Домашнее Задание по алгоритмам №3

Павливский Сергей Алексеевич , 873

24.02.2019

Задание №1

а)

238x + 385y = 133 Пользуясь расширенным алгоритмом Евклида :

- найдем НОД(385;238) -> НОД(238;147) -> НОД(147;91) -> НОД(91;56) ->

-> НОД(56;35) -> НОД(35;21) -> НОД(21;14) -> НОД(14;7) -> НОД(7;0) -> 7

- (1; 0) -> (0; 1) -> (1; -1) -> (-1; 2) -> (2; -3) -> (-3; 5) -> (5; -8) -> (-8; 13) -> (13; -21)

Частное решение :

238 * (-21) + 385 * 13 = 7

Тогда (x, y) = (-399, 247) - частное решение

Пусть 238x + 385y = 133; 238x1 + 385y1 = 133; 238(x - x1) + 385(y - y1) = 0; 34(x - x1) + 55(y - y1) = 0; НОД(34; 55) = 1 -> x - x1 = 55*n1; y - y1 = 34 * n2; n1 , n2 - целые . Подаставляя частные (x1, y1) = (-399, 247) общим решением на (x, y) будет :

x = -399 + 55*n1;

y = 247 + 34*n2;

n1, n2 $\in \mathbb{Z}$

б)

143x + 121y = 52 Пользуясь расширенным алгоритмом Евклида :

- найдем НОД(143;121) -> НОД(121;22) -> НОД(22;11) -> НОД(11;0)

- (1; 0) -> (0; 1) -> (1; -5) -> (-5; 6)

Частное решение :

143 * (-5) + 121 * 6 = 11

Но 52 mod 11 != 0 . Значит решений нет .

Задание №2

$7^{13} = 7^6 * 7^6 * 7 = a$

$7^6 = 7^3 * 7^3 = b$

$7^3 = 7 * 7 * 7 = c$

c mod 167 = 343 mod 167 = 9

b mod 167 = (c mod 167) * (c mod 167) mod 167 = 81 a mod 167 = (b mod 167) * (b mod 167) * 7 mod 167 = 567 * 81 mod 167 =

=66 * 81 mod 167=594 * 9 mod 167=93 * 9 mod 167=837 mod 167=2

Задание №3

Корректность :

Докажем по индукции . База : x = 0 .

Пусть у нас есть некоторый x > 0 , для всех x1 < x алгоритм выдает корректное значение . Тогда (q, r) <- Divide([x/2], y) заполнит в (q, r) такие числа , что [x/2] = y * q' + r' .

1) Если x четно , то x = y *2q' + 2r'. После последующей операции x = y*q + r .

Последующая операция не выполняется , т.к. x четно , а последняя операция обеспечит выполнение неравенства 0 <= r < y .

2) Если x нечетно , то x - 1 = y *2q' + 2r'. После последующей операции x - 1= y*2q' + 2r' + 1 . После последующей операции x - 1= y*2q' + 2r' + 1 . Последующая операция приведет это равенство к x - 1 = y*q + r - 1, т.е. x = y*q + r .

Последняя операция обеспечит выполнение неравенства 0 <= r < y .

Верхняя оценка :

Так как число n-битовое , рекурсивный спуск идет до тех пор , пока число не становится равным 0 , а количество делений не более чем n , то рекурсивных вызовов не более чем n . На каждом шаге рекурсии операций константа , значит верхняя оценка O(n) .

Задание №4

1)

Пусть у нас есть T(n1) , где n1 достаточно большое . Тогда T(n1) = c*n1+T(n1-1) = c*n1 + c*(n1-1) + T(n2-2) = ... = c*n1 + c*(n1-1) + c(n2-2) + ... +

1 + 1 + 1 . Это арифметическая прогрессия , ассимптотика которой - $\theta(n^2)$

2)

Докажем , что 2^{n-3} < T(n) < 2^n по индукции . База индукции :

T(1) , T(2), T(3) - они равны 1 , для них оценка очевидна .

Переход :

Пусть это верно для всех i < n . Тогда :

для n - 1 :

2^{n-4} < T(n-1) < 2^{n-1}

для n - 3 :

2^{n-6} < T(n-3) < 2^{n-3}

$2^{n-6} * 4$ < 4T(n-3) < $2^{n-3} * 4$

T(n) = T(n-1) + 4T(n-3)

Тогда :

2^{n-4} + $2^{n-6} * 4$ < T(n-1) + 4T(n-3) < $2^{n-3} * 4 + 2^{n-1}$

2^{n-3} < T(n) < 2^n

Значит T(n) = $\theta(2^n)$, т.е. log T(n) = $\theta(n)$

3)

Из пункта 2 :

T(n) = $\theta(2^n)$

Задание №5

1) Пусть на некотором шаге m>=n . Тогда m1 = m - n , v1 = v + u, u1 = u; n1 = n .

m1 * u1 + v1 * n1 = (m - n) * u + (v + u) * n = m * u - n * u + v * n + u * n = m * u + v * n .

2) Пусть на некотором шаге m < n . Тогда m1 = m , v1 = v, u1 = u + v; n1 = n - m.

m1 * u1 + v1 * n1 = m * (u + v) + v * (n - m) = m * u + m * v + v * n - v * m= m * u + v * n .

Значит $\forall$ i mi * ui + vi * ni = m * u + v * n = a * b + a * b = 2 * a * b = const .

Значит и после окончания цикла mk * uk + vk * nk = 2 * a * b = НОД(a, b) * z .

Также известный факт , что НОД(a, b) * НОК(a, b) = a * b.

Значит выполнения программы НОД(a, b) * НОК(a, b) = $\frac{2*a*b}{z}$ * НОК(a, b) = a * b , т. е. z = 2 * НОК(a, b) ч.т.д.