

Алгоритм Шора, часть II

М. В. Волков

Уральский федеральный университет
Институт естественных наук и математики
кафедра алгебры и фундаментальной информатики

2020/2021 учебный год

Здесь собраны необходимые для алгоритма Шора факты из теории чисел.

Здесь собраны необходимые для алгоритма Шора факты из теории чисел. Начнем с обоснования леммы, которая гарантирует «достаточный запас» чисел y , используемых в алгоритме Шора.

Лемма

Пусть N есть произведение двух простых чисел p и q , а $S = \{y : 1 \leq y < N, (y, N) = 1\}$. Тогда по крайней мере половина чисел $y \in S$ имеет четный период $2k$ и притом $y^k + 1$ не делится на N .

Здесь собраны необходимые для алгоритма Шора факты из теории чисел. Начнем с обоснования леммы, которая гарантирует «достаточный запас» чисел y , используемых в алгоритме Шора.

Лемма

Пусть N есть произведение двух простых чисел p и q , а $S = \{y : 1 \leq y < N, (y, N) = 1\}$. Тогда по крайней мере половина чисел $y \in S$ имеет четный период $2k$ и притом $y^k + 1$ не делится на N .

Нам потребуется такой классический результат:

Китайская теорема об остатках

Пусть $0 \leq a < p$, $0 \leq b < q$, где $(p, q) = 1$. Тогда существует единственное число x такое, что $0 \leq x < pq$ и при том $x \equiv a \pmod{p}$, $x \equiv b \pmod{q}$.

Здесь собраны необходимые для алгоритма Шора факты из теории чисел. Начнем с обоснования леммы, которая гарантирует «достаточный запас» чисел y , используемых в алгоритме Шора.

Лемма

Пусть N есть произведение двух простых чисел p и q , а $S = \{y : 1 \leq y < N, (y, N) = 1\}$. Тогда по крайней мере половина чисел $y \in S$ имеет четный период $2k$ и притом $y^k + 1$ не делится на N .

Нам потребуется такой классический результат:

Китайская теорема об остатках

Пусть $0 \leq a < p$, $0 \leq b < q$, где $(p, q) = 1$. Тогда существует единственное число x такое, что $0 \leq x < pq$ и при том $x \equiv a \pmod{p}$, $x \equiv b \pmod{q}$.

Доказательство. Поскольку $(p, q) = 1$, существуют такие целые числа r, s , что $rp + qs = 1$. Положим $x' := brp + asq$.

Здесь собраны необходимые для алгоритма Шора факты из теории чисел. Начнем с обоснования леммы, которая гарантирует «достаточный запас» чисел y , используемых в алгоритме Шора.

Лемма

Пусть N есть произведение двух простых чисел p и q , а $S = \{y : 1 \leq y < N, (y, N) = 1\}$. Тогда по крайней мере половина чисел $y \in S$ имеет четный период $2k$ и притом $y^k + 1$ не делится на N .

Нам потребуется такой классический результат:

Китайская теорема об остатках

Пусть $0 \leq a < p$, $0 \leq b < q$, где $(p, q) = 1$. Тогда существует единственное число x такое, что $0 \leq x < pq$ и при том $x \equiv a \pmod{p}$, $x \equiv b \pmod{q}$.

Доказательство. Поскольку $(p, q) = 1$, существуют такие целые числа r, s , что $rp + qs = 1$. Положим $x' := brp + asq$. Тогда

$$\begin{aligned}x' &\equiv asq \equiv a \pmod{p}, & \text{так как } sq &\equiv 1 \pmod{p}, \\x' &\equiv brp \equiv b \pmod{q}, & \text{так как } rp &\equiv 1 \pmod{q}.\end{aligned}$$

Здесь собраны необходимые для алгоритма Шора факты из теории чисел. Начнем с обоснования леммы, которая гарантирует «достаточный запас» чисел y , используемых в алгоритме Шора.

Лемма

Пусть N есть произведение двух простых чисел p и q , а $S = \{y : 1 \leq y < N, (y, N) = 1\}$. Тогда по крайней мере половина чисел $y \in S$ имеет четный период $2k$ и притом $y^k + 1$ не делится на N .

Нам потребуется такой классический результат:

Китайская теорема об остатках

Пусть $0 \leq a < p$, $0 \leq b < q$, где $(p, q) = 1$. Тогда существует единственное число x такое, что $0 \leq x < pq$ и при том $x \equiv a \pmod{p}$, $x \equiv b \pmod{q}$.

Доказательство. Поскольку $(p, q) = 1$, существуют такие целые числа r, s , что $rp + qs = 1$. Положим $x' := brp + asq$. Тогда

$$x' \equiv asq \equiv a \pmod{p}, \quad \text{так как } sq \equiv 1 \pmod{p},$$

$$x' \equiv brp \equiv b \pmod{q}, \quad \text{так как } rp \equiv 1 \pmod{q}.$$

В роли x годится остаток от деления x' на pq . Единственность очевидна. □

Здесь собраны необходимые для алгоритма Шора факты из теории чисел. Начнем с обоснования леммы, которая гарантирует «достаточный запас» чисел y , используемых в алгоритме Шора.

Лемма

Пусть N есть произведение двух простых чисел p и q , а $S = \{y : 1 \leq y < N, (y, N) = 1\}$. Тогда по крайней мере половина чисел $y \in S$ имеет четный период $2k$ и притом $y^k + 1$ не делится на N .

Нам потребуется такой классический результат:

Китайская теорема об остатках

Пусть $0 \leq a < p$, $0 \leq b < q$, где $(p, q) = 1$. Тогда существует единственное число x такое, что $0 \leq x < pq$ и при том $x \equiv a \pmod{p}$, $x \equiv b \pmod{q}$.

«Физический смысл» китайской теоремы об остатках состоит в том, что есть взаимно однозначное соответствие между остатками от деления на pq и парами вида (остаток от деления на p , остаток от деления на q).

Здесь собраны необходимые для алгоритма Шора факты из теории чисел. Начнем с обоснования леммы, которая гарантирует «достаточный запас» чисел y , используемых в алгоритме Шора.

Лемма

Пусть N есть произведение двух простых чисел p и q , а $S = \{y : 1 \leq y < N, (y, N) = 1\}$. Тогда по крайней мере половина чисел $y \in S$ имеет четный период $2k$ и притом $y^k + 1$ не делится на N .

Нам потребуется такой классический результат:

Китайская теорема об остатках

Пусть $0 \leq a < p$, $0 \leq b < q$, где $(p, q) = 1$. Тогда существует единственное число x такое, что $0 \leq x < pq$ и при том $x \equiv a \pmod{p}$, $x \equiv b \pmod{q}$.

«Физический смысл» китайской теоремы об остатках состоит в том, что есть взаимно однозначное соответствие между остатками от деления на pq и парами вида (остаток от деления на p , остаток от деления на q).

Этому соответствию можно дать такую вероятностную интерпретацию: если случайная величина x из $\{x : 0 \leq x < pq\}$ распределена равномерно, то остатки x по модулю p и по модулю q также распределены равномерно.

Напомним *теорему Эйлера*: если $(x, m) = 1$, то $x^{\varphi(m)} \equiv 1 \pmod{m}$, где $\varphi(m)$ — *функция Эйлера*, число чисел, меньших m и взаимно простых с m .

Напомним *теорему Эйлера*: если $(x, m) = 1$, то $x^{\varphi(m)} \equiv 1 \pmod{m}$, где $\varphi(m)$ — *функция Эйлера*, число чисел, меньших m и взаимно простых с m . В частности, если $m = p$ — простое число, то $x^{p-1} \equiv 1 \pmod{p}$ для любого x , не делящегося на p (*теорема Ферма*).

Напомним *теорему Эйлера*: если $(x, m) = 1$, то $x^{\varphi(m)} \equiv 1 \pmod{m}$, где $\varphi(m)$ — *функция Эйлера*, число чисел, меньших m и взаимно простых с m . В частности, если $m = p$ — простое число, то $x^{p-1} \equiv 1 \pmod{p}$ для любого x , не делящегося на p (*теорема Ферма*). Скажем, что x — *первообразный корень по модулю p* , если период x по модулю p равен $p - 1$.

Напомним *теорему Эйлера*: если $(x, m) = 1$, то $x^{\varphi(m)} \equiv 1 \pmod{m}$, где $\varphi(m)$ — *функция Эйлера*, число чисел, меньших m и взаимно простых с m . В частности, если $m = p$ — простое число, то $x^{p-1} \equiv 1 \pmod{p}$ для любого x , не делящегося на p (*теорема Ферма*). Скажем, что x — *первообразный корень по модулю p* , если период x по модулю p равен $p-1$. Наша ближайшая цель — доказать, что первообразные корни по модулю p существуют.

Напомним *теорему Эйлера*: если $(x, m) = 1$, то $x^{\varphi(m)} \equiv 1 \pmod{m}$, где $\varphi(m)$ — *функция Эйлера*, число чисел, меньших m и взаимно простых с m . В частности, если $m = p$ — простое число, то $x^{p-1} \equiv 1 \pmod{p}$ для любого x , не делящегося на p (*теорема Ферма*). Скажем, что x — *первообразный корень по модулю p* , если период x по модулю p равен $p-1$. Наша ближайшая цель — доказать, что первообразные корни по модулю p существуют.

$\forall 1$ Если x не делится на p , то период x по модулю p делит $p-1$.

Напомним *теорему Эйлера*: если $(x, m) = 1$, то $x^{\varphi(m)} \equiv 1 \pmod{m}$, где $\varphi(m)$ — *функция Эйлера*, число чисел, меньших m и взаимно простых с m . В частности, если $m = p$ — простое число, то $x^{p-1} \equiv 1 \pmod{p}$ для любого x , не делящегося на p (*теорема Ферма*). Скажем, что x — *первообразный корень по модулю p* , если период x по модулю p равен $p-1$. Наша ближайшая цель — доказать, что первообразные корни по модулю p существуют.

$\nabla 1$ Если x не делится на p , то период x по модулю p делит $p-1$.

Доказательство. Пусть k — период x по модулю p . Положим $\ell := (k, p-1)$.

Напомним *теорему Эйлера*: если $(x, m) = 1$, то $x^{\varphi(m)} \equiv 1 \pmod{m}$, где $\varphi(m)$ — *функция Эйлера*, число чисел, меньших m и взаимно простых с m . В частности, если $m = p$ — простое число, то $x^{p-1} \equiv 1 \pmod{p}$ для любого x , не делящегося на p (*теорема Ферма*). Скажем, что x — *первообразный корень по модулю p* , если период x по модулю p равен $p-1$. Наша ближайшая цель — доказать, что первообразные корни по модулю p существуют.

$\forall 1$ Если x не делится на p , то период x по модулю p делит $p-1$.

Доказательство. Пусть k — период x по модулю p . Положим $\ell := (k, p-1)$. Существуют такие целые числа r, s , что $kr + (p-1)s = \ell$.

Напомним *теорему Эйлера*: если $(x, m) = 1$, то $x^{\varphi(m)} \equiv 1 \pmod{m}$, где $\varphi(m)$ — *функция Эйлера*, число чисел, меньших m и взаимно простых с m . В частности, если $m = p$ — простое число, то $x^{p-1} \equiv 1 \pmod{p}$ для любого x , не делящегося на p (*теорема Ферма*). Скажем, что x — *первообразный корень по модулю p* , если период x по модулю p равен $p-1$. Наша ближайшая цель — доказать, что первообразные корни по модулю p существуют.

∇1 Если x не делится на p , то период x по модулю p делит $p-1$.

Доказательство. Пусть k — период x по модулю p . Положим $\ell := (k, p-1)$. Существуют такие целые числа r, s , что $kr + (p-1)s = \ell$. Тогда

$$x^\ell = x^{kr+(p-1)s} = x^{kr} x^{(p-1)s} = (x^k)^r (x^{p-1})^s \equiv 1 \pmod{p}.$$

Напомним *теорему Эйлера*: если $(x, m) = 1$, то $x^{\varphi(m)} \equiv 1 \pmod{m}$, где $\varphi(m)$ — *функция Эйлера*, число чисел, меньших m и взаимно простых с m . В частности, если $m = p$ — простое число, то $x^{p-1} \equiv 1 \pmod{p}$ для любого x , не делящегося на p (*теорема Ферма*). Скажем, что x — *первообразный корень по модулю p* , если период x по модулю p равен $p-1$. Наша ближайшая цель — доказать, что первообразные корни по модулю p существуют.

$\forall 1$ Если x не делится на p , то период x по модулю p делит $p-1$.

Доказательство. Пусть k — период x по модулю p . Положим $\ell := (k, p-1)$. Существуют такие целые числа r, s , что $kr + (p-1)s = \ell$. Тогда

$$x^\ell = x^{kr+(p-1)s} = x^{kr} x^{(p-1)s} = (x^k)^r (x^{p-1})^s \equiv 1 \pmod{p}.$$

По определению периода k — наименьшее натуральное число со свойством $x^k \equiv 1 \pmod{p}$, а $\ell \leq k$.

Напомним *теорему Эйлера*: если $(x, m) = 1$, то $x^{\varphi(m)} \equiv 1 \pmod{m}$, где $\varphi(m)$ — *функция Эйлера*, число чисел, меньших m и взаимно простых с m . В частности, если $m = p$ — простое число, то $x^{p-1} \equiv 1 \pmod{p}$ для любого x , не делящегося на p (*теорема Ферма*). Скажем, что x — *первообразный корень по модулю p* , если период x по модулю p равен $p-1$. Наша ближайшая цель — доказать, что первообразные корни по модулю p существуют.

$\forall 1$ Если x не делится на p , то период x по модулю p делит $p-1$.

Доказательство. Пусть k — период x по модулю p . Положим $\ell := (k, p-1)$. Существуют такие целые числа r, s , что $kr + (p-1)s = \ell$. Тогда

$$x^\ell = x^{kr+(p-1)s} = x^{kr} x^{(p-1)s} = (x^k)^r (x^{p-1})^s \equiv 1 \pmod{p}.$$

По определению периода k — наименьшее натуральное число со свойством $x^k \equiv 1 \pmod{p}$, а $\ell \leq k$. Поэтому $k = \ell$ делит $p-1$. \square

Напомним *теорему Эйлера*: если $(x, m) = 1$, то $x^{\varphi(m)} \equiv 1 \pmod{m}$, где $\varphi(m)$ — *функция Эйлера*, число чисел, меньших m и взаимно простых с m . В частности, если $m = p$ — простое число, то $x^{p-1} \equiv 1 \pmod{p}$ для любого x , не делящегося на p (*теорема Ферма*). Скажем, что x — *первообразный корень по модулю p* , если период x по модулю p равен $p-1$. Наша ближайшая цель — доказать, что первообразные корни по модулю p существуют.

∇1 Если x не делится на p , то период x по модулю p делит $p-1$.

∇2 Не более $\varphi(d)$ чисел, меньших p , имеет период d по модулю p .

Напомним *теорему Эйлера*: если $(x, m) = 1$, то $x^{\varphi(m)} \equiv 1 \pmod{m}$, где $\varphi(m)$ — *функция Эйлера*, число чисел, меньших m и взаимно простых с m . В частности, если $m = p$ — простое число, то $x^{p-1} \equiv 1 \pmod{p}$ для любого x , не делящегося на p (*теорема Ферма*). Скажем, что x — *первообразный корень по модулю p* , если период x по модулю p равен $p-1$. Наша ближайшая цель — доказать, что первообразные корни по модулю p существуют.

∇1 Если x не делится на p , то период x по модулю p делит $p-1$.

∇2 Не более $\varphi(d)$ чисел, меньших p , имеет период d по модулю p .

Доказательство. Пусть $a < p$ имеет период d по модулю p . Тогда числа a, a^2, \dots, a^d попарно несравнимы по модулю p и являются решениями сравнения $x^d \equiv 1 \pmod{p}$.

Напомним *теорему Эйлера*: если $(x, m) = 1$, то $x^{\varphi(m)} \equiv 1 \pmod{m}$, где $\varphi(m)$ — *функция Эйлера*, число чисел, меньших m и взаимно простых с m . В частности, если $m = p$ — простое число, то $x^{p-1} \equiv 1 \pmod{p}$ для любого x , не делящегося на p (*теорема Ферма*). Скажем, что x — *первообразный корень по модулю p* , если период x по модулю p равен $p-1$. Наша ближайшая цель — доказать, что первообразные корни по модулю p существуют.

∇1 Если x не делится на p , то период x по модулю p делит $p-1$.

∇2 Не более $\varphi(d)$ чисел, меньших p , имеет период d по модулю p .

Доказательство. Пусть $a < p$ имеет период d по модулю p . Тогда числа a, a^2, \dots, a^d попарно несравнимы по модулю p и являются решениями сравнения $x^d \equiv 1 \pmod{p}$. Это сравнение есть уравнение d -й степени над полем вычетов по модулю p , поэтому оно имеет не более d решений.

Напомним *теорему Эйлера*: если $(x, m) = 1$, то $x^{\varphi(m)} \equiv 1 \pmod{m}$, где $\varphi(m)$ — *функция Эйлера*, число чисел, меньших m и взаимно простых с m . В частности, если $m = p$ — простое число, то $x^{p-1} \equiv 1 \pmod{p}$ для любого x , не делящегося на p (*теорема Ферма*). Скажем, что x — *первообразный корень по модулю p* , если период x по модулю p равен $p-1$. Наша ближайшая цель — доказать, что первообразные корни по модулю p существуют.

$\nabla 1$ Если x не делится на p , то период x по модулю p делит $p-1$.

$\nabla 2$ Не более $\varphi(d)$ чисел, меньших p , имеет период d по модулю p .

Доказательство. Пусть $a < p$ имеет период d по модулю p . Тогда числа a, a^2, \dots, a^d попарно несравнимы по модулю p и являются решениями сравнения $x^d \equiv 1 \pmod{p}$. Это сравнение есть уравнение d -й степени над полем вычетов по модулю p , поэтому оно имеет не более d решений. Заключаем, что остатки от деления a^k на p , $k = 1, \dots, d$, суть все его решения.

Напомним *теорему Эйлера*: если $(x, m) = 1$, то $x^{\varphi(m)} \equiv 1 \pmod{m}$, где $\varphi(m)$ — *функция Эйлера*, число чисел, меньших m и взаимно простых с m . В частности, если $m = p$ — простое число, то $x^{p-1} \equiv 1 \pmod{p}$ для любого x , не делящегося на p (*теорема Ферма*). Скажем, что x — *первообразный корень по модулю p* , если период x по модулю p равен $p-1$. Наша ближайшая цель — доказать, что первообразные корни по модулю p существуют.

$\nabla 1$ Если x не делится на p , то период x по модулю p делит $p-1$.

$\nabla 2$ Не более $\varphi(d)$ чисел, меньших p , имеет период d по модулю p .

Доказательство. Пусть $a < p$ имеет период d по модулю p . Тогда числа a, a^2, \dots, a^d попарно несравнимы по модулю p и являются решениями сравнения $x^d \equiv 1 \pmod{p}$. Это сравнение есть уравнение d -й степени над полем вычетов по модулю p , поэтому оно имеет не более d решений. Заключаем, что остатки от деления a^k на p , $k = 1, \dots, d$, суть все его решения.

Если $\ell := (k, d) > 1$, то $(a^k)^{\frac{d}{\ell}} = (a^d)^{\frac{k}{\ell}} \equiv 1 \pmod{p}$, откуда период a^k по модулю p меньше d .

Напомним *теорему Эйлера*: если $(x, m) = 1$, то $x^{\varphi(m)} \equiv 1 \pmod{m}$, где $\varphi(m)$ — *функция Эйлера*, число чисел, меньших m и взаимно простых с m . В частности, если $m = p$ — простое число, то $x^{p-1} \equiv 1 \pmod{p}$ для любого x , не делящегося на p (*теорема Ферма*). Скажем, что x — *первообразный корень по модулю p* , если период x по модулю p равен $p-1$. Наша ближайшая цель — доказать, что первообразные корни по модулю p существуют.

∇1 Если x не делится на p , то период x по модулю p делит $p-1$.

∇2 Не более $\varphi(d)$ чисел, меньших p , имеет период d по модулю p .

Доказательство. Пусть $a < p$ имеет период d по модулю p . Тогда числа a, a^2, \dots, a^d попарно несравнимы по модулю p и являются решениями сравнения $x^d \equiv 1 \pmod{p}$. Это сравнение есть уравнение d -й степени над полем вычетов по модулю p , поэтому оно имеет не более d решений. Заключаем, что остатки от деления a^k на p , $k = 1, \dots, d$, суть все его решения.

Если $\ell := (k, d) > 1$, то $(a^k)^{\frac{d}{\ell}} = (a^d)^{\frac{k}{\ell}} \equiv 1 \pmod{p}$, откуда период a^k по модулю p меньше d . Итак, период d по модулю p могут иметь только такие остатки от деления a^k на p , что $(k, d) = 1$, а число таких k равно $\varphi(d)$. \square

Напомним *теорему Эйлера*: если $(x, m) = 1$, то $x^{\varphi(m)} \equiv 1 \pmod{m}$, где $\varphi(m)$ — *функция Эйлера*, число чисел, меньших m и взаимно простых с m . В частности, если $m = p$ — простое число, то $x^{p-1} \equiv 1 \pmod{p}$ для любого x , не делящегося на p (*теорема Ферма*). Скажем, что x — *первообразный корень по модулю p* , если период x по модулю p равен $p - 1$. Наша ближайшая цель — доказать, что первообразные корни по модулю p существуют.

∇1 Если x не делится на p , то период x по модулю p делит $p - 1$.

∇2 Не более $\varphi(d)$ чисел, меньших p , имеет период d по модулю p .

∇3 (*Тождество Гаусса*) $\sum_{d|n} \varphi(d) = n$ для любого натурального n .

Напомним *теорему Эйлера*: если $(x, m) = 1$, то $x^{\varphi(m)} \equiv 1 \pmod{m}$, где $\varphi(m)$ — *функция Эйлера*, число чисел, меньших m и взаимно простых с m . В частности, если $m = p$ — простое число, то $x^{p-1} \equiv 1 \pmod{p}$ для любого x , не делящегося на p (*теорема Ферма*). Скажем, что x — *первообразный корень по модулю p* , если период x по модулю p равен $p-1$. Наша ближайшая цель — доказать, что первообразные корни по модулю p существуют.

∇1 Если x не делится на p , то период x по модулю p делит $p-1$.

∇2 Не более $\varphi(d)$ чисел, меньших p , имеет период d по модулю p .

∇3 (*Тождество Гаусса*) $\sum_{d|n} \varphi(d) = n$ для любого натурального n .

Пример. $20 = \varphi(1) + \varphi(2) + \varphi(4) + \varphi(5) + \varphi(10) + \varphi(20) = 1 + 1 + 2 + 4 + 4 + 8$.

Напомним *теорему Эйлера*: если $(x, m) = 1$, то $x^{\varphi(m)} \equiv 1 \pmod{m}$, где $\varphi(m)$ — *функция Эйлера*, число чисел, меньших m и взаимно простых с m . В частности, если $m = p$ — простое число, то $x^{p-1} \equiv 1 \pmod{p}$ для любого x , не делящегося на p (*теорема Ферма*). Скажем, что x — *первообразный корень по модулю p* , если период x по модулю p равен $p-1$. Наша ближайшая цель — доказать, что первообразные корни по модулю p существуют.

∇1 Если x не делится на p , то период x по модулю p делит $p-1$.

∇2 Не более $\varphi(d)$ чисел, меньших p , имеет период d по модулю p .

∇3 (*Тождество Гаусса*) $\sum_{d|n} \varphi(d) = n$ для любого натурального n .

Доказательство. Рассмотрим все дроби со знаменателем n и числителями от 1 до n , т.е. $\frac{1}{n}, \frac{2}{n}, \dots, \frac{n}{n}$.

Напомним *теорему Эйлера*: если $(x, m) = 1$, то $x^{\varphi(m)} \equiv 1 \pmod{m}$, где $\varphi(m)$ — *функция Эйлера*, число чисел, меньших m и взаимно простых с m . В частности, если $m = p$ — простое число, то $x^{p-1} \equiv 1 \pmod{p}$ для любого x , не делящегося на p (*теорема Ферма*). Скажем, что x — *первообразный корень по модулю p* , если период x по модулю p равен $p-1$. Наша ближайшая цель — доказать, что первообразные корни по модулю p существуют.

∇1 Если x не делится на p , то период x по модулю p делит $p-1$.

∇2 Не более $\varphi(d)$ чисел, меньших p , имеет период d по модулю p .

∇3 (*Тождество Гаусса*) $\sum_{d|n} \varphi(d) = n$ для любого натурального n .

Доказательство. Рассмотрим все дроби со знаменателем n и числителями от 1 до n , т.е. $\frac{1}{n}, \frac{2}{n}, \dots, \frac{n}{n}$. Сократив их на НОД числителя и знаменателя, получим n несократимых дробей, знаменатели которых суть всевозможные делители числа n . Число дробей со знаменателем d равно $\varphi(d)$. \square

Напомним *теорему Эйлера*: если $(x, m) = 1$, то $x^{\varphi(m)} \equiv 1 \pmod{m}$, где $\varphi(m)$ — *функция Эйлера*, число чисел, меньших m и взаимно простых с m . В частности, если $m = p$ — простое число, то $x^{p-1} \equiv 1 \pmod{p}$ для любого x , не делящегося на p (*теорема Ферма*). Скажем, что x — *первообразный корень по модулю p* , если период x по модулю p равен $p-1$. Наша ближайшая цель — доказать, что первообразные корни по модулю p существуют.

∇1 Если x не делится на p , то период x по модулю p делит $p-1$.

∇2 Не более $\varphi(d)$ чисел, меньших p , имеет период d по модулю p .

∇3 (*Тождество Гаусса*) $\sum_{d|n} \varphi(d) = n$ для любого натурального n .

Доказательство. Рассмотрим все дроби со знаменателем n и числителями от 1 до n , т.е. $\frac{1}{n}, \frac{2}{n}, \dots, \frac{n}{n}$. Сократив их на НОД числителя и знаменателя, получим n несократимых дробей, знаменатели которых суть всевозможные делители числа n . Число дробей со знаменателем d равно $\varphi(d)$. □

Пример к доказательству:

$$\frac{1}{20}, \frac{2}{20}, \frac{3}{20}, \frac{4}{20}, \frac{5}{20}, \frac{6}{20}, \frac{7}{20}, \frac{8}{20}, \frac{9}{20}, \frac{10}{20}, \frac{11}{20}, \frac{12}{20}, \frac{13}{20}, \frac{14}{20}, \frac{15}{20}, \frac{16}{20}, \frac{17}{20}, \frac{18}{20}, \frac{19}{20}, \frac{20}{20}.$$

$$\frac{1}{20}, \frac{1}{10}, \frac{3}{20}, \frac{1}{5}, \frac{1}{4}, \frac{3}{10}, \frac{7}{20}, \frac{2}{5}, \frac{9}{20}, \frac{1}{2}, \frac{11}{20}, \frac{3}{5}, \frac{13}{20}, \frac{7}{10}, \frac{3}{4}, \frac{4}{5}, \frac{17}{20}, \frac{9}{10}, \frac{19}{20}, \frac{1}{1}$$

Напомним *теорему Эйлера*: если $(x, m) = 1$, то $x^{\varphi(m)} \equiv 1 \pmod{m}$, где $\varphi(m)$ — *функция Эйлера*, число чисел, меньших m и взаимно простых с m . В частности, если $m = p$ — простое число, то $x^{p-1} \equiv 1 \pmod{p}$ для любого x , не делящегося на p (*теорема Ферма*). Скажем, что x — *первообразный корень по модулю p* , если период x по модулю p равен $p-1$. Наша ближайшая цель — доказать, что первообразные корни по модулю p существуют.

∇1 Если x не делится на p , то период x по модулю p делит $p-1$.

∇2 Не более $\varphi(d)$ чисел, меньших p , имеет период d по модулю p .

∇3 (*Тождество Гаусса*) $\sum_{d|n} \varphi(d) = n$ для любого натурального n .

Доказательство существования первообразных корней. Для каждого делителя d числа $p-1$ обозначим через $\psi(d)$ число чисел, меньших p , с периодом d по модулю p .

Напомним *теорему Эйлера*: если $(x, m) = 1$, то $x^{\varphi(m)} \equiv 1 \pmod{m}$, где $\varphi(m)$ — *функция Эйлера*, число чисел, меньших m и взаимно простых с m . В частности, если $m = p$ — простое число, то $x^{p-1} \equiv 1 \pmod{p}$ для любого x , не делящегося на p (*теорема Ферма*). Скажем, что x — *первообразный корень по модулю p* , если период x по модулю p равен $p-1$. Наша ближайшая цель — доказать, что первообразные корни по модулю p существуют.

∇1 Если x не делится на p , то период x по модулю p делит $p-1$.

∇2 Не более $\varphi(d)$ чисел, меньших p , имеет период d по модулю p .

∇3 (*Тождество Гаусса*) $\sum_{d|n} \varphi(d) = n$ для любого натурального n .

Доказательство существования первообразных корней. Для каждого делителя d числа $p-1$ обозначим через $\psi(d)$ число чисел, меньших p , с периодом d по модулю p . Тогда $\sum_{d|p-1} \psi(d) = p-1$, так как у каждого числа, меньшего $p-1$, есть период по модулю p , и он делит $p-1$ по ∇1.

Напомним *теорему Эйлера*: если $(x, m) = 1$, то $x^{\varphi(m)} \equiv 1 \pmod{m}$, где $\varphi(m)$ — *функция Эйлера*, число чисел, меньших m и взаимно простых с m . В частности, если $m = p$ — простое число, то $x^{p-1} \equiv 1 \pmod{p}$ для любого x , не делящегося на p (*теорема Ферма*). Скажем, что x — *первообразный корень по модулю p* , если период x по модулю p равен $p-1$. Наша ближайшая цель — доказать, что первообразные корни по модулю p существуют.

∇1 Если x не делится на p , то период x по модулю p делит $p-1$.

∇2 Не более $\varphi(d)$ чисел, меньших p , имеет период d по модулю p .

∇3 (*Тождество Гаусса*) $\sum_{d|n} \varphi(d) = n$ для любого натурального n .

Доказательство существования первообразных корней. Для каждого делителя d числа $p-1$ обозначим через $\psi(d)$ число чисел, меньших p , с периодом d по модулю p . Тогда $\sum_{d|p-1} \psi(d) = p-1$, так как у каждого числа, меньшего $p-1$, есть период по модулю p , и он делит $p-1$ по ∇1. Из ∇3 следует, что $\sum_{d|p-1} \psi(d) = \sum_{d|p-1} \varphi(d)$, но $\psi(d) \leq \varphi(d)$ для каждого делителя d числа $p-1$ в силу ∇2.

Напомним *теорему Эйлера*: если $(x, m) = 1$, то $x^{\varphi(m)} \equiv 1 \pmod{m}$, где $\varphi(m)$ — *функция Эйлера*, число чисел, меньших m и взаимно простых с m . В частности, если $m = p$ — простое число, то $x^{p-1} \equiv 1 \pmod{p}$ для любого x , не делящегося на p (*теорема Ферма*). Скажем, что x — *первообразный корень по модулю p* , если период x по модулю p равен $p-1$. Наша ближайшая цель — доказать, что первообразные корни по модулю p существуют.

∇1 Если x не делится на p , то период x по модулю p делит $p-1$.

∇2 Не более $\varphi(d)$ чисел, меньших p , имеет период d по модулю p .

∇3 (*Тождество Гаусса*) $\sum_{d|n} \varphi(d) = n$ для любого натурального n .

Доказательство существования первообразных корней. Для каждого делителя d числа $p-1$ обозначим через $\psi(d)$ число чисел, меньших p , с периодом d по модулю p . Тогда $\sum_{d|p-1} \psi(d) = p-1$, так как у каждого числа, меньшего $p-1$, есть период по модулю p , и он делит $p-1$ по ∇1. Из ∇3 следует, что $\sum_{d|p-1} \psi(d) = \sum_{d|p-1} \varphi(d)$, но $\psi(d) \leq \varphi(d)$ для каждого делителя d числа $p-1$ в силу ∇2. Отсюда $\psi(d) = \varphi(d)$ для каждого делителя d числа $p-1$.

Напомним *теорему Эйлера*: если $(x, m) = 1$, то $x^{\varphi(m)} \equiv 1 \pmod{m}$, где $\varphi(m)$ — *функция Эйлера*, число чисел, меньших m и взаимно простых с m . В частности, если $m = p$ — простое число, то $x^{p-1} \equiv 1 \pmod{p}$ для любого x , не делящегося на p (*теорема Ферма*). Скажем, что x — *первообразный корень по модулю p* , если период x по модулю p равен $p-1$. Наша ближайшая цель — доказать, что первообразные корни по модулю p существуют.

∇1 Если x не делится на p , то период x по модулю p делит $p-1$.

∇2 Не более $\varphi(d)$ чисел, меньших p , имеет период d по модулю p .

∇3 (*Тождество Гаусса*) $\sum_{d|n} \varphi(d) = n$ для любого натурального n .

Доказательство существования первообразных корней. Для каждого делителя d числа $p-1$ обозначим через $\psi(d)$ число чисел, меньших p , с периодом d по модулю p . Тогда $\sum_{d|p-1} \psi(d) = p-1$, так как у каждого числа, меньшего $p-1$, есть период по модулю p , и он делит $p-1$ по ∇1. Из ∇3 следует, что $\sum_{d|p-1} \psi(d) = \sum_{d|p-1} \varphi(d)$, но $\psi(d) \leq \varphi(d)$ для каждого делителя d числа $p-1$ в силу ∇2. Отсюда $\psi(d) = \varphi(d)$ для каждого делителя d числа $p-1$. В частности, существует $\varphi(p-1)$ чисел, меньших p , с периодом $p-1$ по модулю p , т.е. первообразных корней по модулю p . \square

Напомним, что $S = \{y : 1 \leq y < N, (y, N) = 1\}$. Берем число $y \in S$ и пусть r — период числа y по модулю $N = pq$, где p и q — простые числа.

Напомним, что $S = \{y : 1 \leq y < N, (y, N) = 1\}$. Берем число $y \in S$ и пусть r — период числа y по модулю $N = pq$, где p и q — простые числа.

Покажем сначала, что $r = \text{НОК}(s, t)$, где s — период y по модулю p , а t — период y по модулю q .

Напомним, что $S = \{y : 1 \leq y < N, (y, N) = 1\}$. Берем число $y \in S$ и пусть r — период числа y по модулю $N = pq$, где p и q — простые числа.

Покажем сначала, что $r = \text{НОК}(s, t)$, где s — период y по модулю p , а t — период y по модулю q . Пусть (временно) $n := \text{НОК}(s, t)$.

Напомним, что $S = \{y : 1 \leq y < N, (y, N) = 1\}$. Берем число $y \in S$ и пусть r — период числа y по модулю $N = pq$, где p и q — простые числа.

Покажем сначала, что $r = \text{НОК}(s, t)$, где s — период y по модулю p , а t — период y по модулю q . Пусть (временно) $n := \text{НОК}(s, t)$. Имеем

$$\begin{aligned} y^s &\equiv 1 \pmod{p} && \Rightarrow && y^n &\equiv 1 \pmod{p}, \\ y^t &\equiv 1 \pmod{q} && \Rightarrow && y^n &\equiv 1 \pmod{q}, \end{aligned}$$

откуда $y^n \equiv 1 \pmod{N}$ и, следовательно, r делит n .

Напомним, что $S = \{y : 1 \leq y < N, (y, N) = 1\}$. Берем число $y \in S$ и пусть r — период числа y по модулю $N = pq$, где p и q — простые числа.

Покажем сначала, что $r = \text{НОК}(s, t)$, где s — период y по модулю p , а t — период y по модулю q . Пусть (временно) $n := \text{НОК}(s, t)$. Имеем

$$\begin{aligned} y^s &\equiv 1 \pmod{p} && \Rightarrow && y^n &\equiv 1 \pmod{p}, \\ y^t &\equiv 1 \pmod{q} && \Rightarrow && y^n &\equiv 1 \pmod{q}, \end{aligned}$$

откуда $y^n \equiv 1 \pmod{N}$ и, следовательно, r делит n . С другой стороны, раз $y^r \equiv 1 \pmod{N}$, то $y^r \equiv 1 \pmod{p}$, откуда s делит r .

Напомним, что $S = \{y : 1 \leq y < N, (y, N) = 1\}$. Берем число $y \in S$ и пусть r — период числа y по модулю $N = pq$, где p и q — простые числа.

Покажем сначала, что $r = \text{НОК}(s, t)$, где s — период y по модулю p , а t — период y по модулю q . Пусть (времененно) $n := \text{НОК}(s, t)$. Имеем

$$\begin{aligned} y^s &\equiv 1 \pmod{p} && \Rightarrow && y^n &\equiv 1 \pmod{p}, \\ y^t &\equiv 1 \pmod{q} && \Rightarrow && y^n &\equiv 1 \pmod{q}, \end{aligned}$$

откуда $y^n \equiv 1 \pmod{N}$ и, следовательно, r делит n . С другой стороны, раз $y^r \equiv 1 \pmod{N}$, то $y^r \equiv 1 \pmod{p}$, откуда s делит r . Аналогично показывается, что t делит r , но тогда и $n = \text{НОК}(s, t)$ делит r .

Напомним, что $S = \{y : 1 \leq y < N, (y, N) = 1\}$. Берем число $y \in S$ и пусть r — период числа y по модулю $N = pq$, где p и q — простые числа.

Покажем сначала, что $r = \text{НОК}(s, t)$, где s — период y по модулю p , а t — период y по модулю q . Пусть (времененно) $n := \text{НОК}(s, t)$. Имеем

$$\begin{aligned}y^s &\equiv 1 \pmod{p} && \Rightarrow && y^n &\equiv 1 \pmod{p}, \\y^t &\equiv 1 \pmod{q} && \Rightarrow && y^n &\equiv 1 \pmod{q},\end{aligned}$$

откуда $y^n \equiv 1 \pmod{N}$ и, следовательно, r делит n . С другой стороны, раз $y^r \equiv 1 \pmod{N}$, то $y^r \equiv 1 \pmod{p}$, откуда s делит r . Аналогично показывается, что t делит r , но тогда и $n = \text{НОК}(s, t)$ делит r . Итак, $r = n$.

Напомним, что $S = \{y : 1 \leq y < N, (y, N) = 1\}$. Берем число $y \in S$ и пусть r — период числа y по модулю $N = pq$, где p и q — простые числа.

Покажем сначала, что $r = \text{НОК}(s, t)$, где s — период y по модулю p , а t — период y по модулю q . Пусть (времененно) $n := \text{НОК}(s, t)$. Имеем

$$\begin{aligned} y^s &\equiv 1 \pmod{p} && \Rightarrow && y^n &\equiv 1 \pmod{p}, \\ y^t &\equiv 1 \pmod{q} && \Rightarrow && y^n &\equiv 1 \pmod{q}, \end{aligned}$$

откуда $y^n \equiv 1 \pmod{N}$ и, следовательно, r делит n . С другой стороны, раз $y^r \equiv 1 \pmod{N}$, то $y^r \equiv 1 \pmod{p}$, откуда s делит r . Аналогично показывается, что t делит r , но тогда и $n = \text{НОК}(s, t)$ делит r . Итак, $r = n$.

Если $s = 2^i u$, $t = 2^j v$, где u, v нечетны, то $r = 2^{\max\{i, j\}} \text{НОК}(u, v)$.

Напомним, что $S = \{y : 1 \leq y < N, (y, N) = 1\}$. Берем число $y \in S$ и пусть r — период числа y по модулю $N = pq$, где p и q — простые числа.

Покажем сначала, что $r = \text{НОК}(s, t)$, где s — период y по модулю p , а t — период y по модулю q . Пусть (временно) $n := \text{НОК}(s, t)$. Имеем

$$\begin{aligned} y^s &\equiv 1 \pmod{p} && \Rightarrow && y^n &\equiv 1 \pmod{p}, \\ y^t &\equiv 1 \pmod{q} && \Rightarrow && y^n &\equiv 1 \pmod{q}, \end{aligned}$$

откуда $y^n \equiv 1 \pmod{N}$ и, следовательно, r делит n . С другой стороны, раз $y^r \equiv 1 \pmod{N}$, то $y^r \equiv 1 \pmod{p}$, откуда s делит r . Аналогично показывается, что t делит r , но тогда и $n = \text{НОК}(s, t)$ делит r . Итак, $r = n$.

Если $s = 2^i u$, $t = 2^j v$, где u, v нечетны, то $r = 2^{\max\{i, j\}} \text{НОК}(u, v)$. В частности, r нечетно тогда и только тогда, когда $i = j = 0$.

Напомним, что $S = \{y : 1 \leq y < N, (y, N) = 1\}$. Берем число $y \in S$ и пусть r — период числа y по модулю $N = pq$, где p и q — простые числа.

Покажем сначала, что $r = \text{НОК}(s, t)$, где s — период y по модулю p , а t — период y по модулю q . Пусть (временно) $n := \text{НОК}(s, t)$. Имеем

$$\begin{aligned} y^s &\equiv 1 \pmod{p} && \Rightarrow && y^n &\equiv 1 \pmod{p}, \\ y^t &\equiv 1 \pmod{q} && \Rightarrow && y^n &\equiv 1 \pmod{q}, \end{aligned}$$

откуда $y^n \equiv 1 \pmod{N}$ и, следовательно, r делит n . С другой стороны, раз $y^r \equiv 1 \pmod{N}$, то $y^r \equiv 1 \pmod{p}$, откуда s делит r . Аналогично показывается, что t делит r , но тогда и $n = \text{НОК}(s, t)$ делит r . Итак, $r = n$.

Если $s = 2^i u$, $t = 2^j v$, где u, v нечетны, то $r = 2^{\max\{i, j\}} \text{НОК}(u, v)$. В частности, r нечетно тогда и только тогда, когда $i = j = 0$. Напомним, что это первая «плохая» ситуация. Вторая «плохая» ситуация случается, когда $r = 2k$, но $y^k \equiv -1 \pmod{N}$.

Напомним, что $S = \{y : 1 \leq y < N, (y, N) = 1\}$. Берем число $y \in S$ и пусть r — период числа y по модулю $N = pq$, где p и q — простые числа.

Покажем сначала, что $r = \text{НОК}(s, t)$, где s — период y по модулю p , а t — период y по модулю q . Пусть (времененно) $n := \text{НОК}(s, t)$. Имеем

$$\begin{aligned} y^s &\equiv 1 \pmod{p} && \Rightarrow && y^n &\equiv 1 \pmod{p}, \\ y^t &\equiv 1 \pmod{q} && \Rightarrow && y^n &\equiv 1 \pmod{q}, \end{aligned}$$

откуда $y^n \equiv 1 \pmod{N}$ и, следовательно, r делит n . С другой стороны, раз $y^r \equiv 1 \pmod{N}$, то $y^r \equiv 1 \pmod{p}$, откуда s делит r . Аналогично показывается, что t делит r , но тогда и $n = \text{НОК}(s, t)$ делит r . Итак, $r = n$.

Если $s = 2^i u$, $t = 2^j v$, где u, v нечетны, то $r = 2^{\max\{i, j\}} \text{НОК}(u, v)$. В частности, r нечетно тогда и только тогда, когда $i = j = 0$. Напомним, что это первая «плохая» ситуация. Вторая «плохая» ситуация случается, когда

$r = 2k$, но $y^k \equiv -1 \pmod{N}$. Заметим, что тогда $\begin{cases} y^k \equiv -1 \pmod{p}, \\ y^k \equiv -1 \pmod{q}. \end{cases}$

Итак, $s = 2^i u$, $t = 2^j v$, где u, v нечетны; допустим, что $i < j$.

Итак, $s = 2^i u$, $t = 2^j v$, где u, v нечетны; допустим, что $i < j$.
В этом случае $r = 2^j \text{НОК}(u, v)$ и $k = 2^{j-1} \text{НОК}(u, v)$ делится на s .

Итак, $s = 2^i u$, $t = 2^j v$, где u, v нечетны; допустим, что $i < j$.

В этом случае $r = 2^j \text{НОК}(u, v)$ и $k = 2^{j-1} \text{НОК}(u, v)$ делится на s .

Но $y^s \equiv 1 \pmod{p}$, откуда $y^k \equiv 1 \pmod{p}$, что противоречит условию $y^k \equiv -1 \pmod{p}$.

Итак, $s = 2^i u$, $t = 2^j v$, где u, v нечетны; допустим, что $i < j$.

В этом случае $r = 2^j \text{НОК}(u, v)$ и $k = 2^{j-1} \text{НОК}(u, v)$ делится на s .

Но $y^s \equiv 1 \pmod{p}$, откуда $y^k \equiv 1 \pmod{p}$, что противоречит условию $y^k \equiv -1 \pmod{p}$. Аналогично, допущение $i > j$ ведет к противоречию.

Итак, $s = 2^i u$, $t = 2^j v$, где u, v нечетны; допустим, что $i < j$.

В этом случае $r = 2^j \text{НОК}(u, v)$ и $k = 2^{j-1} \text{НОК}(u, v)$ делится на s .

Но $y^s \equiv 1 \pmod{p}$, откуда $y^k \equiv 1 \pmod{p}$, что противоречит условию $y^k \equiv -1 \pmod{p}$. Аналогично, допущение $i > j$ ведет к противоречию.

Итак, если $y^k \equiv -1 \pmod{N}$, то $i = j$.

Итак, $s = 2^i u$, $t = 2^j v$, где u, v нечетны; допустим, что $i < j$.

В этом случае $r = 2^j \text{НОК}(u, v)$ и $k = 2^{j-1} \text{НОК}(u, v)$ делится на s .

Но $y^s \equiv 1 \pmod{p}$, откуда $y^k \equiv 1 \pmod{p}$, что противоречит условию $y^k \equiv -1 \pmod{p}$. Аналогично, допущение $i > j$ ведет к противоречию.

Итак, если $y^k \equiv -1 \pmod{N}$, то $i = j$.

Вывод: «плохие» ситуации означают, что $i = j$ ($i = j = 0$ в первом случае, $i = j > 0$ во втором). Подсчитаем, как часто такое может произойти.

Итак, $s = 2^i u$, $t = 2^j v$, где u, v нечетны; допустим, что $i < j$.

В этом случае $r = 2^j \text{НОК}(u, v)$ и $k = 2^{j-1} \text{НОК}(u, v)$ делится на s .

Но $y^s \equiv 1 \pmod{p}$, откуда $y^k \equiv 1 \pmod{p}$, что противоречит условию $y^k \equiv -1 \pmod{p}$. Аналогично, допущение $i > j$ ведет к противоречию.

Итак, если $y^k \equiv -1 \pmod{N}$, то $i = j$.

Вывод: «плохие» ситуации означают, что $i = j$ ($i = j = 0$ в первом случае, $i = j > 0$ во втором). Подсчитаем, как часто такое может произойти.

Представим $p - 1$ как $p - 1 = 2^m x$, где x нечетно, и пусть z — некоторый первообразный корень по модулю p .

Итак, $s = 2^i u$, $t = 2^j v$, где u, v нечетны; допустим, что $i < j$.

В этом случае $r = 2^j \text{НОК}(u, v)$ и $k = 2^{j-1} \text{НОК}(u, v)$ делится на s .

Но $y^s \equiv 1 \pmod{p}$, откуда $y^k \equiv 1 \pmod{p}$, что противоречит условию $y^k \equiv -1 \pmod{p}$. Аналогично, допущение $i > j$ ведет к противоречию.

Итак, если $y^k \equiv -1 \pmod{N}$, то $i = j$.

Вывод: «плохие» ситуации означают, что $i = j$ ($i = j = 0$ в первом случае, $i = j > 0$ во втором). Подсчитаем, как часто такое может произойти.

Представим $p - 1$ как $p - 1 = 2^m x$, где x нечетно, и пусть z — некоторый первообразный корень по модулю p . Тогда любое число b , не делящееся на p , сравнимо по модулю p с какой-то степенью z^g .

Итак, $s = 2^i u$, $t = 2^j v$, где u, v нечетны; допустим, что $i < j$.

В этом случае $r = 2^j \text{НОК}(u, v)$ и $k = 2^{j-1} \text{НОК}(u, v)$ делится на s .

Но $y^s \equiv 1 \pmod{p}$, откуда $y^k \equiv 1 \pmod{p}$, что противоречит условию $y^k \equiv -1 \pmod{p}$. Аналогично, допущение $i > j$ ведет к противоречию.

Итак, если $y^k \equiv -1 \pmod{N}$, то $i = j$.

Вывод: «плохие» ситуации означают, что $i = j$ ($i = j = 0$ в первом случае, $i = j > 0$ во втором). Подсчитаем, как часто такое может произойти.

Представим $p - 1$ как $p - 1 = 2^m x$, где x нечетно, и пусть z — некоторый первообразный корень по модулю p . Тогда любое число b , не делящееся на p , сравнимо по модулю p с какой-то степенью z^g . Если h — период b по модулю p , то $z^{gh} \equiv b^h \equiv 1 \pmod{p}$, откуда gh делится на $p - 1 = 2^m x$.

Итак, $s = 2^i u$, $t = 2^j v$, где u, v нечетны; допустим, что $i < j$.

В этом случае $r = 2^j \text{НОК}(u, v)$ и $k = 2^{j-1} \text{НОК}(u, v)$ делится на s .

Но $y^s \equiv 1 \pmod{p}$, откуда $y^k \equiv 1 \pmod{p}$, что противоречит условию $y^k \equiv -1 \pmod{p}$. Аналогично, допущение $i > j$ ведет к противоречию.

Итак, если $y^k \equiv -1 \pmod{N}$, то $i = j$.

Вывод: «плохие» ситуации означают, что $i = j$ ($i = j = 0$ в первом случае, $i = j > 0$ во втором). Подсчитаем, как часто такое может произойти.

Представим $p - 1$ как $p - 1 = 2^m x$, где x нечетно, и пусть z — некоторый первообразный корень по модулю p . Тогда любое число b , не делящееся на p , сравнимо по модулю p с какой-то степенью z^g . Если h — период b по модулю p , то $z^{gh} \equiv b^h \equiv 1 \pmod{p}$, откуда gh делится на $p - 1 = 2^m x$. Видно, что h будет нечетным тогда и только тогда, когда g делится на 2^m , т.е. когда b сравнимо с $z^{2^m w}$, где $1 \leq w \leq x$.

Итак, $s = 2^i u$, $t = 2^j v$, где u, v нечетны; допустим, что $i < j$.

В этом случае $r = 2^j \text{НОК}(u, v)$ и $k = 2^{j-1} \text{НОК}(u, v)$ делится на s .

Но $y^s \equiv 1 \pmod{p}$, откуда $y^k \equiv 1 \pmod{p}$, что противоречит условию $y^k \equiv -1 \pmod{p}$. Аналогично, допущение $i > j$ ведет к противоречию.

Итак, если $y^k \equiv -1 \pmod{N}$, то $i = j$.

Вывод: «плохие» ситуации означают, что $i = j$ ($i = j = 0$ в первом случае, $i = j > 0$ во втором). Подсчитаем, как часто такое может произойти.

Представим $p - 1$ как $p - 1 = 2^m x$, где x нечетно, и пусть z — некоторый первообразный корень по модулю p . Тогда любое число b , не делящееся на p , сравнимо по модулю p с какой-то степенью z^g . Если h — период b по модулю p , то $z^{gh} \equiv b^h \equiv 1 \pmod{p}$, откуда gh делится на $p - 1 = 2^m x$.

Видно, что h будет нечетным тогда и только тогда, когда g делится на 2^m , т.е. когда b сравнимо с $z^{2^m w}$, где $1 \leq w \leq x$. Доля таких чисел равна 2^{-m} .

Итак, $s = 2^i u$, $t = 2^j v$, где u, v нечетны; допустим, что $i < j$.

В этом случае $r = 2^j \text{НОК}(u, v)$ и $k = 2^{j-1} \text{НОК}(u, v)$ делится на s .

Но $y^s \equiv 1 \pmod{p}$, откуда $y^k \equiv 1 \pmod{p}$, что противоречит условию $y^k \equiv -1 \pmod{p}$. Аналогично, допущение $i > j$ ведет к противоречию.

Итак, если $y^k \equiv -1 \pmod{N}$, то $i = j$.

Вывод: «плохие» ситуации означают, что $i = j$ ($i = j = 0$ в первом случае, $i = j > 0$ во втором). Подсчитаем, как часто такое может произойти.

Представим $p - 1$ как $p - 1 = 2^m x$, где x нечетно, и пусть z — некоторый первообразный корень по модулю p . Тогда любое число b , не делящееся на p , сравнимо по модулю p с какой-то степенью z^g . Если h — период b по модулю p , то $z^{gh} \equiv b^h \equiv 1 \pmod{p}$, откуда gh делится на $p - 1 = 2^m x$.

Видно, что h будет нечетным тогда и только тогда, когда g делится на 2^m , т.е. когда b сравнимо с $z^{2^m w}$, где $1 \leq w \leq x$. Доля таких чисел равна 2^{-m} .

Аналогично, чтобы период b по модулю p делился в точности на 2^i , необходимо и достаточно, чтобы g равнялось $2^{m-i} w$, где w нечетно и $1 \leq w \leq 2^i x - 1$.

Итак, $s = 2^i u$, $t = 2^j v$, где u, v нечетны; допустим, что $i < j$.

В этом случае $r = 2^j \text{НОК}(u, v)$ и $k = 2^{j-1} \text{НОК}(u, v)$ делится на s .

Но $y^s \equiv 1 \pmod{p}$, откуда $y^k \equiv 1 \pmod{p}$, что противоречит условию $y^k \equiv -1 \pmod{p}$. Аналогично, допущение $i > j$ ведет к противоречию.

Итак, если $y^k \equiv -1 \pmod{N}$, то $i = j$.

Вывод: «плохие» ситуации означают, что $i = j$ ($i = j = 0$ в первом случае, $i = j > 0$ во втором). Подсчитаем, как часто такое может произойти.

Представим $p - 1$ как $p - 1 = 2^m x$, где x нечетно, и пусть z — некоторый первообразный корень по модулю p . Тогда любое число b , не делящееся на p , сравнимо по модулю p с какой-то степенью z^g . Если h — период b по модулю p , то $z^{gh} \equiv b^h \equiv 1 \pmod{p}$, откуда gh делится на $p - 1 = 2^m x$.

Видно, что h будет нечетным тогда и только тогда, когда g делится на 2^m , т.е. когда b сравнимо с $z^{2^m w}$, где $1 \leq w \leq x$. Доля таких чисел равна 2^{-m} .

Аналогично, чтобы период b по модулю p делился в точности на 2^i , необходимо и достаточно, чтобы g равнялось $2^{m-i} w$, где w нечетно и $1 \leq w \leq 2^i x - 1$. Число таких b равно $2^{i-1} x$, а их доля равна 2^{-m+i-1} .

Итак, $s = 2^i u$, $t = 2^j v$, где u, v нечетны; допустим, что $i < j$.

В этом случае $r = 2^j \text{НОК}(u, v)$ и $k = 2^{j-1} \text{НОК}(u, v)$ делится на s .

Но $y^s \equiv 1 \pmod{p}$, откуда $y^k \equiv 1 \pmod{p}$, что противоречит условию $y^k \equiv -1 \pmod{p}$. Аналогично, допущение $i > j$ ведет к противоречию.

Итак, если $y^k \equiv -1 \pmod{N}$, то $i = j$.

Вывод: «плохие» ситуации означают, что $i = j$ ($i = j = 0$ в первом случае, $i = j > 0$ во втором). Подсчитаем, как часто такое может произойти.

Представим $p - 1$ как $p - 1 = 2^m x$, где x нечетно, и пусть z — некоторый первообразный корень по модулю p . Тогда любое число b , не делящееся на p , сравнимо по модулю p с какой-то степенью z^g . Если h — период b по модулю p , то $z^{gh} \equiv b^h \equiv 1 \pmod{p}$, откуда gh делится на $p - 1 = 2^m x$.

Видно, что h будет нечетным тогда и только тогда, когда g делится на 2^m , т.е. когда b сравнимо с $z^{2^m w}$, где $1 \leq w \leq x$. Доля таких чисел равна 2^{-m} .

Аналогично, чтобы период b по модулю p делился в точности на 2^i , необходимо и достаточно, чтобы g равнялось $2^{m-i} w$, где w нечетно и $1 \leq w \leq 2^i x - 1$. Число таких b равно $2^{i-1} x$, а их доля равна 2^{-m+i-1} .

В силу тех же аргументов, если $q - 1 = 2^n x'$, где x' нечетно, то доля чисел с нечетным периодом по модулю q равна 2^{-n} , а доля чисел, период которых по модулю q делится в точности на 2^i , равна 2^{-n+i-1} .

Без ограничения общности можно считать, что $m \leq n$.

Без ограничения общности можно считать, что $m \leq n$.

Из вероятностной интерпретации китайской теоремы об остатках получаем, что вероятность того, что период числа y по модулю $N = pq$ нечетен, равна $(\frac{1}{2})^{m+n}$, а вероятность того, что период y по модулю N равен $2k$, но $y^k \equiv -1 \pmod{N}$, равна $\sum_{i=1}^m (\frac{1}{2})^{m+n-2i+2}$.

Без ограничения общности можно считать, что $m \leq n$.

Из вероятностной интерпретации китайской теоремы об остатках получаем, что вероятность того, что период числа y по модулю $N = pq$ нечетен, равна $(\frac{1}{2})^{m+n}$, а вероятность того, что период y по модулю N равен $2k$, но $y^k \equiv -1 \pmod{N}$, равна $\sum_{i=1}^m (\frac{1}{2})^{m+n-2i+2}$.

Вычисляя, находим

$$\begin{aligned} \left(\frac{1}{2}\right)^{m+n} + \sum_{i=1}^m \left(\frac{1}{2}\right)^{m+n-2i+2} &= \left(\frac{1}{2}\right)^{m+n} \left(1 + \sum_{i=1}^m 4^{i-1}\right) = \\ &= \left(\frac{1}{2}\right)^{m+n} \left(1 + \frac{4^m - 1}{3}\right) = \frac{1}{4^m 2^{n-m}} \left(\frac{4^m}{3} + \frac{2}{3}\right) = \\ &= \frac{1}{2^{n-m}} \left(\frac{1}{3} + \frac{2}{3 \cdot 4^m}\right) \leq \frac{1}{3} + \frac{1}{6} = \frac{1}{2}. \end{aligned}$$

Без ограничения общности можно считать, что $m \leq n$.

Из вероятностной интерпретации китайской теоремы об остатках получаем, что вероятность того, что период числа y по модулю $N = pq$ нечетен, равна $(\frac{1}{2})^{m+n}$, а вероятность того, что период y по модулю N равен $2k$, но $y^k \equiv -1 \pmod{N}$, равна $\sum_{i=1}^m (\frac{1}{2})^{m+n-2i+2}$.

Вычисляя, находим

$$\begin{aligned} \left(\frac{1}{2}\right)^{m+n} + \sum_{i=1}^m \left(\frac{1}{2}\right)^{m+n-2i+2} &= \left(\frac{1}{2}\right)^{m+n} \left(1 + \sum_{i=1}^m 4^{i-1}\right) = \\ &= \left(\frac{1}{2}\right)^{m+n} \left(1 + \frac{4^m - 1}{3}\right) = \frac{1}{4^m 2^{n-m}} \left(\frac{4^m}{3} + \frac{2}{3}\right) = \\ &= \frac{1}{2^{n-m}} \left(\frac{1}{3} + \frac{2}{3 \cdot 4^m}\right) \leq \frac{1}{3} + \frac{1}{6} = \frac{1}{2}. \end{aligned}$$

Тем самым лемма доказана. Равенство возможно, если $m = n = 1$, например, при $N = 7 \cdot 11 = 77$.

Выбираем такое n , чтобы $N^2 \leq 2^n < 2N^2$. Заметим, что n приходится выбирать намного бóльшим, чем в упрощенной версии алгоритма (для произведения простых чисел Ферма).

Выбираем такое n , чтобы $N^2 \leq 2^n < 2N^2$. Заметим, что n приходится выбирать намного бóльшим, чем в упрощенной версии алгоритма (для произведения простых чисел Ферма).
Для облегчения обозначений положим $S := 2^n$.

Выбираем такое n , чтобы $N^2 \leq 2^n < 2N^2$. Заметим, что n приходится выбирать намного бóльшим, чем в упрощенной версии алгоритма (для произведения простых чисел Ферма).

Для облегчения обозначений положим $S := 2^n$.

Логика алгоритма не меняется. Работаем с системой $H := H_S \otimes H_S$. Вместо $|a\rangle \otimes |b\rangle$ пишем $|a\rangle|b\rangle$ и ссылаемся на $|a\rangle$ и соответственно $|b\rangle$ как на *содержимое* первого и соответственно второго регистра.

Выбираем такое n , чтобы $N^2 \leq 2^n < 2N^2$. Заметим, что n приходится выбирать намного бóльшим, чем в упрощенной версии алгоритма (для произведения простых чисел Ферма).

Для облегчения обозначений положим $S := 2^n$.

Логика алгоритма не меняется. Работаем с системой $H := H_S \otimes H_S$. Вместо $|a\rangle \otimes |b\rangle$ пишем $|a\rangle|b\rangle$ и ссылаемся на $|a\rangle$ и соответственно $|b\rangle$ как на *содержимое* первого и соответственно второго регистра.

Алгоритм Шора

- 1 Инициализируем H в состояние $|0\rangle|0\rangle$.
- 2 Применяем преобразование Адамара R_S к первому регистру.
- 3 Применяем оператор $U_f: |a\rangle|b\rangle \mapsto |a\rangle|f(a) \oplus b\rangle$, связанный с функцией $f: k \mapsto y^k \pmod{N}$.
- 4 Применяем дискретное преобразование Фурье F_S к первому регистру:
$$F_S|k\rangle := \frac{1}{\sqrt{S}} \sum_{u=0}^{S-1} e^{\frac{2\pi ijk}{S}} |u\rangle$$
- 5 Измеряя первый регистр, находим вектор, с помощью которого делаем вывод о периоде u по модулю N .

Вычислим состояние системы на каждом шаге алгоритма Шора.

Вычислим состояние системы на каждом шаге алгоритма Шора.
После шага 1 состояние $|0\rangle|0\rangle$.

Вычислим состояние системы на каждом шаге алгоритма Шора.
После шага 1 состояние $|0\rangle|0\rangle$.

На шаге 2 к первому регистру применяется преобразование Адамара.
Получится $\frac{1}{\sqrt{S}} \sum_{k=0}^{S-1} |k\rangle|0\rangle$.

Вычислим состояние системы на каждом шаге алгоритма Шора.

После шага 1 состояние $|0\rangle|0\rangle$.

На шаге 2 к первому регистру применяется преобразование Адамара.

Получится $\frac{1}{\sqrt{S}} \sum_{k=0}^{S-1} |k\rangle|0\rangle$.

На шаге 3 применяется оператор U_f . Получим $\frac{1}{\sqrt{S}} \sum_{k=0}^{S-1} |k\rangle|f(k)\rangle$.

Вычислим состояние системы на каждом шаге алгоритма Шора.

После шага 1 состояние $|0\rangle|0\rangle$.

На шаге 2 к первому регистру применяется преобразование Адамара.

Получится $\frac{1}{\sqrt{S}} \sum_{k=0}^{S-1} |k\rangle|0\rangle$.

На шаге 3 применяется оператор U_f . Получим $\frac{1}{\sqrt{S}} \sum_{k=0}^{S-1} |k\rangle|f(k)\rangle$.

На шаге 4 к первому регистру применяется преобразование Фурье F_S .

Получим $\frac{1}{\sqrt{S}} \sum_{k=0}^{S-1} F_S |k\rangle|f(k)\rangle = \frac{1}{S} \sum_{u=0}^{S-1} |u\rangle \left(\sum_{k=0}^{S-1} e^{\frac{2\pi i u k}{S}} |f(k)\rangle \right)$.

Вычислим состояние системы на каждом шаге алгоритма Шора.
После шага 1 состояние $|0\rangle|0\rangle$.

На шаге 2 к первому регистру применяется преобразование Адамара.
Получится $\frac{1}{\sqrt{S}} \sum_{k=0}^{S-1} |k\rangle|0\rangle$.

На шаге 3 применяется оператор U_f . Получим $\frac{1}{\sqrt{S}} \sum_{k=0}^{S-1} |k\rangle|f(k)\rangle$.

На шаге 4 к первому регистру применяется преобразование Фурье F_S .
Получим $\frac{1}{\sqrt{S}} \sum_{k=0}^{S-1} F_S |k\rangle|f(k)\rangle = \frac{1}{S} \sum_{u=0}^{S-1} |u\rangle \left(\sum_{k=0}^{S-1} e^{\frac{2\pi i u k}{S}} |f(k)\rangle \right)$.

Если r — период числа y по модулю N , то $f(k+r) \equiv y^{k+r} \equiv y^k y^r \equiv y^k \equiv f(k) \pmod{N}$, т.е. $f(k+r) = f(k)$.

Вычислим состояние системы на каждом шаге алгоритма Шора.

После шага 1 состояние $|0\rangle|0\rangle$.

На шаге 2 к первому регистру применяется преобразование Адамара.

Получится $\frac{1}{\sqrt{S}} \sum_{k=0}^{S-1} |k\rangle|0\rangle$.

На шаге 3 применяется оператор U_f . Получим $\frac{1}{\sqrt{S}} \sum_{k=0}^{S-1} |k\rangle|f(k)\rangle$.

На шаге 4 к первому регистру применяется преобразование Фурье F_S .

Получим $\frac{1}{\sqrt{S}} \sum_{k=0}^{S-1} F_S|k\rangle|f(k)\rangle = \frac{1}{S} \sum_{u=0}^{S-1} |u\rangle \left(\sum_{k=0}^{S-1} e^{\frac{2\pi i u k}{S}} |f(k)\rangle \right)$.

Если r — период числа y по модулю N , то $f(k+r) \equiv y^{k+r} \equiv y^k y^r \equiv y^k \equiv f(k) \pmod{N}$, т.е. $f(k+r) = f(k)$. Пусть $k = m + rj$, где $0 \leq m < r$, $0 \leq j < A$, где $A := \lceil \frac{S}{r} \rceil$.

Вычислим состояние системы на каждом шаге алгоритма Шора.

После шага 1 состояние $|0\rangle|0\rangle$.

На шаге 2 к первому регистру применяется преобразование Адамара.

Получится $\frac{1}{\sqrt{S}} \sum_{k=0}^{S-1} |k\rangle|0\rangle$.

На шаге 3 применяется оператор U_f . Получим $\frac{1}{\sqrt{S}} \sum_{k=0}^{S-1} |k\rangle|f(k)\rangle$.

На шаге 4 к первому регистру применяется преобразование Фурье F_S .

Получим $\frac{1}{\sqrt{S}} \sum_{k=0}^{S-1} F_S |k\rangle|f(k)\rangle = \frac{1}{S} \sum_{u=0}^{S-1} |u\rangle \left(\sum_{k=0}^{S-1} e^{\frac{2\pi i uk}{S}} |f(k)\rangle \right)$.

Если r — период числа y по модулю N , то $f(k+r) \equiv y^{k+r} \equiv y^k y^r \equiv y^k \equiv f(k) \pmod{N}$, т.е. $f(k+r) = f(k)$. Пусть $k = m + rj$, где $0 \leq m < r$, $0 \leq j < A$,

где $A := \lceil \frac{S}{r} \rceil$. Введем индикатор $I(m + rj < S) := \begin{cases} 1, & \text{если } m + rj < S, \\ 0, & \text{если } m + rj \geq S. \end{cases}$

Вычислим состояние системы на каждом шаге алгоритма Шора.

После шага 1 состояние $|0\rangle|0\rangle$.

На шаге 2 к первому регистру применяется преобразование Адамара.

Получится $\frac{1}{\sqrt{S}} \sum_{k=0}^{S-1} |k\rangle|0\rangle$.

На шаге 3 применяется оператор U_f . Получим $\frac{1}{\sqrt{S}} \sum_{k=0}^{S-1} |k\rangle|f(k)\rangle$.

На шаге 4 к первому регистру применяется преобразование Фурье F_S .

Получим $\frac{1}{\sqrt{S}} \sum_{k=0}^{S-1} F_S |k\rangle|f(k)\rangle = \frac{1}{S} \sum_{u=0}^{S-1} |u\rangle \left(\sum_{k=0}^{S-1} e^{\frac{2\pi i u k}{S}} |f(k)\rangle \right)$.

Если r — период числа y по модулю N , то $f(k+r) \equiv y^{k+r} \equiv y^k y^r \equiv y^k \equiv f(k) \pmod{N}$, т.е. $f(k+r) = f(k)$. Пусть $k = m + rj$, где $0 \leq m < r$, $0 \leq j < A$,

где $A := \lceil \frac{S}{r} \rceil$. Введем индикатор $I(m + rj < S) := \begin{cases} 1, & \text{если } m + rj < S, \\ 0, & \text{если } m + rj \geq S. \end{cases}$

Группируя слагаемые с одинаковым значением $f(k)$, получаем

$$\begin{aligned} \frac{1}{S} \sum_{u=0}^{S-1} |u\rangle \left(\sum_{k=0}^{S-1} e^{\frac{2\pi i u k}{S}} |f(k)\rangle \right) &= \\ &= \frac{1}{S} \sum_{u=0}^{S-1} |u\rangle \left(\sum_{m=0}^{r-1} |f(m)\rangle e^{\frac{2\pi i u m}{S}} \left(\sum_{j=0}^{A-1} e^{\frac{2\pi i u j r}{S}} I(m + rj < S) \right) \right). \end{aligned}$$

Положим $b_{u,m} := \frac{1}{S} \sum_{j=0}^{A-1} e^{\frac{2\pi iujr}{S}} I(m+rj < S)$, тогда выражение, описывающее состояние системы после шага 4, можно записать как

$$\sum_{u=0}^{S-1} |u\rangle \left(\sum_{m=0}^{r-1} |f(m)\rangle e^{\frac{2\pi ium}{S}} b_{u,m} \right). \quad (\star)$$

Положим $b_{u,m} := \frac{1}{S} \sum_{j=0}^{A-1} e^{\frac{2\pi iujr}{S}} I(m+rj < S)$, тогда выражение, описывающее состояние системы после шага 4, можно записать как

$$\sum_{u=0}^{S-1} |u\rangle \left(\sum_{m=0}^{r-1} |f(m)\rangle e^{\frac{2\pi ium}{S}} b_{u,m} \right). \quad (\star)$$

Напомним: $A = \lceil \frac{S}{r} \rceil$. Если $A = \frac{S}{r}$, то $I(m+rj < S) = 1$ при $m < r$ и $j < A$.

Положим $b_{u,m} := \frac{1}{S} \sum_{j=0}^{A-1} e^{\frac{2\pi iujr}{S}} I(m + rj < S)$, тогда выражение, описывающее состояние системы после шага 4, можно записать как

$$\sum_{u=0}^{S-1} |u\rangle \left(\sum_{m=0}^{r-1} |f(m)\rangle e^{\frac{2\pi ium}{S}} b_{u,m} \right). \quad (\star)$$

Напомним: $A = \lceil \frac{S}{r} \rceil$. Если $A = \frac{S}{r}$, то $I(m + rj < S) = 1$ при $m < r$ и $j < A$. Действительно, если $j < A$, то $j \leq A - 1$ и

$$m + rj \leq m + r(A - 1) = m + r \left(\frac{S}{r} - 1 \right) = m + S - r < S.$$

Положим $b_{u,m} := \frac{1}{S} \sum_{j=0}^{A-1} e^{\frac{2\pi iujr}{S}} I(m+rj < S)$, тогда выражение, описывающее состояние системы после шага 4, можно записать как

$$\sum_{u=0}^{S-1} |u\rangle \left(\sum_{m=0}^{r-1} |f(m)\rangle e^{\frac{2\pi ium}{S}} b_{u,m} \right). \quad (\star)$$

Напомним: $A = \lceil \frac{S}{r} \rceil$. Если $A = \frac{S}{r}$, то $I(m+rj < S) = 1$ при $m < r$ и $j < A$. Действительно, если $j < A$, то $j \leq A-1$ и

$$m+rj \leq m+r(A-1) = m+r\left(\frac{S}{r}-1\right) = m+S-r < S.$$

Допустим, что $A > \frac{S}{r}$. Тогда $A-1 < \frac{S}{r}$, откуда $S = (A-1)r + k$ для некоторого k такого, что $0 < k \leq r-1$.

Положим $b_{u,m} := \frac{1}{S} \sum_{j=0}^{A-1} e^{\frac{2\pi iujr}{S}} I(m+rj < S)$, тогда выражение, описывающее состояние системы после шага 4, можно записать как

$$\sum_{u=0}^{S-1} |u\rangle \left(\sum_{m=0}^{r-1} |f(m)\rangle e^{\frac{2\pi ium}{S}} b_{u,m} \right). \quad (\star)$$

Напомним: $A = \lceil \frac{S}{r} \rceil$. Если $A = \frac{S}{r}$, то $I(m+rj < S) = 1$ при $m < r$ и $j < A$. Действительно, если $j < A$, то $j \leq A-1$ и

$$m+rj \leq m+r(A-1) = m+r\left(\frac{S}{r}-1\right) = m+S-r < S.$$

Допустим, что $A > \frac{S}{r}$. Тогда $A-1 < \frac{S}{r}$, откуда $S = (A-1)r + k$ для некоторого k такого, что $0 < k \leq r-1$. Поэтому $I(m+rj < S) = 1$ для всех m и j , кроме $j = A-1$ и $k \leq m \leq r-1$.

Положим $b_{u,m} := \frac{1}{S} \sum_{j=0}^{A-1} e^{\frac{2\pi iujr}{S}} I(m+rj < S)$, тогда выражение, описывающее состояние системы после шага 4, можно записать как

$$\sum_{u=0}^{S-1} |u\rangle \left(\sum_{m=0}^{r-1} |f(m)\rangle e^{\frac{2\pi ium}{S}} b_{u,m} \right). \quad (*)$$

Напомним: $A = \lceil \frac{S}{r} \rceil$. Если $A = \frac{S}{r}$, то $I(m+rj < S) = 1$ при $m < r$ и $j < A$. Действительно, если $j < A$, то $j \leq A-1$ и

$$m+rj \leq m+r(A-1) = m+r\left(\frac{S}{r}-1\right) = m+S-r < S.$$

Допустим, что $A > \frac{S}{r}$. Тогда $A-1 < \frac{S}{r}$, откуда $S = (A-1)r+k$ для некоторого k такого, что $0 < k \leq r-1$. Поэтому $I(m+rj < S) = 1$ для всех m и j , кроме $j = A-1$ и $k \leq m \leq r-1$. Число таких исключений мало по сравнению с общим числом слагаемых, поэтому сумму $b_{u,m} = \frac{1}{S} \sum_{j=0}^{A-1} e^{\frac{2\pi iujr}{S}} I(m+rj < S)$ можно приблизить суммой $b_u := \frac{1}{S} \sum_{j=0}^{A-1} e^{\frac{2\pi iujr}{S}}$, которую легче подсчитать.

Положим $b_{u,m} := \frac{1}{S} \sum_{j=0}^{A-1} e^{\frac{2\pi iujr}{S}} I(m+rj < S)$, тогда выражение, описывающее состояние системы после шага 4, можно записать как

$$\sum_{u=0}^{S-1} |u\rangle \left(\sum_{m=0}^{r-1} |f(m)\rangle e^{\frac{2\pi ium}{S}} b_{u,m} \right). \quad (\star)$$

Напомним: $A = \lceil \frac{S}{r} \rceil$. Если $A = \frac{S}{r}$, то $I(m+rj < S) = 1$ при $m < r$ и $j < A$. Действительно, если $j < A$, то $j \leq A-1$ и

$$m+rj \leq m+r(A-1) = m+r\left(\frac{S}{r}-1\right) = m+S-r < S.$$

Допустим, что $A > \frac{S}{r}$. Тогда $A-1 < \frac{S}{r}$, откуда $S = (A-1)r+k$ для некоторого k такого, что $0 < k \leq r-1$. Поэтому $I(m+rj < S) = 1$ для всех m и j , кроме $j = A-1$ и $k \leq m \leq r-1$. Число таких исключений мало по сравнению с общим числом слагаемых, поэтому сумму $b_{u,m} = \frac{1}{S} \sum_{j=0}^{A-1} e^{\frac{2\pi iujr}{S}} I(m+rj < S)$ можно приблизить суммой $b_u := \frac{1}{S} \sum_{j=0}^{A-1} e^{\frac{2\pi iujr}{S}}$, которую легче подсчитать. Итак, заменим (\star) на $\sum_{u=0}^{S-1} \sum_{m=0}^{r-1} b_u e^{\frac{2\pi ium}{S}} |u\rangle |f(m)\rangle$.

Положим $b_{u,m} := \frac{1}{S} \sum_{j=0}^{A-1} e^{\frac{2\pi iujr}{S}} I(m+rj < S)$, тогда выражение, описывающее состояние системы после шага 4, можно записать как

$$\sum_{u=0}^{S-1} |u\rangle \left(\sum_{m=0}^{r-1} |f(m)\rangle e^{\frac{2\pi ium}{S}} b_{u,m} \right). \quad (*)$$

Напомним: $A = \lceil \frac{S}{r} \rceil$. Если $A = \frac{S}{r}$, то $I(m+rj < S) = 1$ при $m < r$ и $j < A$. Действительно, если $j < A$, то $j \leq A-1$ и

$$m+rj \leq m+r(A-1) = m+r\left(\frac{S}{r}-1\right) = m+S-r < S.$$

Допустим, что $A > \frac{S}{r}$. Тогда $A-1 < \frac{S}{r}$, откуда $S = (A-1)r+k$ для некоторого k такого, что $0 < k \leq r-1$. Поэтому $I(m+rj < S) = 1$ для всех m и j , кроме $j = A-1$ и $k \leq m \leq r-1$. Число таких исключений мало по сравнению с общим числом слагаемых, поэтому сумму $b_{u,m} = \frac{1}{S} \sum_{j=0}^{A-1} e^{\frac{2\pi iujr}{S}} I(m+rj < S)$ можно приблизить суммой $b_u := \frac{1}{S} \sum_{j=0}^{A-1} e^{\frac{2\pi iujr}{S}}$, которую легче подсчитать. Итак, заменим (*) на $\sum_{u=0}^{S-1} \sum_{m=0}^{r-1} b_u e^{\frac{2\pi ium}{S}} |u\rangle |f(m)\rangle$. Замерив первый регистр, получим $|u\rangle$ с вероятностью $r|b_u|^2$.

Положим $b_{u,m} := \frac{1}{S} \sum_{j=0}^{A-1} e^{\frac{2\pi iujr}{S}} I(m+rj < S)$, тогда выражение, описывающее состояние системы после шага 4, можно записать как

$$\sum_{u=0}^{S-1} |u\rangle \left(\sum_{m=0}^{r-1} |f(m)\rangle e^{\frac{2\pi ium}{S}} b_{u,m} \right). \quad (*)$$

Напомним: $A = \lceil \frac{S}{r} \rceil$. Если $A = \frac{S}{r}$, то $I(m+rj < S) = 1$ при $m < r$ и $j < A$. Действительно, если $j < A$, то $j \leq A-1$ и

$$m+rj \leq m+r(A-1) = m+r\left(\frac{S}{r}-1\right) = m+S-r < S.$$

Допустим, что $A > \frac{S}{r}$. Тогда $A-1 < \frac{S}{r}$, откуда $S = (A-1)r+k$ для некоторого k такого, что $0 < k \leq r-1$. Поэтому $I(m+rj < S) = 1$ для всех m и j , кроме $j = A-1$ и $k \leq m \leq r-1$. Число таких исключений мало по сравнению с общим числом слагаемых, поэтому сумму $b_{u,m} = \frac{1}{S} \sum_{j=0}^{A-1} e^{\frac{2\pi iujr}{S}} I(m+rj < S)$ можно приблизить суммой $b_u := \frac{1}{S} \sum_{j=0}^{A-1} e^{\frac{2\pi iujr}{S}}$, которую легче подсчитать. Итак, заменим (*) на $\sum_{u=0}^{S-1} \sum_{m=0}^{r-1} b_u e^{\frac{2\pi ium}{S}} |u\rangle |f(m)\rangle$. Замерив первый регистр, получим $|u\rangle$ с вероятностью $r|b_u|^2$. Теперь по u нужно найти r .

Мы подсчитаем, что вероятность получить $|u\rangle$, для которого существует такое число k , что

$$-\frac{r}{2} \leq ur - kS \leq \frac{r}{2}, \quad (*)$$

не меньше $\frac{1}{r} \frac{4}{\pi^2} \left(1 - \frac{2}{N}\right) \geq \frac{0.4}{r}$, а число таких u примерно равно r .

Мы подсчитаем, что вероятность получить $|u\rangle$, для которого существует такое число k , что

$$-\frac{r}{2} \leq ur - kS \leq \frac{r}{2}, \quad (*)$$

не меньше $\frac{1}{r} \frac{4}{\pi^2} \left(1 - \frac{2}{N}\right) \geq \frac{0.4}{r}$, а число таких u примерно равно r .

Поэтому вероятность получить один из таких векторов $|u\rangle$ не меньше 0.4.

Мы подсчитаем, что вероятность получить $|u\rangle$, для которого существует такое число k , что

$$-\frac{r}{2} \leq ur - kS \leq \frac{r}{2}, \quad (*)$$

не меньше $\frac{1}{r} \frac{4}{\pi^2} \left(1 - \frac{2}{N}\right) \geq \frac{0.4}{r}$, а число таких u примерно равно r .

Поэтому вероятность получить один из таких векторов $|u\rangle$ не меньше 0.4.

Неравенство (*) можно переписать так:

$$\left| \frac{u}{S} - \frac{k}{r} \right| \leq \frac{1}{2S} < \frac{1}{2N^2}.$$

Мы подсчитаем, что вероятность получить $|u\rangle$, для которого существует такое число k , что

$$-\frac{r}{2} \leq ur - kS \leq \frac{r}{2}, \quad (*)$$

не меньше $\frac{1}{r} \frac{4}{\pi^2} \left(1 - \frac{2}{N}\right) \geq \frac{0.4}{r}$, а число таких u примерно равно r .

Поэтому вероятность получить один из таких векторов $|u\rangle$ не меньше 0.4.

Неравенство (*) можно переписать так:

$$\left| \frac{u}{S} - \frac{k}{r} \right| \leq \frac{1}{2S} < \frac{1}{2N^2}.$$

Итак, мы приближаем *известную* дробь $\frac{u}{S}$ *неизвестной* дробью $\frac{k}{r}$ со знаменателем $r < N$ с точностью, лучшей, чем $\frac{1}{2N^2}$.

Мы подсчитаем, что вероятность получить $|u\rangle$, для которого существует такое число k , что

$$-\frac{r}{2} \leq ur - kS \leq \frac{r}{2}, \quad (*)$$

не меньше $\frac{1}{r} \frac{4}{\pi^2} \left(1 - \frac{2}{N}\right) \geq \frac{0.4}{r}$, а число таких u примерно равно r .

Поэтому вероятность получить один из таких векторов $|u\rangle$ не меньше 0.4.

Неравенство (*) можно переписать так:

$$\left| \frac{u}{S} - \frac{k}{r} \right| \leq \frac{1}{2S} < \frac{1}{2N^2}.$$

Итак, мы приближаем *известную* дробь $\frac{u}{S}$ *неизвестной* дробью $\frac{k}{r}$ со знаменателем $r < N$ с точностью, лучшей, чем $\frac{1}{2N^2}$. Если такая дробь $\frac{k}{r}$ существует, то она определяется однозначно и равная ей *несократимая* дробь может быть вычислена за полиномиальное время от длины записи N с помощью известного в теории чисел алгоритма.

Мы подсчитаем, что вероятность получить $|u\rangle$, для которого существует такое число k , что

$$-\frac{r}{2} \leq ur - kS \leq \frac{r}{2}, \quad (*)$$

не меньше $\frac{1}{r} \frac{4}{\pi^2} \left(1 - \frac{2}{N}\right) \geq \frac{0.4}{r}$, а число таких u примерно равно r .

Поэтому вероятность получить один из таких векторов $|u\rangle$ не меньше 0.4.

Неравенство (*) можно переписать так:

$$\left| \frac{u}{S} - \frac{k}{r} \right| \leq \frac{1}{2S} < \frac{1}{2N^2}.$$

Итак, мы приближаем *известную* дробь $\frac{u}{S}$ *неизвестной* дробью $\frac{k}{r}$ со знаменателем $r < N$ с точностью, лучшей, чем $\frac{1}{2N^2}$. Если такая дробь $\frac{k}{r}$ существует, то она определяется однозначно и равная ей *несократимая* дробь может быть вычислена за полиномиальное время от длины записи N с помощью известного в теории чисел алгоритма. Можно взять в качестве r знаменатель этой несократимой дроби.

Мы подсчитаем, что вероятность получить $|u\rangle$, для которого существует такое число k , что

$$-\frac{r}{2} \leq ur - kS \leq \frac{r}{2}, \quad (*)$$

не меньше $\frac{1}{r} \frac{4}{\pi^2} \left(1 - \frac{2}{N}\right) \geq \frac{0.4}{r}$, а число таких u примерно равно r .

Поэтому вероятность получить один из таких векторов $|u\rangle$ не меньше 0.4.

Неравенство (*) можно переписать так:

$$\left| \frac{u}{S} - \frac{k}{r} \right| \leq \frac{1}{2S} < \frac{1}{2N^2}.$$

Итак, мы приближаем *известную* дробь $\frac{u}{S}$ *неизвестной* дробью $\frac{k}{r}$ со знаменателем $r < N$ с точностью, лучшей, чем $\frac{1}{2N^2}$. Если такая дробь $\frac{k}{r}$ существует, то она определяется однозначно и равная ей *несократимая* дробь может быть вычислена за полиномиальное время от длины записи N с помощью известного в теории чисел алгоритма. Можно взять в качестве r знаменатель этой несократимой дроби. Если нам повезло и $(k, r) = 1$, верное значение r найдено.

Мы подсчитаем, что вероятность получить $|u\rangle$, для которого существует такое число k , что

$$-\frac{r}{2} \leq ur - kS \leq \frac{r}{2}, \quad (*)$$

не меньше $\frac{1}{r} \frac{4}{\pi^2} \left(1 - \frac{2}{N}\right) \geq \frac{0.4}{r}$, а число таких u примерно равно r .

Поэтому вероятность получить один из таких векторов $|u\rangle$ не меньше 0.4.

Неравенство (*) можно переписать так:

$$\left| \frac{u}{S} - \frac{k}{r} \right| \leq \frac{1}{2S} < \frac{1}{2N^2}.$$

Итак, мы приближаем *известную* дробь $\frac{u}{S}$ *неизвестной* дробью $\frac{k}{r}$ со знаменателем $r < N$ с точностью, лучшей, чем $\frac{1}{2N^2}$. Если такая дробь $\frac{k}{r}$ существует, то она определяется однозначно и равная ей *несократимая* дробь может быть вычислена за полиномиальное время от длины записи N с помощью известного в теории чисел алгоритма. Можно взять в качестве r знаменатель этой несократимой дроби. Если нам повезло и $(k, r) = 1$, верное значение r найдено. Если не повезло, верное значение r — какое-то кратное знаменателя, и можно пробовать эти кратные или начать заново.

Если считать, что числитель k дроби $\frac{k}{r} < 1$ — равномерно распределённое случайное число, то вероятность того, что $(k, r) = 1$, равна $\frac{\varphi(r)}{r}$.

Если считать, что числитель k дроби $\frac{k}{r} < 1$ — равномерно распределённое случайное число, то вероятность того, что $(k, r) = 1$, равна $\frac{\varphi(r)}{r}$.

Последняя дробь обычно близка к 1. В теории чисел доказывается, что $\overline{\lim}_{n \rightarrow \infty} \frac{\varphi(n)}{n} = 1$ и $\frac{\varphi(n)}{n^{1-\delta}} \rightarrow \infty$ при $n \rightarrow \infty$ для любого $\delta > 0$.

Если считать, что числитель k дроби $\frac{k}{r} < 1$ — равномерно распределённое случайное число, то вероятность того, что $(k, r) = 1$, равна $\frac{\varphi(r)}{r}$.

Последняя дробь обычно близка к 1. В теории чисел доказывается, что $\overline{\lim}_{n \rightarrow \infty} \frac{\varphi(n)}{n} = 1$ и $\frac{\varphi(n)}{n^{1-\delta}} \rightarrow \infty$ при $n \rightarrow \infty$ для любого $\delta > 0$.

Но для нас важнее оценка снизу. Она такова: при $r > 2$

$$\frac{\varphi(r)}{r} > \frac{1}{e^\gamma \log \log r + \frac{3}{\log \log r}},$$

где $\gamma = 0.5772\dots$ — константа Эйлера, т.е. $\gamma = \lim_{n \rightarrow \infty} (-\ln n + \sum_{k=1}^n \frac{1}{k})$.

Если считать, что числитель k дроби $\frac{k}{r} < 1$ — равномерно распределённое случайное число, то вероятность того, что $(k, r) = 1$, равна $\frac{\varphi(r)}{r}$.

Последняя дробь обычно близка к 1. В теории чисел доказывается, что $\overline{\lim}_{n \rightarrow \infty} \frac{\varphi(n)}{n} = 1$ и $\frac{\varphi(n)}{n^{1-\delta}} \rightarrow \infty$ при $n \rightarrow \infty$ для любого $\delta > 0$.

Но для нас важнее оценка снизу. Она такова: при $r > 2$

$$\frac{\varphi(r)}{r} > \frac{1}{e^\gamma \log \log r + \frac{3}{\log \log r}},$$

где $\gamma = 0.5772\dots$ — константа Эйлера, т.е. $\gamma = \lim_{n \rightarrow \infty} (-\ln n + \sum_{k=1}^n \frac{1}{k})$.

Итак, вероятность того, что $(k, r) = 1$, не меньше, чем $\frac{e^{-\gamma}}{\log \log N}$.

Если считать, что числитель k дроби $\frac{k}{r} < 1$ — равномерно распределённое случайное число, то вероятность того, что $(k, r) = 1$, равна $\frac{\varphi(r)}{r}$.

Последняя дробь обычно близка к 1. В теории чисел доказывается, что $\overline{\lim}_{n \rightarrow \infty} \frac{\varphi(n)}{n} = 1$ и $\frac{\varphi(n)}{n^{1-\delta}} \rightarrow \infty$ при $n \rightarrow \infty$ для любого $\delta > 0$.

Но для нас важнее оценка снизу. Она такова: при $r > 2$

$$\frac{\varphi(r)}{r} > \frac{1}{e^\gamma \log \log r + \frac{3}{\log \log r}},$$

где $\gamma = 0.5772\dots$ — константа Эйлера, т.е. $\gamma = \lim_{n \rightarrow \infty} (-\ln n + \sum_{k=1}^n \frac{1}{k})$.

Итак, вероятность того, что $(k, r) = 1$, не меньше, чем $\frac{e^{-\gamma}}{\log \log N}$. Значит, запуская алгоритм Шора $\log \log N$ раз, мы определим верное значение r с вероятностью по крайней мере

$$\underbrace{0.5}_{\text{нужное } y} \cdot \underbrace{0.4}_{\text{нужное } u} \cdot \underbrace{e^{-\gamma} (= 0.56)}_{\text{нужное } k} > 0.1.$$

- Мы доказали, что вероятность выбрать взаимно простое с N число y с периодом $2s$ таким, что $y^s + 1$ не делится на N , не меньше 0.5.

- Мы доказали, что вероятность выбрать взаимно простое с N число u с периодом $2s$ таким, что $u^s + 1$ не делится на N , не меньше 0.5.
- Нужно проверить, что вероятность получить при измерении системы на шаге 5 алгоритма Шора один из векторов $|u\rangle$, для которых существует такое k , что $-\frac{r}{2} \leq ur - kS \leq \frac{r}{2}$, не меньше 0.4.

- Мы доказали, что вероятность выбрать взаимно простое с N число u с периодом $2s$ таким, что $u^s + 1$ не делится на N , не меньше 0.5.
- Нужно проверить, что вероятность получить при измерении системы на шаге 5 алгоритма Шора один из векторов $|u\rangle$, для которых существует такое k , что $-\frac{r}{2} \leq ur - kS \leq \frac{r}{2}$, не меньше 0.4.
- Нужно объяснить, как построить за полиномиальное от $\log N$ время несократимую дробь, равную $\frac{k}{r}$, из условия $\left| \frac{u}{S} - \frac{k}{r} \right| < \frac{1}{2N^2}$.

- Мы доказали, что вероятность выбрать взаимно простое с N число u с периодом $2s$ таким, что $u^s + 1$ не делится на N , не меньше 0.5.
- Нужно проверить, что вероятность получить при измерении системы на шаге 5 алгоритма Шора один из векторов $|u\rangle$, для которых существует такое k , что $-\frac{r}{2} \leq ur - kS \leq \frac{r}{2}$, не меньше 0.4.
- Нужно объяснить, как построить за полиномиальное от $\log N$ время несократимую дробь, равную $\frac{k}{r}$, из условия $\left| \frac{u}{S} - \frac{k}{r} \right| < \frac{1}{2N^2}$.
- Нужно обосновать нижнюю оценку на $\frac{\varphi(r)}{r}$ (но эту проверку я опущу).