Домашняя работа №3

Бредихин Александр

1 марта 2020 г.

Задача 1

а) Решить уравнения в целых числах, используя расширенный алгоритм Евклида: $238x + 385y = 133$ (общий вид уравнения: $a \cdot x + b \cdot y = c$)

Найдём $NOD(a, b)$ с помощью обычного алгоритма Евклида и проверим, делится ли на него коэффициент $c = 133$ или нет (если не делится, то уравнение не имеет решение)

a	b	a//b	a%b
385	238	1	147
238	147	1	91
147	91	1	56
91	56	1	35
56	35	1	21
35	21	1	14
21	14	1	7
14	7	2	0

Получается, $NOD(a, b) = 7$. Коэффициент c делится на 7 $\longrightarrow$ Разделим все коэффициенты уравнения на $NOD(a, b) = 7$, получится уравнение: $34x + 55y = 19$. Применяем к полученному уравнению расширенный алгоритм Евклида:

x	y	$34x + 55y$
0	1	55
1	0	34
-1	1	21
2	-1	13
-3	2	8
5	-3	5
-8	5	3
13	-8	2
-21	13	1

Отсюда получаем: $x^* = -21, y^* = 13$, тогда частное решение будет иметь вид:
$x_0 = x^* \cdot \frac{c}{NOD(a,b)} = -21 \cdot 19 = -399$
$y_0 = y^* \cdot \frac{c}{NOD(a,b)} = 13 \cdot 19 = 247$
Откуда получаем общее решение уравнения:
Ответ: $x = -399 + 55k$, $y = 247 - 34k$, где $k \in \mathbb{Z}$

а) Уравнение $143x + 121y = 52$. Найдём $NOD(a, b) = NOD(143, 121)$ с помощью алгоритма Евклида:

a	b	$a//b$	$a\%b$
143	121	1	22
121	22	5	11
22	11	2	0
11	0		

Значит $NOD(a, b) = 11$. Коэффициент $c = 52$ не делится на 11, следовательно, уравнение не имеет решения.
Ответ: нет решения.

Задача 2

Вычислите $7^{13} \mod 167$, используя алгоритм быстрого возведения в степень.

Применяем алгоритм: $13_{10} = 1101_2 \longrightarrow$
$7^{13_{10}} = 7^{1101_2} = 7\left(7^{110_2}\right)^2 = 7\left(\left(7^{11_2}\right)^2\right)^2 = 7\left(7 \cdot 7^2\right)^4 = 7(7 \cdot 49)^4 = [\text{mod } 167] = 7 \cdot (81)^2 = [\text{mod}167] = 7 \cdot 48 = [\text{mod}167] = 2$
Ответ: 2

Задача 3

Докажем корректность даного рекурсивного алгоритма по индукции по x (то есть на каждом шаге рекурсии возвращаемая пара (q, r) – верная):
База индукции: $x = 0 \longrightarrow (q, r) = (0, 0)$ – верно.
Предположение индукции: пусть для пары $\left(\left[\frac{x}{2}\right], y\right)$ – алгоритм вернул верную пару (q, r)
Шаг индукции: покажем, что для пары (x, y) получается верный ответ.
Из П.И. $\left[\frac{x}{2}\right] = q \cdot y + r$ и $r < y$. Домножим это равенство на 2, получается:

$$2 \cdot \left[\frac{x}{2}\right] = 2qy + 2r \tag{1}$$

1 Если x – чётное. Тогда уравнение (1) принимает вид $x = 2qy + 2r$. Пусть $q^* = 2q$ $r^* = 2r$, так как по П.И. $r < y \longrightarrow 2r$ не может превышать y больше, чем в 2 раза (следовательно, можно не брать остаток по модулю, а просто вычитать). Если $r^* \geq y$, тогда нужно проделать следующие операции: $r^* = r^* - y; q^* = q^* + 1$. Теперь $r^* < y$, значит, пара (q^*, r^*) является ответом (что и делает наш алгоритм) – верно.

2 Если x – нечётное. Тогда $2 \cdot \left[\frac{x}{2}\right] = x - 1$, следовательно уравнение (1) принимает вид $x = 2qy + 2r + 1$. Если $2r + 1 \geq y$, то получаем (аналогичные рассуждения предыдущему пункту):

$$x = (2q + 1)\, y + ((2r + 1) - q)$$

И пара $((2q + 1), ((2r + 1) - q))$ - является ответом. Верно.

Алгоритм выводит верные пары, следовательно, корректность доказана по индукции.

Сложность алгоритма:
Числа записаны побитово (n битов каждое число, в худшем случае), следовательно при вызове $\left[\frac{x}{2}\right]$ у числа убирается 1 бит. Составим рекуренту этого алгоритма:

$$T(n) = T(n-1) + n$$

На каждом шаге n операций (побитовое сложение чисел длинной n бит).
Решая рекуренту аналогично задаче 4, получим $\mathcal{O}(n^2)$
Ответ: $\mathcal{O}(n^2)$

Задача 4

1) $T_1(1) = T_1(2) = T_1(3)$
Пошагово раскрываем рекуренту и пользуемся формулой арифметической прогрессии:

$$\begin{aligned} &T_1(n) = T_1(n-1) + cn = T_1(n-2) + c(n-1) + cn = \dots \\ &= T_1(3) + c(4 + \dots + n - 1 + n) = 1 + (n-3) \cdot \tfrac{4+n}{2} = \\ &= c \cdot \tfrac{n^2+n}{2} - 3c + 1 = \theta\left(n^2\right) \end{aligned}$$

Ответ: $\theta\left(n^2\right)$

2) Доказать, что для рекуренты $T_2(n) = T_2(n-1) + 4T_2(n-3)$ (при $n > 3$) справедлива оценка $\log T_2(n) = \Theta(n)$ (в асимптотической оценке основание логарифма неважно, поэтому без ограничения общности возьмём его равным 2).
Доказазываем по индукции по n:
База индукции: $n = 1, 2, 3$ - верно. Предположение индукции: пусть для $\forall k \le n$ - утверждение верно. Докажем для $k = n + 1$
По предположению индукции имеем соотножения (должны быть разные константы, но от этого суть далнейших выкладок не меняется):

$$c_2 \cdot n \le \log T_2(k) \le c_1 \cdot n$$
$$c_2 \cdot n \le \log T_2(k-2) \le c_1 \cdot n$$

Получаем оценку на шаг индукции:

$$T_2(k+1) = T_2(k) + 4T_2(k-2) \le 2^{c_1 k} + 4 \cdot 2^{c_1(k-2)} \le 2^{c_1 k} + \frac{4}{2^{c_1}} \cdot 2^{c_1 k} \le 4 \cdot 2^{c_1 k} \le 4 \cdot 2^{c_1(k+1)}$$

Если возьмём логарифм от полученного неравенства, получим нужное выражение: $\log T_2(k+1) \le C \cdot (k+1)$. Оценка сниза получается также, следовательно, по индукции мы доказали, что $\log T_2(n) = \Theta(n)$.

Задача 5

Заметим, что значение величины $m \cdot u + n \cdot v = inv = 2ab$, так как:

- если $m \ge n$, то значение этой величины: $(m-n)u + n(v+u) = mu - nu + nv + nu = mu + nv = inv$
- иначе: $m(u+v) + (n-m)v = mu + nv = inv$

Получается для любой ветки в цикле наша величина остаётся инвариантной и первоначально равняется $2ab$. После выполнения цикла в одной из переменной m или n будет лежать значение $NOD(a, b)$, а вдругой 0. Также известно соотношение: $NOD(a, b) \cdot NOK(a, b) = ab$, следовательно, после выполнения работы в переменной z будет лежать $2NOK(a, b)$.