Задание 6. Разное, модульная арифметика и алгоритм Евклида.

1[1] Докажите корректность бинпоиска.

2[1] Постройте алгоритм, принимающий на вход массив $a_1, \ldots, a_n$ и позволяющий находить значения сумм вида $(a_{m+1} - a_m)^2 + \cdots + (a_k - a_{k-1})^2$ за $O(1)$. Оцените необходимый объем дополнительной памяти.

3[2] Оцените трудоемкость алгоритма, разбивающего задачу размера n на n подзадач размера $\frac{n}{2}$, используя для этого $\Theta(n)$ операций.

4[1+1+1] На лекции был выведен алгоритм нахождения x, y, удовлетворяющих уравнению $ax + by = d$, где $d = \gcd(a, b)$.

1. Обобщите алгоритм на случай, когда уравнение имеет вид $ax + by = kd$, то есть правая часть не является gcd, а делится на него.
2. Найдите и докажите критерий разрешимости таких уравнений в общем виде. Какие требования нужно наложить на коэффициенты, чтобы уравнение имело решения?
3. На лекции и в первых двух пунктах речь шла о частных решениях, рассмотрим также и общий вид решения. Утверждается, что если у линейного диофантова уравнения есть одно решение, у него бесконечно много решений. Например, числа $(-4, 3)$ являются решением уравнения $2x + 3y = 1$, но кроме того решениями является пара $(-7, 5)$, пара $(-10, 7)$ и так далее. Выведите общий вид решения линейных диофантовых уравнений.

5[1+1] Решите уравнения в целых числах. Нужно найти все решения, а не только частное.

1. $238x + 385y = 133$
2. $143x + 121y = 52$

6[1] Решите сравнение $68x + 85 \equiv 0 \mod 561$ с помощью расширенного алгоритма Евклида. Требуется найти все решения в вычетах.

7[1] Найдите обратный остаток $7^{-1} \mod 102$ с помощью расширенного алгоритма Евклида.

8[1] Предложите эффективный алгоритм вычисления наименьшего общего кратного (НОК) двух чисел в битовой модели вычислений (время выполнения операций зависит от длины битовой записи чисел). Докажите его корректность и оцените сложность.