

Домашнее задание

1. Решите уравнения в целых числах, используя расширенный алгоритм Евклида. Внимание! Требуется найти все решения, а не только частное решение, которое находит алгоритм Евклида. Выведите самостоятельно формулу для общего решения или воспользуйтесь помощью литературы.

а) $238x + 385y = 133$; б) $143x + 121y = 52$.

2. Решите сравнение $68x + 85 \equiv 0 \pmod{561}$ с помощью расширенного алгоритма Евклида. (Требуется найти все решения в вычетах)

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

4 [ДПВ 1.8]. Доказать корректность рекурсивного алгоритма умножения Divide (раздел 1.1., рис. 1.2.) и получить верхнюю оценку на время работы.

5. Функции $T_1(n)$ и $T_2(n)$ заданы рекуррентными формулами, известно что $T_i(1) = T_i(2) = T_i(3) = 1, i = 1, 2$.

1. Найдите асимптотику роста функции $T_1(n) = T_1(n - 1) + cn$ (при $n > 3$);

2. Докажите, что для функции $T_2(n) = T_2(n - 1) + 4T_2(n - 3)$ (при $n > 3$) справедлива оценка $\log T_2(n) = \Theta(n)$.

3*. Найдите (точную) асимптотику роста функции $T_2(n)$.

6 [Шень 1.1.17]. Добавим в алгоритм Евклида дополнительные переменные u, v, z :

```

    m := a; n := b; u := b; v := a;
    {инвариант: НОД (a,b) = НОД (m,n); m,n >= 0 }
    while not ((m=0) or (n=0)) do begin
    | if m >= n then begin
    | | m := m - n; v := v + u;
    | end else begin
    | | n := n - m; u := u + v;
    | end;
    end;
    if m = 0 then begin
    | z:= v;
    end else begin {n=0}
    | z:= u;
    end;

```

Докажите, что после исполнения алгоритма значение z равно удвоенному наименьшему общему кратному чисел a, b : $z = 2 \cdot \text{НОК}(a, b)$.

7*. Предложите $O(\sqrt{m} \log m)$ алгоритм нахождения длины периода десятичной дроби $\frac{n}{m}$. Докажите его корректность и оцените асимптотику.

8*. Доказать, что `inv(i, p): return i > 1 ? -(p/i)*inv(p%i, p) % p : 1` возвращает обратный остаток, доказать, что работает за логарифм и развернуть рекурсию.

9*. $f(1) = g(1) = 1$ $f(n) = a \cdot g(n - 1) + b \cdot f(n - 1)$ $g(n) = c \cdot g(n - 1) + d \cdot f(n - 1)$ где a, b, c, d положительные константы. Предложите алгоритм вычисляющий $f(n)$ со сложностью $O(\log n)$ арифметических операций.