Филиппова Анастасия

Домашнее задание 5

1

Построим рекуррентное соотношение: заполним первую ячейку размером 2×1 серым прямоугольником, останется еще $f(n-1)$ способ заполнить оставшуюся часть. Теперь посмотрим на первый квадрат размером 2×2, способов его заполнить 3: черный квадрат, белый и серые полоски, повернутые на 90 градусов. И $f(n-2)$ способами можем заполнить оставшуюся часть. Получаем $f(n) = f(n-1) + 3f(n-2)$.
Получим аналитическое выражение:
$\lambda^2 - \lambda - 3 = 0$,
$\lambda = \frac{1 \pm \sqrt{13}}{2}$,
$f(n) = C_1(\frac{1+\sqrt{13}}{2})^n + C_2(\frac{1-\sqrt{13}}{2})^n, f_0 = 0, f_1 = 1$, получаем, что $C_1 = 1/\sqrt{13}, C_2 = -1/\sqrt{13}, f(n) = \frac{1}{\sqrt{13}}((\frac{1+\sqrt{13}}{2})^n - (\frac{1-\sqrt{13}}{2})^n)$
$13^{(31-1)/2} = 13^{15} = 13^4 \cdot 13^4 \cdot 13^4 \cdot 13^3 = 1000 \cdot 27 = 30 = -1 \ mod\ 31 \Rightarrow$ квадратичный невычет. Аналогично задаче $2.D-1$: $2^{-1} = 16 \ mod\ 31, 13^{-1} = 12 \ mod\ 31$,
$12x((16+16x)^n - (16-16x)^n)$,
$31 \cdot 31 = 961, 30000 = 3 \cdot 10^4 = 3 \cdot 80 = 240 \ mod\ 960. g_(240) = g_(30000)$.

2.1

(i) $g(2) = 4+4+2+2$.Количество возможных путей,если первой вершиной, которою мы посещаем будет 1 или 4 — $4+4=8$, $2, 3$ — $2+2$. Итог: 12.
(ii) Посчитаем все возможные пути на n шаге, очевидно, что $g(n) = g_1(n) + g_2(n) + g_3(n) + g_4(n)$, где $g_i(n)$ — путь, оканчивающийся в i-ой вершине. Тогда $g(n+1) = 4g_1(n) + 4g_4(n) + 2g_2(n) + 2g_3(n) = 2g(n) + 4g(n-1)$
$\lambda^2 - 2\lambda - 4\lambda = 0 \iff \lambda = 1+\sqrt{5}, 1-\sqrt{5}$, получаем $g_n = C_1 \cdot (1+\sqrt{5}) + C_2 \cdot 1 - \sqrt{5}, g_0 = 1, g_1 = 4$. При начальных условиях получаем: $g_n = \frac{\sqrt{5}+3}{2\sqrt{5}}(1+\sqrt{5})^n + \frac{\sqrt{5}-3}{2\sqrt{5}}(1-\sqrt{5})^n$.
Чтобы вычислить g_n надо посчитать $(1 \pm \sqrt{5})^n$ по модулю 29. Это можно сделать с помощью быстрого возведения в степень за $O(\log n)$.
(iv) Пусть k — период. Пара g_i, g_{i-1} однозначно определяет пару g_{i+1}, g_i, получается, что, если встретится пара еще раз, то алгоритм зациклится. Возможных пар p^2 (остатки по модулю p). Посмотрим, когда повториться: $(g_n, g_{n-1}) = (g_{n-k}, g_{n-k-1}) = ... = (g_{n \ mod\ k}, g_{n \ mod\ k-1})$. Деление по модулю выполняется за $O((\log n)^3)$ (Дасгупта, алгоритмы, страница 21). П (iii) $11^2 = 5 \ mod\ 29, 22^{-1} = 4 \ mod\ 29$, получаем: $g_n = 14 \cdot 4 \cdot (12)^n + 32 \cdot (-10)^n \ mod\ 29, g_n = (-2) \cdot (12)^n + 3 \cdot (-10)^n$.
$12^{20000} = 12^{714 \cdot 28 + 8} = 12^8 = 144 = 1 \ mod\ 29$,
$(-10)^{20000} = (-10)^{714 \cdot 28 + 8} = 10^8 = 25 = \ mod\ 29$,
$g_{20000} = -2 + 3 \cdot 25 = 15$.

2.Д-1

5 — квадратичный невычет по модулю 23. Работаем в кольце $Z_{23}[x]$ — кольцо многочленов над полем Z_{23}. $Z_{23}[x]/(x^2-5)$ — поле, так как многочлен не приводим в кольце. $\sqrt{5} = x$, полуаем $g_n = \frac{(x+3)\sqrt{5}}{10}(1+x)^n + \frac{(x-3)\sqrt{5}}{10}(1-x)^n = 7x(x+3)(1+x)^n + 7x(x-3)(1-x)^n = 7x((x+3)(1+x)^n + (x-3)(1-x)^n) \ mod\ 23$, так как $10^{-1} = 7 \ mod\ 23$.
Порядок $Z_{23}[x]/(x^2-5)$ равен $23^2 - 1 = 528 = 3 \cdot 11 \cdot 16 \Rightarrow F_{528} = Z_3 \otimes Z_{16} \otimes Z_{11}$, имеем: $(1-x)^{528} = 1 = (1+x)^{528}, F^{23}_{528+n} = F^{23}_n$.
$10000 = 10^4$, находим $10^4 = 528 \cdot 19 - 32 \ mod\ 528$, тогда: $496 \longleftrightarrow$найдем F_{496} :
$(1 \pm x)^2 = 1 \pm 2x + x^2 = 6 \pm 2x$,
$(1 \pm x)^4 = 36 \pm 24x + 4x^2 = 10 \pm x$,

$(1 \pm x)^8 = 100 + x^2 \pm 20x = 13 \mp 3x$,
$(1 \pm x)^{16} = 100 + 9x^2 \mp 60x = 7 \mp 9x$,
$(7 \pm 9x)^2 = (49 + 81x^2 \pm 14 \cdot 9x) = (-6 \mp 11x)$,
$(-6 \mp 11x)^2 = 36 \mp 132x + 121x) = (-3 \mp 6x)$,
$(-3 \mp 6x)^2 = (9 + 36x^2 \pm 36x) = (5 \pm 13x)$,
$(5 \pm 13x)^2 = (25 + 169x^2 \pm 130x) = (-4 \mp 8x)$.
$(x \pm 1)^{496} = (x \pm 1)^{256+128+64+32+16} = (-4 \mp 8x)(5 \mp 13x)(-3 \mp 6x)(-6 \mp 11x)(7 \mp 9x) = (7 \mp 9x)(-14+3)3 = -10(7 \mp 9x)$. $-x((x+3)(7-9x) + (x-3)(7+9x)) = -x(7x + 21 - 45 - 27x + 7x - 21 + 45 - 27x) = -x \cdot (-40x) = 40 \cdot 5 = 200 = 16$.

3.

Пусть язык $L \in \mathcal{NP}$. Покажите, что он полиномиально сводится (по Карпу) к языку $STOP$ описаний пар (M, ω) машин Тьюринга и входов таких, что M останавливается на входе ω.
$L \in \mathcal{NP} \Rightarrow L \leq 3-SAT$. Теперь построим такую МТ, которая будет выдавать 1, если нашла выполняющий набор для формулы и 0 в противном случае. Пусть ϕ — КНФ, в которой не больше 3 литералов в каждом дизъюнкте. Тогда $f(\phi) = (MT, \phi)$. Получаем, что, если $\phi \in 3 - SAT \Rightarrow (MT, \omega) \in STOP$, если $\phi \notin 3 - SAT \Rightarrow (MT, \omega) \notin STOP$. Сводимость полиномиальная, так как, очевидно, машину Тьюринга можем построить за полином.

4.

Пусть $L \in \mathcal{NP}C \cap co\text{-}\mathcal{NP}$, тогда:
1) $\bar{L} \in \mathcal{NP}$, 2) $L \in \mathcal{NP}$, 3) $\forall A \in \mathcal{NP}\ \exists f : x \in A \iff f(x) \in L$. Докажем, дополнение любого языка из $\mathcal{NP}$ лежит в $\mathcal{NP}$. Действительно, $\forall A \in \mathcal{NP}\ \exists f : x \notin A \iff f(x) \notin L$, то есть $\forall A \in \mathcal{NP}\ \exists f : x \in \bar{A} \iff f(x) \in \bar{L}$, следовательно, $\forall A \in \mathcal{NP} \hookrightarrow \bar{A} \leq \bar{L}$. То есть дополнение любого языка сводится к языку из $\mathcal{NP}$, следовательно, лежит в $\mathcal{NP}$. Доказано.

6.

(i) Схема испытаний Бернулли с k успехами (за успех будем принимать выпадение орла, за неуспех — выпадение решки). Получаем: $C_{10}^5(\frac{1}{2})^5(\frac{1}{2})^5 = C_{10}^5(\frac{1}{2})^{10} = \frac{126}{512}$.
(ii) Пусть A — событие, при котором выпало больше орлов чем решек. Очевидно, что события A и $\bar{A}$ — выпало больше решек, равновероятны. $P(=)$ — вероятность того, что количества равны. $P(A) + P(\bar{A}) + P(=) = 1 \iff 2P(A) = 1 - \frac{126}{512} \iff P(A) = \frac{386}{1024} = \frac{193}{512}$.
(iii) Количество элементарных исходов 2^{10}, количество благоприятных исходов 2^5, тогда вероятность равна $\frac{1}{2^5} = \frac{1}{32}$.
(iv)

7.

(i) Пусть A — на первой выпало 6, B — сумма равна 7. $P(A|B) = \frac{P(B|A)P(A)}{P(B)} = \frac{\frac{1}{6}\frac{1}{6}}{\frac{1}{6}} = \frac{1}{6}$
(ii) $E(X) = \sum y_i \cdot P(X = y_i)$, тогда $E(max(X_1, X_2)) = 1 \cdot 1/36 + 2 \cdot 3/36 + 3 \cdot 5/36 + 4 \cdot 7/36 + 5 \cdot 9/36 + 6 \cdot 11/36 = \sum\limits_{i=1}^{6} i \cdot (\frac{2i-1}{36})$

$E(min(X_1, X_2)) = 1 \cdot 11/36 + 2 \cdot 9/36 + 33/36 + 4 \cdot 5/36 + 5 \cdot 3/36 + 6 \cdot 1/36 = \sum\limits_{i=1}^{6} i \cdot (\frac{13-2i}{36})$, тогда

$E(max(X_1, X_2)) + E(min(X_1, X_2)) = \frac{1}{36}\sum\limits_{i=1}^{6}(13i - 2i^2 + 2i^2 - i) = \frac{1}{3}\sum\limits_{i=1}^{6} i = 7$.
(iii) A — выпало четное, B — выпало кратное 3.
$P(A|B) = \frac{1}{2}, P(A) = \frac{3}{6} = \frac{1}{2} \rightarrow$ события независимы.
(можно было так: $P(A \cap B) = \frac{1}{6}, P(A) \cdot P(B) = \frac{1}{2} \cdot \frac{1}{3} = \frac{1}{6}$).
(iv) В полном графе на n вершинах $C_n^2 = \frac{n(n-1)}{2}$ ребер, следовательно, всего графов на n вершинах (пространство элементарных исходов) $2^{\frac{n(n-1)}{2}}$. Посчитаем еоличество простых циклов. Занумеруем

вершины от 1 до n. Тогда циклы вида $1-2-3-4-1$ и $2-3-4-1-2$, очевидно, являются одинаковыми (полученные циклическим сдвигом). Следовательно, всего протых циклов будет $\frac{n!}{2n}$ (2 так как можем сдвигать вправо и влево). P(случайный граф является простым циклом) $= \frac{\frac{n!}{2n}}{2^{\frac{n(n-1)}{2}}}$.
$P(A) < \frac{n^n}{2^{\frac{n(n-1)}{2}}} = \frac{2^{n\cdot\log_2 n}}{2^{\frac{n(n-1)}{2}}}$, n^2 растет гораздо быстрее $n\log_2 n \Rightarrow \lim\limits_{n\to\infty} P(A) = 0$.

8 (ВТФ?).

Пусть m — количество шаров в каждой урне, l, p — количество белых шаров в первой и второй урнах соответственно. A — из превой урны все шары белые, B, C — из второй урны все шары белые, черные, тогда $P(A) = P(B) + P(C) \Rightarrow (\frac{l}{m})^n = (\frac{p}{m})^n + (\frac{m-p}{m})^n$, пусть $x = m - p, l^n = x^n + p^n$, но это уравнение не имеет решений в целых ненулевых числах l, p, x (великая теорема Ферма). Следовательно, $n = 0$, обе урны пустые.

9.

(Ссылаюсь на данную статью https://www.pvsm.ru/algoritmy/117848) Авторы показывают, что математическое ожидание числа нажатий клавиатуру для почучения строки s есть сумма обратных вероятностей каждого префикса в этой строке, который также является суффиксом этого же слова. Тогда, для последовательности PPO математическое ожидание числа бросков: PPO $---$ $1/8 \Rightarrow M(N) = 8$, POP — $1/8$ и $1/2 \Rightarrow 10$. Получаем, что число шагов в среднем, чтобы получить последовательность PPO меньше, следовательно, мы с большей вероятностью встретим ее раньше чем POP.

10.

Возьмем последовательность из двух цифр:00 — будет означать 0, $10, 01$ - будут означать 1, 11 - запустить алгоритм заново. Очевидно, что вероятность получить 0 — $1/3$, 1 — $2/3$.
Пусть исходный генератор печатает бит за $O(1)$. Пусть задача — получить последовательность из 0 и 1 длиной n (0 с вероятностью $1/3$, 1 — $2/3$), тогда в лучшем случае ни разу не придется запускать алгоритм заново, следовательно, исходному генератору с вероятностями $1/2$ понадобится $O(2n)$ времени.
В худшем случае исходный генератор всегда будет выдавать 11 и каждый раз алгоритм придется перезапускать. Оценим математическое ожидание числа ходов исходного генератора для получения последовательности 11: посчитаем префиксы, которые одновременно являются и суффиксами и сложим их обратные вероятности, получим: $1 - p(1) = 1/2, 11 - p(11) = 1/4$, получаем M(число шагов для получения последовательности 11) $= 6$. Получается, что в среднем, чтобы получить последовательность из n битов, потребуется $2n + n/2$ тактов (то есть исходный генератор выводит 6 битов, 4 из которых преобразуются в нужную часть последовательности, а остальные 2 — 11. Обратно:

3.

Рассматривается язык L выполнимых формул от n переменных вида $C_1 \wedge C_2 \wedge \ldots \wedge C_m$, где каждый C_k имеет один из трех видов: $(x_i \equiv x_j)$, $(\overline{x_i} \equiv x_j)$, $(x_i \equiv \overline{x_j})$, $(\overline{x_i} \equiv \overline{x_j})$
Эквивалентности такого вида $(x_i \equiv x_j)$ можно заменить на равновыполнимые дизъюнкты: $(x_i \vee \bar{x}_j) \wedge (\bar{x}_i \vee x_j)$, тогда любая формула из L будет представима в виде КНФ с $2m$ дизъюнктами. Далее к полученному языку сведем язык РОВНО-3 $- SAT$. Для этого