Алгоритм Шора, часть III

М. В. Волков

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

2022/2023 учебный год

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 $\log N$. Для этого достаточно найти такое число y, взаимно простое с N, что его период по модулю N есть четное число $2s$ и притом $y^s + 1$ не делится на N.

Выбираем наугад взаимно простое с N число y и пытаемся найти его период r по модулю N. Для этого проделываем над квантовой системой $H := H_S \otimes H_S$, где $N^2 \leq S := 2^n < 2N^2$, некоторую последовательность унитарных преобразований, а потом замеряем первый регистр. Замер дает один из базисных векторов $|u\rangle$ с вероятностью примерно $r|b_u|^2$, где

$$b_u := \frac{1}{S}\sum_{j=0}^{A-1} e^{\frac{2\pi iujr}{S}}, \quad A := \left\lceil \frac{S}{r} \right\rceil.$$

Утверждается, что вероятность получить при этом один из векторов $|u\rangle$, для которых существует k со свойством $-\frac{r}{2} \leq ur - kS \leq \frac{r}{2}$, не меньше 0.4, а количество таких векторов примерно равно r.

Проверкой этих утверждений мы сейчас и займемся.

Вычисление вероятности

Неравенство $-\frac{r}{2} \leq ur - kS \leq \frac{r}{2}$ можно переписать так:

$$-\frac{1}{2} \leq u - k\frac{S}{r} \leq \frac{1}{2}. \qquad (\star)$$

Поскольку $\frac{S}{r} \approx A$, а $u \leq S$, количество чисел u, для которых есть k такое, что выполнено $(\star)$, примерно равно r: такие u отвечают кратным числа A. А именно, для $u \approx A$ годится $k = 1$, для $u \approx 2A$ подходит $k = 2$, и т.д.

Теперь оценим $r|b_u|^2$. Суммируя геометрическую прогрессию, получаем

$$b_u := \frac{1}{S}\sum_{j=0}^{A-1} e^{\frac{2\pi iujr}{S}} = \frac{1}{S}\frac{1 - e^{\frac{2\pi iuAr}{S}}}{1 - e^{\frac{2\pi iur}{S}}}.$$

Отсюда и из формулы $\cos\varphi = \frac{1}{2}(e^{i\varphi} + e^{-i\varphi})$ получаем:

$$|b_u|^2 = b_u\overline{b_u} = \frac{1}{S^2}\frac{(1 - e^{\frac{2\pi iuAr}{S}})(1 - e^{-\frac{2\pi iuAr}{S}})}{(1 - e^{\frac{2\pi iur}{S}})(1 - e^{-\frac{2\pi iur}{S}})}$$

$$= \frac{1}{S^2}\frac{2 - \left(e^{\frac{2\pi iuAr}{S}} + e^{-\frac{2\pi iuAr}{S}}\right)}{2 - \left(e^{\frac{2\pi iur}{S}} + e^{-\frac{2\pi iur}{S}}\right)} = \frac{1}{S^2}\frac{1 - \cos\frac{2\pi uAr}{S}}{1 - \cos\frac{2\pi ur}{S}}.$$

Итак, $r|b_u|^2 = \dfrac{r}{S^2}\dfrac{1-\cos\frac{2\pi uAr}{S}}{1-\cos\frac{2\pi ur}{S}} = \dfrac{r}{S^2}\dfrac{\sin^2\frac{\pi uAr}{S}}{\sin^2\frac{\pi ur}{S}}$. Мы хотим оценить дробь $\dfrac{\sin^2\frac{\pi uAr}{S}}{\sin^2\frac{\pi ur}{S}}$ снизу. Оценим ее знаменатель сверху, а числитель снизу.

В силу неравенства $-\dfrac{r}{2} \le ur - kS \le \dfrac{r}{2}$ имеем $\dfrac{ur}{S} = k + t$, где $|t| \le \frac{1}{2}$.

Рассмотрим функцию $g(x) := \dfrac{\sin x}{x}$. Имеем $|g(x)| \le 1$ при всех x, откуда

$$\sin^2\frac{\pi ur}{S} = \sin^2(\pi k + \pi t) = \sin^2(\pi t) = (\pi t)^2 g^2(\pi t) \le (\pi t)^2.$$

Теперь займемся числителем. В силу неравенства $-\dfrac{r}{2} \le ur - kS \le \dfrac{r}{2}$ имеем

$$-\frac{Ar}{2S} \le \frac{Aur}{S} - Ak = At \le \frac{Ar}{2S}. \qquad (\dagger)$$

Напомним, что $A = \left\lceil \dfrac{S}{r} \right\rceil$, откуда $A - 1 < \dfrac{S}{r} \le A$. Деля на A и переворачивая, получаем $1 \le \dfrac{Ar}{S} < \dfrac{A}{A-1} = 1 + \dfrac{1}{A-1}$. Используя это, выводим из $(\dagger)$ неравенство

$$-\frac{\pi}{2}\left(1 + \frac{1}{A-1}\right) < \pi At < \frac{\pi}{2}\left(1 + \frac{1}{A-1}\right).$$

Имеем $r < N$ и $N^2 \leq S$, откуда $N < \dfrac{S}{r} \leq A$. Поэтому замена A на N в крайних выражениях двойного неравенства

$$-\frac{\pi}{2}\left(1+\frac{1}{A-1}\right) < \pi At < \frac{\pi}{2}\left(1+\frac{1}{A-1}\right)$$

показывает, что

$$-\frac{\pi}{2}\left(1+\frac{1}{N-1}\right) < \pi At < \frac{\pi}{2}\left(1+\frac{1}{N-1}\right).$$

В частности, $|\pi At| < \pi$, а на $[0,\pi]$ функция $g(x) = \dfrac{\sin x}{x}$ убывает. Отсюда

$$\sin^2\frac{\pi Aur}{S} = \sin^2(\pi Ak + \pi At) = \sin^2(\pi At) = (\pi At)^2 g^2(A\pi t) \geq$$
$$\geq (\pi At)^2 g^2\left(\frac{\pi}{2}\left(1+\frac{1}{N-1}\right)\right).$$

Вычисление вероятности (4)

Напомним цель: оценить снизу выражение $r|b_u|^2 = \dfrac{r}{S^2}\dfrac{\sin^2\frac{\pi uAr}{S}}{\sin^2\frac{\pi ur}{S}}$. Мы оценили знаменатель сверху как $\sin^2\dfrac{\pi ur}{S} \le (\pi t)^2$, а числитель снизу как $\sin^2\dfrac{\pi Aur}{S} \ge (\pi At)^2 g^2\left(\dfrac{\pi}{2}\left(1+\dfrac{1}{N-1}\right)\right)$. Деля второе на первое, имеем

$$r|b_u|^2 \ge \frac{rA^2}{S^2}g^2\left(\frac{\pi}{2}\left(1+\frac{1}{N-1}\right)\right) = \frac{rA^2}{S^2}\frac{4}{\pi^2}\left(\frac{N-1}{N}\right)^2\sin^2\left(\frac{\pi}{2}\left(1+\frac{1}{N-1}\right)\right).$$

Разберемся с непостоянными сомножителями. $A = \left\lceil\dfrac{S}{r}\right\rceil$, откуда $\dfrac{S}{r} \le A$.

Поэтому $\dfrac{rA}{S} \ge 1$ и $\dfrac{rA^2}{S^2} \ge \dfrac{1}{r}$. 3-й сомножитель с точностью до $\dfrac{1}{N^2}$ равен $1-\dfrac{2}{N}$. Наконец,

$\sin\left(\frac{\pi}{2}\left(1+\frac{1}{N-1}\right)\right) = \cos\dfrac{\pi}{2(N-1)} = 1 - \dfrac{\pi^2}{8(N-1)^2} + \cdots$, поэтому точностью до $\left(\dfrac{1}{N-1}\right)^\alpha$, где $\alpha \ge 2$, 4-й сомножитель равен 1. Итак,

$r|b_u|^2 \ge \dfrac{1}{r}\dfrac{4}{\pi^2}\left(1-\dfrac{2}{N}\right) \ge \dfrac{0.4}{r}$. Поэтому вероятность получить один из r «хороших» векторов $|u\rangle$ не меньше 0.4.

На прошлой лекции мы показали, что вероятность угадать «правильное» число y не меньше 0.5, а сейчас проверили, что вероятность получить как результат алгоритма Шора один из векторов $|u\rangle$, для которых существует k со свойством $-\frac{r}{2} \leq ur - kS \leq \frac{r}{2}$, не меньше 0.4.

Объясним, как по такому u найти период r.

Неравенство $-\frac{r}{2} \leq ur - kS \leq \frac{r}{2}$ 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 равная ей *несократимая* дробь может быть вычислена за полиномиальное время от длины записи N с помощью известного в теории чисел алгоритма. Опишем этот алгоритм.

Цепная дробь — это конечное или бесконечное выражение вида

$$[a_0; a_1, a_2, a_3, \cdots] := a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ldots}}},$$

где a_0 — целое число, а все остальные a_n — натуральные числа.
Любое действительное число представимо в виде цепной дроби.
Нам цепные дроби понадобятся только для рациональных чисел. Цепная дробь, представляющая данное рациональное число $\frac{P}{Q}$, где P целое, а Q натуральное, всегда конечна, и ее элементы $a_0, a_1, a_2, a_3, \ldots, a_n$ суть в точности неполные частные в алгоритме Евклида, примененном к P и Q:

$$\begin{aligned} P &= Qa_0 + r_1 \\ Q &= r_1 a_1 + r_2 \\ r_1 &= r_2 a_2 + r_3 \\ &\ldots\ldots\ldots\ldots\ldots \\ r_{n-1} &= r_n a_n \end{aligned}$$

Поэтому $a_0, a_1, a_2, \ldots, a_n$ вычислимы за полиномиальное от $\log PQ$ время.

Пример разложения в цепную дробь

Пример: разложим в цепную дробь число $\frac{105}{38}$.
Запускаем алгоритм Евклида.

$$\begin{aligned} 105 &= 38 \cdot \underline{2} + 29 \\ 38 &= 29 \cdot \underline{1} + 9 \\ 29 &= 9 \cdot \underline{3} + 2 \\ 9 &= 2 \cdot \underline{4} + 1 \\ 2 &= 1 \cdot \underline{2} \end{aligned}$$

Значит, $\dfrac{105}{38} = 2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{4 + \cfrac{1}{2}}}} = [2; 1, 3, 4, 2]$.

Подходящие дроби

Пусть $x = [a_0; a_1, a_2, a_3, \cdots]$ — число, представленное цепной дробью. *n-й подходящей дробью* для x называется конечная цепная дробь $[a_0; a_1, \cdots, a_n]$, значение которой есть некоторое рациональное число $\frac{p_n}{q_n}$.

Есть несложные рекуррентные формулы для вычисления числителей и знаменателей подходящих дробей:

$$p_{-1} = 1, \quad p_0 = a_0, \quad p_n = a_n p_{n-1} + p_{n-2};$$
$$q_{-1} = 0, \quad q_0 = 1, \quad q_n = a_n q_{n-1} + q_{n-2}.$$

Поэтому подходящие дроби к рациональному числу $\frac{P}{Q}$ вычислимы за полиномиальное от $\log PQ$ время.

Пример: подсчитаем подходящие дроби к числу $\frac{105}{38} = [2; 1, 3, 4, 2]$.

n	–1	0	1	2	3	4
a_n		2	1	3	4	2
p_n	1	2	3	11	47	105
q_n	0	1	1	4	17	38

Итак, подходящие дроби суть 2, 3, $\frac{11}{4}$, $\frac{47}{17}$, $\frac{105}{38}$.

По индукции легко доказывается, что числители и знаменатели соседних подходящих дробей связаны равенством:

$$p_n q_{n-1} - q_n p_{n-1} = (-1)^{n-1}. \qquad (*)$$

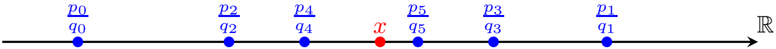
Из $(*)$ следует, что все подходящие дроби несократимы. Из $(*)$ следует и равенство $\dfrac{p_n}{q_n} - \dfrac{p_{n-1}}{q_{n-1}} = \dfrac{(-1)^{n-1}}{q_n q_{n-1}}$. Знаменатели подходящих дробей растут, поэтому расстояние между соседними подходящими дробями убывает.

При $n \geq 2$ имеем

$$p_n q_{n-2} - q_n p_{n-2} = (a_n p_{n-1} + p_{n-2}) q_{n-2} - (a_n q_{n-1} + q_{n-2}) p_{n-2} =$$
$$= a_n (p_{n-1} q_{n-2} - q_{n-1} p_{n-2}) \overset{(*)}{=} (-1)^{n-2} a_n = (-1)^n a_n.$$

Отсюда $\dfrac{p_n}{q_n} - \dfrac{p_{n-2}}{q_{n-2}} = \dfrac{(-1)^n a_n}{q_n q_{n-2}}$, поэтому подходящие дроби с четными номерами возрастают, а с нечетными – убывают. При этом подходящие к $x = [a_0; a_1, a_2, a_3, \cdots]$ дроби с четными номерами меньше или равны x, а подходящие дроби с нечетными номерами – больше или равны x.

Приближения подходящими дробями



Подходящие дроби отлично приближают «свое» число:

$$\left|x - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}} < \frac{1}{q_n^2}.$$

Пример: подходящие дроби для π – это $3, \frac{22}{7}, \frac{333}{106}, \frac{355}{113}, \frac{103993}{33102}$.

Но для нас важнее обратный результат:

Теорема

Если целое число a и натуральное число b взаимно просты и

$$\left|x - \frac{a}{b}\right| < \frac{1}{2b^2}, \qquad (!)$$

то $\frac{a}{b}$ – одна из подходящих дробей к x.

В частности, если $x = \frac{P}{Q}$, найти дробь $\frac{a}{b}$, удовлетворяющую неравенству (!), если она существует, можно за полиномиальное от $\log PQ$ время.

Назовем дробь $\frac{a}{b}$ *наилучшим приближением* числа x, если для любой дроби $\frac{c}{d} \neq \frac{a}{b}$, такой, что $d \leq b$,

$$|dx - c| > |bx - a|.$$

Заметим, что в этом случае $\left|x - \frac{c}{d}\right| > \left|x - \frac{a}{b}\right|$ (но обратное неверно).

Теорема

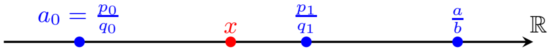
Всякое наилучшее приближение есть подходящая дробь.

Доказательство. Пусть дробь $\frac{a}{b}$ есть наилучшее приближение числа $x = [a_0; a_1, a_2, a_3, \cdots]$. Если $\frac{a}{b} < a_0$, то

$$|1 \cdot x - a_0| = x - a_0 < x - \frac{a}{b} = \left|x - \frac{a}{b}\right| \leq |bx - a|,$$

противоречие ($1 \leq b$, а дробь $\frac{1}{a\,0}$ приближает лучше, чем дробь $\frac{a}{b}$). Значит, $a_0 \leq \frac{a}{b}$. Если предположить, что $\frac{a}{b}$ не есть подходящая дробь, то либо $\frac{a}{b} > \frac{p_1}{q_1}$, либо $\frac{a}{b}$ лежит между $\frac{p_{k-1}}{q_{k-1}}$ и $\frac{p_{k+1}}{q_{k+1}}$ для некоторого $k > 0$.

Случай 1: $\dfrac{a}{b} > \dfrac{p_1}{q_1}$.



Имеем

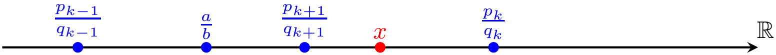
$$\left|x - \frac{a}{b}\right| > \left|\frac{p_1}{q_1} - \frac{a}{b}\right| \geq \frac{1}{bq_1}.$$

Отсюда $|bx - a| > \dfrac{1}{q_1} = \dfrac{1}{a_1}$. С другой стороны, $|1 \cdot x - a_0| \leq \dfrac{1}{a_1}$. Итак,

$$|1 \cdot x - a_0| < |bx - a|,$$

противоречие ($1 \leq b$, а дробь $\dfrac{1}{a_0}$ приближает лучше, чем дробь $\dfrac{a}{b}$).

Случай 2: $\dfrac{a}{b}$ лежит между $\dfrac{p_{k-1}}{q_{k-1}}$ и $\dfrac{p_{k+1}}{q_{k+1}}$ для некоторого $k > 0$.



Имеем

$$\left|\frac{a}{b} - \frac{p_{k-1}}{q_{k-1}}\right| \geq \frac{1}{bq_{k-1}} \quad \text{и} \quad \left|\frac{a}{b} - \frac{p_{k-1}}{q_{k-1}}\right| < \left|\frac{p_k}{a_k} - \frac{p_{k-1}}{q_{k-1}}\right| = \frac{1}{q_k q_{k-1}}.$$

Отсюда $b \geq q_k$.

С другой стороны,

$$\left|x - \frac{a}{b}\right| \geq \left|\frac{p_{k+1}}{q_{k+1}} - \frac{a}{b}\right| \geq \frac{1}{bq_{k+1}}.$$

Отсюда $|bx - a| > \dfrac{1}{q_{k+1}}$. Поскольку

$$\left|x - \frac{p_k}{q_k}\right| < \frac{1}{q_k q_{k+1}},$$

имеем $|q_k x - p_k| < \dfrac{1}{q_{k+1}}$. Итак,

$$|q_k x - p_k| < |bx - a|,$$

противоречие ($q_k \leq b$, а дробь $\dfrac{p_k}{q_k}$ приближает лучше, чем дробь $\dfrac{a}{b}$).

Теорема

Если целое число a и натуральное число b взаимно просты и $\left|x-\frac{a}{b}\right|<\frac{1}{2b^2}$, то $\frac{a}{b}$ – одна из подходящих дробей к x.

Доказательство. Проверим, что $\frac{a}{b}$ – наилучшее приближение к x. Пусть $\frac{c}{d}\neq\frac{a}{b}$ и $|dx-c|\le|bx-a|<\frac{1}{2b}$. Тогда $\left|x-\frac{c}{d}\right|<\frac{1}{2bd}$. Поэтому

$$\left|\frac{c}{d}-\frac{a}{b}\right|\le\left|x-\frac{c}{d}\right|+\left|x-\frac{a}{b}\right|<\frac{1}{2bd}+\frac{1}{2b^2}=\frac{b+d}{2b^2d}.$$

С другой стороны, поскольку $\frac{c}{d}\neq\frac{a}{b}$,

$$\left|\frac{c}{d}-\frac{a}{b}\right|\ge\frac{1}{bd}.$$

Итак, $\frac{1}{bd}<\frac{b+d}{2b^2d}$, откуда $2b<b+d$ и $b<d$.

Итак, из неравенства

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

можно за полиномиальное от длины записи числа N найти несократимую дробь, равную дроби $\dfrac{k}{r}$.

Как обсуждалось в конце прошлой лекции, вероятность того, что дробь $\dfrac{k}{r}$ несократима, равна $\dfrac{\varphi(r)}{r}$, а для $\dfrac{\varphi(r)}{r}$ есть нижняя оценка вида $\dfrac{0.56}{\log\log N}$.

Значит, запуская алгоритм Шора $\log\log N$ раз, мы определим верное значение r с вероятностью по крайней мере

$$\underbrace{0.5}_{\text{нужное } y} \cdot \underbrace{0.4}_{\text{нужное } u} \cdot \underbrace{0.56}_{\text{нужное } k} > 0.1.$$