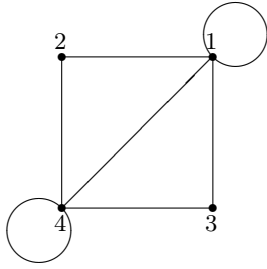


Задача 1. (4×0.02) Ср. [Кормен 1, задача 33.3]. Диаграмма графа G изображена на рисунке.



Путь в графе — это произвольная последовательность смежных вершин (возможны возвраты): $c = \{v_1, \dots, v_l\}$. По определению, длина пути c равна $l - 1$.

Пусть g_n — это число путей в G длины n , которые начинаются в вершине 1. Из определения следует, что $g(0) = 1$ (единственный путь: $0 \rightarrow 0$), а $g(1) = 4$ (пути: $1 \rightarrow 1$, $1 \rightarrow 2$, $1 \rightarrow 4$, $1 \rightarrow 3$).

Пусть A — это матрица инцидентий графа G :

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$

(i) Вычислите число $g(2)$ путей в G длины 2 и проверьте, что оно равно сумме элементов первой строки матрицы A^2 . Объясните это совпадение и докажите общую формулу для $g(n)$.

(ii) Найдите рекуррентное соотношение, которому удовлетворяет последовательность $\{g_n, n = 0, 1, \dots\}$.

Подсказка. В ответе должна получиться рекуррентность с целыми коэффициентами типа рекуррентности Фибоначчи: $g_{n+2} = Pg_{n+1} + Qg_n$. Можно просто подобрать коэффициенты и доказать, что они искомые. При этом необходимо вычислить хотя бы еще одно значение $g(n)$.

Рассмотрим два способа вычисления $\{g_n, n = 0, 1, \dots\}$.

Первый, основан на том, что последовательность $\{g_n\}$ удовлетворяет рекуррентному соотношению, т. е. разностному уравнению, и это подсказывает следующий матричный способ ее вычисления. Имеет место матричная формула¹ $\begin{pmatrix} g_n \\ g_{n+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ Q & P \end{pmatrix}^{n-1} \begin{pmatrix} g_1 \\ g_2 \end{pmatrix}$.

При вычислении $\{g_n\}$ этим способом можно использовать быстрое, например, “индийское возведение в степень” n за $O(\log n)$ тактов².

Второй способ вычислений основан на явном аналитическом решении линейной рекуррентности, которое можно получить самостоятельно или воспользоваться алгоритмом из текста на сайте. Например, для чисел Фибоначчи ($F_1 = 1, F_2 = 1, \dots, F_{n+2} = F_{n+1} + F_n$) этот способ приводит к известной формуле Бине: $F_n = \frac{(\frac{1+\sqrt{5}}{2})^n - (\frac{1-\sqrt{5}}{2})^n}{\sqrt{5}}$. У вас должна получиться похожая формула, также содержащая квадратичную иррациональность $\sqrt{d} = \sqrt{P^2 + 4Q}$. Вычисление по аналитической формуле реализуется чуть хитрее, чем по матричной. Для каждого значения n нужно специфицировать операции и указать с какой точностью их нужно проводить (например, для вычисления \sqrt{d} нужно указать процедуру вычисления, задать точность вычисления и оценить битовую трудоемкость процедуры).

На самом деле, переход к собственным векторам матрицы $\begin{pmatrix} 0 & 1 \\ Q & P \end{pmatrix}$ показывает, что оба алгоритма тесно связаны, и матричный алгоритм можно рассматривать как корректный способ округления ответа, полученного по аналитической формуле.

Оценим трудоемкость нескольких алгоритмов вычисления g_n по простому модулю p .

¹Поскольку для $\{g_n\}$ коэффициенты P и Q — целые, то при вычислениях можно использовать только целую арифметику.

²Мы разбирали этот алгоритм в первом задании, и он с необходимыми изменениями переносится на матрицы.

(iii) Непосредственное вычисление по рекуррентной формуле. Оцените его трудоемкость при вычислении $A = g_{20000} \pmod{29}$.

(iv) Докажите, что последовательность $\{g_n\}$ периодична по любому модулю. Оцените ее период для $\pmod{29}$ и найдите трудоемкость вычисления (сложность нахождения периода + сложность вычисления A) этим способом.

Задача Д-1. (3×0.02) (i) Пусть известно, что 5 является квадратичным вычетом по \pmod{p} , например, $p = 29$, т. е. разрешимо уравнение $x^2 = 5 \pmod{p}$. Обоснуйте алгоритм непосредственного вычисления A по аналитической формуле, т. е. прямо извлекая квадратный корень в конечном поле \pmod{p} и проводя дальнейшие арифметические вычисления. Вычислите A этим способом. Оцените трудоемкость вычисления $g_n \pmod{p}$ для этого случая.

(ii) Пусть теперь 5 НЕ является квадратичным вычетом по \pmod{p} , например, $p = 23$. Придумайте и обоснуйте использующий аналитическую формулу алгоритм вычисления чисел $\{g_n\}$ по такому модулю. Проведите вычисления $A = g_{10000} \pmod{23}$. Оцените трудоемкость вычисления $g_n \pmod{p}$ для этого случая.

В этой задаче вам предстоит разобраться, как использовать матричный алгоритм для вычисления рекуррентности по простому модулю. Мы уже знаем, что эффективность процедуры сильно (или даже критически) зависит от вычисления периода $\{g_n\} \pmod{p}$. И, собственно, основной вопрос, на который хочется найти ответ, как найти период в матричном представлении $\{g_n\}$. Предлагается придумать алгоритм самостоятельно и/или проанализировать следующий способ. Заметим, что нам повезло, и матрицу $\begin{pmatrix} 0 & 1 \\ Q & P \end{pmatrix}$ можно диагонализировать, т. е. привести ее к виду $S \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} S^{-1}$, где λ_1, λ_2 — это собственные числа, а S — невырожденная матрица. Возводя в n -ю степень, получим $S \begin{pmatrix} \lambda_1^n & 0 \\ 0 & \lambda_2^n \end{pmatrix} S^{-1}$.

(iii) Наша задача состоит в том, чтобы обосновать эти манипуляции при вычислениях \pmod{p} и понять, в какую степень нужно возвести матрицу, чтобы получилась единичная матрица, т. е. получить аналог малой теоремы Ферма для матриц указанного вида³.

Оцените сложность вычисления периода и вычисления $\{g_n\} \pmod{p}$ матричным способом и сравните его с алгоритмами из пунктов (i)–(ii).

Комментарий. В последней задаче в пунктах (i)–(ii) речь идет о т.н. квадратичных вычетах и возникает естественный вопрос, как по данному числу a проверить разрешимость уравнения $x^2 = a \pmod{p}$ (в задаче $a = 5, n = 29, 23$). Можно, конечно, перебрать все вычеты, используя $O(p)$ операций, но есть и более интеллигентный полиномиальный по длине записи $\log p$ алгоритм. Он основан на знаменитом квадратичном законе взаимности, о котором можно прочитать в книге [Виноградов, гл. 2] (и придумать алгоритм самостоятельно). Но есть и еще более простой способ, основанный на обобщении малой теоремы Ферма. Если определить (см., [Виноградов, гл. 2]) т.н. символ Лежандра: $\left(\frac{a}{p}\right)$, равный $+1$, если число $a \not\equiv 0 \pmod{p}$ является квадратичным вычетом

³Обратите внимания, что прямого аналога малой теоремы Ферма для матриц быть не может, поскольку, например, существуют т.н. нильпотентные матрицы (какая-то их степень равна нулевой матрице). Удивительно, но тексты, посвященные аналогам теоремы Ферма для матриц, появились только в этом тысячелетии (см., www.mathnet.ru/mp238). В принципе, их мог написать сильный студент.

$(\bmod p)$, и, равный -1 , в противном случае, то имеет место равенство $a^{\frac{p-1}{2}} = \left(\frac{a}{p}\right) (\bmod p)$. Таким образом, можно эффективно проверить, является ли a квадратичным вычетом, используя быстрое возведение в степень. Кроме того, можно построить быстрый вероятностный алгоритм поиска квадратичного вычета или невычета. Что понимается по этим, поясняет следующая задача.

Задача 2. (i) Пусть $\text{НОД}(a, N) = 1$ и $a^{N-1} \neq 1 (\bmod N)$. Тогда по крайней мере для половины чисел из промежутка $1 \leq b < N$ выполнено $b^{N-1} \neq 1 (\bmod N)$.