Задание 6. Модульная арифметика и алгоритм Евклида.

1[3] На лекции был выведен алгоритм нахождения a, b, удовлетворяющих уравнению $ax + by = d$, где $d = \gcd(x, y)$.

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.

2[2] Решите уравнения в целых числах. Нужно найти все решения, а не только частное.

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

3[1] Решите сравнение $68x + 85 \equiv 0 \mod 561$ с помощью расширенного алгоритма Евклида. Требуется найти все решения в вычетах.

4[1] Найдите обратный остаток $7^{-1} \mod 102$ с помощью расширенного алгоритма Евклида.

5[2] 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.