

Алгоритм Шора, часть I

М. В. Волков

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

2020/2021 учебный год

Дано натуральное число N , о котором заранее известно, что оно есть произведение двух простых чисел p и q .

Дано натуральное число N , о котором заранее известно, что оно есть произведение двух простых чисел p и q .

Требуется найти p и q за время, полиномиальное *от длины записи* числа N , т.е. от $\log N$.

Дано натуральное число N , о котором заранее известно, что оно есть произведение двух простых чисел p и q .

Требуется найти p и q за время, полиномиальное *от длины записи* числа N , т.е. от $\log N$.

Задача факторизации (разложения на множители) имеет огромное практическое значение, так как на допущении о ее сложности основана широко используемая криптосистема RSA.

Дано натуральное число N , о котором заранее известно, что оно есть произведение двух простых чисел p и q .

Требуется найти p и q за время, полиномиальное *от длины записи* числа N , т.е. от $\log N$.

Задача факторизации (разложения на множители) имеет огромное практическое значение, так как на допущении о ее сложности основана широко используемая криптосистема RSA.

Лучшие из известных классических алгоритмов для задачи факторизации работают за время $N^{\frac{1}{4}}$.

Дано натуральное число N , о котором заранее известно, что оно есть произведение двух простых чисел p и q .

Требуется найти p и q за время, полиномиальное *от длины записи* числа N , т.е. от $\log N$.

Задача факторизации (разложения на множители) имеет огромное практическое значение, так как на допущении о ее сложности основана широко используемая криптосистема RSA.

Лучшие из известных классических алгоритмов для задачи факторизации работают за время $N^{\frac{1}{4}}$.

Питер Шор в 1994 г. предложил для нее квантовый вероятностный алгоритм, который работает за полиномиальное от $\log N$ время.

Дано натуральное число N , о котором заранее известно, что оно есть произведение двух простых чисел p и q .

Требуется найти p и q за время, полиномиальное *от длины записи* числа N , т.е. от $\log N$.

Задача факторизации (разложения на множители) имеет огромное практическое значение, так как на допущении о ее сложности основана широко используемая криптосистема RSA.

Лучшие из известных классических алгоритмов для задачи факторизации работают за время $N^{\frac{1}{4}}$.

Питер Шор в 1994 г. предложил для нее квантовый вероятностный алгоритм, который работает за полиномиальное от $\log N$ время. В 1998 г. Шор был удостоен премии Невалинны за это достижение.

Берем число $y < N$. Проверяем, верно ли, что $(y, N) = 1$. Алгоритм Евклида позволяет это сделать за время, полиномиальное от $\log N$.

Берем число $y < N$. Проверяем, верно ли, что $(y, N) = 1$. Алгоритм Евклида позволяет это сделать за время, полиномиальное от $\log N$. Если $(y, N) > 1$, нам повезло: мы нашли нетривиальный делитель числа N . Поэтому будем считать, что $(y, N) = 1$.

Берем число $y < N$. Проверяем, верно ли, что $(y, N) = 1$. Алгоритм Евклида позволяет это сделать за время, полиномиальное от $\log N$. Если $(y, N) > 1$, нам повезло: мы нашли нетривиальный делитель числа N . Поэтому будем считать, что $(y, N) = 1$. В этом случае найдется такое натуральное r , что $y^r \equiv 1 \pmod{N}$.

Берем число $y < N$. Проверяем, верно ли, что $(y, N) = 1$. Алгоритм Евклида позволяет это сделать за время, полиномиальное от $\log N$. Если $(y, N) > 1$, нам повезло: мы нашли нетривиальный делитель числа N . Поэтому будем считать, что $(y, N) = 1$.

В этом случае найдется такое натуральное r , что $y^r \equiv 1 \pmod{N}$. Например, $y^{\varphi(N)} \equiv 1 \pmod{N}$, где $\varphi(N)$ — *функция Эйлера*, т.е. число чисел, меньших N и взаимно простых с N (*теорема Эйлера*).

Берем число $y < N$. Проверяем, верно ли, что $(y, N) = 1$. Алгоритм Евклида позволяет это сделать за время, полиномиальное от $\log N$. Если $(y, N) > 1$, нам повезло: мы нашли нетривиальный делитель числа N . Поэтому будем считать, что $(y, N) = 1$. В этом случае найдется такое натуральное r , что $y^r \equiv 1 \pmod{N}$. Например, $y^{\varphi(N)} \equiv 1 \pmod{N}$, где $\varphi(N)$ — *функция Эйлера*, т.е. число чисел, меньших N и взаимно простых с N (*теорема Эйлера*). Наименьшее такое число r называется *периодом* числа y по модулю N .

Берем число $y < N$. Проверяем, верно ли, что $(y, N) = 1$. Алгоритм Евклида позволяет это сделать за время, полиномиальное от $\log N$. Если $(y, N) > 1$, нам повезло: мы нашли нетривиальный делитель числа N . Поэтому будем считать, что $(y, N) = 1$.

В этом случае найдется такое натуральное r , что $y^r \equiv 1 \pmod{N}$. Например, $y^{\varphi(N)} \equiv 1 \pmod{N}$, где $\varphi(N)$ — *функция Эйлера*, т.е. число чисел, меньших N и взаимно простых с N (*теорема Эйлера*).

Наименьшее такое число r называется *периодом* числа y по модулю N .

Допустим, что период числа y по модулю N оказался четным, скажем, $2s$.

Берем число $y < N$. Проверяем, верно ли, что $(y, N) = 1$. Алгоритм Евклида позволяет это сделать за время, полиномиальное от $\log N$.

Если $(y, N) > 1$, нам повезло: мы нашли нетривиальный делитель числа N . Поэтому будем считать, что $(y, N) = 1$.

В этом случае найдется такое натуральное r , что $y^r \equiv 1 \pmod{N}$.

Например, $y^{\varphi(N)} \equiv 1 \pmod{N}$, где $\varphi(N)$ — *функция Эйлера*, т.е. число чисел, меньших N и взаимно простых с N (*теорема Эйлера*).

Наименьшее такое число r называется *периодом* числа y по модулю N .

Допустим, что период числа y по модулю N оказался четным, скажем, $2s$. Тогда $y^{2s} - 1 = (y^s - 1)(y^s + 1)$ делится на N , но $y^s - 1$ не делится на N .

Берем число $y < N$. Проверяем, верно ли, что $(y, N) = 1$. Алгоритм Евклида позволяет это сделать за время, полиномиальное от $\log N$. Если $(y, N) > 1$, нам повезло: мы нашли нетривиальный делитель числа N . Поэтому будем считать, что $(y, N) = 1$.

В этом случае найдется такое натуральное r , что $y^r \equiv 1 \pmod{N}$. Например, $y^{\varphi(N)} \equiv 1 \pmod{N}$, где $\varphi(N)$ — *функция Эйлера*, т.е. число чисел, меньших N и взаимно простых с N (*теорема Эйлера*).

Наименьшее такое число r называется *периодом* числа y по модулю N .

Допустим, что период числа y по модулю N оказался четным, скажем, $2s$. Тогда $y^{2s} - 1 = (y^s - 1)(y^s + 1)$ делится на N , но $y^s - 1$ не делится на N . Допустим, что нам снова повезло, и $y^s + 1$ не делится на N .

Берем число $y < N$. Проверяем, верно ли, что $(y, N) = 1$. Алгоритм Евклида позволяет это сделать за время, полиномиальное от $\log N$. Если $(y, N) > 1$, нам повезло: мы нашли нетривиальный делитель числа N . Поэтому будем считать, что $(y, N) = 1$.

В этом случае найдется такое натуральное r , что $y^r \equiv 1 \pmod{N}$. Например, $y^{\varphi(N)} \equiv 1 \pmod{N}$, где $\varphi(N)$ — *функция Эйлера*, т.е. число чисел, меньших N и взаимно простых с N (*теорема Эйлера*).

Наименьшее такое число r называется *периодом* числа y по модулю N .

Допустим, что период числа y по модулю N оказался четным, скажем, $2s$. Тогда $y^{2s} - 1 = (y^s - 1)(y^s + 1)$ делится на N , но $y^s - 1$ не делится на N . Допустим, что нам снова повезло, и $y^s + 1$ не делится на N . Тогда из

$$(y^s - 1)(y^s + 1) = kN = kprq$$

вытекает, что либо p делит $y^s - 1$, а q делит $y^s + 1$, либо наоборот.

Берем число $y < N$. Проверяем, верно ли, что $(y, N) = 1$. Алгоритм Евклида позволяет это сделать за время, полиномиальное от $\log N$. Если $(y, N) > 1$, нам повезло: мы нашли нетривиальный делитель числа N . Поэтому будем считать, что $(y, N) = 1$.

В этом случае найдется такое натуральное r , что $y^r \equiv 1 \pmod{N}$. Например, $y^{\varphi(N)} \equiv 1 \pmod{N}$, где $\varphi(N)$ — *функция Эйлера*, т.е. число чисел, меньших N и взаимно простых с N (*теорема Эйлера*).

Наименьшее такое число r называется *периодом* числа y по модулю N .

Допустим, что период числа y по модулю N оказался четным, скажем, $2s$. Тогда $y^{2s} - 1 = (y^s - 1)(y^s + 1)$ делится на N , но $y^s - 1$ не делится на N . Допустим, что нам снова повезло, и $y^s + 1$ не делится на N . Тогда из

$$(y^s - 1)(y^s + 1) = kN = kprq$$

вытекает, что либо p делит $y^s - 1$, а q делит $y^s + 1$, либо наоборот. В любом случае, вычислив с помощью алгоритма Евклида $(y^s \pm 1, N)$, мы найдем нетривиальный делитель числа N .

Берем число $y < N$. Проверяем, верно ли, что $(y, N) = 1$. Алгоритм Евклида позволяет это сделать за время, полиномиальное от $\log N$.

Если $(y, N) > 1$, нам повезло: мы нашли нетривиальный делитель числа N . Поэтому будем считать, что $(y, N) = 1$.

В этом случае найдется такое натуральное r , что $y^r \equiv 1 \pmod{N}$.

Например, $y^{\varphi(N)} \equiv 1 \pmod{N}$, где $\varphi(N)$ — *функция Эйлера*, т.е. число чисел, меньших N и взаимно простых с N (*теорема Эйлера*).

Наименьшее такое число r называется *периодом* числа y по модулю N .

Допустим, что *период числа y по модулю N оказался четным*, скажем, $2s$. Тогда $y^{2s} - 1 = (y^s - 1)(y^s + 1)$ делится на N , но $y^s - 1$ не делится на N . Допустим, что нам снова повезло, и *$y^s + 1$ не делится на N* . Тогда из

$$(y^s - 1)(y^s + 1) = kN = kprq$$

вытекает, что либо p делит $y^s - 1$, а q делит $y^s + 1$, либо наоборот.

В любом случае, вычислив с помощью алгоритма Евклида $(y^s \pm 1, N)$, мы найдем нетривиальный делитель числа N .

Чтобы этот подход сработал, нужно, во-первых, угадать с выбором числа y и, во-вторых, уметь вычислять период y по модулю N .

Пусть $N = 15$. Выберем $y = 13$ и подсчитаем период y по модулю N .

Пусть $N = 15$. Выберем $y = 13$ и подсчитаем период y по модулю N .

$$13^2 = 169 \equiv 4 \pmod{15}$$

Пусть $N = 15$. Выберем $y = 13$ и подсчитаем период y по модулю N .

$$13^2 = 169 \equiv 4 \pmod{15}$$

$$13^3 = 4 \cdot 13 = 52 \equiv 7 \pmod{15}$$

Пусть $N = 15$. Выберем $y = 13$ и подсчитаем период y по модулю N .

$$13^2 = 169 \equiv 4 \pmod{15}$$

$$13^3 = 4 \cdot 13 = 52 \equiv 7 \pmod{15}$$

$$13^4 = 7 \cdot 13 = 91 \equiv 1 \pmod{15}$$

Пусть $N = 15$. Выберем $y = 13$ и подсчитаем период y по модулю N .

$$13^2 = 169 \equiv 4 \pmod{15}$$

$$13^3 = 4 \cdot 13 = 52 \equiv 7 \pmod{15}$$

$$13^4 = 7 \cdot 13 = 91 \equiv 1 \pmod{15}$$

Мы видим, что период 13 по модулю 15 равен 4, это четное число. Кроме того, $13^2 + 1 = 170$ не делится на 15.

Пусть $N = 15$. Выберем $y = 13$ и подсчитаем период y по модулю N .

$$13^2 = 169 \equiv 4 \pmod{15}$$

$$13^3 = 4 \cdot 13 = 52 \equiv 7 \pmod{15}$$

$$13^4 = 7 \cdot 13 = 91 \equiv 1 \pmod{15}$$

Мы видим, что период 13 по модулю 15 равен 4, это четное число.

Кроме того, $13^2 + 1 = 170$ не делится на 15.

Значит, наш выбор $y = 13$ был удачным.

Пусть $N = 15$. Выберем $y = 13$ и подсчитаем период y по модулю N .

$$13^2 = 169 \equiv 4 \pmod{15}$$

$$13^3 = 4 \cdot 13 = 52 \equiv 7 \pmod{15}$$

$$13^4 = 7 \cdot 13 = 91 \equiv 1 \pmod{15}$$

Мы видим, что период 13 по модулю 15 равен 4, это четное число.

Кроме того, $13^2 + 1 = 170$ не делится на 15.

Значит, наш выбор $y = 13$ был удачным.

Вычисляя $(168, 15) = 3$ и $(170, 15) = 5$, находим оба множителя числа 15.

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 $2s$ и при том $y^s + 1$ не делится на N .

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 $2s$ и при том $y^s + 1$ не делится на N .

Мы докажем лемму позже. Она гарантирует, что если выбирать $y \in S$ наугад, то вероятность удачного выбора — по крайней мере $\frac{1}{2}$.

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 $2s$ и при том $y^s + 1$ не делится на N .

Мы докажем лемму позже. Она гарантирует, что если выбирать $y \in S$ наугад, то вероятность удачного выбора — по крайней мере $\frac{1}{2}$.

Отметим, что для большинства чисел N вероятность удачного выбора даже больше. Но есть N , для которых эта оценка точна, например, $N = 77$.

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 $2s$ и при том $y^s + 1$ не делится на N .

Мы докажем лемму позже. Она гарантирует, что если выбирать $y \in S$ наугад, то вероятность удачного выбора — по крайней мере $\frac{1}{2}$.

Отметим, что для большинства чисел N вероятность удачного выбора даже больше. Но есть N , для которых эта оценка точна, например, $N = 77$.

Считая, что лемма закрывает проблему выбора y , займемся второй проблемой — вычислением периода y по модулю N .

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 $2s$ и при том $y^s + 1$ не делится на N .

Мы докажем лемму позже. Она гарантирует, что если выбирать $y \in S$ наугад, то вероятность удачного выбора — по крайней мере $\frac{1}{2}$.

Отметим, что для большинства чисел N вероятность удачного выбора даже больше. Но есть N , для которых эта оценка точна, например, $N = 77$.

Считая, что лемма закрывает проблему выбора y , займемся второй проблемой — вычислением периода y по модулю N . Действовать, как в примере выше, — т.е. последовательно вычислять y^2, y^3, y^4, \dots — слишком долго, поскольку период y по модулю N может достигать половины значения функции Эйлера от N , т.е. $\frac{(p-1)(q-1)}{2}$.

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 $2s$ и при том $y^s + 1$ не делится на N .

Мы докажем лемму позже. Она гарантирует, что если выбирать $y \in S$ наугад, то вероятность удачного выбора — по крайней мере $\frac{1}{2}$.

Отметим, что для большинства чисел N вероятность удачного выбора даже больше. Но есть N , для которых эта оценка точна, например, $N = 77$.

Считая, что лемма закрывает проблему выбора y , займемся второй проблемой — вычислением периода y по модулю N . Действовать, как в примере выше, — т.е. последовательно вычислять y^2, y^3, y^4, \dots — слишком долго, поскольку период y по модулю N может достигать половины значения функции Эйлера от N , т.е. $\frac{(p-1)(q-1)}{2}$.

Именно здесь нужно квантовое ускорение.

Выбираем такое n , чтобы $2^n \geq N$ (при $N = 15$ годится $n = 4$).

Выбираем такое n , чтобы $2^n \geq N$ (при $N = 15$ годится $n = 4$).

Работаем с квантовой системой $H := H_{2^n} \otimes H_{2^n}$, где, как обычно, $H_{2^n} = \underbrace{H_2 \otimes \dots \otimes H_2 \otimes H_2}_{n \text{ раз}}$ — это n -я тензорная степень двумерного гильбертова

пространства H_2 . 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 $2^n \geq N$ (при $N = 15$ годится $n = 4$).

Работаем с квантовой системой $H := H_{2^n} \otimes H_{2^n}$, где, как обычно, $H_{2^n} = \underbrace{H_2 \otimes \cdots \otimes H_2 \otimes H_2}_{n \text{ раз}}$ — это n -я тензорная степень двумерного гильбертова

пространства H_2 . 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 состоянии $|0\rangle|0\rangle$.
- 2 Применяем преобразование Адамара R_{2^n} 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_{2^n} к первому регистру:
$$F_{2^n}|k\rangle := \frac{1}{\sqrt{2^n}} \sum_{u=0}^{2^n-1} e^{\frac{2\pi i u k}{2^n}} |u\rangle$$
- 5 Измеряя первый регистр, находим вектор, с помощью которого делаем вывод о периоде y по модулю N .

Отметим два важных отличия алгоритма Шора.

Отметим два важных отличия алгоритма Шора.

Во-первых, оператор U_f связан не с какой-то «секретной» функцией f , а с вполне явной и очевидно вычислимой функцией $f: k \mapsto y^k \pmod{N}$.

Отметим два важных отличия алгоритма Шора.

Во-первых, оператор U_f связан не с какой-то «секретной» функцией f , а с вполне явной и очевидно вычислимой функцией $f: k \mapsto y^k \pmod{N}$.

Во-вторых, возник новый оператор — дискретное преобразование Фурье.

Отметим два важных отличия алгоритма Шора.

Во-первых, оператор U_f связан не с какой-то «секретной» функцией f , а с вполне явной и очевидно вычислимой функцией $f: k \mapsto y^k \pmod{N}$.

Во-вторых, возник новый оператор — дискретное преобразование Фурье.

Роль его объясним ниже, пока же проверим, что F_{2^n} — унитарный оператор.

Отметим два важных отличия алгоритма Шора.

Во-первых, оператор U_f связан не с какой-то «секретной» функцией f , а с вполне явной и очевидно вычислимой функцией $f: k \mapsto y^k \pmod{N}$.

Во-вторых, возник новый оператор — дискретное преобразование Фурье.

Роль его объясним ниже, пока же проверим, что F_{2^n} — унитарный оператор.

$F_{2^n}|k\rangle = \frac{1}{\sqrt{2^n}} \sum_{u=0}^{2^n-1} e^{\frac{2\pi i uk}{2^n}} |u\rangle$, т.е. у матрицы оператора в строке u и столбце k стоит $e^{\frac{2\pi i uk}{2^n}}$.

Отметим два важных отличия алгоритма Шора.

Во-первых, оператор U_f связан не с какой-то «секретной» функцией f , а с вполне явной и очевидно вычислимой функцией $f: k \mapsto y^k \pmod{N}$.

Во-вторых, возник новый оператор — дискретное преобразование Фурье.

Роль его объясним ниже, пока же проверим, что F_{2^n} — унитарный оператор.

$F_{2^n}|k\rangle = \frac{1}{\sqrt{2^n}} \sum_{u=0}^{2^n-1} e^{\frac{2\pi i uk}{2^n}} |u\rangle$, т.е. у матрицы оператора в строке u и столбце k стоит $e^{\frac{2\pi i uk}{2^n}}$. Поэтому у матрицы сопряженного оператора, т.е. у эрмитово сопряженной матрицы, в строке k и столбце u стоит $e^{-\frac{2\pi i uk}{2^n}}$.

Отметим два важных отличия алгоритма Шора.

Во-первых, оператор U_f связан не с какой-то «секретной» функцией f , а с вполне явной и очевидно вычислимой функцией $f: k \mapsto y^k \pmod{N}$.

Во-вторых, возник новый оператор — дискретное преобразование Фурье.

Роль его объясним ниже, пока же проверим, что F_{2^n} — унитарный оператор.

$F_{2^n}|k\rangle = \frac{1}{\sqrt{2^n}} \sum_{u=0}^{2^n-1} e^{\frac{2\pi i u k}{2^n}} |u\rangle$, т.е. у матрицы оператора в строке u и столбце k стоит $e^{\frac{2\pi i u k}{2^n}}$. Поэтому у матрицы сопряженного оператора, т.е. у эрмитово сопряженной матрицы, в строке k и столбце u стоит $e^{-\frac{2\pi i u k}{2^n}}$. Отсюда $F_{2^n}^*|u\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{-\frac{2\pi i u k}{2^n}} |k\rangle$.

Отметим два важных отличия алгоритма Шора.

Во-первых, оператор U_f связан не с какой-то «секретной» функцией f , а с вполне явной и очевидно вычислимой функцией $f: k \mapsto y^k \pmod{N}$.

Во-вторых, возник новый оператор — дискретное преобразование Фурье.

Роль его объясним ниже, пока же проверим, что F_{2^n} — унитарный оператор.

$F_{2^n}|k\rangle = \frac{1}{\sqrt{2^n}} \sum_{u=0}^{2^n-1} e^{\frac{2\pi i u k}{2^n}} |u\rangle$, т.е. у матрицы оператора в строке u и столбце k стоит $e^{\frac{2\pi i u k}{2^n}}$. Поэтому у матрицы сопряженного оператора, т.е. у эрмитово сопряженной матрицы, в строке k и столбце u стоит $e^{-\frac{2\pi i u k}{2^n}}$. Отсюда

$F_{2^n}^*|u\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{-\frac{2\pi i u k}{2^n}} |k\rangle$. Вычислим теперь произведение $F_{2^n}^* F_{2^n}$:

$$\begin{aligned} F_{2^n}^* F_{2^n} |k\rangle &= \frac{1}{\sqrt{2^n}} \sum_{u=0}^{2^n-1} e^{\frac{2\pi i u k}{2^n}} F_{2^n}^* |u\rangle = \frac{1}{2^n} \sum_{u=0}^{2^n-1} e^{\frac{2\pi i u k}{2^n}} \sum_{\ell=0}^{2^n-1} e^{-\frac{2\pi i u \ell}{2^n}} |\ell\rangle = \\ &= \frac{1}{2^n} \sum_{\ell=0}^{2^n-1} \left(\sum_{u=0}^{2^n-1} e^{\frac{2\pi i u (k-\ell)}{2^n}} \right) |\ell\rangle = |k\rangle, \end{aligned}$$

так как $\sum_{u=0}^{2^n-1} e^{\frac{2\pi i u (k-\ell)}{2^n}} = \begin{cases} 2^n, & \text{если } \ell = k, \\ 0, & \text{если } \ell \neq k. \end{cases}$

Отметим два важных отличия алгоритма Шора.

Во-первых, оператор U_f связан не с какой-то «секретной» функцией f , а с вполне явной и очевидно вычислимой функцией $f: k \mapsto y^k \pmod{N}$.

Во-вторых, возник новый оператор — дискретное преобразование Фурье.

Роль его объясним ниже, пока же проверим, что F_{2^n} — унитарный оператор.

$F_{2^n}|k\rangle = \frac{1}{\sqrt{2^n}} \sum_{u=0}^{2^n-1} e^{\frac{2\pi iuk}{2^n}} |u\rangle$, т.е. у матрицы оператора в строке u и столбце k стоит $e^{\frac{2\pi iuk}{2^n}}$. Поэтому у матрицы сопряженного оператора, т.е. у эрмитово сопряженной матрицы, в строке k и столбце u стоит $e^{-\frac{2\pi iuk}{2^n}}$. Отсюда $F_{2^n}^*|u\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{-\frac{2\pi iuk}{2^n}} |k\rangle$. Вычислим теперь произведение $F_{2^n}^*F_{2^n}$:

$$\begin{aligned} F_{2^n}^*F_{2^n}|k\rangle &= \frac{1}{\sqrt{2^n}} \sum_{u=0}^{2^n-1} e^{\frac{2\pi iuk}{2^n}} F_{2^n}^*|u\rangle = \frac{1}{2^n} \sum_{u=0}^{2^n-1} e^{\frac{2\pi iuk}{2^n}} \sum_{\ell=0}^{2^n-1} e^{-\frac{2\pi iu\ell}{2^n}} |\ell\rangle = \\ &= \frac{1}{2^n} \sum_{\ell=0}^{2^n-1} \left(\sum_{u=0}^{2^n-1} e^{\frac{2\pi iu(k-\ell)}{2^n}} \right) |\ell\rangle = |k\rangle, \end{aligned}$$

так как $\sum_{u=0}^{2^n-1} e^{\frac{2\pi iu(k-\ell)}{2^n}} = \begin{cases} 2^n, & \text{если } \ell = k, \\ 0, & \text{если } \ell \neq k. \end{cases}$ Во втором случае вычислена

сумма 2^n членов геометрической прогрессии со знаменателем $e^{\frac{2\pi i(k-\ell)}{2^n}}$.

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 $\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle|0\rangle$.

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 $\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle|0\rangle$.

На шаге 3 применяется оператор U_f . Получим $\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle|f(k)\rangle$.

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 $\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle|0\rangle$.

На шаге 3 применяется оператор U_f . Получим $\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle|f(k)\rangle$.

На шаге 4 к первому регистру применяется преобразование Фурье F_{2^n} .

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

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 $\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle|0\rangle$.

На шаге 3 применяется оператор U_f . Получим $\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle|f(k)\rangle$.

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

Пусть r — период числа y по модулю N . Тогда $f(k+r) \equiv y^{k+r} \equiv y^k y^r \equiv y^k \equiv f(k) \pmod{N}$, 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 $\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle|0\rangle$.

На шаге 3 применяется оператор U_f . Получим $\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle|f(k)\rangle$.

На шаге 4 к первому регистру применяется преобразование Фурье F_{2^n} .

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

Пусть r — период числа y по модулю N . Тогда $f(k+r) \equiv y^{k+r} \equiv y^k y^r \equiv y^k \equiv f(k) \pmod{N}$, т.е. $f(k+r) = f(k)$. Сгруппируем слагаемые с одинаковым значением $f(k)$.

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 $\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle|0\rangle$.

На шаге 3 применяется оператор U_f . Получим $\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle|f(k)\rangle$.

На шаге 4 к первому регистру применяется преобразование Фурье F_{2^n} .

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

Пусть r — период числа y по модулю N . Тогда $f(k+r) \equiv y^{k+r} \equiv y^k y^r \equiv y^k \equiv f(k) \pmod{N}$, т.е. $f(k+r) = f(k)$. Сгруппируем слагаемые с одинаковым значением $f(k)$. Для этого запишем $k = m + jr$, где $0 \leq m < r$, $0 \leq j < \frac{2^n}{r}$.

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 $\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle|0\rangle$.

На шаге 3 применяется оператор U_f . Получим $\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle|f(k)\rangle$.

На шаге 4 к первому регистру применяется преобразование Фурье F_{2^n} .

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

Пусть r — период числа y по модулю N . Тогда $f(k+r) \equiv y^{k+r} \equiv y^k y^r \equiv y^k \equiv f(k) \pmod{N}$, т.е. $f(k+r) = f(k)$. Сгруппируем слагаемые с одинаковым значением $f(k)$. Для этого запишем $k = m + jr$, где $0 \leq m < r$, $0 \leq j < \frac{2^n}{r}$. Тогда $f(k) = f(m)$ и

$$\frac{1}{2^n} \sum_{u=0}^{2^n-1} |u\rangle \left(\sum_{k=0}^{2^n-1} e^{\frac{2\pi i u k}{2^n}} |f(k)\rangle \right) = \frac{1}{2^n} \sum_{u=0}^{2^n-1} |u\rangle \left(\sum_{m=0}^{r-1} |f(m)\rangle e^{\frac{2\pi i u m}{2^n}} \left(\sum_{j=0}^{\frac{2^n}{r}-1} e^{\frac{2\pi i u j r}{2^n}} \right) \right).$$

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 $\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle|0\rangle$.

На шаге 3 применяется оператор U_f . Получим $\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle|f(k)\rangle$.

На шаге 4 к первому регистру применяется преобразование Фурье F_{2^n} .

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

Пусть r — период числа u по модулю N . Тогда $f(k+r) \equiv y^{k+r} \equiv y^k y^r \equiv y^k \equiv f(k) \pmod{N}$, т.е. $f(k+r) = f(k)$. Сгруппируем слагаемые с одинаковым значением $f(k)$. Для этого запишем $k = m + jr$, где $0 \leq m < r$, $0 \leq j < \frac{2^n}{r}$. Тогда $f(k) = f(m)$ и

$$\frac{1}{2^n} \sum_{u=0}^{2^n-1} |u\rangle \left(\sum_{k=0}^{2^n-1} e^{\frac{2\pi i uk}{2^n}} |f(k)\rangle \right) = \frac{1}{2^n} \sum_{u=0}^{2^n-1} |u\rangle \left(\sum_{m=0}^{r-1} |f(m)\rangle e^{\frac{2\pi i um}{2^n}} \left(\sum_{j=0}^{\frac{2^n}{r}-1} e^{\frac{2\pi i ujr}{2^n}} \right) \right).$$

Подсчитаем сумму, выделенную красным цветом.

Если ur делится на 2^n , то $e^{\frac{2\pi iujr}{2^n}} = e^{2\pi ij \frac{ur}{2^n}} = 1$ и $\sum_{j=0}^{\frac{2^n}{r}-1} e^{\frac{2\pi iujr}{2^n}} = \frac{2^n}{r}$.

Если ur делится на 2^n , то $e^{\frac{2\pi iujr}{2^n}} = e^{2\pi ij \frac{ur}{2^n}} = 1$ и $\sum_{j=0}^{\frac{2^n}{r}-1} e^{\frac{2\pi iujr}{2^n}} = \frac{2^n}{r}$.

Если ur не делится на 2^n , то $t := e^{\frac{2\pi iur}{2^n}} \neq 1$ и сумма $\sum_{j=0}^{\frac{2^n}{r}-1} e^{\frac{2\pi iujr}{2^n}}$ вычисляется как сумма $\frac{2^n}{r}$ членов геометрической прогрессии со знаменателем t и первым членом 1 по формуле $\frac{t^{\frac{2^n}{r}} - 1}{t - 1}$.

Если ur делится на 2^n , то $e^{\frac{2\pi iujr}{2^n}} = e^{2\pi ij \frac{ur}{2^n}} = 1$ и $\sum_{j=0}^{\frac{2^n}{r}-1} e^{\frac{2\pi iujr}{2^n}} = \frac{2^n}{r}$.

Если ur не делится на 2^n , то $t := e^{\frac{2\pi iur}{2^n}} \neq 1$ и сумма $\sum_{j=0}^{\frac{2^n}{r}-1} e^{\frac{2\pi iujr}{2^n}}$ вычисляется как сумма $\frac{2^n}{r}$ членов геометрической прогрессии со знаменателем t и первым членом 1 по формуле $\frac{t^{\frac{2^n}{r}} - 1}{t - 1}$. Учитывая, что $t^{\frac{2^n}{r}} = e^{2\pi iur} = 1$, видим, что сумма равна 0.

Если ur делится на 2^n , то $e^{\frac{2\pi iujr}{2^n}} = e^{2\pi ij \frac{ur}{2^n}} = 1$ и $\sum_{j=0}^{\frac{2^n}{r}-1} e^{\frac{2\pi iujr}{2^n}} = \frac{2^n}{r}$.

Если ur не делится на 2^n , то $t := e^{\frac{2\pi iur}{2^n}} \neq 1$ и сумма $\sum_{j=0}^{\frac{2^n}{r}-1} e^{\frac{2\pi iujr}{2^n}}$ вычисляется как сумма $\frac{2^n}{r}$ членов геометрической прогрессии со знаменателем t и первым членом 1 по формуле $\frac{t^{\frac{2^n}{r}} - 1}{t - 1}$. Учитывая, что $t^{\frac{2^n}{r}} = e^{2\pi iu} = 1$, видим, что сумма равна 0.

Итак, $\sum_{j=0}^{\frac{2^n}{r}-1} e^{\frac{2\pi iujr}{2^n}} = \begin{cases} \frac{2^n}{r}, & \text{если } ur \text{ делится на } 2^n, \\ 0, & \text{если } ur \text{ не делится на } 2^n. \end{cases}$ Поэтому состояние системы после шага 4 описывается выражением

$$\frac{1}{2^n} \sum_{u=0}^{2^n-1} |u\rangle \left(\sum_{m=0}^{r-1} |f(m)\rangle e^{\frac{2\pi ium}{2^n}} \left(\sum_{j=0}^{\frac{2^n}{r}-1} e^{\frac{2\pi iujr}{2^n}} \right) \right) = \frac{1}{r} \sum_{2^n|ur} |u\rangle \sum_{m=0}^{r-1} |f(m)\rangle e^{\frac{2\pi ium}{2^n}}.$$

Если ur делится на 2^n , то $e^{\frac{2\pi iujr}{2^n}} = e^{2\pi ij \frac{ur}{2^n}} = 1$ и $\sum_{j=0}^{\frac{2^n}{r}-1} e^{\frac{2\pi iujr}{2^n}} = \frac{2^n}{r}$.

Если ur не делится на 2^n , то $t := e^{\frac{2\pi iur}{2^n}} \neq 1$ и сумма $\sum_{j=0}^{\frac{2^n}{r}-1} e^{\frac{2\pi iujr}{2^n}}$ вычисляется как сумма $\frac{2^n}{r}$ членов геометрической прогрессии со знаменателем t и первым членом 1 по формуле $\frac{t^{\frac{2^n}{r}} - 1}{t - 1}$. Учитывая, что $t^{\frac{2^n}{r}} = e^{2\pi iu} = 1$, видим, что сумма равна 0.

Итак, $\sum_{j=0}^{\frac{2^n}{r}-1} e^{\frac{2\pi iujr}{2^n}} = \begin{cases} \frac{2^n}{r}, & \text{если } ur \text{ делится на } 2^n, \\ 0, & \text{если } ur \text{ не делится на } 2^n. \end{cases}$ Поэтому состояние системы после шага 4 описывается выражением

$$\frac{1}{2^n} \sum_{u=0}^{2^n-1} |u\rangle \left(\sum_{m=0}^{r-1} |f(m)\rangle e^{\frac{2\pi ium}{2^n}} \left(\sum_{j=0}^{\frac{2^n}{r}-1} e^{\frac{2\pi iujr}{2^n}} \right) \right) = \frac{1}{r} \sum_{2^n|ur} |u\rangle \sum_{m=0}^{r-1} |f(m)\rangle e^{\frac{2\pi ium}{2^n}}.$$

Измерение первого регистра на шаге 5 с вероятностью $\frac{1}{r}$ вернет одно из таких u , что число ur делится на 2^n .

Итак, мы получим одно из таких u , что число ug делится на 2^n .

Итак, мы получим одно из таких u , что число ur делится на 2^n .
Напомним, что найти надо r . Какую информацию о r мы можем извлечь?

Итак, мы получим одно из таких u , что число ur делится на 2^n .
Напомним, что найти надо r . Какую информацию о r мы можем извлечь?
Вернемся к примеру с $N = 15$ и $y = 13$. В этом случае мы знаем, что $r = 4$.

Итак, мы получим одно из таких u , что число ur делится на 2^n .
Напомним, что найти надо r . Какую информацию о r мы можем извлечь?
Вернемся к примеру с $N = 15$ и $y = 13$. В этом случае мы знаем, что $r = 4$.
Алгоритм вернет такое u , что ur делится на $2^n = 16$. Поэтому возможны четыре значения $u = 0, 4, 8, 12$.

Итак, мы получим одно из таких u , что число ur делится на 2^n .
Напомним, что найти надо r . Какую информацию о r мы можем извлечь?
Вернемся к примеру с $N = 15$ и $y = 13$. В этом случае мы знаем, что $r = 4$.
Алгоритм вернет такое u , что ur делится на $2^n = 16$. Поэтому возможны четыре значения $u = 0, 4, 8, 12$.
Если $u = 0$, никакого заключения о r извлечь нельзя.

Итак, мы получим одно из таких u , что число ur делится на 2^n .
Напомним, что найти надо r . Какую информацию о r мы можем извлечь?
Вернемся к примеру с $N = 15$ и $y = 13$. В этом случае мы знаем, что $r = 4$.
Алгоритм вернет такое u , что ur делится на $2^n = 16$. Поэтому возможны четыре значения $u = 0, 4, 8, 12$.
Если $u = 0$, никакого заключения о r извлечь нельзя.
Если $u = 4$, из того, что $4r$ делится на 16, можно предположить, что $r = 4$ (что верно).

Итак, мы получим одно из таких u , что число ur делится на 2^n .
Напомним, что найти надо r . Какую информацию о r мы можем извлечь?

Вернемся к примеру с $N = 15$ и $y = 13$. В этом случае мы знаем, что $r = 4$.

Алгоритм вернет такое u , что ur делится на $2^n = 16$. Поэтому возможны четыре значения $u = 0, 4, 8, 12$.

Если $u = 0$, никакого заключения о r извлечь нельзя.

Если $u = 4$, из того, что $4r$ делится на 16, можно предположить, что $r = 4$ (что верно).

Если $u = 8$, из того, что $8r$ делится на 16, можно предположить, что $r = 2$ (что неверно).

Итак, мы получим одно из таких u , что число ur делится на 2^n .
Напомним, что найти надо r . Какую информацию о r мы можем извлечь?

Вернемся к примеру с $N = 15$ и $y = 13$. В этом случае мы знаем, что $r = 4$.

Алгоритм вернет такое u , что ur делится на $2^n = 16$. Поэтому возможны четыре значения $u = 0, 4, 8, 12$.

Если $u = 0$, никакого заключения о r извлечь нельзя.

Если $u = 4$, из того, что $4r$ делится на 16, можно предположить, что $r = 4$ (что верно).

Если $u = 8$, из того, что $8r$ делится на 16, можно предположить, что $r = 2$ (что неверно).

Если $u = 12$, из того, что $12r$ делится на 16, можно предположить, что $r = 4$ (что верно).

Итак, мы получим одно из таких u , что число ur делится на 2^n .
Напомним, что найти надо r . Какую информацию о r мы можем извлечь?

Вернемся к примеру с $N = 15$ и $y = 13$. В этом случае мы знаем, что $r = 4$.

Алгоритм вернет такое u , что ur делится на $2^n = 16$. Поэтому возможны четыре значения $u = 0, 4, 8, 12$.

Если $u = 0$, никакого заключения о r извлечь нельзя.

Если $u = 4$, из того, что $4r$ делится на 16, можно предположить, что $r = 4$ (что верно).

Если $u = 8$, из того, что $8r$ делится на 16, можно предположить, что $r = 2$ (что неверно).

Если $u = 12$, из того, что $12r$ делится на 16, можно предположить, что $r = 4$ (что верно).

Итак, в 50% случаев, мы сможем сделать верный вывод о величине r !

Итак, мы получим одно из таких u , что число ur делится на 2^n .
Напомним, что найти надо r . Какую информацию о r мы можем извлечь?

Вернемся к примеру с $N = 15$ и $y = 13$. В этом случае мы знаем, что $r = 4$.

Алгоритм вернет такое u , что ur делится на $2^n = 16$. Поэтому возможны четыре значения $u = 0, 4, 8, 12$.

Если $u = 0$, никакого заключения о r извлечь нельзя.

Если $u = 4$, из того, что $4r$ делится на 16, можно предположить, что $r = 4$ (что верно).

Если $u = 8$, из того, что $8r$ делится на 16, можно предположить, что $r = 2$ (что неверно).

Если $u = 12$, из того, что $12r$ делится на 16, можно предположить, что $r = 4$ (что верно).

Итак, в 50% случаев, мы сможем сделать верный вывод о величине r !

В случае неудачи (любого сорта) запускаем алгоритм снова.

Теперь понятна роль преобразования Фурье: оно позволяет трансформировать периодичность функции $f: k \mapsto y^k \pmod{N}$ в некоторое свойство коэффициентов, которое мы можем измерить. (Физики в таких случаях говорят о переводе фазы в амплитуду.)

Теперь понятна роль преобразования Фурье: оно позволяет трансформировать периодичность функции $f: k \mapsto y^k \pmod{N}$ в некоторое свойство коэффициентов, которое мы можем измерить. (Физики в таких случаях говорят о переводе фазы в амплитуду.) Коэффициенты в преобразовании Фурье — комплексные корни из 1, и они позволяют описывать периодические процессы с любым данным периодом так же, как $(-1)^n$ позволяет описать периодический процесс с периодом 2.

Теперь понятна роль преобразования Фурье: оно позволяет трансформировать периодичность функции $f: k \mapsto y^k \pmod{N}$ в некоторое свойство коэффициентов, которое мы можем измерить. (Физики в таких случаях говорят о переводе фазы в амплитуду.) Коэффициенты в преобразовании Фурье — комплексные корни из 1, и они позволяют описывать периодические процессы с любым данным периодом так же, как $(-1)^n$ позволяет описать периодический процесс с периодом 2. Все это остроумно и элегантно, но, к сожалению, почти никогда не работает.

Теперь понятна роль преобразования Фурье: оно позволяет трансформировать периодичность функции $f: k \mapsto y^k \pmod{N}$ в некоторое свойство коэффициентов, которое мы можем измерить.

(Физики в таких случаях говорят о переводе фазы в амплитуду.)

Коэффициенты в преобразовании Фурье — комплексные корни из 1, и они позволяют описывать периодические процессы с любым данным периодом так же, как $(-1)^n$ позволяет описать периодический процесс с периодом 2.

Все это остроумно и элегантно, но, к сожалению, почти никогда не работает.

Дело в том, что проведенные выше выкладки молчаливо используют то обстоятельство, что $\frac{2^n}{r}$ — целое число.

Теперь понятна роль преобразования Фурье: оно позволяет трансформировать периодичность функции $f: k \mapsto y^k \pmod{N}$ в некоторое свойство коэффициентов, которое мы можем измерить.

(Физики в таких случаях говорят о переводе фазы в амплитуду.)

Коэффициенты в преобразовании Фурье — комплексные корни из 1, и они позволяют описывать периодические процессы с любым данным периодом так же, как $(-1)^n$ позволяет описать периодический процесс с периодом 2.

Все это остроумно и элегантно, но, к сожалению, почти никогда не работает.

Дело в том, что проведенные выше выкладки молчаливо используют то обстоятельство, что $\frac{2^n}{r}$ — целое число. Это так, только если r — степень двойки (как в случае $N = 15$).

Теперь понятна роль преобразования Фурье: оно позволяет трансформировать периодичность функции $f: k \mapsto y^k \pmod{N}$ в некоторое свойство коэффициентов, которое мы можем измерить. (Физики в таких случаях говорят о переводе фазы в амплитуду.)

Коэффициенты в преобразовании Фурье — комплексные корни из 1, и они позволяют описывать периодические процессы с любым данным периодом так же, как $(-1)^n$ позволяет описать периодический процесс с периодом 2.

Все это остроумно и элегантно, но, к сожалению, почти никогда не работает.

Дело в том, что проведенные выше выкладки молчаливо используют то обстоятельство, что $\frac{2^n}{r}$ — целое число. Это так, только если r — степень двойки (как в случае $N = 15$). Период любого числа по модулю $N = pq$ есть делитель функции Эйлера $\varphi(N) = (p-1)(q-1)$. Поэтому для того, чтобы r было степенью двойки, нужно, чтобы $p-1$ и $q-1$ были степенями двойки, т.е. чтобы p и q имели вид $2^m + 1$.

Теперь понятна роль преобразования Фурье: оно позволяет трансформировать периодичность функции $f: k \mapsto y^k \pmod{N}$ в некоторое свойство коэффициентов, которое мы можем измерить.

(Физики в таких случаях говорят о переводе фазы в амплитуду.)

Коэффициенты в преобразовании Фурье — комплексные корни из 1, и они позволяют описывать периодические процессы с любым данным периодом так же, как $(-1)^n$ позволяет описать периодический процесс с периодом 2.

Все это остроумно и элегантно, но, к сожалению, почти никогда не работает.

Дело в том, что проведенные выше выкладки молчаливо используют то обстоятельство, что $\frac{2^n}{r}$ — целое число. Это так, только если r — степень двойки (как в случае $N = 15$). Период любого числа по модулю $N = pq$ есть делитель функции Эйлера $\varphi(N) = (p-1)(q-1)$. Поэтому для того, чтобы r было степенью двойки, нужно, чтобы $p-1$ и $q-1$ были степенями двойки, т.е. чтобы p и q имели вид $2^m + 1$. Простые числа вида $2^m + 1$ называются *простыми числами Ферма*; несложно доказать, что для простоты таких чисел необходимо, чтобы показатель m сам был степенью двойки.

На 2020 год известны только 5 простых чисел Ферма:

$$2^{2^0} + 1 = 2^1 + 1 = 3,$$

$$2^{2^1} + 1 = 2^2 + 1 = 5,$$

$$2^{2^2} + 1 = 2^4 + 1 = 17,$$

$$2^{2^3} + 1 = 2^8 + 1 = 257,$$

$$2^{2^4} + 1 = 2^{16} + 1 = 65537.$$

На 2020 год известны только 5 простых чисел Ферма:

$$2^{2^0} + 1 = 2^1 + 1 = 3,$$

$$2^{2^1} + 1 = 2^2 + 1 = 5,$$

$$2^{2^2} + 1 = 2^4 + 1 = 17,$$

$$2^{2^3} + 1 = 2^8 + 1 = 257,$$

$$2^{2^4} + 1 = 2^{16} + 1 = 65537.$$

Для произведений любых других простых чисел описанный выше алгоритм работать *не будет*.

На 2020 год известны только 5 простых чисел Ферма:

$$2^{2^0} + 1 = 2^1 + 1 = 3,$$

$$2^{2^1} + 1 = 2^2 + 1 = 5,$$

$$2^{2^2} + 1 = 2^4 + 1 = 17,$$

$$2^{2^3} + 1 = 2^8 + 1 = 257,$$

$$2^{2^4} + 1 = 2^{16} + 1 = 65537.$$

Для произведений любых других простых чисел описанный выше алгоритм работать *не будет*.

Чтобы заставить этот подход работать, нужно привлечь дополнительные идеи из классического раздела теории чисел — *теории непрерывных дробей*.