# Вероятностный алгоритм проверки чисел на простоту

А.М. Миронов

## 1 Необходимые сведения из теории групп

### 1.1 Определение группы

**Группой** называется множество $G$, на котором задана бинарная операция, т.е. правило, сопоставляющее каждой паре $a, b$ элементов $G$ некоторый элемент $ab \in G$, называемый **произведением** элементов $a$ и $b$, причём выполнены следующие условия:

1. операция **ассоциативна**, т.е. для всех $a, b, c \in G$
$$a(bc) = (ab)c$$
2. существует элемент $e \in G$ (называемый **нейтральным элементом**), такой, что для всех $a \in G$
$$ae = ea = a$$
3. для каждого $a \in G$ существует элемент $a^{-1} \in G$, называемый **обратным к** $a$, такой, что
$$aa^{-1} = a^{-1}a = e$$

Группа $G$ называется **коммутативной** (или **абелевой**) если для всех $a, b \in G \quad ab = ba$.

В группах имеют место **законы сокращения**:

- если $ab = ac$, то $b = c$, и
- если $ba = ca$, то $b = c$.

Действительно, если $ab = ac$, то, умножая обе части данного равенства слева на $a^{-1}$, получаем:

$$a^{-1}(ab) = a^{-1}(ac)$$

что по свойству ассоциативности равносильно равенству $(a^{-1}a)b = (a^{-1}a)c$, или $eb = ec$, или $b = c$. Аналогично доказывается другой закон сокращения.

**Подгруппой** группы $G$ называется произвольное непустое подмножество $H \subseteq G$, удовлетворяющее следующим условиям:

1. для всех $a, b \in H \quad ab \in H$
2. для каждого $a \in H \quad a^{-1} \in H$.

В частности, $e \in H$, т.к., беря произвольный элемент $a \in H$, на основании приведённых выше условий получаем: $aa^{-1} = e \in H$.

### 1.2 Смежные классы

Пусть заданы некоторая группа $G$ некоторая её подгруппа $H$.

**Смежным классом** по подгруппе $H$ называется подмножество группы $G$, состоящее из произведений вида $gh$, где $g$ – некоторый фиксированный элемент группы $G$, и $h$ – произвольный элемент подгруппы $H$. Данное множество обозначается символом $gH$.

Очевидно, что $g \in gH$ поскольку $e \in H$.

Если подгруппа $H$ состоит из конечного числа элементов, и список всех различных элементов $H$ имеет вид $h_1, \ldots, h_k$, то все элементы смежного класса $gH$ содержатся в списке

$$gh_1 \ \ldots \ gh_k \tag{1}$$

Все элементы списка (1) различны т.к. из $gh_i = gh_j$ по закону сокращения следует, что $h_i = h_j$.

Следовательно,

$$|gH| = |H| \tag{2}$$

Пусть $g_1$ и $g_2$ – произвольные элементы группы $G$. Докажем, что смежные классы $g_1H$ и $g_2H$ обладают следующим свойством: либо

$$g_1H \cap g_2H = \emptyset \tag{3}$$

либо

$$g_1H = g_2H \tag{4}$$

Если неверно (3), то существует элемент $a$, принадлежащий обоим классам, т.е.

- $a \in g_1H$, т.е. $a = g_1h_1$ для некоторого $h_1 \in H$, и
- $a \in g_2H$, т.е. $a = g_2h_2$ для некоторого $h_2 \in H$.

Таким образом, $a = g_1h_1 = g_2h_2$. Умножая равенство $g_1h_1 = g_2h_2$ справа на $h_1^{-1}$, получаем:

$$g_1 = g_2h_2h_1^{-1} \tag{5}$$

Произвольный элемент класса $g_1H$ имеет вид $g_1h$ для некоторого $h \in H$. Согласно (5), элемент $g_1h$ равен произведению

$$g_2h_2h_1^{-1}h \tag{6}$$

т.е. элемент $g_1h$ принадлежит $g_2H$.

Мы доказали включение $g_1H \subseteq g_2H$. Аналогично доказывается обратное включение. Таким образом, мы доказали, что если неверно (3), то имеет место (4).

## 1.3 Теорема Лагранжа

Пусть группа $G$ состоит из конечного числа элементов, и список всех её элементов имеет вид

$$g_1 \ \dots \ g_n \tag{7}$$

Пусть $H$ – произвольная подгруппа группы $G$.

Рассмотрим список всех смежных классов по $H$:

$$g_1H \ \dots \ g_nH \tag{8}$$

Очевидно, что объединение всех множеств из списка (8) совпадает с $G$, т.к. каждый элемент $g_i$ из списка (7) принадлежит смежному классу $g_iH$.

Возможно, что некоторые смежные классы из списка (8) совпадают. В этом случае мы удалим из списка (8) лишние копии смежных классов, т.е. если

$$g_iH = g_jH$$

при $i \neq j$, то один из данных смежных классов мы удаляем, и поступаем так до тех пор, пока все из оставшихся смежных классов не станут различными (т.е. среди них не будет двух совпадающих).

Пусть список оставшихся смежных классов имеет вид

$$g_{i_1}H \ \dots \ g_{i_m}H \tag{9}$$

Очевидно, что

- объединение смежных классов из списка (9) по прежнему совпадает с $G$, и,
- как было установлено выше, все смежные классы из списка (9) попарно не пересекаются.

Следовательно,

$$|G| = |g_{i_1}H| \ + \ \dots \ + \ |g_{i_m}H| \tag{10}$$

Из (10) и (2) следует, что

$$|G| = \underbrace{|H| \ + \ \dots \ + \ |H|}_{m \text{ слагаемых}} = m|H|$$

Мы доказали **теорему Лагранжа**, которая утверждает, что

если $G$ – конечная группа, и $H$ – её подгруппа,
то $|G|$ делится на $|H|$

## 1.4 Циклические подгруппы

Пусть $G$ – конечная группа, и $g$ – элемент $G$, отличный от $e$.

Рассмотрим список элементов $G$ следующего вида:

$$g^0, \ g^1, \ g^2, \ g^3, \ g^4, \ \dots \tag{11}$$

где

$$g^0 \stackrel{\text{def}}{=} e$$

$$g^1 \stackrel{\text{def}}{=} g$$

$$g^2 \stackrel{\text{def}}{=} gg$$

$$\dots$$

$$g^k \stackrel{\text{def}}{=} \underbrace{gg\dots g}_{k \text{ множителей}}$$

Поскольку в группе $G$ число элементов конечно, то список (11) не может быть бесконечным, и, следовательно, некоторые его элементы совпадают, т.е. существуют различные числа $i, j$, такие, что

$$g^i = g^j \tag{12}$$

Пусть например $i < j$.

Из (12) следует, что

$$g^{j-i} = e$$

Пусть $k$ – наименьшее положительное целое число, удовлетворяющее условию

$$g^k = e$$

Очевидно, что совокупность элементов

$$e, \ g, \ g^2, \ \dots, \ g^{k-1} \tag{13}$$

является подгруппой группы $G$.

Подгруппа (13) обозначается символом $\langle g \rangle$ и называется **циклической подгруппой**, порождённой элементом $g$.

Поскольку число элементов в (13) равно $k$, то по теореме Лагранжа

$$|G| = km$$

для некоторого целого числа $m$.

Поскольку $g^k = e$, то

$$g^{|G|} = g^{km} = (g^k)^m = e^m = e$$

Таким образом, мы доказали, что

для любого элемента $g$ конечной группы $G$
имеет место соотношение $g^{|G|} = e$ (14)

## 1.5 Гомоморфизмы групп

Пусть задана пара групп $G_1, G_2$.

**Гомоморфизм из $G_1$ в $G_2$** – это произвольное отображение $f$ вида

$$G_1 \xrightarrow{\ f\ } G_2 \tag{15}$$

такое, что для всех $a, b \in G_1$

$$f(ab) = f(a)f(b)$$

Пусть $e_1$ и $e_2$ – нейтральные элементы групп $G_1$ и $G_2$ соответственно.

Докажем, что

$$f(e_1) = e_2$$

Действительно, в любой группе нейтральный элемент - это единственный элемент $a$, обладающий свойством

$$a = aa$$

и, поскольку

$$e_1 = e_1 e_1$$

то

$$f(e_1) = f(e_1)f(e_1)$$

и, следовательно, $f(e_1)$ является нейтральным элементом $G_2$.

**Ядро** гомоморфизма $f$ – это подмножество $Ker(f)$ группы $G_1$, определяемое следующим образом:

$$Ker(f) \stackrel{\text{def}}{=} \{a \in G_1 \mid f(a) = e_2\} \tag{16}$$

Нетрудно доказать, что $Ker(f)$ является подгруппой $G_1$.

**Образ** гомоморфизма $f$ – это подмножество $Im(f)$ группы $G_2$, определяемое следующим образом:

$$Im(f) \stackrel{\text{def}}{=} \{b \in G_2 \mid b = f(a) \text{ для некоторого } a \in G_1\}$$

Нетрудно доказать, что $Im(f)$ является подгруппой $G_2$.

Пусть группа $G_1$ конечна, и список всех различных смежных классов группы $G_1$ по подгруппе $Ker(f)$ имеет вид

$$g_1Ker(f) \quad g_2Ker(f) \quad \ldots \quad g_mKer(f) \tag{17}$$

где $g_1, \ldots, g_m$ – некоторые элементы группы $G_1$.

Заметим, что для каждого $i \in \{1, \ldots, m\}$ все элементы смежного класса

$$g_iKer(f) \tag{18}$$

переходят при отображении $f$ в один и тот же элемент группы $G_2$, т.к. произвольный элемент смежного класса (18) имеет вид $g_ih$ для некоторого $h \in Ker(f)$, и, следовательно,

$$f(g_ih) = f(g_i)f(h) = f(g_i)e_2 = f(g_i)$$

В частности, поскольку каждый элемент из $G_1$ попадает в один из классов в списке (17), то все элементы $Im(f)$ содержатся в списке

$$f(g_1) \quad f(g_2) \quad \ldots \quad f(g_m) \tag{19}$$

Заметим, что все элементы в списке (19) различны, поскольку если

$$f(g_i) = f(g_j)$$

для некоторой пары различных индексов $i, j$, то

$$f(g_i^{-1}g_i) = f(g_i^{-1})f(g_i) = f(g_i^{-1})f(g_j) = f(g_i^{-1}g_j) \tag{20}$$

Но левая часть в цепочне равенств (20) равна элементу

$$f(e_1)$$

который, как было установлено выше, совпадает с $e_2$. Таким образом,

$$f(g_i^{-1}g_j) = e_2$$

т.е.

$$g_i^{-1}g_j = h \in Ker(f)$$

т.е.

$$g_j = g_ih \quad \text{где} \quad h \in Ker(f)$$

т.е. смежные классы

$$g_jKer(f) \quad \text{и} \quad g_iKer(f)$$

имеют непустое пересечение, и, следовательно, совпадают, что невозможно, т.е. все смежные классы в списке (17) по предположению различны.

Таким образом

$$|Im(f)| \;=\; m \tag{21}$$

где $m$ есть количество различных смежных классов по $Ker(f)$.

Из (21) и из теоремы Лагранжа следует, что

$$|G_1| = |Ker(f)| \cdot |Im(f)| \tag{22}$$

В частности, имеет место импликация (которая будет использоваться ниже)

$$|Im(f)| > 1 \quad \Rightarrow \quad |Ker(f)| \leq \frac{1}{2} \cdot |G_1| \tag{23}$$

Гомоморфизм (15) называется **эпиморфизмом**, если отображение $f$ является сюръективным, т.е. если

$$Im(f) = G_2$$

Из (22) следует, что если $f$ – эпиморфизм, то

$$|G_1| = |Ker(f)| \cdot |G_2| \tag{24}$$

Гомоморфизм (15) называется **изоморфизмом**, если отображение $f$ является взаимно-однозначным.

Если пара групп $G_1, G_2$ такова, что существует изоморфизм из $G_1$ в $G_2$, то мы будем считать группы $G_1$ и $G_2$ равными.

Наше желание считать изоморфные группы равными обосновывается тем, что при анализе алгебраических свойств группы природа её элементов не имеет никакого значения – важно лишь то, как на этих элементах действует операция произведения. Поскольку между изоморфными группами $G_1$ и $G_2$ можно установить взаимно-однозначное соответствие, при котором произведению произвольной пары $a, b$ элементов $G_1$ будет соответствовать произведение тех элементов $G_2$, которые соответствуют $a$ и $b$, то это означает, что операция произведения на $G_1$ и $G_2$ действует одинаково, и у нас нет никаких причин считать $G_1$ и $G_2$ разными с точки зрения их алгебраических свойств.

### 1.6 Прообразы элементов относительно гомоморфизмов

Пусть заданы

- пара групп $G_1, G_2$, и
- гомоморфизм $f$ из $G_1$ в $G_2$.

Для каждого $g \in G_2$ символ $f^{-1}(g)$ обозначает множество

$$f^{-1}(g) \stackrel{\text{def}}{=} \{a \in G_1 \mid f(a) = g\} \tag{25}$$

Из данного определения следует, что множество (25)

- либо является пустым,
- либо является некоторым смежным классом по подгруппе $Ker(f)$.

Ниже мы будем также использовать следующее обозначение: для каждого $g \in Im(f)$ символ

$$\overline{f^{-1}(g)}$$

обозначает множество, определяемое следующим образом:

$$\overline{f^{-1}(g)} \stackrel{\text{def}}{=} \{a \in G_1 \mid f(a) \neq g\} \tag{26}$$

### 1.7 Декартово произведение групп

Пусть задан конечный список групп вида

$$G_1, \ldots, G_n \tag{27}$$

**Декартовым произведением** групп из списка (27) называется группа, обозначаемая символом

$$G_1 \times \ldots \times G_n \tag{28}$$

элементами которой являются списки вида

$$(g_1, \ldots, g_n) \tag{29}$$

где $g_1 \in G_1, \ldots, g_n \in G_n$.

Операция произведения на (28) определяется покомпонентно:

$$(g_1, \ldots, g_n)(g'_1, \ldots, g'_n) \stackrel{\text{def}}{=} (g_1 g'_1, \ldots, g_n g'_n)$$

т.е. для каждого $i \in \{1, \ldots, n\}$ компоненты с индексом $i$ перемножаются согласно операции произведения в группе $G_i$.

Нейтральным элементом группы (28) является список

$$(e_1, \ldots, e_n)$$

где для каждого $i \in \{1, \ldots, n\}$ элемент $e_i$ является нейтральным элементом группы $G_i$.

Обратным элементом к произвольному элементу (29) группы (28) является список вида

$$(g_1^{-1}, \ldots, g_n^{-1})$$

где для каждого $i \in \{1, \ldots, n\}$ элемент $g_i^{-1}$ является обратным к $g_i$ в группе $G_i$.

## 2 Группы, связанные с целыми числами

### 2.1 Группа целых чисел и её подгруппы

Множество целых чисел $\mathbf{Z}$ с операцией сложения является группой. Нейтральным элементом этой группы является число 0, и для каждого $a \in \mathbf{Z}$ обратным к $a$ является число $-a$.

Нетрудно доказать, что для каждого целого числа $n > 0$ множество

$$n\mathbf{Z} \stackrel{\text{def}}{=} \{ni \mid i \in \mathbf{Z}\} \tag{30}$$

является подгруппой группы $\mathbf{Z}$.

Докажем, что любая подгруппа группы $\mathbf{Z}$ имеет вид (30).

Для этого сначала докажем **теорему о делении с остатком**, которая утверждает, что для произвольной пары

$$a, n$$

целых чисел, где $n > 0$, существуют единственная пара чисел

$$q, r$$

удовлетворяющих следующим условиям:

$$a = nq + r \tag{31}$$

$$0 \leq r < n \tag{32}$$

Числа из множества (30) разбивают множество $\mathbf{Z}$ на отрезки длины $n$: каждый отрезок имеет вид

$$[ni, n(i+1)] \qquad (i \in \mathbf{Z}) \tag{33}$$

Для произвольного числа $a$ существуют две возможности: либо

1. $a$ является концом одного из отрезков вида (33), либо
2. $a$ является внутренней точкой одного из отрезков вида (33).

В первом случае

$$a = nq \tag{34}$$

для некоторого $q \in \mathbf{Z}$, и мы полагаем $r$ равным 0, а во втором –

$$nq < a < n(q+1) \tag{35}$$

для некоторого $q \in \mathbf{Z}$, и мы полагаем $r$ равным разности

$$a - nq$$

Получаем, что в обоих случаях $r$ удовлетворяет равенству (31) и неравенству (32).

Если $q', r'$ – другая пара чисел, удовлетворяющих соотношениям

$$a = nq' + r' \tag{36}$$

$$0 \le r' < n \tag{37}$$

то из (31) и (36) следует, что

$$n(q' - q) = r - r' \tag{38}$$

Поэтому

- если $q' = q$, то $r' = r$, и
- если $q' \neq q$, то пусть например $q' > q$, тогда левая часть (38) удовлетворяет соотношению

  $$n(q' - q) \ge n$$

  а правая –

  $$r - r' < n$$

  т.к. $r - r'$ есть расстояние между точками $r$ и $r'$, которые обе лежат в отрезке $[0, n-1]$, и мы получили противоречие.

Таким образом, пара чисел $q, r$, удовлетворяющих условиям (31) и (32), определена однозначно.

Теперь можно доказать, что произвольная подгруппа $H$ группы $\mathbf{Z}$ имеет вид (30).

1. Если $H = \{0\}$, то $H = 0\mathbf{Z}$.
2. Если $H \neq \{0\}$, то $H$ содержит ненулевое число $a$.

   Следовательно, $H$ содержит положительное число, т.к. если $a < 0$, то $(-a) > 0$ и $(-a) \in H$.

   Определим $n$ как наименьшее положительное число, принадлежащее $H$.

   Очевидно, что

   $$n\mathbf{Z} \subseteq H \tag{39}$$

   Если

   $$n\mathbf{Z} \neq H \tag{40}$$

   то существует число $a \in H$, такое, что

   $$a \notin n\mathbf{Z}$$

   т.е. в разложении (31)

   $$r \neq 0 \tag{41}$$

   Т.к.

   $$r = a - nq = a + n \cdot (-q)$$

   то

   $$r \in H$$

   Но из (32) и из (41) следует, что $r$ – положительное число, принадлежащее $H$, которое меньше чем $n$.

   Это противоречит определению $n$.

   Таким образом, предположение (40) ошибочно, и из (39) следует, что

   $$H = n\mathbf{Z}$$

## 2.2 Представление наибольшего общего делителя

Пусть $a, b$ – некоторая пара целых чисел, отличных от нуля.

Рассмотрим множество

$$a\mathbf{Z} \ + \ b\mathbf{Z} \stackrel{\text{def}}{=} \{ai + bj \mid i, j \in \mathbf{Z}\} \tag{42}$$

Нетрудно проверить, что данное множество является подгруппой в $\mathbf{Z}$.

Следовательно, по доказанному в предыдущей секции, существует целое положительное число $d$, такое, что подгруппа (42) имеет вид

$$d\mathbf{Z} \tag{43}$$

Поскольку числа $a$ и $b$ принадлежат (42), то следовательно они принадлежат и (43), т.е.

$$a = d \cdot a_1 \quad \text{и} \quad b = d \cdot b_1$$

т.е. $d$ является делителем чисел $a$ и $b$.

Докажем, что $d$ является наибольшим общим делителем чисел $a$ и $b$.

Пусть $d'$ – какой-либо общий положительный делитель чисел $a$ и $b$, т.е.

$$a = d' \cdot a'_1 \quad \text{и} \quad b = d' \cdot b'_1 \tag{44}$$

Поскольку $d$ принадлежит множеству (43), то, следовательно, $d$ принадлежит множеству (42), т.е. $d$ имеет вид

$$d = ai + bj \tag{45}$$

для некоторых целых чисел $i, j$.

Подставим в (45) вместо чисел $a$ и $b$ их представления из (44), получим

$$d = d' \cdot a'_1 \cdot i + d' \cdot b'_1 \cdot j = d' \cdot k \tag{46}$$

где $k \stackrel{\text{def}}{=} a'_1 \cdot i + b'_1 \cdot j$.

Поскольку числа $d$ и $d'$ положительные, то число $k$ тоже положительное.

Следовательно,

$$d = d' \cdot k \ge d'$$

т.е. $d$ – наибольший общий делитель чисел $a$ и $b$.

В частности, если $a$ и $b$ – взаимно простые числа, то существуют такие целые числа $u$ и $v$, что

$$au + bv = 1 \tag{47}$$

Очевидно, что верно и обратное - если числа $a$ и $b$ таковы, что существуют целые числа $u$ и $v$, удовлетворяющие условию (47), то числа $a$ и $b$ взаимно просты.

## 2.3 Группа вычетов по модулю $n$

Пусть $n$ – некоторое положительное целое число.

Обозначим символом $\mathbf{Z}_n$ множество

$$\{0, 1, \ldots, n-1\}$$

Определим отображение

$$r_n : \mathbf{Z} \to \mathbf{Z}_n$$

следующим образом: для каждого $a \in \mathbf{Z}$ элемент $r_n(a)$ по определению равен тому единственному $r$, который (совместно с $q$) удовлетворяет условиям (31) и (32), т.е. для каждого $a \in \mathbf{Z}$

$$a = nq + r_n(a)$$

для некоторого целого числа $q$.

Докажем, что для всех $a, b \in \mathbf{Z}$

$$r_n(a+b) = r_n(r_n(a) + r_n(b)) \tag{48}$$

и

$$r_n(a \cdot b) = r_n(r_n(a) \cdot r_n(b)) \tag{49}$$

Из определения функции $r_n$ следуют равенства

$$a = n \cdot q_1 + r_n(a) \tag{50}$$

$$b = n \cdot q_2 + r_n(b) \tag{51}$$

$$a + b = n \cdot q_3 + r_n(a+b) \tag{52}$$

$$r_n(a) + r_n(b) = n \cdot q_4 + r_n(r_n(a) + r_n(b)) \tag{53}$$

$$a \cdot b = n \cdot q_5 + r_n(a \cdot b) \tag{54}$$

$$r_n(a) \cdot r_n(b) = n \cdot q_6 + r_n(r_n(a) \cdot r_n(b)) \tag{55}$$

Сложив (50), (51), (53), и сократив одинаковые слагаемые в обоих частях полученной суммы, получаем равенство

$$a + b = n \cdot q_1 + n \cdot q_2 + n \cdot q_4 + r_n(r_n(a) + r_n(b)) \tag{56}$$

т.е.

$$a + b = n \cdot q_7 + r_n(r_n(a) + r_n(b)) \tag{57}$$

Из (57) и (52) следует (48).

Далее, из (50) и (51) следует, что

$$(a - n \cdot q_1) \cdot (b - n \cdot q_2) = r_n(a) \cdot r_n(b) \tag{58}$$

т.е.

$$a \cdot b = n \cdot q_8 + r_n(a) \cdot r_n(b) \tag{59}$$

Сложив (59) с (55), и сократив одинаковое слагаемое в обоих частях полученной суммы, получаем равенство

$$a \cdot b = n \cdot q_9 + r_n(r_n(a) \cdot r_n(b)) \tag{60}$$

Из (60) и (54) следует (49).

Определим операции

$$\underset{n}{+} \quad \text{и} \quad \underset{n}{\cdot} \tag{61}$$

на множестве $\mathbf{Z}_n$ следующим образом: для всех $a, b$ из множества $\mathbf{Z}_n$

$$a \underset{n}{+} b \stackrel{\text{def}}{=} r_n(a+b), \quad a \underset{n}{\cdot} b \stackrel{\text{def}}{=} r_n(a \cdot b)$$

В новых обозначениях соотношения (48) и (49) выглядят следующим образом:

$$r_n(a+b) = r_n(a) \underset{n}{+} r_n(b) \tag{62}$$

и

$$r_n(a \cdot b) = r_n(a) \underset{n}{\cdot} r_n(b) \tag{63}$$

Из соотношений (62) и (63) нетрудно вывести, что

- операции (61) ассоциативны и коммутативны, и
- операция "$\underset{n}{\cdot}$" дистрибутивна относительно операции "$\underset{n}{+}$".

Докажем например, что операция "$\underset{n}{+}$" ассоциативна, т.е. для всех $a, b, c$ из множества $\mathbf{Z}_n$ имеет место равенство

$$a \underset{n}{+} (b \underset{n}{+} c) = (a \underset{n}{+} b) \underset{n}{+} c$$

Т.к.

$$a = r_n(a), \quad b = r_n(b), \quad c = r_n(c)$$

то

$$\begin{aligned}
& a \underset{n}{+} (b \underset{n}{+} c) = \\
= \; & r_n(a) \underset{n}{+} (r_n(b) \underset{n}{+} r_n(c)) = \\
= \; & r_n(a) \underset{n}{+} r_n(b+c) = \\
= \; & r_n(a + (b+c)) = \\
= \; & r_n((a+b) + c) = \\
= \; & r_n(a+b) \underset{n}{+} r_n(c) = \\
= \; & (r_n(a) \underset{n}{+} r_n(b)) \underset{n}{+} r_n(c) = \\
= \; & (a \underset{n}{+} b) \underset{n}{+} c
\end{aligned}$$

Другие упомянутые выше свойства операций (61) доказываются аналогично.

Ниже мы будем называть операции (61) соответственно сложением и умножением по модулю $n$ (или просто сложением и умножением), и для каждой пары $a, b \in \mathbf{Z}_n$ мы будем обозначать элементы

$$a \underset{n}{+} b \quad \text{и} \quad a \underset{n}{\cdot} b$$

знакосочетаниями

$$a + b \quad \text{и} \quad ab$$

соответственно.

Кроме того, для произвольных целых чисел $a, b$ знакосочетание

$$a \underset{n}{=} b$$

означает, что

$$r_n(a) = r_n(b)$$

Из вышесказанного вытекает, что

- операция сложения на множестве $\mathbf{Z}_n$ является ассоциативной
- число 0 является нейтральным элементом относительно операции сложения, и
- для каждого $a \in \mathbf{Z}_n$ число

$$r_n(-a) = \begin{cases} n-a, & \text{если } a > 0 \\ 0, & \text{если } a = 0 \end{cases}$$

является обратным к $a$ относительно операции сложения.

Таким образом, множество $\mathbf{Z}_n$ является группой относительно операции сложения.

Данная группа называется **группой вычетов по модулю** $n$.

## 2.4 Мультипликативная группа в $\mathbf{Z}_n$

Как было отмечено выше, операция умножения на множестве $\mathbf{Z}_n$ тоже является ассоциативной, и нетрудно доказать, что число 1 является нейтральным элементом относительно операции умножения.

Однако множество $\mathbf{Z}_n$ не является группой относительно операции умножения, т.к. не для каждого элемента $a \in \mathbf{Z}_n$ существует обратный элемент относительно операции умножения (например, для числа 0 не существет обратного относительно умножения).

Тем не менее, в $\mathbf{Z}_n$ существует подмножество, которое является группой относительно операции умножения.

Данное подмножество обозначается символом

$$\mathbf{Z}_n^*$$

Множество $\mathbf{Z}_n^*$ состоит из всех элементов $\mathbf{Z}_n$, которые взаимно просты с $n$.

Из рассуждений в конце в пункта 2.2 вытекает, что число $a \in \mathbf{Z}_n$ является взаимно простым с $n$ тогда и только тогда, когда существуют целые числа $u$ и $v$, такие, что

$$a \cdot u + n \cdot v = 1 \tag{64}$$

Применяя $r_n$ к обеим частям (64), и учитывая, что

$$r_n(a) = a, \quad r_n(n) = 0, \quad r_n(1) = 1$$

получаем, что в $\mathbf{Z}_n$ имеет место равенство

$$a \cdot r_n(u) = 1 \tag{65}$$

т.е. если элемент $a$ принадлежит подмножеству $\mathbf{Z}_n^*$, то к нему существует обратный элемент относительно операции умножения.

Нетрудно доказать, что верно и обратное: если к элементу $a \in \mathbf{Z}_n$ существует обратный относительно операции умножения, то $a$ является взаимно простым с $n$.

Таким образом,

- для каждой пары $a, b$ элементов $\mathbf{Z}_n^*$ их произведение

$$ab$$

тоже принадлежит $\mathbf{Z}_n^*$

- операция умножения на множестве $\mathbf{Z}_n^*$ ассоциативна
- число 1 принадлежит $\mathbf{Z}_n^*$ и является нейтральным элементом относительно операции умножения
- для каждого элемента $a \in \mathbf{Z}_n^*$ существует элемент $a^{-1} \in \mathbf{Z}_n^*$, такой, что

$$aa^{-1} = a^{-1}a = 1$$

т.е. $\mathbf{Z}_n^*$ является группой относительно операции умножения.

Эта группа называется **мультипликативной группой в** $\mathbf{Z}_n$.

## 2.5 Малая теорема Ферма

Пусть число $n$ является простым.

В этом случае

$$\mathbf{Z}_n^* = \{1, \ldots, n-1\} \tag{66}$$

В частности,

$$|\mathbf{Z}_n^*| = n - 1 \tag{67}$$

Из (14) следует, что для любого $a$ из множества (67) имеет место соотношение

$$a^{n-1} \underset{n}{=} 1 \tag{68}$$

Данное утверждение называется **малой теоремой Ферма**.

## 2.6 Разложение группы $\mathbf{Z}_n$ в декартово произведение

Пусть число $n$ являетя произведением вида

$$n = uv \tag{69}$$

где числа $u$ и $v$ взаимно просты.

Докажем, что в этом случае имеет место равенство

$$\mathbf{Z}_n = \mathbf{Z}_u \times \mathbf{Z}_v$$

Определим отображение

$$\mathbf{Z}_n \xrightarrow{f} \mathbf{Z}_u \times \mathbf{Z}_v \tag{70}$$

следующим образом: для каждого $a \in \mathbf{Z}_n$

$$f(a) \stackrel{\text{def}}{=} (r_u(a), r_v(a))$$

Докажем, что (70) является изоморфизмом, т.е.

- (70) является взаимно однозначным, и

- (70) сохраняет операцию сложения.

Из (69) следует, что количество элементов в множестве $\mathbf{Z}_n$ равно количеству элементов в множестве $\mathbf{Z}_u \times \mathbf{Z}_v$.

Поэтому для того, чтобы доказать взаимную однозначность отображения (70), достаточно доказать, что отображение (70) является инъективным, т.е. для всех $a, b \in \mathbf{Z}_n$ из

$$f(a) = f(b) \tag{71}$$

следует, что

$$a = b \tag{72}$$

Пусть верно (71), т.е.

$$r_u(a) = r_u(b) \tag{73}$$

и

$$r_v(a) = r_v(b) \tag{74}$$

(73) эквивалентно тому, что существует число $q_1$, такое, что

$$a - b = u \cdot q_1 \tag{75}$$

и (74) эквивалентно тому, что существует число $q_2$, такое, что

$$a - b = v \cdot q_2 \tag{76}$$

Из (75) и (76) следует, что

$$u \cdot q_1 = v \cdot q_2 \tag{77}$$

Поскольку $u$ и $v$ взаимно просты, то существуют такие целые числа $i$ и $j$, что

$$u \cdot i + v \cdot j = 1 \tag{78}$$

Из (78) следует, что

$$u \cdot i \cdot q_1 + v \cdot j \cdot q_1 = q_1 \tag{79}$$

Из (77) и (79) следует, что

$$v \cdot q_2 \cdot i + v \cdot j \cdot q_1 = q_1 \tag{80}$$

т.е.

$$v \cdot q_3 = q_1 \tag{81}$$

для некоторого целого $q_3$.

Из (75) и (81) следует, что

$$a - b = u \cdot v \cdot q_3 \tag{82}$$

т.е.

$$a - b = n \cdot q_3 \tag{83}$$

Поскольку $a$ и $b$ являются элементами $\mathbf{Z}_n$, то, следовательно, равенство (83) возможно только в том случае, когда

$$q_3 = 0$$

т.е. только тогда, когда $a$ и $b$ совпадают.

Теперь докажем, что (70) сохраняет операцию сложения, т.е. для всех $a, b \in \mathbf{Z}_n$

$$f(a \underset{n}{+} b) = f(a) + f(b)$$

т.е.

$$(r_u(a \underset{n}{+} b), r_v(a \underset{n}{+} b)) = (r_u(a), r_v(a)) + (r_u(b), r_v(b))$$

т.е.

$$(r_u(a \underset{n}{+} b), r_v(a \underset{n}{+} b)) = (r_u(a) \underset{u}{+} r_u(b), r_v(a) \underset{v}{+} r_v(b))$$

т.е.

$$r_u(a \underset{n}{+} b) = r_u(a) \underset{u}{+} r_u(b) \tag{84}$$

и

$$r_v(a \underset{n}{+} b) = r_v(a) \underset{v}{+} r_v(b) \tag{85}$$

Доказательства истинности равенств (84) и (85) аналогичны, поэтому мы обоснуем лишь равенство (84).

Из (62) следует, что правая часть (84) равна

$$r_u(a + b)$$

т.е. (84) эквивалентно равенству

$$r_u(a \underset{n}{+} b) = r_u(a + b) \tag{86}$$

Имеют место равенства

$$a + b = n \cdot q_1 + (a \underset{n}{+} b) \tag{87}$$

и

$$(a \underset{n}{+} b) = u \cdot q_2 + r_u(a \underset{n}{+} b) \tag{88}$$

где $q_1$ и $q_2$ – некоторые целые числа.

Складывая данные равенства почленно, и учитывая (69) получаем равенство

$$a + b = u \cdot (v \cdot q_1 + q_2) + r_u(a \underset{n}{+} b) \tag{89}$$

Из (89) вытекает желаемое равенство (86).

Заметим, что аналогичным образом можно доказать, что (70) сохраняет также и операцию умножения, где умножение на $\mathbf{Z}_u \times \mathbf{Z}_v$ определяется покомпонентно:

$$(a, b) \cdot (a', b') \stackrel{\text{def}}{=} (a \underset{u}{\cdot} a', b \underset{v}{\cdot} b')$$

Нетрудно доказать, что

- пара $(1, 1)$ является нейтральным элементом относительно операции умножения на $\mathbf{Z}_u \times \mathbf{Z}_v$
- к элементу $(a, b) \in \mathbf{Z}_u \times \mathbf{Z}_v$ существует обратный элемент относительно данной операции умножения тогда и только тогда, когда

$$a \in \mathbf{Z}_u^* \quad \text{и} \quad b \in \mathbf{Z}_v^*$$

- для каждого $a \in \mathbf{Z}_n^*$

– элемент $a$ обладает обратным по умножению (в $\mathbf{Z}_n^*$) тогда и только тогда, когда

– его образ $f(a)$ обладает обратным по умножению (в $\mathbf{Z}_u \times \mathbf{Z}_v$)

Из сказанного выше следует, что совокупность элементов

$$\{f(a) \mid a \in \mathbf{Z}_n^*\}$$

совпадает с совокупностью

$$\mathbf{Z}_u^* \times \mathbf{Z}_v^*$$

и сужение отображения $f$ на подмножество $\mathbf{Z}_n^*$ является изоморфизмом из группы $\mathbf{Z}_n^*$ в группу $\mathbf{Z}_u^* \times \mathbf{Z}_v^*$ (относительно операции умножения).

Таким образом, в том случае, когда $n$ является произведением двух взаимно простых чисел $u$ и $v$, имеют место равенства

$$\mathbf{Z}_n = \mathbf{Z}_u \times \mathbf{Z}_v \tag{90}$$

и

$$\mathbf{Z}_n^* = \mathbf{Z}_u^* \times \mathbf{Z}_v^* \tag{91}$$

# 3 Вероятностный алгоритм проверки числа на простоту

Одним из приложений изложенных выше понятий и результатов является построение и анализ вероятностных алгоритмов.

Пусть задано некоторое целое число $n \geq 2$.

Требуется определить, является ли $n$ простым числом.

Для решения этой задачи предлагается нижеследующий алгоритм.

В данном алгоритме

- все числа интерпретируются как соответствующие им элементы $\mathbf{Z}_n$ (в частности, символ "$-1$", рассматриваемый, как элемент $\mathbf{Z}_n$, обозначает число $n-1$), и
- все операции понимаются как соответствующие операции в $\mathbf{Z}_n$.

## 3.1 Описание алгоритма

Алгоритм состоит из последовательного выполнения излагаемых ниже шагов.

Если на каком-либо шаге алгоритм определил, что $n$ – составное, то после этого он сразу заканчивает работу, в противном случае происходит переход к следующему шагу.

1. Если $n$ – чётное, то $n$ – составное.
2. Если $n$ имеет вид $m^i$ для некоторых целых $m \geq 2$ и $i \geq 2$, то $n$ – составное.
3. Представим число $n-1$ в виде
$$2^k \cdot l$$
где $l$ – нечётное число.
4. Выберем случайным образом число $a$ из множества
$$\{1, \ldots, n-1\} \tag{92}$$
5. Вычислим следующие числа
$$b_0 \stackrel{\text{def}}{=} a^l$$
$$b_1 \stackrel{\text{def}}{=} b_0^2$$
$$b_2 \stackrel{\text{def}}{=} b_1^2$$
$$\ldots$$
$$b_k \stackrel{\text{def}}{=} b_{k-1}^2$$
Если для некоторого
$$j \in \{0, \ldots, k-1\}$$
выполняются условия
$$\begin{cases} b_j \neq 1 \\ b_j \neq -1 \\ b_{j+1} = 1 \end{cases}$$
то $n$ – составное.
6. Если $b_k \neq 1$, то $n$ – составное.

Если после шестого шага алгоритм не установил, что $n$ – составное, то он объявляет $n$ простым.

## 3.2 Анализ сложности алгоритма

Нетрудно доказать, что сложность данного влгоритма, т.е. количество исполняемых действий, можно оценить следующим выражением:

$$O((\log_2(n))^2) \tag{93}$$

Мы проанализируем лишь сложность шага 2.

Очевидно, что для выяснения того, представимо ли число $n$ в виде $m^i$, достаточно перебрать значения для показателя $i$ в диапазоне

$$\{2, \ldots, [\log_2 n]\}$$

и для каждого конкретного значения показателя $i$, поскольку функция $y = x^i$ монотонна при положительном значении аргумента, то уравнение

$$x^i = n \tag{94}$$

можно решать методом половинного деления, что требует не более $[\log_2 n]$ проверок для возможных кандидатов на решение данного уравнения.

Сложность проверки возможного кандидата $x$ на решение уравнения (94) (т.е. сложность вычисления $x^i$) можно оценить например как $O(\log_2(i))$.

Такую сложность имеет например следующий рекурсивный алгоритм:

$$x^i := \begin{cases} x & \text{если } i = 1 \\ (x^2)^{\frac{i}{2}} & \text{если } i\text{–чётное} \\ x \cdot (x^2)^{\frac{i-1}{2}} & \text{если } i\text{–нечётное} \end{cases}$$

Таким образом, шаг 2 требует выполнения (93) действий.

## 3.3 Обоснование корректности алгоритма

Алгоритм может выдать ответ

$$n - \text{составное} \tag{95}$$

только на шагах 1,2,5 и 6.

Очевидно, что если ответ (95) был выдан на шагах 1 или 2, то $n$ действительно является составным.

Докажем, что если ответ (95) был выдан на шагах 5 или 6, то $n$ тоже действительно является составным.

Пусть ответ (95) был выдан на шаге 5, т.е. для некоторого $j \in \{0, \ldots, k-1\}$ выполняются условия

$$b_j \neq 1, \quad b_j \neq -1 \tag{96}$$

$$b_j^2 = 1 \tag{97}$$

Из (97) следует, что

$$(b_j - 1)(b_j + 1) = 0 \tag{98}$$

причём из (96) следует, что оба сомножителя в (98) отличны от нуля.

Если бы $n$ было простым, то из (66) следует, что произведение отличных от нуля элементов $\mathbf{Z}_n$ не может быть равно нулю, т.е. (98) было бы невозможно.

Следовательно, если ответ был выдан на шаге 5, то он является правильным.

Теперь предположим, что ответ (95) был выдан на шаге 6.

Из определений чисел $b_0, \ldots, b_k$ следует, что

$$b_k = a^{2^k \cdot l} = a^{n-1}$$

Если бы $n$ было простым, то, согласно малой теореме Ферма, имело бы место соотношение (68), т.е. $b_k = 1$, что противоречит нашему предположению.

Следовательно, если ответ был выдан на шаге 6, то он тоже является правильным.

Таким образом,

1. в том случае, когда $n$ является простым, наш алгоритм никогда не выдаст ответ (95), т.е. в случае простого $n$ ответ алгоритма всегда будет правильным

2. в том случае, когда $n$ является составным, наш алгоритм иногда может выдать ошибочный ответ

   $$n - \text{простое}$$

   и это произойдёт в том и только в том случае, когда на шагах 1,2,5 и 6 не был выдан ответ (95), т.е. имеют место следующие соотношения:

   $$n - \text{нечётное число} \tag{99}$$

   $$n \text{ не имеет вид } m^i, \text{ где } m \geq 2 \text{ и } i \geq 2 \tag{100}$$

   $$\left.\begin{array}{l} \text{для каждого } j \in \{0, \ldots, k-1\} \\ \text{выполнено одно из условий :} \\ b_j = 1 \quad \text{или} \\ b_j = -1 \quad \text{или} \\ b_{j+1} \neq 1 \end{array}\right\} \tag{101}$$

   $$b_k = 1 \tag{102}$$

## 3.4 Оценка вероятности ошибки

Из (99) и (100) следует, что в том случае, когда алгоритм выдаёт ошибочный ответ, число $n$ должно обладать следующим свойством:

$$\begin{array}{l} \text{существуют некоторые взаимно простые} \\ \text{нечётные числа } u, v \text{ такие, что } n = uv \end{array} \tag{103}$$

Истинность или ложность соотношений (101) и (102) зависит только от выбора числа $a$, поскольку все числа из списка

$$b_0, b_1, \ldots, b_n$$

являются степенями числа $a$.

Назовём число из множества (92) **плохим**, если при выборе этого числа в качестве значения $a$ выполняются соотношения (101) и (102).

Очевидно, что вероятность выдачи ошибочного ответа в рассматриваемом случае равна доле плохих "$a$" среди всех чисел из множества (92).

Заметим, что

$$\text{все плохие "}a\text{" принадлежат множеству } \mathbf{Z}_n^* \tag{104}$$

т.к. если $a \notin \mathbf{Z}_n^*$, то $a$ и $n$ имеют общий делитель $d > 1$:

$$a = d \cdot a_1$$

$$n = d \cdot n_1$$

и в этом случае не будет выполнено соотношение (102), т.к. если

$$b_k = a^{n-1} = 1$$

то

$$\begin{aligned} & n_1 \cdot a^{n-1} = n_1 \quad \Rightarrow \\ \Rightarrow \quad & n_1 \cdot (d \cdot a_1)^{n-1} = n_1 \quad \Rightarrow \\ \Rightarrow \quad & n_1 \cdot d^{n-1} \cdot a_1^{n-1} = n_1 \quad \Rightarrow \\ \Rightarrow \quad & n \cdot d^{n-2} \cdot a_1^{n-1} = n_1 \end{aligned}$$

но т.к. $n \underset{n}{=} 0$, то

$$n \cdot d^{n-2} \cdot a_1^{n-1} = 0$$

и мы получили противоречие.

(104) позволяет переписать соотношения (101) и (102) в другой форме, для чего мы введём следующие обозначения.

Пусть

- $A$ – произвольная абелева группа, и
- $m$ – некоторое положительное целое число.

Обозначим символом $A^m$ совокупность элементов $A$ вида

$$\{g^m \mid g \in A\}$$

Очевидно, что $A^m$ является подгруппой в $A$.

Обозначим символом $\wedge m$ отображение вида

$$\wedge m : \quad A \longrightarrow A^m \tag{105}$$

которое сопоставляет каждому $g \in A$ элемент $g^m$.

Очевидно, что $\wedge m$ является эпиморфизмом.

Рассмотрим следующую цепочку эпиморфизмов:

$$G \xrightarrow{\wedge l} G_0 \xrightarrow{\wedge 2} G_1 \xrightarrow{\wedge 2} \ldots \xrightarrow{\wedge 2} G_k$$

где

$$G \stackrel{\text{def}}{=} \mathbf{Z}_n^*$$
$$G_0 \stackrel{\text{def}}{=} G^l$$
$$G_1 \stackrel{\text{def}}{=} G_0^2$$
$$\ldots$$
$$G_k \stackrel{\text{def}}{=} G_{k-1}^2$$

Для каждого $j \in \{0, \ldots, k\}$ обозначим символом $f_j$ сквозной эпиморфизм из $G$ в $G_j$ в данной цепочке, т.е.

$$f_j = \wedge(2^j \cdot l)$$

Очевидно, что

$$b_0 = f_0(a)$$
$$b_1 = f_1(a)$$
$$\ldots$$
$$b_k = f_k(a)$$

Поэтому

- соотношение (101) можно эквивалентным образом сформулировать так:

$$\left.\begin{array}{l} \text{для каждого } j \in \{0, \ldots, k-1\} \\ \text{выполнено одно из условий :} \\ f_j(a) = 1 \quad \text{или} \\ f_j(a) = -1 \quad \text{или} \\ f_{j+1}(a) \neq 1 \end{array}\right\} \tag{106}$$

- соотношение (102) можно эквивалентным образом сформулировать так:

$$f_k(a) = 1 \tag{107}$$

В свою очередь,

- соотношение (106) можно эквивалентным образом сформулировать так:

$$\begin{array}{l} \text{для каждого } j \in \{0, \ldots, k-1\} \\ a \in f_j^{-1}(1) \cup f_j^{-1}(-1) \cup \overline{f_{j+1}^{-1}(1)} \end{array} \tag{108}$$

- соотношение (107) можно эквивалентным образом сформулировать так:

$$a \in f_k^{-1}(1) \tag{109}$$

(108) можно переписать так:

$$a \quad \in \quad \bigcap_{j=0}^{k-1} \quad ( \; f_j^{-1}(1) \cup f_j^{-1}(-1) \cup \overline{f_{j+1}^{-1}(1)} \; ) \tag{110}$$

Из сказанного выше следует, что если для числа $n$ алгоритм может выдать ошибочный ответ, то

- имеет место (103), и
- вероятность выдачи ошибочного ответа в рассматриваемом случае равна отношению числа элементов в пересечении множеств

$$\bigcap_{j=0}^{k-1} \quad ( \; f_j^{-1}(1) \cup f_j^{-1}(-1) \cup \overline{f_{j+1}^{-1}(1)} \; ) \tag{111}$$

и

$$f_k^{-1}(1) \tag{112}$$

к числу элементов множества (92).

Для оценки вероятности выдачи ошибочного ответа мы отдельно рассмотрим случаи, когда

$$|G_k| \neq 1 \tag{113}$$

и

$$|G_k| = 1 \tag{114}$$

1. Пусть имеет место (113).

   Поскольку $f_k$ является эпиморфизмом вида

   $$f_k : G \to G_k$$

   то, согласно (23), имеет место неравенство

   $$|f_k^{-1}(1)| = |Ker(f_k)| \leq \frac{1}{2} \cdot |G|$$

   Следовательно, число элементов в пересечении (111) и (112) также не превосходит числа

   $$\frac{1}{2} \cdot |G| \tag{115}$$

Поскольку (115) не превосходит половины от числа элементов множества (92), то, следовательно, в случае (113) вероятность выдачи ошибочного ответа не превосходит $1/2$.

2. Теперь рассмотрим случай (114).

   Заметим, что группа $G$ не является одноэлементным множеством, т.к. она содержит по меньшей мере два элемента -

   $$1 \quad \text{и} \quad -1 \tag{116}$$

   Кроме того, группа $G_0$ $(= G^l)$ также не является одноэлементным множеством, поскольку, ввиду того, что число $l$ – нечётное, то

   $$(-1)^l = -1$$

   и, следовательно, группа $G_0$ также содержит по меньшей мере два элемента (116).

   Таким образом, существует номер

   $$j_0 \in \{0, \ldots, k-1\}$$

   такой, что

   $$|G_{j_0}| \neq 1 \tag{117}$$

   и

   $$|G_{j_0+1}| = 1 \tag{118}$$

   Докажем, что для данного номера $j_0$ число элементов в множестве

   $$f_{j_0}^{-1}(1) \cup f_{j_0}^{-1}(-1) \cup \overline{f_{j_0+1}^{-1}(1)} \tag{119}$$

   не превосходит числа (115).

   В частности, число элементов в пересечении (111) и (112) в этом случае также не будет превосходить числа (115), и, поскольку (115) не превосходит половины от числа элементов множества (92), то, следовательно, в случае (114) вероятность выдачи ошибочного ответа также не будет превосходить $1/2$.

   Из (118) следует, что

   $$\overline{f_{j_0+1}^{-1}(1)} \quad = \quad \emptyset$$

   Поэтому для доказательства того, что число элементов в множестве (119) не превосходит числа (115), достаточно доказать неравенство

   $$|f_{j_0}^{-1}(1)| \quad + \quad |f_{j_0}^{-1}(-1)| \quad \leq \quad \frac{1}{2} \cdot |G| \tag{120}$$

   Введём следующие обозначения:

   $$\begin{array}{ll} U \stackrel{\text{def}}{=} \mathbf{Z}_u^* & V \stackrel{\text{def}}{=} \mathbf{Z}_v^* \\ U_0 \stackrel{\text{def}}{=} U^l & V_0 \stackrel{\text{def}}{=} V^l \\ U_1 \stackrel{\text{def}}{=} U_0^2 & V_1 \stackrel{\text{def}}{=} V_0^2 \\ \ldots & \ldots \\ U_k \stackrel{\text{def}}{=} U_{k-1}^2 & V_k \stackrel{\text{def}}{=} V_{k-1}^2 \end{array}$$

   В данных обозначениях равенство (91) имеет вид

   $$G = U \times V$$

   и для каждого $j \in \{0, \ldots, k-1\}$ имеет место равенство

   $$G_j = U_j \times V_j$$

   поскольку возведение в степень пар из $U \times V$ осуществляется покомпонентно.

   Согласно определению отображения (70), которое индуцирует изоморфизм

   $$G \to U \times V$$

   элементу $-1$ группы $G$ при данном изоморфизме соответствует в декартовом произведении $U \times V$ пара

   $$(-1, -1) \tag{121}$$

   (левая компонента которой понимается как $r_u(-1)$, а правая - как $r_v(-1)$).

   Заметим, что в обоих группах $U$ и $V$ элементы "$-1$" не совпадают с элементами "1".

   Рассмотрим следующие случаи:

   (a) $|U_{j_0}| = 1$ или $|V_{j_0}| = 1$.
   В этом случае пара (121) не может принадлежать декартову произведению

   $$U_{j_0} \times V_{j_0}$$

   поэтому элемент "$-1$" группы $G$ (соответствующий данной паре) не принадлежит группе $G_{j_0}$, т.е.

   $$f_{j_0}^{-1}(-1) = \emptyset$$

   и, следовательно, второе слагаемое в левой части неравенства (120) равно нулю.

   Таким образом, в данном случае для доказательства неравенства (120) достаточно доказать неравенство

   $$|f_{j_0}^{-1}(1)| \quad \leq \quad \frac{1}{2} \cdot |G| \tag{122}$$

   Неравенство (122) следует из (23): поскольку $f_{j_0}$ является эпиморфизмом вида

   $$f_{j_0} : G \to G_{j_0}$$

   и $|G_{j_0}| > 1$, то на основании (23) имеет место неравенство

   $$|f_{j_0}^{-1}(1)| = |Ker(f_{j_0})| \leq \frac{1}{2} \cdot |G|$$

   (b) $|U_{j_0}| > 1$ и $|V_{j_0}| > 1$.
   В этом случае

   $$|Im(f_{j_0})| \quad = \quad |G_{j_0}| \quad \geq \quad 4$$

и, следовательно, на основании (22) можно заключить, что

$$|Ker(f_{j_0})| \leq \frac{1}{4} \cdot |G| \qquad (123)$$

Ввиду того, что

- $f_{j_0}^{-1}(1) = Ker(f_{j_0})$, и
- множество $f_{j_0}^{-1}(-1)$ является одним из смежных классов по подгруппе $Ker(f_{j_0})$, т.е., в частности,

$$|f_{j_0}^{-1}(-1)| = |Ker(f_{j_0})|$$

то

$$|f_{j_0}^{-1}(1)| \ + \ |f_{j_0}^{-1}(-1)| \ = \ 2 \cdot |Ker(f_{j_0})| \quad (124)$$

Искомое неравенство (120) следует из (124) и (123).

## 3.5 Уменьшение вероятности ошибки

Предложенный алгоритм можно немного модицифировать так, чтобы вероятность ошибочного ответа существенно уменьшилась.

Данная модификация заключается в том, что вместо однократного применения данного алгоритма к числу $n$ мы применим его к числу $n$ несколько раз.

Пусть символ $d$ обозначает количество применений данного алгоритма к числу $n$.

В качестве окончательного ответа мы выдаём

- ответ
$$n - \text{простое} \qquad (125)$$
если при всех $d$ применениях данного алгоритма к числу $n$ был получен ответ (125), и

- ответ
$$n - \text{составное} \qquad (126)$$
если при хотя бы одном из $d$ применений данного алгоритма к числу $n$ был получен ответ (126).

Нетрудно видеть, что окончательный ответ является ошибочным только тогда, когда при каждом из $d$ применений то число "$a$", которое выбиралось на шаге 4, было плохим.

Таким образом, вероятность ошибки можно оценить как вероятность того, что при $d$ независимых выборах чисел

$$a_1, \ldots, a_d \qquad (127)$$

из множества (92) все выбранные числа будут плохими.

Обозначим символом $p$ вероятность того, что при однократном выборе числа $a$ из множества (92) данное число будет плохим.

Как было установлено выше, $p \leq 1/2$.

Поскольку все числа из списка (127) порождаются независимо друг от друга, то вероятность того, что все они одновременно будут плохими, равна $p^d$.

Таким образом, вероятность ошибки модифицированного алгоритма не превосходит числа $2^{-d}$.