Домашняя работа №9

Бредихин Александр

6 мая 2020 г.

Задача 1

Задача: Имеются окрашенные прямоугольные таблички трёх типов: черный квадрат размера 2×2, белый квадрат того же размера и серый прямоугольник 2×1 (последний можно поворачивать на $90°$). Нужно подсчитать число способов F_n замостить полосу размера $2 \times n$. Найдите явную аналитическую формулу для F_n и вычислите F_{30000} по модулю 31.

Для начала составим рекурентную формулу для нахождения кол-ва замощений полоски: $F(1) = 1$ (так как полоску 2×1 можно замостить только серой полоской), $F(2) = 4$ (можем поставить 2 квадратика разного цвета или две вертикальные или горизонтальные серые полоски).

Заметим, что мы можем ставить одну серую вертикальную полоску и тогда задача сведётся к этой же только размер будет на 1 меньше (то есть $F(n-1)$), также можем поставить квадратик какого-то цвета или две горизонтальные полоски и тогда задача с ведётся к этой же только размер полоски будет меньше на 2 (не учитываем вариант с двумя вертикальными, так как он получается применением первого случая дважды). Получаем:

$$F(n) = F(n-1) + 3 \cdot F(n-2)$$
$$F(1) = 1$$
$$F(2) = 4$$

Нам нужно получить явную аналитическую формулу, для этого воспользуемся методом производящих функций (считаем, что $F(0) = 1$ для удобства вывода производящей функции):

Пусть $g(x) = F(1) \cdot x + F(2) \cdot x^2 + \ldots + F(n) \cdot x^n = \sum\limits_{n=0}^{\infty} F(n)x^n$.
Домножим этот ряд на x и на $3x^2$, получим:

$$xg(x) = \sum_{n=0}^{\infty} F(n)x^{n+1} = x + F(2)x^2 + \sum_{n=3}^{\infty} F(n)x^{n+1}$$

$$3x^2g(x) = \sum_{n=0}^{\infty} 3F(n)x^{n+2} = 3F(1) + \sum_{n=2}^{\infty} 3F(n)x^{n+2}$$

Складываем полученные ряды, получаем:

$$g(x)(x+3x^2) = x + \sum_{n=2}^{\infty}(3F(n-2)+F(n-1))x^n = x + g(x) - (F(1) + F(2)x)$$

После преобразования:

$$g(x) = \frac{2x+1}{1-x-3x^2}$$

Раскладываем на простые множители полученную функцию:

$$g(x) = \frac{2x+1}{-3\left(x - \frac{-1+\sqrt{13}}{6}\right)\left(x - \frac{-1-\sqrt{13}}{6}\right)}$$

Методом неопределённых коэффициентов получаем сумму таких дробей:

$$g(x) = \frac{1+\frac{2}{\sqrt{13}}}{-3x+\frac{-1+\sqrt{13}}{2}} + \frac{1-\frac{2}{\sqrt{13}}}{-3x+\frac{-1-\sqrt{13}}{2}}$$

Теперь находим коэффициент при x^n раскладывая слагаемые в ряд используя расширенные биноминальные коэффициенты

$$g(x) = \frac{2+\frac{4}{\sqrt{13}}}{-1+\sqrt{13}\left(1-\frac{6}{-1+\sqrt{13}}x\right)} + \frac{2-\frac{4}{\sqrt{13}}}{-1-\sqrt{13}\left(1-\frac{6}{-1-\sqrt{13}}x\right)}$$

Получается:

$$F(n) = \frac{2\sqrt{13}+4}{-\sqrt{13}+13} \cdot \left(\frac{6}{-1+\sqrt{13}}\right)^n + \frac{2\sqrt{13}-4}{-\sqrt{13}-13} \cdot \left(\frac{6}{-1-\sqrt{13}}\right)^n$$

Полученная формула является явной для nго члена. Преобразуем её: избавимся от иррациональности в знаменателе и приведём подобные слагаемые:

$$F(n) = \frac{(13+\sqrt{13})(2\sqrt{13}+4)}{169-13}\left(\frac{6+6\sqrt{13}}{12}\right)^n - \frac{(2\sqrt{13}-4)(13-\sqrt{13})}{156}\left(\frac{-6(\sqrt{13}-1)}{12}\right)^n$$

$$F(n) = \frac{30\sqrt{13}+78}{156}\left(\frac{1+\sqrt{13}}{2}\right)^n - \frac{30\sqrt{13}-78}{156}\left(\frac{1-\sqrt{13}}{2}\right)^n$$

В итоге:

$$F(n) = \frac{15\sqrt{13}+39}{78}\left(\frac{1+\sqrt{13}}{2}\right)^n - \frac{15\sqrt{13}-39}{78}\left(\frac{1-\sqrt{13}}{2}\right)^n \qquad (1)$$

Получили похожую задачу семинарской только для другой аналитической формулы. Производим похожие рассуждения:

Проверим 13 квадратичный вычет по модулю p или нет (сразу проверим для $p = 29$ и $p = 31$)
для $p = 31$ (аналогично примеру из 3ей задачи)

$$\left(\frac{3}{31}\right) =_6 \left(\frac{31}{13}\right) = \left(\frac{5}{13}\right) = \left(\frac{13}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -\left(\frac{3}{2}\right) = -\left(\frac{1}{2}\right) = -1$$

То есть получаем, что по модулю 31 это не квадротичный вычет. Для $p = 29$

$$\left(\frac{13}{29}\right) = \left(\frac{29}{13}\right) = \left(\frac{3}{13}\right) = \left(\frac{13}{3}\right) = \left(\frac{1}{3}\right) = 1$$

Это квадратичный вычет, поэтому можем найти $\sqrt{13}$, подставляем в уравнение и находим $F_n \mod p$ как любую другую формулу используя свойства вычетов и сравнений по модулю (смотреть задачу 2).

В этом случае 13 не вычет по модулю 31. Многочлен $x^2 - 13$ неприводим в $\mathbb{Z}_p[x]$, поэтому по нему можно факторизовать, и рассматривать вычеты не просто в виде чисел от 0 до p, а вычеты — многочлены степени не более 1 и коэффициентами из $\mathbb{Z}_p$. Такая конструкция называется алгебраическим расширением поля, и также реализована для комплексных чисел: многочлен $i^2 + 1$ от переменной i неприводим на $\mathbb{R}$, поэтому рассматриваются многочлены степени не более 1, и составляют они привычное $\mathbb{C}$. Операции с многочленами в таком алгебраическом расширении работают так: как только встречаем x^2, заменяем на 13 (i^2 на -1), и снова остаёмся среди тех же остатков степени не более 1.

Получается, заменяем $\sqrt{13} = x$ находим обратные элементы по модулю 31 к 2 и к 78 (делаем алгоритмом Евклида, как в задаче 3), получаем такую формулу:

$$F_n = (30x + 78)\,(16 + 16x)^n - (30x - 78)\,(16 - 16x)^n\,.$$

Ненулевые многочлены из $\mathbb{Z}_p[x]/(x^2 + 13)$, которых $31^2 - 1 = 960$, образуют конечное поле. Это значит, что мультипликативная группа этого поля, то есть поле без нуля (обозначается как $(\mathbb{Z}_p[x]/(x^2 + 13))^{\times}$), циклична, то есть существует генератор — элемент, который в порождает все остальные своими разными степенями.
Всего элементов 960, поэтому, если генератор g, $g^{960} = g$, или $g^{960} = 1$.
$\forall (ax + b)\ \exists t : g^t = ax + b \implies (ax + b)^{960} = g^{960t} = 1^t = 1$.
Ищем для $k = 30000$, $k \mod 960 = 240 \mod 960$
Следовательно, $F_k = (30x + 78)\,(16 + 16x)^{240} - (30x - 78)\,(16 - 16x)^{240}$.
Считаем $(16 \pm 16x)^{240}$ пошаговым возведением в квадрат до 16 степени, получаем $15(\mp x + 1)$. Затем возводим этот многочлен в 15ую степень: получили для 2ой и 4ой то есть:

$$19(\pm x + 12) \cdot 3(\pm x + 20) \cdot 16\,(\mp x - 6) \cdot 15(\mp x + 1) = 9(\pm x - 6)$$

(каждый раз перемножаю многочлены и затем делю с остатком на многочлен $x^2 + 13$ произвожу операции с полученным остатком и так далее).

Подставляем полученное выражение в формулу, получаем:

$$F_k = 9(30x + 78)(x - 6) - 9(30x - 78)(-x - 6)$$

$$F_k = \left[30x^2 - 180x + 78x - 468 - \left(-30x^2 - 180x + 78x + 468\right)\right]$$

$$F_k = 9\left[60x^2 - 936\right] = -9 \cdot 156 \mod 31 = 22$$

Ответ: 22 (когда пересчитывал ещё раз, получилось 1)

Задача 2

Задача: Решите предыдущую задачу по модулю 29.

Мы выяснили, что 13 является квадратичным вычетом по модулю 29. Найдём $\sqrt{13}$ решив уравнение: $x^2 = 13 \mod 29$ решаем аналогично 3ей задаче, получаем $x = 10, 19$. Подставляем эти значения в уравнение (1), получаем:

$$\frac{15\cdot 19+39}{78}(10)^{30000}-\frac{15\cdot 19-39}{78}(9)^{30000}=10^{30000}-9^{30000}=25 \mod 29$$

(остаток ищем пользуясь малой теоремой Ферма)

Ответ: 25

P.S. подставил значение $x=10$ и почему-то получил другой ответ (28), перепроверил, вроде бы нигде не ошибаюсь, но должен же быть один остаток так как F_{30000} - конкретное число, у которого может быть 1 остаток при делении на 29. В этом не смог до конца разобраться.

Задача 3

Задача:

а) Делится ли $4^{1356}-9^{4824}$ на 35? Делится ли $5^{30000}-6^{123456}$ на 31?

Решение: заметим, что $35=5\cdot 7$, а $4^{1356}-9^{4824}=2^{2712}-3^{9648}$. Применяем малую теорему Ферма (так как 2, 3 - простые числа) для 5 и для 7:

$$2^4=1(\text{mod } 5) \quad \text{так как } 4|2712 \rightarrow 2^{2712}=1(\text{mod } 5)$$
$$3^4=1(\text{mod } 5) \quad \text{так как } 4|9648 \rightarrow 3^{9648}=1(\text{mod } 5)$$

Получили равные остатки, при вычитании получим 0, то есть наша разность делится на 5: $4^{1356}-9^{4824}=0(\text{mod } 5)$, покажем, что она будет делиться и на 5 аналогично:

$$2^6=1(\text{mod } 7)\rightarrow 2^{2712}=1(\text{mod } 7)$$

$$3^6=1(\text{mod } 7)\rightarrow 3^{9648}=1(\text{mod } 7)$$

Получили, что $4^{1356}-9^{4824}=0(\text{mod } 7)$. То есть делится и на 5 и на 7, следовательно, делится на 35.

Ответ: делится

Рассмотрим: $5^{30000}-6^{123456}$ на 31. Тут 31 - простое число, поэтому можно снова применить малую теорему Ферма:

$$5^{30}=1(\text{mod } 31)\rightarrow 5^{30000}=1(\text{mod } 31)$$

$$6^{30} = 1(\text{mod } 31) \to 6^{123450} = 1(\text{mod } 31)$$

Но у нас степень 6ки – 123456: поэтому нам нужно остаток от деления: $6^{123456}(\text{mod } 31) = 6^6(\text{mod } 31) = 1$. Получили равные остатки, при вычитании получится 0, следовательно, эта разность тоже делится.

Ответ: делится

б) Найдите обратные 20 (mod 79), 3 (mod 62).

Решение: с помощью алгоритма Евклида решаем уравнения:

$$20a + 79b = 1$$

79	20	3	19
20	19	1	1
19	1	19	0

$$1 = 20 - 19 = 20 - (79 - 3 \cdot 20) = 4 \cdot 20 - 79$$

Получается, что $a = 4$, $b = 1$. Сделовательно:

Ответ: $4 = 20^{-1}(\text{mod } 79)$

Найдём: $3^{-1}(\text{mod } 79) = \quad ?$

$$3a + 62b = 1$$

62	3	20	2
3	2	1	1
2	1	2	0

$$1 = 3 - 2 = 3 - (62 - 3 \cdot 20) = 21 \cdot 3 - 62$$

Получается, что $a = 21$

Ответ: $21 = 3^{-1}(\text{mod } 79)$

в) Найдите все решения уравнения $35x = 10$ (mod 50).

Решение: для этого решим с помощью алгоритма Евклида такое диофантово уравнение:

$$35x + 50y = 10$$

разделим на НОД коэффицинтов в левой части, получим:

$$7x + 10y = 2$$

По алгоритму Евклида:

10	7	1	3
7	3	2	1
3	1	3	0

Получается:

$$1 = 7 - (2 \cdot 3) = 7 - 2\,(10 - 7) = 3 \cdot 7 - 2 \cdot 10$$

$$2 = 6 \cdot 7 - 4 \cdot 10$$

Частное решение: $x_0 = 6$, тогда из курса алгоритмов общее решение записывается как: $x = 6 + 10k$, где k - целое.

Ответ: $x = 6 + 10k$

г) Имеет ли решение сравнение $x^2 = 1597 \mod 2011$

Решение: для этого надо найти $\left(\frac{1597}{2011}\right)$

$$\left(\frac{1597}{2011}\right) =_6 \left(\frac{2011}{1597}\right) =_1 \left(\frac{414}{1597}\right) =_5 \left(\frac{2}{1597}\right)\left(\frac{9}{1597}\right)\left(\frac{23}{1597}\right) =_3$$

$$=_3 -\left(\frac{3}{1597}\right)\left(\frac{3}{1597}\right)\left(\frac{23}{1597}\right) =_6 -\left(\frac{1597}{3}\right)\left(\frac{1597}{3}\right)\left(\frac{1597}{23}\right) =_1$$

$$=_1 -\left(\frac{1}{3}\right)\left(\frac{1}{3}\right)\left(\frac{10}{23}\right) =_2 -\left(\frac{10}{23}\right) =_5 -\left(\frac{2}{23}\right)\left(\frac{5}{23}\right) =_3$$

$$=_3 -\left(\frac{5}{23}\right) =_6 -\left(\frac{23}{5}\right) =_1 -\left(\frac{3}{5}\right) =_6 -\left(\frac{5}{3}\right) =_1 -\left(\frac{2}{3}\right) =_3 1$$

Получили 1, то есть 1597 квадратичный вычет, поэтому решения для этого уравнения есть.
Ответ: имеет

д) Найдите наименьшее натуральное число, имеющее остатки 2, 3, 1 от деления на 5, 13 и 7 соответственно.

Решение: составим систему сравнений и будем решать её с помощью КТО:

$$\begin{cases} x = 2 \mod 5 \\ x = 3 \mod 13 \\ x = 1 \mod 7 \end{cases}$$

$M = 5 \cdot 13 \cdot 7$, тогда согласно КТО:

$$x = 2 \cdot \frac{455}{5}\left(\left(\frac{455}{5}\right)^{-1} \bmod 5\right) + 3 \cdot \frac{455}{13}\left(\left(\frac{455}{13}\right)^{-1} \bmod 13\right)$$

$$+ 1 \cdot \frac{455}{7}\left(\left(\frac{455}{7}\right)^{-1} \bmod 7\right) == 182(91^{-1} \bmod 5) + 105\left(35^{-1} \bmod 13\right) +$$

$$+ 65\left(65^{-1} \bmod 7\right) = 182 + 105 \cdot 3 + 65 \cdot 4 = 757 \bmod 455 = 302$$

Обратные элементы нахожу с помощью алгоритма Евклида аналогично пункту б. Конечный результат беру по модулю 455 так как в задании требуется наименьшее число.

Ответ: 302

Задача 4

Задача: Найти все генераторы для $(\mathbb{Z}/19\mathbb{Z})^{\times}$.

Из семинара: x является генератором, если: $x^{p-1} = 1 \mod p$, $x^{\frac{p-1}{p_i}} \neq 1 \mod p$. В нашем случае получаем следующую систему:

$$\begin{cases} x^{18} = 1 \mod 19 \\ x^3 \neq 1 \mod 19 \\ x^6 \neq 1 \mod 19 \end{cases}$$

С помощью неё проверяем для каждого числа от 2 до 19 эти условия и определяем генераторы группы. Например, для 10: $10^18 = 1 \mod 19 \quad 10^9 = 18 \neq 1 \quad 10^6 = 11 \neq 1$, следовательно, 10 это генератор. Аналогичным образом проверяем и получаем

Ответ: 2, 3, 10, 13, 14, 15

Задача 5

Задача: Предложите полиномиальный алгоритм нахождения количества натуральных решений диофантова уравнения $ax + by = c$.

Рассмотрим самый общий случай, когда не один из коэффициентов не равен 0 и НОД$(a, b)|c$. Тогда диофантово уравнение в целых числах имеет бесконечно много решений и они записываются с использованием алгоритма Евклида, как:
$x = x_0 + b'k$
$y = y_0 - a'k$
Где k – целое число, а a', b' – коэффициенты после деления на НОД(a, b).
Из курса алгоритмов знаем, что алгоритм Евклида работает за полиномиальное время от длины входа (то есть от длины битовой записи числа). Понятно, что количество решений в натуральных числах конечно, так как из формулы решения видно при увелечении x, значение y уменьшается и когда-то станет отрицательным также работает наоборот для x.

Чтобы определить количество натуральных решений сначала найдём наименьший $x > 0$ (то есть найдём те k для которых значение x натурально). Это мы сможем сделать за $O(1)$, так как мы знаем смещение и частное решение.

Сделаем аналогично для y и найдём тот промежуток для k где решения y принимают натуральные значения (также делаем за $O(1)$). Пересекаем полученные промежутки и получаем отрезок и количество целых чисел в нём и есть количество натуральных решений по построению (и x и y будут натуральными) (пересечение работает за полиномиальное время).
Получили алгоритм, находящий количество натуральных решений за полиномиальное время.

Задача 6

Задача: 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.

Решение 1: построим функцию полиномиальной сводимости f следующим образом: так как $L \in \mathcal{NP}$ то она решается с помощью сертефиката с предикатом, поэтому функция $f(w) = (M, w)$ это МТ, которая подставляется все сертефикаты в предикат и проверяет, чему он будет равен. Если он будет равен 1, то она возвращает пару из МТ и слова, на котором она останавливается («создаёт» эту МТ сама). Если при подставлении сертефикатов предикат будет равен 0, то возвращает пару из

МТ и слова, на котором она **НЕ** останавливается. Получаем:

$$w \in L \to f(w) = (M, w) - \text{останавливается} \to f(w) \in STOP$$
$$w \notin L \to f(w) = (M, w) - \text{не останавливается} \to f(w) \notin STOP$$

Получили определение полиномиальной сводимости: функция работает за полином, так как размер сертефиката и вычисление предиката полиномиальны.

Решение 2: знаем, что любая $L \in \mathcal{NP}$ полиномиально сводится к задаче $3SAT$. Возбемём МТ, которая будет перебирать все возможные значения набора в $3SAT$, если она находит выполняющий, то останавливается, если нет, то работает бесконечно долго, то есть эта МТ остановится тогда и только тогда, когда будет найден выполняющий набор.

Так как размер $3SAT$, конечный то мы можем свести эту задачу к $STOP$ за полиномиальное время (так как сведение к $3SAT$ происходит за полиномиальное время, и передача на вход МТ, так как размер формулы конечен тоже)

Задача 7

Задача: Постройте NP-сертификат простоты числа $p = 3911$, $g = 13$. Известными простыми считаются только числа 2, 3, 5.

В конце семинара был показан алгоритм построения сертефиката для проверки простоты числа: он состоит из генератора циклической группы для простого числа, разложение $p - 1$ на простые множители и рекурсивно сертификаты для множителей $p - 1$. Построим его для нашего простого числа: генератор для каждой группы будем находить из условий $x^{p-1} = 1 \mod p$, $x^{\frac{p-1}{p_i}} \neq 1 \mod p$. Поэтому:

- $p = 3910, \quad g = 13, \quad p - 1 = 3910 = 2 \cdot 5 \cdot 17 \cdot 23$. 2 и 5 известно, что простые, поэтому нужно делать аналогичные сертификаты для 17 и 23
- $p = 17, \quad p - 1 = 16 = 2^4$
  $g = 3$, тогда $3^{\frac{17-1}{2}} = 2^8 \neq 1 \mod 17, \quad 3^{16} = 1 \mod 17$ следовательно, $g = 3$ – генератор.

- $p = 23, \quad p - 1 = 2 \cdot 11$. Аналогично находим, что генератор $g = 5$. Появилось 11, для него проделываем аналогичные действия.

- $p = 11, \quad p - 1 = 2 \cdot 5$. Генератор: $g = 2$.

В итоге получаем такой сертефикат (значения идут в порядке описаных выше рассуждений):

Ответ: 13, 2, 5, 17, 23, 3, 2, 5, 2, 11, 2, 2, 5