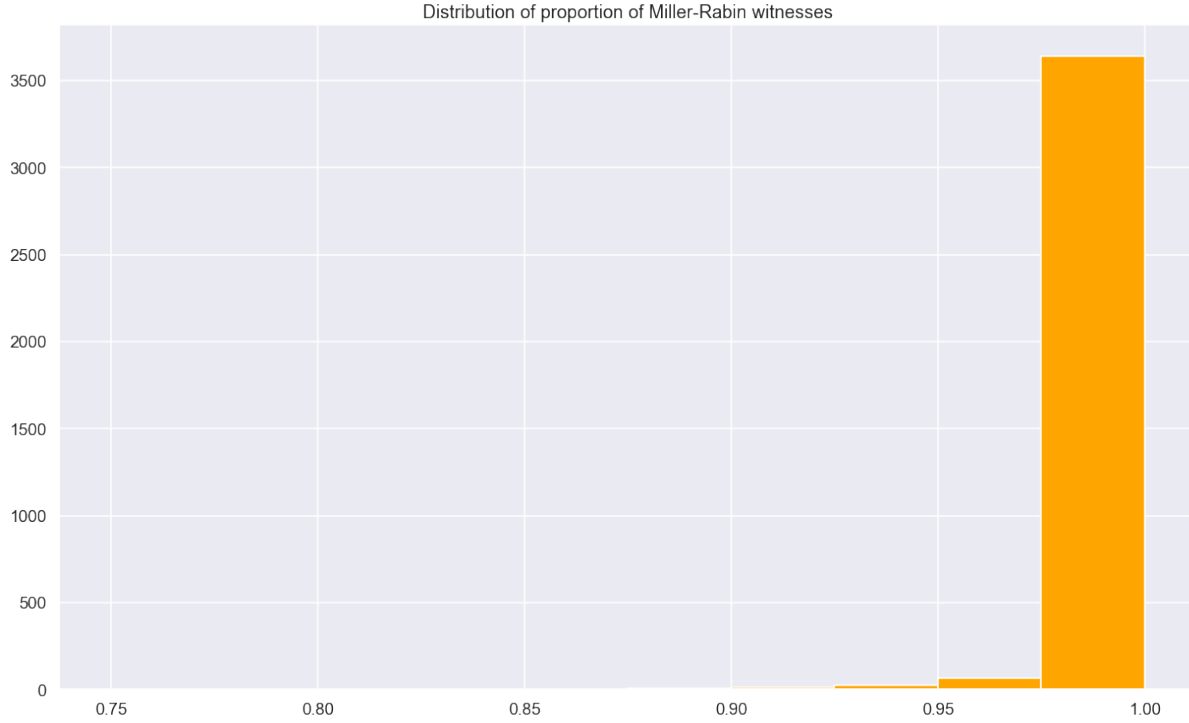
в силу того, что  $-1 \not\equiv 1 \pmod{n'}$  (т.к.  $n' \geq 3$ ). Таким образом,  $a \notin G_n$ , что завершает доказательство данного случая, а с ним и всей теоремы. ■

Теорема 2.1 доказывается аналогичным образом, оценка  $1/4$  на число не свидетелей достигается за счёт двукратного применения приёма с собственной подгруппой. Полное доказательство описано в [2].

### 3.3 Сертификат

Из алгоритма видно, что сертификатом является определённый выше свидетель — число  $a$ , для которого не выполнено необходимое условие простоты. Сложность проверки сертификата составляет  $O(\log^3 n)$ , если умножение производится за  $O(\log^2 n)$ , то есть проверка сертификата полиномиальна.

На самом деле, для большинства составных чисел доля свидетелей гораздо выше 75%. Для демонстрации этого факта построим гистограмму долей свидетелей для всех составных чисел до  $10^4$ :



В следующей секции будет описан алгоритм из **RP**. В силу нетривиальности одного будет дано неформальное интуитивное описание. Полный алгоритм и доказательство корректности доступно в [4].

## 4. Алгоритм Эдельмана-Хуана

Для начала проиллюстрируем метод проверки на простоту, используемый в алгоритме Эдельмана-Хуана.

### 4.1 Пример

Рассмотрим следующее доказательство простоты числа 11:

- (1)  $(4 - 1, 11) = 1$
- (2)  $4^5 = 1024 \equiv 1 \pmod{11}$
- (3) 5 — простое число

Пусть 11 не является простым. Тогда существует простое  $p \leq \sqrt{11} < 4$ , делящее 11. Из (1) получаем, что  $4 \pmod p \not\equiv 1$  в  $\mathbb{Z}/p\mathbb{Z}^* \implies \text{ord}(4 \pmod p) \neq 1$ . Из (2) следует, что  $\text{ord}(4 \pmod p) \mid 5$ . Наконец, из (3) получаем, что  $\text{ord}(4 \pmod p) = 5$ , что невозможно, так как  $p < 4$ .

Заметим, что без (3) рассуждение выше дало бы сведение доказательства простоты числа 11 к простоте числа 5. Идея сведения доказательства простоты одного числа к простоте другого является ключевой в описываемом алгоритме.

Построим алгоритм на технике из примера:



**Алгоритм:** Для достаточно больших  $p$  за вероятностно полиномиальное время можно свести доказательство простоты  $p$  к простоте  $\frac{p-1}{2}$ . Для этого надо лишь перебирать случайные  $a \in Z_{>0}$ , пока не будет выполнено

$$(1) (a-1, p) = 1$$

$$(2) a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

Для  $p > 2$  существует  $\frac{p-3}{2}$  чисел  $a < p$ , удовлетворяющих этим требованиям, так что алгоритм будет работать за вероятностно полиномиальное время.

Возвращаясь к проверке на простоту числа 11, можно было свести простоту числа 5 к простоте числа 2, которую можно проверить явно. В то же время данный алгоритм не применим в общем случае, ибо сведение простоты числа 13 к простоте числа 6 бесполезно.

В следующем подпункте будет описан рабочий алгоритм, обеспечивающий сведение.

## 4.2 Алгоритм Гольдвассер-Килиана

Алгоритм Гольдвассер-Килиана обходит описанную выше проблему за счёт использования групп, отличных от  $Z/pZ^*$ . Для этого введем эллиптические кривые:

**Определение 4.1.** Эллиптической кривой называется кривая, задаваемая уравнением вида

$$y^2 = x^3 + Ax + b,$$

для которой выполнено  $\Delta = 4A^3 + 27B^3 \neq 0$ .

**Алгоритм:** Случайным образом ищем  $a, b \in Z/pZ$ , удовлетворяющие следующим условиям:

$$(1) f(x) = x^3 - ax + b \text{ не имеет кратных корней}$$

$$(2) \text{число рациональных точек на эллиптической кривой } y^2 = f(x) \text{ равно } 2 * m \text{ для некоторого } m \in Z$$

Далее ищем пару  $s, t \in Z/pZ$ , такую что

$$(1) \text{точка } v = \langle s, t \rangle \text{ лежит на кривой}$$

$$(2) m * v = 1 \text{ в группе, ассоциированной с кривой}$$

Можно показать, что если найти  $v$ , удовлетворяющую условию, то доказательство простоты  $p$  сводится к доказательству простоты  $m$  (то есть получено утверждение  $m$  простое  $\implies p$  простое). Кроме того, из гипотезы Римана для конечных полей  $m \approx \frac{p}{2}$ .

С другой стороны, для того, чтобы описанный выше алгоритм был вероятностно полиномиальным, требуется, чтобы на случайно сгенерированной эллиптической

кривой с высокой вероятностью было дважды простое число рациональных точек. Гипотеза Римана гарантирует, что число точек находится в интервале

$$[p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}]$$

В силу того, что этот интервал слишком мал, вероятностная полиномиальность описанного выше алгоритма до сих пор не доказана. Эта проблема решена в алгоритме Эдельмана-Хуана, описанном ниже.

### 4.3 Алгоритм Эдельмана-Хуана

Введём понятие гиперэллиптических кривых:

**Определение 4.2.** Гиперэллиптической кривой рода  $g > 1$  называется алгебраическая кривая, задаваемая уравнением вида

$$y^2 + h(x)y = f(x),$$

где  $f(x)$  — многочлен степени  $n = 2g + 1 > 4$  или с  $n = 2g + 2 > 4$  различными корнями и  $h(x)$  — многочлен степени  $< g + 2$ .

Для расширения множества чисел, для которых существует сведение, описанное в предыдущем пункте, в алгоритме Эдельмана-Хуана используется обобщённый алгоритм Гольдвассер-Килиана. Кроме того, вводится сведение нового типа: в нём эллиптические кривые заменяются на матрицы Якоби гиперэллиптических кривых второго рода. Тогда сведение нового типа вычисляется за вероятностно полиномиальное время следующим образом:

**Алгоритм:**

- 1) Случайным образом ищем многочлен  $f \in \mathbb{Z}/p\mathbb{Z}[x]$  степени 6, который не имеет кратных корней.
- 2) Считаем число  $n$  рациональных точек на матрице Якоби кривой, задаваемой уравнением  $y^2 = f(x)$
- 3) Находим такие  $s, t \in \mathbb{Z}/p\mathbb{Z}, t \neq 0$ , что точка  $\langle s, t \rangle$  лежит на кривой и  $v = \langle s, t \rangle - \langle s, -t \rangle$  (или, точнее,  $v = \phi(\langle s, t \rangle) - \phi(\langle s, -t \rangle)$ , где  $\phi$  — вложение кривой в группу матриц Якоби) удовлетворяет равенству  $n * v = 1$  в группе, ассоциированной с матрицами Якоби.

Получаем сведение доказательства простоты  $p$  к доказательству простоты  $n$ , которое, как и раньше, работает только если  $n$  — простое. В силу того, что  $n$  простое с высокой вероятностью, новый алгоритм является вероятностно полиномиальным.

С другой стороны, в силу гипотезы Римана для конечных полей  $n \approx p^2$ . Таким образом, алгоритм Эдельмана-Хуана обходит числа, для которых не выходит получить сведение с помощью обобщённого алгоритма Гольдвассер-Килиана, производя несколько итераций нового сведения. В силу почти случайного выбора  $n$  данный способ позволяет избежать чисел из плохого множества.

Для завершения построения алгоритма остаётся научиться быстро считать число рациональных точек на эллиптических кривых, алгоритм Шуфа [5] справляется с этой задачей за полиномиальное время. Получаем

**Теорема 4.1.** Существует  $c \in \mathbb{Z}_{\geq 0}$  и полиномиально вычислимая всюду всюду определённая функция  $F : \mathbb{Z}_{\geq 0}^2 \rightarrow \{0, 1\}$ , такая что

1.  $\forall n \in \mathbb{Z}_{\geq 0}$ , где  $n$  составное, и  $\forall r \in \mathbb{Z}_{\geq 0}$

$$F(n, r) = 0$$

2.  $\forall p \in \mathbb{Z}_{\geq 0}$ , где  $p$  простое,

$$\frac{\#\{r : |r| \leq |p|^e \text{ и } F(n, r) = 1\}}{\#\{r : |r| \leq |p|^e\}} \geq \frac{1}{2},$$

то есть проверка на простоту лежит в **RP**. Учитывая, что в секции 3 было показано, что эта задача лежит в **coRP**, получаем, что она лежит в **ZPP** = **RP**  $\cap$  **coRP**.

## 4.4 Сертификат

В данном случае сертификатом является последовательность чисел, к которым производится сведение доказательства простоты в процессе работы алгоритма, а для его проверки требуется лишь проверить корректность сведений и проверить полученное небольшое число на простоту делением на все числа в интервале  $[2, \sqrt{n}]$ , что делается за полином.

Наконец, рассмотрим наиболее эффективный на данный момент **RP** алгоритм проверки на простоту, алгоритм Аткина-Морейна.

## 5. Алгоритм ECPP

### 5.1 Описание

Алгоритм ECPP построен на идее сведений, аналогичной алгоритму Гольдвассер-Килиана, но для ускорения отказывается от использования неэффективного алгоритма Шуфа для подсчёта числа рациональных точек на эллиптической кривой. Вместо этого с помощью комплексного умножения случайно генерируется кривая, число рациональных точек на которой легко подсчитать.

Сведения в алгоритме ECPP основаны на следующей теореме:

**Теорема 5.1.** Пусть  $N \in \mathbb{N}_+$ , и эллиптическая кривая  $E$  задаётся уравнением

$$y^2 = x^3 + ax + b \bmod N$$

Рассмотрим  $E$  над  $\mathbb{Z}/N\mathbb{Z}$ , используя обычный закон сложения и считая 0 нейтральным элементом на  $E$ .

Пусть  $m$  целое. Если существует простое число  $q$ , делящее  $m$  большее, чем  $(\sqrt[4]{N} + 1)^2$  и на  $E$  существует точка  $P$ , для которой выполнено

$$(1) \quad mP = 0$$

$$(2) \quad (m/q)P \text{ определено и не равно } 0,$$

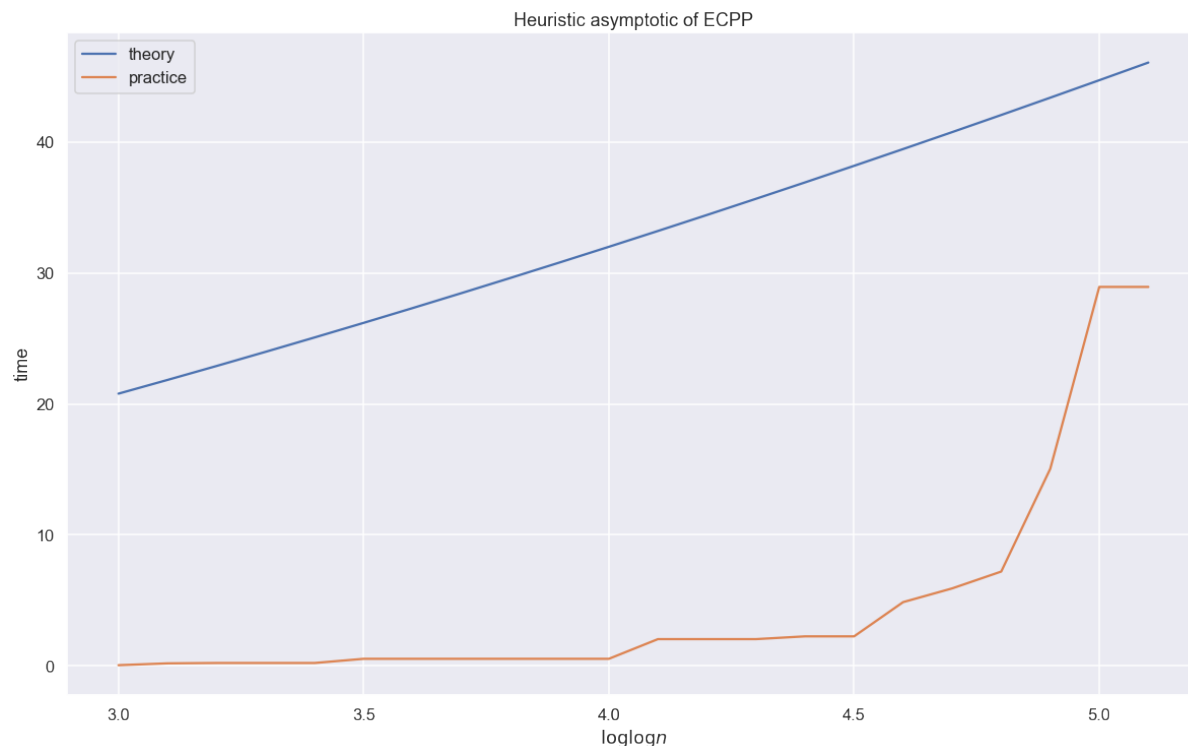
то  $N$  простое.

## 5.2 Сертификат

В силу того, что ЕСРР, также как и Гольдвассер-Килиан, производит цепочку сведений, он также создаёт сертификат, хоть и не является вероятностно полиномиальным

## 5.3 Время работы

Эвристическая (но не доказанная) асимптотика ЕСРР равна  $O(\log^4 n)$ . Продемонстрируем это, построив зависимость *time* от  $\log \log n$ :



## 6. Практика

На практике для проверки на простоту достаточно по очереди запускать алгоритм Миллера-Рабина и ЕСРР, пока один из них не выдаст ответ без ошибки. Чтобы получить вероятностно полиномиальный алгоритм, можно также параллельно запустить алгоритм Эдельмана-Хуана.

## 7. Список литературы

- [1] Д.В. Мусатов. “Сложность вычислений.”
- [2] Conrad, Keith. (2017). “The Miller – Rabin Test.”
- [3] Monier, Louis. (1980). "Evaluation and comparison of two efficient probabilistic primality testing algorithms." Theoretical Computer Science. 12. 97–108.

- [4] M. Adleman, Leonard & A. Huang, Ming-Deh. (1992). "Primality Testing and Abelian Varieties Over Finite Fields."10.1007/BFb0090185.
- [5] Schoof, René. "Counting points on elliptic curves over finite fields."Journal de théorie des nombres de Bordeaux 7.1 (1995): 219-254. <<http://eudml.org/doc/247664>>.
- [6] Atkin, A. O. L., & Morain, F. (1993). "Elliptic curves and primality proving."Mathematics of Computation, 61(203), 29–29. doi:10.1090/s0025-5718-1993-1199989-x