Содержание

Дискретная математика. HSE-SE-DM-HW2.

Ахундов Алексей Назимович

Октябрь 2020

1 Задача 1

Докажем по индукции по n.
База: $n = 1 : \dfrac{1(1+1)(2*1+1)}{6} = 1^2$, верно.
Предполагаем, что для произвольного n утверждение верно. Докажем, что верно и для $n+1$:
Имеем: $1^2+2^2+\cdots+n^2 = \dfrac{n(n+1)(2n+1)}{6}$. Добавим к обоим частям $(n+1)^2$.
$1^2+\cdots+n^2+(n+1)^2 = \dfrac{n(n+1)(2n+1)}{6}+(n+1)^2 = \dfrac{(n+1)(n(2n+1)+6(n+1))}{6} =$
$= \dfrac{(n+1)(2n^2+7n+6)}{6} = \dfrac{2(n+1)(n+2)(n+3/2)}{6} = \dfrac{(n+1)((n+1)+1)(2(n+1)+1)}{6}$

2 Задача 2

Докажем по индукции по числу городов.
База: для одного города из него можно добраться до него самого (потому что мы уже в нем)
Шаг: возьмем граф на $n+1$ вершине и удалим оттуда произвольную вершину D со всеми её ребрами. По предположению индукции, у нас найдется вершина V для которой справдливо доказываемое, тогда если добавить D, то если в него входит чье-нибудь ребро, то ответ сохраняется, иначе из этого города можно добраться до V, то есть ответ теперь D.

3 Задача 3

Докажем по индукции для n.
База: $n = 1 \implies 1 + \cdots + \dfrac{1}{k} \geq 1 \implies k = 1$. Верно.
Предполагаем, что для произвольного $n : 1 + \cdots + \dfrac{1}{k} \geq n$ найдется k
Тогда сведем задачу к тому, чтобы для произвольного l показать, что найдется такое число $r > l$, что: $\dfrac{1}{l} + \dfrac{1}{l+1} \cdots + \dfrac{1}{l+r} \geq 1$.

Если мы это сделаем, то просто выберем $l = k+1$ и найдем r, а затем прибавим к неравенству предположение индукции и получим искомое для $n+1$.

Рассмотрим для $l' > l$ выражение $\frac{1}{l} + \frac{1}{l+1} + \dots + \frac{1}{l+l'}$.
Так как $\frac{1}{l+1} \geq \frac{1}{l+l'}$, $\frac{1}{l+2} \geq \frac{1}{l+l'}, \dots$, то $\frac{1}{l} + \dots + \frac{1}{l+l'} \geq \frac{1}{l} + \frac{l'}{l+l'}$.
Пусть теперь $l' = l$, тогда $\frac{1}{l} + \frac{1}{l+1} + \dots + \frac{1}{l+l'} \geq \frac{1}{l} + \frac{1}{2} \geq \frac{1}{2}$
То есть для любого l мы смогли вычленить подпоследовательность, сумма элементов которой больше равна $\frac{1}{2}$.
Теперь рассмотрим $\frac{1}{l} + \frac{1}{l+1} \dots + \frac{1}{l+r}$. Здесь мы можем вычленить две подпоследовательности суммой больше равной $\frac{1}{2}$. То есть общяя сумма больше равна единице.

4 Задача 4

Вычисление двух последних цифр (в десятичной системе счисления) эквивалентно нахождению остатка по модулю сто, так как любо число $A = 100 \cdot \overline{D_1 D_2 \dots D_{n-2}} + 10 * D_{n-1} + D_n$.

Рассмотрим 99^{1000} по модулю 100:
$99 \cdot 99^{999} \equiv (-1) \cdot 99^{999} \equiv \dots \equiv (-1)^{1000} \equiv 1 \ (mod\ 100)$

Таким, образом последние две цифры этого числа: 0 и 1 ($1 = 10 \cdot 0 + 1$).

5 Задача 5

Пусть k, l - **остатки** при делении соответственно Пусть $a^3 \equiv k \ (mod\ a-b)$, $b^3 \equiv l \ (mod\ a-b)$
Рассмотрим их разность: $a^3 - b^3 = (a-b)(a^2 + ab + b^2) \equiv 0 \ (mod\ a-b)$
С другой стороны: $a^3 - b^3 \equiv k - l \ (mod\ a-b)$, тогда $k - l = 0 \implies k = l$.
Это справедливо при $k = l \implies$ Ч.Т.Д.

6 Задача 6

По условию $5m + 3n \equiv 0 \ (mod\ 11) \implies 5m + 3n = 11\alpha \implies 5m = 11\alpha - 3n$
Тогда $11\alpha - 3n \equiv 0 \ (mod\ 5) \implies 5 \cdot (2\alpha) + \alpha - 3n \equiv 0 \ (mod\ 5) \implies \alpha = 5\beta + 3n$.

Подставим α обратно:
$5m = 11 \cdot (5\beta + 3n) - 3n = 55\beta + 30n$

$m = 11\beta + 6n \implies m - 6n = 11\beta$

Получается, что $m \equiv 6n \ (mod\ 11)$, тогда
$m \equiv 6n \ (mod\ 11) \overset{(9,11)=1}{\implies} 9m \equiv 54n \ (mod\ 11)$
$9m \equiv 55n - n \ (mod\ 11) \implies 9m + n \equiv 0 \ (mod\ 11)$. Ч.Т.Д.

7 Задача 7

7.1 Пункт a

В таком случае $x + M \leq M - 1 + M = 2M - 1 \implies x < 2M$.
Тогда остаток от деления $x + M$ на $2M$ равен самому $x + M$.
$I(x) = x + M - M = x$. Ч.Т.Д.

7.2 Пункт b

Здесь и дальше обозначим для удобства записи остаток$(a, b) = a \ \% \ b$

Рассмотрим $I(x) + I(y) = (x + M) \ \% \ 2M + (y + M) \ \% \ 2M - 2M$.
Фактически мы имеем:
$x + M \equiv (x + M) \ \% \ 2M \ (mod\ 2M)$
$y + M \equiv (y + M) \ \% \ 2M \ (mod\ 2M)$

Тогда: $x + y + 2M \equiv x + y \equiv (x + M) \ \% \ 2M + (y + M) \ \% \ 2M \ (mod\ 2M)$
Получаем: $(x + M) \ \% \ 2M + (y + M) \ \% \ 2M = (x + y) \ \% \ 2M$
Следовательно: $I(x) + I(y) = (x + y) \ \% \ 2M - 2M$

$I(I(x) + I(y)) = ((x + y) \ \% \ 2M + M) \ \% \ 2M - M$

Докажем, что $(a+b)\ \%\ M = (a\ \%\ M + b)\ \%\ M$ (здесь M - **произвольное** натуральное число)
Пусть $a = l \cdot M + a\ \%\ M$, тогда $(a+b)\ \%\ M = (l \cdot M + a\ \%\ M + b)\ \%\ M =$
$= (a\ \%\ M + b)\ \%\ M$. Ч.Т.Д.

Тогда: $I(I(x)+I(y)) = (x+y+M)\ \%\ 2M - M = I(x+y)$. Ч.Т.Д.

7.3 Пункт c

Докажем, что $(a \cdot b)\ \%\ M = ((a\ \%\ M) \cdot (b\ \%\ M))\ \%\ M$ (здесь M - произвольное натуральное число)
$a = \alpha M + a\ \%\ M,\ b = \beta M + b\ \%\ M$
$(\alpha M + a\ \%\ M) \cdot (\beta M + b\ \%\ M) =$
$= \alpha\beta M + \alpha(b\ \%\ M) \cdot M + \beta(a\ \%\ M) \cdot M + (a\ \%\ M) + (b\ \%\ M) \equiv$
$\equiv (a\ \%\ M) + (b\ \%\ M)\ (mod\ M)$. Ч.Т.Д.

Рассмотрим $I(x) \cdot I(y) = ((x+M)\ \%\ 2M - M) \cdot ((y+M)\ \%\ 2M - M) =$
$= ((x+M)\ \%\ 2M) \cdot ((y+M)\ \%\ 2M) - M((x+M)\ \%\ 2M + (y+M)\ \%\ 2M) - M^2 =$
$\equiv (x+M) \cdot (y+M) - M \cdot (x+M) - M \cdot (y+M) - M^2\ (mod\ 2M) \equiv xy - 2M^2 \equiv$
$xy\ (mod\ 2M)$

Тогда $I(I(x) \cdot I(y)) = (I(x) \cdot I(y) + M)\ \%\ 2M - M = (xy+M)\ \%\ 2M - M = I(xy)$

8 Задача 8

Увеличивая степень функции f при подсчете очередного элемента мы будем складывать дроби со знаменателем - двойкой. При этом "этажи"(при наличии таких) выше ситуация такая же (поскольку они получены рекурсивно сложением дробей со знаменателем 2), поэтому каждый член представим для некоторого A как $\forall i:\ f_i^p(a) = \dfrac{A}{2^p}$
При этом в числителе при $a_i,\ \dots\ , a_n$ (в порядке возрастания) будут стоять соответствующие биномиальные коэффициенты, взятые по модулю (так как $i+p$ будет возможно больше n), потому что построение аналогично треугольнику Паскаля (для отдельного икса мы "складываем"два соседних элемента с предыдущей строки). То есть:
$f_i^p(a) = \dfrac{\binom{p}{0}a_i + \binom{p}{1}a_{(i+1) \mod n} +\ \dots\ + \binom{p}{p}a_{(i+p) \mod n}}{2^p}$
Получается, что в какой-то момент все элементы для некоторой степени $p: f^p(a)$ (из-за модулей в индексах) будут равны, а значит мы можем еще раз взять функцию от такого набора чисел и получить $f^{p+1}(a) = f^p(a) \implies$ первое утверждение верно.

9 Задача 9

Если a не делится на 4, то a не может делиться на степень двойки большую 1 (имеется ввиду число 2^1), и, так как оно делится на 2, двойка входит в разложение a в первой степени ($a > 1$). Тогда на каждый нечетный делитель n найдется один четный равный $2 \cdot n$, и на каждый четный делитель m найдется один нечетный равный $\frac{m}{2}$ (мы установили биекцию), то есть их поровну.

10 Задача 10

Сумма цифр этого числа равна $1 \cdot 100 + 2 \cdot 100 = 300$, значит число делится на 3, но оно не делится на 9, а значит оно точно не является квадратом.

11 Задача 11

Пусть их конечное количество. Тогда рассмотрим все простые числа, которые меньше последнего простого числа, имеющего вид $6k + 5$. Обозначим их $p_1, \ldots, p_n$.
Описанные в задаче числа представимы как $6l - 1$, т.к. $5 \equiv -1 \ (mod\ 6)$.
Тогда возьмем число $\alpha = p_1 \cdot p_2 \cdot \dots \cdot p_n - 1$, оно не делится на $p_1, p_2 \ldots p_n$, а значит простое, но при этом так как $p_1 = 2,\ p_2 = 3$, α имеет вид $6p_3 \ldots p_n - 1$.
Противоречие.

12 Задача 12

Рассмотрим произвольные целые x, y. Пусть $gcd(x, y) = \alpha$, тогда $x = \alpha x', y = \alpha y'$, при этом x' и y' взаимно простые (иначе их общие множители пошли бы в α).
Тогда $lcm(x, y) = \alpha x' y'$ (он будет минимальным, поскольку таковой точно должен делиться на наибольший общий делитель этих чисел, а x' и y' взаимнопростые)

$$x \cdot y = \alpha^2 x' y' = gcd(x, y) \cdot lcm(x, y) \implies lcm(x, y) = \frac{xy}{gcd(x, y)}$$

.
Получив это, преобразуем левую часть:

$$lcm(x, y, z) = lcm(lcm(x, y), z) = \frac{lcm(x, y) z}{gcd(lcm(x, y), z)}$$
$$= \frac{xyz}{gcd(lcm(x, y), z) \cdot gcd(x, y)}$$

.
Осталось показать, что $gcd(lcm(x, y), z) = \dfrac{gcd(x, z) \cdot gcd(y, z)}{gcd(x, y, z)}$.

Рассмотрим факторизацию $x = p_1^{\alpha_1} \dots p_n^{\alpha_n},\ y = p_1^{\beta_1} \dots p_n^{\beta_n},\ z = p_1^{\gamma_1} \dots p_n^{\gamma_n}$ для n больше равного наибольшего количества простых в этих числах.

$$lcm(x, y) = p_1^{max(\alpha_1, \beta_1)} \dots p_n^{max(\alpha_n, \beta_n)}$$
$$gcd(lcm(x, y), z) = p_1^{min(max(\alpha_1, \beta_1), \gamma_1)} \dots p_n^{min(max(\alpha_n, \beta_n))}$$

С другой стороны

$$\frac{gcd(x, z) \cdot gcd(y, z)}{gcd(x, y, z)} = p_1^{min(\alpha_1, \gamma_1) + min(\beta_1, \gamma_1) - min(\alpha_1, \beta_1, \gamma_1)} \dots$$

Равенство степеней $p_1 : min(\alpha_1, \gamma_1) + min(\beta_1, \gamma_1) -$
$- min(\alpha_1, \beta_1, \gamma_1) = min(max(\alpha_1, \beta_1), \gamma_1)$

Если минимальное из этих чисел $\gamma_1 :\ \gamma_1 + \gamma_1 - \gamma_1 = \gamma_1$ - верно.
Иначе же если это $\alpha_1 :\ \alpha_1 + min(\beta_1, \gamma_1) - \alpha_1 = min(\beta_1, \gamma)$ - верно.
Иначе если это $\beta_1 :\ min(\alpha_1, \gamma_1) + \beta_1 - \beta_1 = min(\alpha_1, \gamma_1)$ - верно.
Равенство доказано. Аналогично для других степеней, получаем искомое:
$gcd(lcm(x, y), z) = \dfrac{gcd(x, z) \cdot gcd(y, z)}{gcd(x, y, z)}$

Тогда вернемся к выражению в начале

$$\begin{aligned} lcm(x, y, z) &= \frac{xyz}{gcd(lcm(x, y), z) \cdot gcd(x, y)} \\ &= \frac{xyz \cdot gcd(x, y, z)}{gcd(x, z) gcd(y, z) gcd(x, y)} \end{aligned}$$

. Ч.Т.Д.

13 Задача 13

По малой теореме Ферма: $p^2 - 1 \equiv 0$ ($mod\ 3 = 2 + 1$). Также $p^2 - 1 = (p - 1)(p + 1)$. По нечетности p (так как p - простое и больше двух) : $(p - 1)$ и $(p + 1)$ четные, так как в обоих случаях меняется четность. Докажем, что их произведение делится на 8. Пусть $n = p - 1$ не делится на 4, тогда оно точно делится на 2: $n = 2k$, причем k нечетное, тогда, прибавив к нему 2 получим $n + 2 = p + 1 = 2(k + 1)$, тогда $k + 1$ уже точно четное, значит либо $p - 1$, либо $p + 1$ делится на 4, а другое делится на 2, т.е. произведение делится на 8. Таким образом получаем, что $p^2 - 1$ делится и на 8, и на 3. В итоге $p^2 - 1$ делится на 24. Ч.Т.Д.

14 Задача 14

Фактически, требуется показать что $\forall a_1, b\ \exists n, i, j : (a_i, a_j) \neq 1$
Для случая $a_1 \neq 0$ рассмотрим элемент под номером $|a_1| + 1 :\ \ a_{|a_1|+1} = a_1 + |a_1| \cdot b \equiv 0\ (mod\ a_1)$.
В случае, когда $a_1 = 0$ ответ сразу очевиден - любые два члена в таком случае не являются взаимно простыми.

15 Задача 15

Требуется доказать, что $gcd(n^2 - n + 1, n^2 + 1) = 1$, иначе числитель и знаменатель можно поделить на это число.

$$\begin{aligned} gcd(n^2 - n + 1, n^2 + 1) &\overset{\text{Из второго аргумента вычитаем первый}}{=} gcd(n^2 - n + 1, n^2 + 1 - n^2 + n - 1) \\ &\overset{\text{Преобразовываем выражение второго аргумента}}{=} gcd(n^2 - n + 1, n) \\ &\overset{\text{Из первого аргумента n - 1 раз вычитаем второй}}{=} gcd(1, n) = 1 \end{aligned}$$

.
Ч.Т.Д.

16 Задача 16

16.1 Пункт а

По условиям задачи $\gcd(e, m) = 1,\ ed \equiv 1\ (mod\ m)$.
Перепишем последнее: $ed = km + 1 \implies ed - km = 1$ для некоторого $k \in \mathbb{Z}$.

Это линейное диофантовое уравнение относительно d и k, причем так как $\gcd(e, m) = 1$, решения у него есть. Для его нахождения применим расширенный алгоритм Евклида, который работает за время лучше, чем у алгоритма полного перебора.

16.2 Пункт b

Докажем полезную для решения данного пункта задачи лемму:

$$\forall p, q \text{ are primes}: \ \varphi(p \cdot q) = (p-1) \cdot (q-1)$$

Используем определение функции φ и рассмотрим числа от 1 до pq.
Не взаимнопросты с ним числа вида $p,\ 2p,\ \dots\ ,\ q \cdot p$ и $q,\ 2q,\ \dots\ ,\ (p-1)q$ - всего таких $p+q-1$ (исключая во втором случае число pq, так как оно уже посчитано для p).

$$\varphi(pq) = p \cdot q - p - q + 1 = p(q-1) - q + 1 = (q-1)(p-1)$$

Ч.Т.Д.

По условиям задачи:

$$C \equiv P^e \ (mod\ n)$$

Возведем это сравнение в степень d

$$C^d \equiv P^{d \cdot e} \ (mod\ n)$$

При этом нам также известно, что

$$P' \equiv C^d \ (mod\ n)$$

Тогда получаем

$$P' \equiv P^{ed} \ (mod\ n)$$

Рассмотрим

$$ed \equiv 1 \ (mod\ m)$$

Заметим, что $m = (p-1)(q-1)$, поэтому, используя лемму выше, получим $m = \varphi(pq) = \varphi(n)$, тогда

$$ed \equiv 1 \ (mod\ \varphi(n))$$

$$P' \equiv P^{ed} \equiv P^{ed \mod \varphi(n)} \equiv P \ (mod\ n)$$

А поскольку $1 < P, P' < n \implies P = P'$. Ч.Т.Д.

17 Задача 17

Если хотя бы одно число не кратно 11, то по малой теореме Ферма:
$\forall s : s^{11-1} \equiv 1 \ (mod\ 11)$, то есть остаток больше нуля, но, так как чисел всего 6, меньше 11. Значит, посылка верна только когда все числа делятся на 11, тогда произведение очевидно будет делиться на 11^6.

18 Задача 18

Заметим, что пара $x = 7,\ y = -7$ является решением нашего уравнения
Рассмотрим $19x + 22y = 19 \cdot 7 - 22 \cdot 7 = -21$

$$19 \cdot (x - 7) = -22 \cdot (7 - y)$$
$$19 \cdot (7 - x) = 22 \cdot (7 - y)$$

Поскольку 19 и 22 взаимнопростые, множитель при любом них должны делиться на противоположный первый множитель, то есть, например:

$$\forall k \in \mathbb{Z}:\ 7 - x = 22 \cdot k$$

$$x = 7 - 22k$$

Причем этого необходимо и достаточно для образования решений, потому что таким образом y находится однозначно (с точностью до k):

$$19 \cdot (7 - 22k) + 22y = -21$$
$$y = \frac{-21 - 19 \cdot 7 + 19 \cdot 22k}{22} = 19k - 7$$

Ответ: $\forall k \in \mathbb{Z} : \begin{cases} x = -22k + 7 \\ y = 19k - 7 \end{cases}$

19 Задача 19

Рассмотрим диофантово уравнения для некоторого y

$$39x = 221y + 104 \implies 39x - 221y = 104$$

Решим его и посмотрим на x. Для того, чтобы ответить на вопрос задачи, необходимо и достаточно "зажать"все решения x по модулю 221.

$$gcd(39, -221) = 13$$

Решения есть, так как $13 \mid 104$. Упростим, поделив на 13

$$3x - 17y = 8$$

Заметим, что пара $x = 14, y = 2$ является решением этого уравнения.

$$3x - 17y = 3 \cdot 14 - 17 \cdot 2$$

$$3(x - 14) = 17(y - 2)$$

Рассмотрим для некоторого $k \in \mathbb{Z} : x - 14 = 17k$

$$\begin{cases} x = 17k + 14 \\ y = \dfrac{51k + 34}{17} = 3k + 2 \end{cases}$$

Далее заметим, что $17 \mid 221$, а значит достаточно рассмотреть все $k < \dfrac{221}{17} = 13$, поскольку далее остатки по модулю 221 будут повторяться

k	x	$x \mod 221$
0	14	14
1	31	31
2	48	48
3	65	65
4	82	82
5	99	99
6	116	116
7	133	133
8	150	150
9	167	167
10	184	184
11	201	201
12	218	218

20 Задача 20

Перепишем систему в нормальном виде (упростим остатки)

$$\begin{cases} x \equiv 10 \pmod{12} \\ x \equiv 6 \pmod{11} \\ x \equiv 4 \pmod{5} \end{cases}$$

Пусть из первого уравнения для некоторого $k \in \mathbb{Z}$

$$x = 12k + 10$$

Тогда из второго уравнения

$$12k + 10 \equiv 6 \pmod{11}$$

$$k \equiv 7 \pmod{11}$$

Представим k для некоторого $r \in \mathbb{Z}$

$$k = 11r + 7$$

Тогда из третьего уравнения

$$12k + 10 \equiv 4 \pmod{5}$$

$$12 \cdot (11r + 7) + 10 \equiv 4 \pmod{5}$$

$$132r + 94 \equiv 2r + 4 \equiv 4 \pmod{5}$$

Отсюда $r = 5m$ для некоторого $m \in \mathbb{Z}$. Получаем

$$k = 55m + 7$$

А отсюда найдем все решения x

$$\forall m \in \mathbb{Z}: \; x = 12 \cdot (55m + 7) + 10 = 660m + 94$$

21 Задача 21

$$\gcd(3^{168} - 1, 3^{140} - 1) = \gcd(3^{168} - 1 - 3^{140} + 1, 3^{140} - 1) = \gcd(3^{140} \cdot (3^{28} - 1), 3^{140} - 1)$$

$$\overset{\text{Прибавим к первому второе}}{=} \gcd(3^{140} \cdot (3^{28} - 1 - 1) + 1, 3^{140} - 1)$$

$$\overset{\text{Проделав это действие } 3^{28}-1 \text{ раз получим}}{=} \gcd(3^{28} - 1, 3^{140} - 1)$$

Таким образом мы видим, что найдется преобразовение делающее со степенями то же самое, что мы делаем и с обычными числами при нахождении gcd (алгоритм Евклида): $\gcd(a^m - 1, a^n - 1) = \cdots = \gcd(a^{m-n} - 1, a^n - 1)$. Осталось всего лишь найти $\gcd(168, 140) = 28$, а значит ответ $3^{28} - 1$.

22 Задача 22

Обозначим $\underbrace{3^{3^{3^{\cdots}}}}_{\text{n копий 3}}$ как $3 \uparrow\uparrow n$. Из теоремы Эйлера получаем:

$$3 \uparrow\uparrow 2020 \underset{46}{\equiv} 3^{3 \uparrow\uparrow 2019 \mod \varphi(46)}$$

$$3 \uparrow\uparrow 2019 \underset{22}{\equiv} 3^{3 \uparrow\uparrow 2018 \mod \varphi(22)}$$

$$3 \uparrow\uparrow 2018 \underset{10}{\equiv} 3^{3 \uparrow\uparrow 2017 \mod \varphi(10)}$$

$$3 \uparrow\uparrow 2017 \underset{4}{\equiv} 3^{3 \uparrow\uparrow 2016 \mod \varphi(4)}$$

$$3 \uparrow\uparrow 2016 \underset{2}{\equiv} 3^{3 \uparrow\uparrow 2015 \mod \varphi(2)}$$

$$3 \uparrow\uparrow 2015 \underset{1}{\equiv} 0$$

Теперь развернем эту цепочку:

$$3 \uparrow\uparrow 2016 \equiv 3^{3 \uparrow\uparrow 2015 \mod \varphi(2)} \underset{2}{\equiv} 1$$

$$3 \uparrow\uparrow 2017 \equiv 3^1 \underset{4}{\equiv} 3$$

$$3 \uparrow\uparrow 2018 \equiv 3^3 \underset{10}{\equiv} 7$$

$$3 \uparrow\uparrow 2019 \equiv 3^7 \underset{22}{\equiv} 9$$

$$3 \uparrow\uparrow 2020 \equiv 3^9 \underset{46}{\equiv} 41$$

Итого получаем в ответе 41.