ЭЛЕМЕНТЫ ТЕОРИИ ЧИСЕЛ. Лекция 12

Первообразные корни по составным модулям. Индексы.

Механико-математический факультет МГУ
1 поток 1 курса, осень 2026 г.

• Пусть a – целое число, взаимно простое с модулем m.

Напомним, что наименьшее натуральное число d с условием $a^d \equiv 1 \pmod{m}$ называется показателем числа a по модулю m.

• Целое число a взаимно простое с модулем m называется первообразным корнем по модулю m, если его показатель равен $\varphi(m)$.

Теорема 26. Для каждого простого нечетного числа p существуют первообразные корни по модулю p.

Следствие 1. Для каждого простого нечетного p существует в точности $\varphi(p-1)$ первообразных корней по модулю p.

Доказательство.

Пусть g - какой-нибудь первообразный корень по модулю p. Тогда числа $g, g^2, \ldots, g^{p-1}$ составляют приведённую систему вычетов по модулю p.

Выберем какое-нибудь целое число $k, 1 \leq k \leq p-1$ взаимно простое с $p-1$ и обозначим буквой d показатель, которому принадлежит число g^k по модулю p. Так как d - наименьшее натуральное число с условием $g^{dk} \equiv 1 \pmod{p}$, то $d \leq p-1$. $\square$

Поскольку g - первообразный корень по модулю p и $g^{dk} \equiv 1 \pmod{p}$, то $(p-1)|dk$. Учитывая, что $(p-1,k)=1$, заключаем, что $(p-1)|d$ и, значит $d = p-1$. Следовательно, g^k - первообразный корень по модулю p и количество первообразных корней по модулю p не меньше $\varphi(p-1)$.

Если же выбранное число k не взаимно просто с $p-1$ имеем $(p-1,k) = r > 1$. И тогда $\left(g^k\right)^{\frac{p-1}{r}} = \left(g^{p-1}\right)^{\frac{k}{r}} \equiv 1 \pmod{p}$. Значит, g^k не есть первообразный корень по модулю p. Это завершает доказательство следствия.

Для практического нахождения первообразных корней удобно пользоваться следующим утверждением.

Лемма 1. Целое число c, не делящееся на простое нечетное p, будет первообразным корнем по модулю p в том и только том случае, когда для любого простого числа q, делящего $p-1$ выполняется

$$c^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}.$$

Доказательство. Обозначим буквой d показатель числа c по модулю p. Тогда $d|(p-1)$. Если $d < p-1$, то найдется такое простое число q, что $qd|(p-1)$ или $d|\frac{p-1}{q}$. Но тогда $c^{\frac{p-1}{q}} \equiv 1 \pmod{p}$, вопреки условию. Значит, $d = p-1$, и это завершает доказательство леммы.

Пример. Найти наименьший первообразный корень по модулю 23.

Справедливы сравнения по модулю 23

$$2^{11} = 2 \cdot (32)^2 \equiv 2 \cdot 9^2 \equiv 1, \qquad 3^{11} = 9 \cdot (27)^3 \equiv 9 \cdot 4^3 \equiv 1.$$

Из них следует, что числа $2, 3$ не являются первообразными корнями по модулю 23. Кроме того, $4^{11} = \left(2^{11}\right)^2 \equiv 1 \pmod{23}$, так что и 4 не является первообразным корнем по модулю 23. Далее

$$5^{11} = 5 \cdot 25^5 \equiv 5 \cdot 2^5 \equiv -1 \pmod{23}$$

и $5^2 \equiv 2 \pmod{23}$.

Существование первообразных корней по простому модулю

Применяя лемму **??** к простому числу $p = 23$ и $c = 5$, заключаем, что 5 есть первообразный корень по модулю 23, т.е. для каждого натурального числа b, не делящегося на 23, найдется целое k с условием $b \equiv 5^k \pmod{23}$. Другими словами класс вычетов $\overline{5}$ есть образующая в группе $(\mathbb{Z}/23\mathbb{Z})^*$. Количество первообразных корней по модулю 23 равно $\varphi(22) = \varphi(2)\varphi(11) = 10$.

Существование первообразных корней по простому модулю

Если известны все простые делители числа $p-1$, то проверка условий леммы **??** выполняется достаточно быстро с помощью быстрого алгоритма возведения в степень. Множество первообразных корней при заданном p достаточно велико, поэтому выбирая числа c случайным образом на промежутке $0 < c < p$, можно с большой вероятностью попасть на первообразный корень и доказать это с помощью леммы **??**.

Теорема 27. Пусть p – простое нечетное число и $\alpha \geq 1$ – целое. Тогда

1. По модулям p^α и $2p^\alpha$ существуют первообразные корни.

2. Пусть g – первообразный корень по модулю p. Если целое число g_1 удовлетворяет условиям

$$g_1 \equiv g \pmod{p}, \qquad p^2 \nmid g_1^{p-1} - 1, \tag{1}$$

то g_1 – первообразный корень по любому модулю вида p^α, где $\alpha \geq 1$. По крайней мере одно из чисел g или $g + p$ удовлетворяет условиям (**??**).

3. Если g_2 нечетно и $g_2 \equiv g_1 \pmod{p^\alpha}$, то g_2 – первообразный корень по любому модулю вида $2p^\alpha$, где $\alpha \geq 1$. Хотя бы одно из двух чисел g_1 и $g_1 + p^\alpha$ удовлетворяет указанным условиям.

Пример. Доказать, что 2 есть первообразный корень по модулям 37^α при любом целом $\alpha \geq 1$. Найти первообразные корни по модулям $2 \cdot 37^\alpha$.

Докажем сначала, что 2 есть первообразный корень по модулю 37.

Поскольку для $p = 37$ выполняется $p - 1 = 36 = 2^2 \cdot 3^2$, то в силу леммы **??** достаточно проверить, что $2^{18} \not\equiv 1 \pmod{37}$ и $2^{12} \not\equiv 1 \pmod{37}$. Имеем $2^6 = 64 \equiv -10 \pmod{37}$, поэтому

$$2^{12} \equiv (-10)^2 \equiv 26 \pmod{37}, \quad 2^{18} \equiv (-10)^3 \equiv -1 \pmod{37}.$$

Итак, 2 есть первообразный корень по модулю 37.

Предположим теперь, что

$$37^2 | (2^{36} - 1) = (2^{18} - 1)(2^{18} + 1).$$

Так как $2^{18} \equiv -1 \pmod{37}$, то $2^{18} - 1$ не делится на 37 и

$$37^2 | (2^{18} + 1) = (2^6 + 1)(2^{12} - 2^6 + 1).$$

Учитывая, что $2^6 + 1 = 65$ не делится на 37, заключаем, что

$$37^2 | (2^{12} - 2^6 + 1) = 4033 = 37 \cdot 109.$$

Получившееся противоречие означает, что $37^2 \nmid 2^{36} - 1$. Согласно теореме **??** можно утверждать теперь, что 2 есть первообразный корень по модулю 37^α при любом целом $\alpha \geq 2$. Так как $2 + 37 = 39$ нечетно, то согласно последнему утверждению теоремы **??** число 39 есть первообразный корень по любому модулю вида $2 \cdot 37^\alpha$ при целом $\alpha \geq 1$.

Первое утверждение теоремы следует из второго и третьего. Поэтому перейдем непосредственно к их доказательству. Если оба числа $(g+p)^{p-1}-1$ и $g^{p-1}-1$ делятся на p^2, то

$$p^2|(g+p)^{p-1}-g^{p-1}$$

и, раскрывая скобки в $(g+p)^{p-1}$ с помощью формулы Ньютона для бинома, находим

$$0 \equiv (g+p)^{p-1}-g^{p-1} \equiv (p-1)g^{p-2}p \pmod{p^2}.$$

Но тогда $p|(p-1)g^{p-2}$, что невозможно.

Итак, доказано, что по крайней мере одно из чисел $(g+p)^{p-1}-1$ и $g^{p-1}-1$ не делится на p^2, т.е. по крайней мере одно из двух чисел g и $g+p$ удовлетворяет условиям (**??**).

Пусть g_1 – произвольное число с условиями (**??**). Докажем, что при любом целом $\beta \geq 0$ выполняется равенство

$$\nu_p\left(g_1^{p^\beta(p-1)}-1\right)=\beta+1. \tag{2}$$

Воспользуемся для этого математической индукцией по β. При $\beta=0$ утверждение следует из условий теоремы (**??**).

Допустим теперь, что равенство (**??**) справедливо для некоторого $\beta \geq 0$ и докажем его для $\beta + 1$. Из (**??**) следует, что

$$g_1^{p^\beta (p-1)} = 1 + cp^{\beta+1}, \qquad p \nmid c.$$

Возводя это равенство в степень p, находим

$$\begin{aligned} g_1^{p^{\beta+1}(p-1)} &= \left(1 + cp^{\beta+1}\right)^p = \\ &= 1 + cp^{\beta+2} + (cp^{\beta+1})^p + \sum_{k=2}^{p-1} \binom{p}{k} (cp^{\beta+1})^k. \end{aligned}$$

Поскольку при $1 < k < p$ биномиальный коэффициент $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ делится на p и также выполняются неравенства $k(\beta+1)+1 \geq \beta+3$, $p(\beta+1) \geq \beta+3$, находим

$$g_1^{p^{\beta+1}(p-1)} \equiv 1 + cp^{\beta+2} \pmod{p^{\beta+3}}.$$

Из этого сравнения, поскольку $p \nmid c$ следует (**??**) для $\beta+1$.

Пусть теперь $\alpha \geq 2$ – некоторое целое число. Докажем, что g_1 есть первообразный корень по модулю p^α. Обозначим для этого буквой d показатель g_1 по модулю p^α.

Так как $g_1^d \equiv 1 \pmod{p^\alpha}$ и $g_1 \equiv g \pmod{p}$, то справедливо сравнение $g^d \equiv 1 \pmod{p}$. Поскольку g есть первообразный корень по модулю p, т.е. показатель g по модулю p равен $p-1$, заключаем, что $(p-1)|d$.

По теореме Эйлера выполняется сравнение $g_1^{\varphi(p^\alpha)} \equiv 1 \pmod{p^\alpha}$. Показатель g_1 по модулю p^α равен d, поэтому $d|\varphi(p^\alpha) = p^{\alpha-1}(p-1)$. Учитывая установленную ранее делимость $(p-1)|d$, находим, что $d = p^\beta(p-1)$ с некоторым целым β, удовлетворяющим неравенствам $0 \le \beta \le \alpha - 1$.

Согласно определению d должно выполняться

$$p^\alpha \Big| g_1^d - 1 = g_1^{p^\beta (p-1)} - 1.$$

В соответствии с равенством (**??**) отсюда следует, что $\alpha \leq \beta + 1$. Сравнивая это неравенство с доказанным ранее, получаем $\beta = \alpha - 1$ и $d = p^{\alpha-1}(p-1) = \varphi(p^\alpha)$. Таким образом, g_1 есть первообразный корень по модулю p^α.

Для доказательства третьего утверждения теоремы заметим, прежде всего, что оба числа g_1 и $g_1 + p^\alpha$ сравнимы с g_1 по модулю p^α, и в силу нечетности p^α, одно из них будет нечетным, т.е. удовлетворяет условиям, определяющим g_2.

Из сравнений $g_2 \equiv g_1 \pmod{p^\alpha}$ и $g_2 \equiv 1 \pmod{2}$ следует взаимная простота чисел g_2 и $2p^\alpha$. Обозначим буквой s показатель g_2 по модулю $2p^\alpha$. Так как $g_1^s \equiv g_2^s \equiv 1 \pmod{p^\alpha}$ и g_1 есть первообразный корень по модулю p^α, то $s \geq \varphi(p^\alpha) = \varphi(2p^\alpha)$. Теперь согласно теореме Эйлера можно утверждать, что $s = \varphi(2p^\alpha)$. Следовательно, g_2 есть первообразный корень по модулю $2p^\alpha$.

Построение первообразных корней по модулям p^k и $2p^k$

Заметим, что любой первообразный корень по модулю p^n, где $n \geq 2$ будет также и первообразным корнем по модулю p. Действительно, пусть b – первообразный корень по модулю p^n.

• Обозначив буквой d показатель числа b по модулю p. Для любого целого числа a, не делящегося на p, найдется целое число k, удовлетворяющее сравнению $a \equiv b^k \pmod{p^n}$ и тогда $a \equiv b^k \pmod{p}$.

• Пусть r - остаток от деления числа k на d. Тогда $a \equiv b^r \pmod{p}$, $0 \leq r < d$. И так как это справедливо для $a = 1, 2, \ldots, p-1$, то r должно принимать не менее $p-1$ различных значений. Следовательно $d \geq p-1$, что возможно лишь при $d = p-1$. Так доказывается, что b есть первообразный корень по модулю p.

§7.4 Теорема об отсутствии первообразных корней по модулям, отличным от 2, 4, p^k и $2p^k$

В двух предыдущих параграфах были рассмотрены примеры модулей $m = p^\alpha, m = 2p^\alpha$, для которых существуют первообразные корни и описан алгоритм их вычисления. При $m = 4$ первообразным корнем будет число 3. При $m = 2$ существует единственный класс вычетов, состоящий из чисел взаимно простых с 2, а именно, класс $\overline{1}$, состоящий из нечетных чисел. В этом случае первообразным корнем будет 1. В этом параграфе будет доказано, что указанными примерами исчерпываются все случаи существования первообразных корней.

Теорема 28. Пусть $\alpha \geq 3$ – нечетное целое число.

1. Каждое нечетное число a удовлетворяет сравнению

$$a^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}. \tag{3}$$

2. Показатель числа 5 по модулю 2^α равен $2^{\alpha-2}$.

3. Каждое нечетное число сравнимо по модулю 2^α с одним из чисел

$$\pm 5, \pm 5^2, \pm 5^3, \ldots, \pm 5^{2^{\alpha-2}}. \tag{4}$$

Теорема об отсутствии первообразных корней по модулям, отличным от 2, 4, p^k и $2p^k$

Эта теорема на языке теории групп может быть переформулирована как утверждение о том, что мультипликативная группа $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ равна прямому произведению своих циклических подгрупп, порожденных классами вычетов $\overline{-1}$ и $\overline{5}$.

Доказательство. Докажем сначала первое утверждение. При $\alpha = 3$ оно верно, так как для $a = 2b + 1$ выполняется $a^2 - 1 = 4b(b + 1)$, и одно из двух последовательных чисел $b, b + 1$ четно.

Так как a нечетно, то при любом целом $k \geq 0$ число $a^{2^k} + 1$ четно.

Из равенства

$$a^{2^{k+1}} - 1 = \left(a^{2^k} - 1\right)\left(a^{2^k} + 1\right), \tag{5}$$

следует теперь, что

$$\nu_2\left(a^{2^{k+1}} - 1\right) \geq \nu_2\left(a^{2^k} - 1\right) + 1.$$

Так как по доказанному $\nu_2(a^2 - 1) \geq 3$, заключаем отсюда по индукции, что

$$\nu_2(a^{2^k} - 1) \geq k + 2, \qquad k \geq 1.$$

Это неравенство при $k = \alpha - 2$ дает первое утверждение теоремы.

Так как $5 \equiv 1 \pmod 4$, то при любом целом $k \geq 0$ находим $5^{2^k} + 1 \equiv 2 \pmod 4$ и, значит, $\nu_2\left(5^{2^k} + 1\right) = 1$. Теперь из равенства (**??**) при $a = 5$ следует, что

$$\nu_2\left(5^{2^{k+1}} - 1\right) = \nu_2\left(5^{2^k} - 1\right) + 1.$$

Отсюда же, поскольку $\nu_2(5 - 1) = 2$, находим

$$\nu_2\left(5^{2^k} - 1\right) = k + 2, \qquad k \geq 0. \tag{6}$$

Теорема об отсутствии первообразных корней по модулям, отличным от 2, 4, p^k и $2p^k$

Пусть теперь $\alpha \geq 3$ – целое число. Обозначим буквой d показатель числа 5 по модулю 2^α.

Из первого утверждения теоремы следует, что $d|2^{\alpha-2}$, и, значит, $d = 2^\beta$, $\beta \leq \alpha - 2$.

Согласно определению d имеем $2^\alpha|5^{2^\beta} - 1$, откуда в силу (**??**) следует $\alpha \leq \beta + 2$. Таким образом, $\beta = \alpha - 2$ и $d = 2^{\alpha-2}$. Второе утверждение доказано.

Для доказательства третьего утверждения теоремы достаточно установить, что числа (**??**) составляют приведенную систему вычетов по модулю 2^α. Поскольку все эти числа нечетны, достаточно установить их попарную несравнимость по модулю 2^α.

Теорема об отсутствии первообразных корней по модулям, отличным от 2, 4, p^k и $2p^k$

Предположим, что $5^k \equiv -5^\ell \pmod{2^\alpha}, 1 \leq k, \ell \leq 2^{\alpha-2}$. Тогда $5^k \equiv -5^\ell \pmod 4$ и, значит, $1 \equiv -1 \pmod 4$, что неверно.

Итак, числа с разными знаками из набора (**??**) не сравнимы друг с другом по модулю 2^α.

Если предположить, что сравнимы какие-либо два числа (**??**) с одинаковыми знаками, имеем $5^k \equiv 5^\ell \pmod{2^\alpha}$, $1 \leq \ell < k \leq 2^{\alpha-2}$. Тогда $5^{k-\ell} \equiv 1 \pmod{2^\alpha}$, $0 < k - \ell < 2^{\alpha-2}$. Но это противоречит второму утверждению теоремы.

Теорема об отсутствии первообразных корней по модулям, отличным от 2, 4, p^k и $2p^k$

Теорема 29. Первообразные корни существуют лишь для модулей

$$2,\ 4,\ p^{\alpha},\ 2p^{\alpha}, \tag{7}$$

где p – простое нечетное и α – целое положительное числа.

Доказательство. Существование первообразных корней в случаях (**??**) доказано ранее.

Теорема об отсутствии первообразных корней по модулям, отличным от 2, 4, p^k и $2p^k$

Ниже будет показано, что если m отлично от чисел вида (**??**), то для любого целого a, взаимно простого с m, выполняется сравнение

$$a^{\frac{\varphi(m)}{2}} \equiv 1 \pmod{m}. \tag{8}$$

Это сравнение означает, что показатель каждого числа a с условием $(a, m) = 1$ меньше $\varphi(m)$, так что первообразных корней в этом случае не существует.

Теорема об отсутствии первообразных корней по модулям, отличным от 2, 4, p^k и $2p^k$

Итак, пусть $m = 2^\alpha \cdot p_1^{\alpha_1} \dots p_r^{\alpha_r}$ отлично от чисел вида (**??**).

Тогда возможны следующие три случая:

1) $r = 0, \alpha \geq 3$,

2) $r = 1, \alpha \geq 2$,

3) $r \geq 2$.

В каждом из них выполняется равенство

$$\varphi(m) = \varphi(2^\alpha) \cdot \varphi(p_1^{\alpha_1}) \cdots \varphi(p_r^{\alpha_r}). \tag{9}$$

В первом случае имеем $m = 2^\alpha, \alpha \geq 3$. Тогда сравнение (**??**) совпадает с (**??**), и уже доказано в теореме **??**.

Во втором и третьем случаях среди чисел

$$\varphi(2^\alpha), \quad \varphi(p_1^{\alpha_1}), \quad \ldots, \quad \varphi(p_r^{\alpha_r}) \tag{10}$$

найдется по крайней мере два чётных. Действительно, в третьем случае $r \geq 2$ и таким будет каждое из чисел $\varphi(p_i^{\alpha_i})$, $i = 1, \ldots, r$. Во втором же случае, т.е. при $r = 1$, выполняется неравенство $\alpha \geq 2$, так что чётным помимо $\varphi(p_1^{\alpha_1})$ будет и $\varphi(2^\alpha)$.

Теорема об отсутствии первообразных корней по модулям, отличным от 2, 4, p^k и $2p^k$

В каждом из двух последних случаев $\varphi(m)$ делится не только на $\varphi(2^\alpha)$ или на какое-нибудь $\varphi(p_i^{\alpha_i})$ при $i \geq 1$, но ещё и на 2. Поэтому

$$2\varphi(2^\alpha)\Big|\varphi(m), \quad 2\varphi(p_1^{\alpha_1})\Big|\varphi(m), \quad \ldots, \quad 2\varphi(p_r^{\alpha_r})\Big|\varphi(m).$$

и $\frac{\varphi(m)}{2}$ делится на каждое из чисел $\varphi(2^\alpha)$, $\varphi(p_i^{\alpha_i})$, $1 \leq i \leq r$. Следовательно

$$a^{\frac{\varphi(m)}{2}} \equiv 1 \pmod{2^\alpha}, \qquad a^{\frac{\varphi(m)}{2}} \equiv 1 \pmod{p_i^{\alpha_i}}, \quad i = 1, \ldots, r.$$

Итак

$$a^{\frac{\varphi(m)}{2}} \equiv 1 \pmod{2^\alpha}, \qquad a^{\frac{\varphi(m)}{2}} \equiv 1 \pmod{p_i^{\alpha_i}}, \quad i = 1, \ldots, r.$$

Из этих сравнений, поскольку все числа 2^α, $p_i^{\alpha_i}$, $1 \le i \le r$, попарно взаимно просты, следует, что разность $a^{\frac{\varphi(m)}{2}} - 1$ делится на их произведение, т.е. делится на число m. Сравнение (**??**) доказано во всех случаях.

Оно, как указывалось раньше, означает, что показатель по модулю m каждого числа a взаимно простого с m не превосходит $\frac{\varphi(m)}{2}$ и значит меньше $\varphi(m)$. Поэтому первообразных корней по модулю m не существует.

Будем далее рассматривать случаи, когда $m = p^k$ или $m = 2p^k$, где p – простое нечетное число и $k \geq 1$, в которых, по доказанному, существует первообразный корень.

Пусть g – первообразный корень по модулю m. Тогда для любого целого взаимно простого с m числа a существует единственное целое γ, удовлетворяющее условиям

$$a \equiv g^{\gamma} \pmod{m}, \qquad 0 \leq \gamma < \varphi(m).$$

Это число γ называется *индексом числа* a по модулю m при основании g и обозначается символом $\operatorname{ind}_g a$ или $\operatorname{ind} a$, если указание на первообразный корень, относительно которого определяется индекс, не существенно.

Итак, имеем

$$a \equiv g^{\operatorname{ind}_g a} \pmod{m}, \qquad 0 \leq \operatorname{ind}_g a < \varphi(m). \tag{11}$$

Свойства индексов описывает следующая лемма.

Лемма 2. Пусть $m = p^k$ или $m = 2p^k$. Тогда

1) $\operatorname{ind}_g ab \equiv \operatorname{ind}_g a + \operatorname{ind}_g b \pmod{\varphi(m)}$;

2) если a, b – первообразные корни по модулю m, то для любого числа c взаимно простого с m выполняется сравнение

$$\operatorname{ind}_b c \equiv \operatorname{ind}_a c \cdot \operatorname{ind}_b a \pmod{\varphi(m)},$$

причем $(\operatorname{ind}_b a, \varphi(m)) = 1$.

Доказательство. Справедливы сравнения

$$g^{\operatorname{ind}_g ab} \equiv ab \equiv g^{\operatorname{ind}_g a} \cdot g^{\operatorname{ind}_g b} = g^{\operatorname{ind}_g a + \operatorname{ind}_g b} \pmod{m}$$

из которых, так как g – первообразный корень по модулю m, получаем первое утверждение леммы, см. следствие, доказанное на прошлой лекции.
С помощью (**??**) находим

$$b^{\operatorname{ind}_a c \cdot \operatorname{ind}_b a} = \left(b^{\operatorname{ind}_b a}\right)^{\operatorname{ind}_a c} \equiv a^{\operatorname{ind}_a c} \equiv c \equiv b^{\operatorname{ind}_b c} \pmod{m}.$$

Как и в доказательстве первого утверждения леммы, находим

$$\varphi(m) | (\operatorname{ind}_a c \cdot \operatorname{ind}_b a - \operatorname{ind}_b c).$$

Это доказывает сравнение из второго утверждения леммы **??**.

Обозначим $d = (\operatorname{ind}_b a, \varphi(m))$. Справедливы сравнения по модулю m

$$a^{\frac{\varphi(m)}{d}} \equiv b^{\frac{\varphi(m)}{d} \cdot \operatorname{ind}_b a} = \left(b^{\varphi(m)}\right)^{\frac{\operatorname{ind}_b a}{d}} \equiv 1 \pmod{m}.$$

Так как a первообразный корень по модулю m, это сравнение возможно лишь в случае $d = 1$.