МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ФАКУЛЬТЕТ ПРИКЛАДНОЙ МАТЕМАТИКИ И ИНФОРМАТИКИ
Кафедра дискретной математики и алгоритмики

ИСПОЛЬЗОВАНИЕ АЛГОРИТМА ЕВКЛИДА В ЗАДАЧАХ С ЦЕЛОЧИСЛЕННЫМИ ПАРАМЕТРАМИ

Курсовая работа

Якубовсвкого Владислава
Александровича
студента 3 курса,
специальность «информатика»
Научный руководитель:
старший преподаватель кафедры ДМА
Ким Д.В.

Минск, 2022

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Алгоритм Евклида - эффективный алгоритм для нахождения наибольшего общего делителя двух целых чисел, описанный Евклидом в книге «Начала» (около 300 г. до н.э.). На этом алгоритме строятся эффективные решения большого количества задач с целочисленными параметрами. Примерами таких задач могут быть нахождение решений линейных Диофантовых уравнений, нахождение обратного числа по простому модулю и т.д. В этой работе рассматриваются нетривиальные применения алгоритма Евклида для разработки алгоритмов решения задач.

ГЛАВА 1
АЛГОРИТМ ЕВКЛИДА

1.1 Алгоритм Евклида

Определение. Наибольшим общим делителем 2 чисел a и b называется наибольшее неотрицательное число, которое является делителем a и b одновременно, то есть:

$$\gcd(a, b) = \max_{k=1...\infty \,:\, k \mid a \text{ и } k \mid b} k \tag{1.1}$$

Полагаем:

$$\gcd(0, 0) = 0 \tag{1.2}$$
$$\gcd(0, a) = a, a \neq 0$$

Формулировка. Даны два целых неотрицательных числа a и b. Требуется найти их наибольший общий делитель($\gcd(a, b)$). Утверждается, что:

$$\gcd(a, b) = \begin{cases} a & b = 0, \\ \gcd(b, a \bmod b) & \text{иначе.} \end{cases} \tag{1.3}$$

Доказательство корректности. Сначала заметим, что при каждой итерации алгоритма Евклида его второй аргумент строго убывает, следовательно, поскольку он неотрицательный, то алгоритм Евклида всегда завершается.

Для доказательства корректности нам необходимо показать, что:

$$\gcd(a, b) = \gcd(b, a \bmod b), \forall a \geqslant 0, b > 0 \tag{1.4}$$

Покажем, что величина, стоящая в левой части равенства, делится на стоящую в правой, а стоящая в правой — делится на стоящую в левой. Очевидно, это будет означать, что левая и правая части совпадают, что и докажет корректность алгоритма Евклида.

Обозначим $d = \gcd(a, b)$. Тогда, по определению, $d|a$ и $d|b$.

$$a \bmod b = a - b \left\lfloor \frac{a}{b} \right\rfloor \tag{1.5}$$

Но тогда отсюда следует, что $d \mid (a \bmod b)$.

Итак, вспоминая утверждение $d \mid b$, получаем систему:

$$\begin{cases} d \mid b, \\ d \mid (a \bmod b) \end{cases} \tag{1.6}$$

Воспользуемся теперь следующим простым фактом: если для каких-то трёх чисел p, q, r выполнено: $p \mid q$ и $p \mid r$, то выполняется и: $p \mid \gcd(q, r)$. В нашей ситуации получаем:

$$d \mid \gcd(b, a \bmod b) \tag{1.7}$$

Или, подставляя вместо d его определение как $\gcd(a, b)$, получаем:

$$\gcd(a, b) \mid \gcd(b, a \bmod b) \tag{1.8}$$

Итак, мы провели половину доказательства: показали, что левая часть делит правую. Вторая половина доказательства производится аналогично [1].

Т.к. a и b убывают, то и $(a \bmod b)$ тоже убывает. Из этого следует, что алгоритм придет в ситуацию $(a^* \bmod b^*) = 0$, то есть b^* делит a^*, и следующим шагом вернет b^*, а в силу эквивалентности переходов получаем:

$$\gcd(a, b) \ = \gcd(a^*, b^*) \ = \gcd(b^*, a^* \bmod b^*) = b^* \tag{1.9}$$

■

Оценим временную сложность алгоритма Евклида. Для этого покажем, что:

$$a \bmod b \leqslant \frac{a}{2}, \forall a \geqslant b \tag{1.10}$$

Рассмотрим 2 случая:
1) $b \leqslant \frac{a}{2}$, тогда очевидно (1.10) выполняется.
2) $b > \frac{a}{2}$, тогда a представим в виде:

$$a = b + (a \bmod b) \tag{1.11}$$

Из этого получаем:

$$a \bmod b = a - b \leqslant a - \frac{a}{2} = \frac{a}{2} \tag{1.12}$$

Что и требовалось показать.

Из (1.10) следует, что наибольшее число в алгоритме Евклида с каждым шагом уменьшается минимум в 2 раза. Тогда, в силу того, что на каждый переход требуется $\mathcal{O}(1)$ операций, временная сложность алгоритма Евклида $\mathcal{O}\left(log((max(a, b)))\right)$.

ГЛАВА 2
ЗАДАЧА ДИСКРЕТНОЙ ОПТИМИЗАЦИИ

2.1 Постановка задачи

В связи с использованием модульной арифметики при решении частных комбинаторных задач часто встречается, что дроби $\frac{a}{b}$ закодированы следующим образом:

1) Заранее фиксируется простой модуль p, одинаковый для всех дробей и преобразований в рамках задачи.

2) Находят обратное число к b по модулю p, то есть такое число b^{-1}, что $bb^{-1} = 1 \pmod p$.

3) Находят такое число $q < p$, что $a = b^{-1}q \pmod p$ и говорят, что дробь $\frac{a}{b}$ по модулю p имеет остаток q.

Задача.

Есть дробь $\frac{a}{b}$, которая по простому модулю p имеет остаток $q < p$, то есть:

$$a = (bq) \bmod p \tag{2.1}$$

Заданы p и q, найти такие целые $a \geqslant 0$, $b > 0$ удовлетворяющие условию (2.1), что сумма $a + b$ — минимальная.

2.2 Необходимые определения

Определение 1. Функция, которая в соответствие каждому действительному числу x ставит наименьшее целое число y, не меньшее чем x, называется $ceil$:

$$ceil(x) - 1 < x \leqslant ceil(x) \tag{2.2}$$
$$ceil(x) \in \mathbb{Z}$$

Определение 2. Функция, которая в соответствие каждому действительному числу x ставит наименьшее целое число y, строго большее чем x, называется $loft$:

$$loft(x) - 1 \leqslant x < loft(x) \tag{2.3}$$
$$loft(x) \in \mathbb{Z}$$

Определение 3. Функция, которая в соответствие каждому действительному числу x ставит наибольшее целое число y, не большее чем x, называется $floor$:

$$floor(x) \leqslant x < floor(x) + 1 \tag{2.4}$$
$$floor(x) \in \mathbb{Z}$$

Определение 4. Функция, которая в соответствие каждому действительному числу x ставит наибольшее целое число y, строго меньшее чем x, называется $cellar$:

$$cellar(x) < x \leqslant cellar(x) + 1 \tag{2.5}$$
$$cellar(x) \in \mathbb{Z}$$

2.3 Решение

Преобразуем (2.1):

$$a = (bq) \bmod p = bq - floor\left(\frac{bq}{p}\right) p \tag{2.6}$$

Получается, что теперь нужно минимизировать по b функцию

$$a + b = (q+1)b - floor\left(\frac{bq}{p}\right) p \tag{2.7}$$

Вообще говоря, задачи нахождения минимума/максимума, где целевая функция имеет вид:

$$f(x) = Ax + Bg\left(\frac{P}{Q}x\right) \tag{2.8}$$
$$x \in [l, l+1, ..., r-1, r], A, B \in \mathbb{R},$$
$$P, Q \in \mathbb{N}, l, r \in \mathbb{N}^0,$$
$$g \text{ — } floor, cellar, ceil \text{ или } loft$$

можно решить за $\mathcal{O}\left(\log(\max(P, Q))\right)$

Опишем такое рекурсивное решение и оценим его время работы:

Если $l = r$ вернем l.

а) $g = floor$, тогда имеем:

$$f(x) = Ax + B \cdot floor\left(\frac{P}{Q}x\right) \tag{2.9}$$

Если P делится на Q — посчитаем значение $floor$, получим:

$$f(x) = Ax + B\frac{P}{Q}x = A'x \tag{2.10}$$

Тогда просто возвращаем решение: максимальный или минимальный x, в зависимости от знака A' и задачи, которую мы решаем(минимум или максимум).

Пусть P не делится на Q, тогда возьмем $k = floor\left(\frac{P}{Q}\right)$, и вынесем kx из-под $floor$:

$$Ax + B \cdot floor\left(\frac{P}{Q}x\right) = (A + Bk)x + B \cdot floor\left((\frac{P}{Q} - k)x\right) =$$

$$= A^{'}x + B \cdot floor\left(\frac{P^{'}}{Q}x\right) \tag{2.11}$$

Положим $y = floor\left(\frac{P^{'}}{Q}x\right)$. Поменяем порядок суммирования, для этого попробуем выразить иксы через игреки. Из (2.4) получается:

$$y \leqslant \frac{P^{'}}{Q}x < y + 1 \Rightarrow y\frac{Q}{P^{'}} \leqslant x < (y + 1)\frac{Q}{P^{'}} \tag{2.12}$$

Теперь для каждого игрека выберем оптимальный икс. Опять же это зависит от задачи(минимум или максимум) и от знака $A^{'}$. Пусть мы решаем задачу на минимум:

1) $A^{'} < 0$ — нужно взять наибольший икс, в соответствие которому ставится этот игрек — $x = cellar\left((y + 1)\frac{Q}{P^{'}}\right)$. Получается новая задача на минимум вида (2.8):

$$By + A^{'} \cdot cellar\left(\frac{Q}{P^{'}}(y + 1)\right) \tag{2.13}$$

$$l_{new} = floor\left(\frac{P^{'}}{Q}l\right), r_{new} = floor\left(\frac{P^{'}}{Q}r\right),$$

$$A_{new} = B, B_{new} = A^{'} = A + Bk,$$

$$P_{new} = Q, Q_{new} = P^{'} = P \bmod Q, g_{new} = ceil$$

Замечание. $y+1$ нам не мешает: в этом случае можно, например, «сдвинуть» все индексы игреков влево.

Здесь важно заметить, что в соответствие самому большому игреку мы хотели бы поставить:

$$x = cellar\left((y_{max} + 1)\frac{Q}{P^{'}}\right) \tag{2.14}$$

и чаще всего у нас удается это сделать, кроме случаев, когда оказыается, что значение в (2.14) больше, чем r. В таком случае нужно для этого игрека взять $x = r$.

2) $A^{'} \geqslant 0$ — нужно взять наименьший икс, в соответствие которому ставится этот игрек $x = ceil\left(\frac{Q}{P^{'}}y\right)$. Получается новая задача на минимум вида (2.8):

$$By + A^{'} \cdot ceil\left(\frac{Q}{P^{'}}y\right) \tag{2.15}$$

$$l_{new} = floor(\frac{P^{'}}{Q}l), r_{new} = floor(\frac{P^{'}}{Q}r),$$

$$A_{new} = B, B_{new} = A^{'} = A + Bk,$$

$$P_{new} = Q, Q_{new} = P^{'} = P \bmod Q, g_{new} = ceil$$

Здесь важно заметить, что в соответствие самому маленькому игреку мы хотели бы поставить:

$$x = ceil\left(\frac{Q}{P'}y_{min}\right) \tag{2.16}$$

и чаще всего у нас удается это сделать, кроме случаев, когда оказыается, что значение в (2.16) меньше, чем l. В таком случае нужно для этого игрека взять $x = l$. Дальше подобные замечания будут опускаться.

Для задачи на максимум все показывается точно так же.

б) $g = ceil$, тогда вместо (2.20) получаем:

$$y - 1 < \frac{P^{'}}{Q}x \leqslant y \Rightarrow (y-1)\frac{Q}{P'} < x \leqslant y\frac{Q}{P'} \tag{2.17}$$

Пусть задача на максимум:

1) $A^{'} < 0$ — нужно взять наименьший икс, в соответствие которому ставится этот игрек — $x = loft\left((y-1)\frac{Q}{P'}\right)$. Получается новая задача на максимум вида (2.8):

$$By + A^{'} \cdot loft\left(\frac{Q}{P'}(y-1)\right) \tag{2.18}$$

$$l_{new} = ceil\left(\frac{P^{'}}{Q}l\right), r_{new} = ceil\left(\frac{P^{'}}{Q}r\right),$$

$$A_{new} = B, B_{new} = A^{'},$$

$$P_{new} = Q, Q_{new} = P^{'} = P \bmod Q, g_{new} = loft$$

2) $A \geqslant 0$ — нужно взять наибольший икс, в соответствие которому ставится этот игрек — $x = floor\left(\frac{Q}{P'}y\right)$. Получается новая задача на максимум вида (2.8):

$$By + A^{'} \cdot floor\left(\frac{Q}{P'}y\right) \tag{2.19}$$

$$l_{new} = ceil\left(\frac{P^{'}}{Q}l\right), r_{new} = ceil\left(\frac{P^{'}}{Q}r\right),$$

$$A_{new} = B, B_{new} = A^{'},$$

$$P_{new} = Q, Q_{new} = P^{'} = P \bmod Q, g_{new} = floor$$

в) g = loft, вместо (2.20), получим:

$$y - 1 \leqslant \frac{P'}{Q}x < y \Rightarrow (y-1)\frac{Q}{P'} \leqslant x < y\frac{Q}{P'} \tag{2.20}$$

Аналогично в зависимости от задачи и от знака A нужно положить

$$x = ceil\left((y-1)\frac{Q}{P'}\right) \tag{2.21}$$

или

$$x = cellar\left(y\frac{Q}{P'}\right) \tag{2.22}$$

г) $g = cellar$, вместо (2.20), получим:

$$y < \frac{P'}{Q}x \leqslant y + 1 \Rightarrow y\frac{Q}{P'} < x \leqslant (y+1)\frac{Q}{P'} \tag{2.23}$$

Точно так же в зависимости от задачи и от знака A нужно положить

$$x = loft\left(y\frac{Q}{P'}\right) \tag{2.24}$$

или

$$x = floor\left((y+1)\frac{Q}{P'}\right) \tag{2.25}$$

Заметим, что с каждым шагом между P и Q происходят те же действия, что и происходили бы в алгоритме Евклида ($Q_{new} = P \bmod Q, P_{new} = Q$). Из этого следует, что за $\mathcal{O}\left(\log\left(\max\left(P, Q\right)\right)\right)$ шагов(если алгоритм еще не завершится на проверке $l = r$), в аргументе функции g будет целое число, и наша функция сведется к функции, подобной (2.10), после чего завершится.

Из этого следует, что сложность описанного выше алгоритма — $\mathcal{O}\left(\log(max(P, Q))\right)$.

Возвращаясь к (2.7), положив в алгоритм, описанный выше

$$l = 1, r = p, A = q + 1, B = p, P = q, Q = p, g = floor$$

сначала получим оптимальное b, потом, подставив b в (2.6), получим a.

ГЛАВА 3
КОЛИЧЕСТВО ЦЕЛЫХ ТОЧЕК ПОД И НА ПРЯМОЙ

3.1 Постановка задачи

Дана прямая $y = \frac{P}{Q}x$ на плоскости, $P \in \mathbb{N}^0, Q \in \mathbb{N} - \{0\}$. Дано целое число r.

Сколько целых точек плоскости с $0 \leqslant x \leqslant r$ суммарно находится «на» и «под» этой прямой?

«Под» прямой подразумеваются точки, которые находятся непосредственно под прямой, и у которых $y \geqslant 0$.

3.2 Количество целых точек на прямой

Для начала научимся считать количество целых точек на прямой $y = \frac{P}{Q}x$. Это сделать несложно:

1) Если $P = 0$, то таких точек ровно $r + 1$.

2) Пусть $P \neq 0$, поделим P и Q на $gcd(P, Q)$:

$$P^* = P \setminus gcd(P, Q), Q^* = Q \setminus gcd(P, Q) \tag{3.1}$$

Чтобы в (3.1) y был целым при каком-то целом x, необходимо и достаточно, чтобы $x = 0$ или:

$$gcd(P^* \cdot x, Q^*) = Q^* \tag{3.2}$$

Т.к. $gcd(P^*, Q^*) = 1$, то:

$$gcd(x, Q^*) = Q^* \tag{3.3}$$

Отсюда получаем:

$$x = kQ^*, k \in \mathbb{N}^0 \tag{3.4}$$

Тогда:

$$k_{max} = floor\left(\frac{r}{Q^*}\right) = floor\left(\frac{r \cdot gcd(P, Q)}{Q}\right) \tag{3.5}$$

Тогда количество целых точек на прямой это:

$$1 + floor\left(\frac{r \cdot gcd(P, Q)}{Q}\right) \tag{3.6}$$

3.3 Количество целых точек строго под прямой

Дальше научимся считать количество целых точек, находящихся строго под прямой $y = kx, k \in \mathbb{N}^0$.

Переберем иксы:

0) при $x = 0$ число точек, лежащих строго под прямой, равно 0.

1) при $x = 1$ нам подходят все целые точки $(1, y)$, в которых $0 \leqslant y < k \cdot 1$. Таких точек ровно k штук.

...

j) при $x = j$ нам подходят все целые точки (j, y), в которых $0 \leqslant y < k \cdot j$. Таких точек ровно $k \cdot j$ штук.

...

r) при $x = r$ нам подходят все целые точки (r, y), в которых $0 \leqslant y < k \cdot r$. Таких точек ровно $r \cdot j$ штук.

Получается сумма:

$$\sum_{i=0}^{r} ki = \frac{kr(r+1)}{2} \tag{3.7}$$

3.4 Полное решение

Вернемся к исходной задаче. Имеем:

$$y = \frac{P}{Q}x \tag{3.8}$$

Проведем прямую

$$y = \frac{(P - P \bmod Q)}{Q}x \tag{3.9}$$

Посчитаем число целых точек, лежащих строго под этой прямой. Т.к. $\frac{(P-P \bmod Q)}{Q} \in \mathbb{N}^0$, это число будет в точности (3.7), где

$$k = \frac{(P - P \bmod Q)}{Q} \tag{3.10}$$

Нам осталось посчитать количество точек на исходной прямой (3.8),на проведенной прямой (3.9), и между двумя этими прямыми.

Дальше нужно «передвинуть» все точки (x, y) на вектор $(0, -\frac{(P-P \bmod Q)}{Q}x)$:

$$y^* + \frac{(P - P \bmod Q)}{Q})x^* = \frac{P}{Q}x^* \tag{3.11}$$

Перенесем икс вправо и раскроем скобки:

$$y^* = \frac{P \bmod Q}{Q}x^* \tag{3.12}$$

Заметим, что после преобразования целые точки с прямой (3.9) перейдут на прямую $y = 0$, а все целые точки с прямой (3.8) перейдут на прямую (3.12). Соответственно целые точки между этими прямыми, перейдут на плоскость, находящуюся выше чем $y = 0$, и ниже, чем $y = \frac{(P - P \bmod Q)}{Q} x$.

Преобразование имеет такой вид: мы от y отнимаем какое-то целое число, поэтому все целые точки до преобразования, перейдут в другие целые точки, а все точки с нецелыми игреками перейдут в другие точки с нецелыми игреками.

Так же стоит отметить, что все точки, которые мы уже посчитали в (3.7)-(3.10) перейдут строго под прямую $y = 0$.

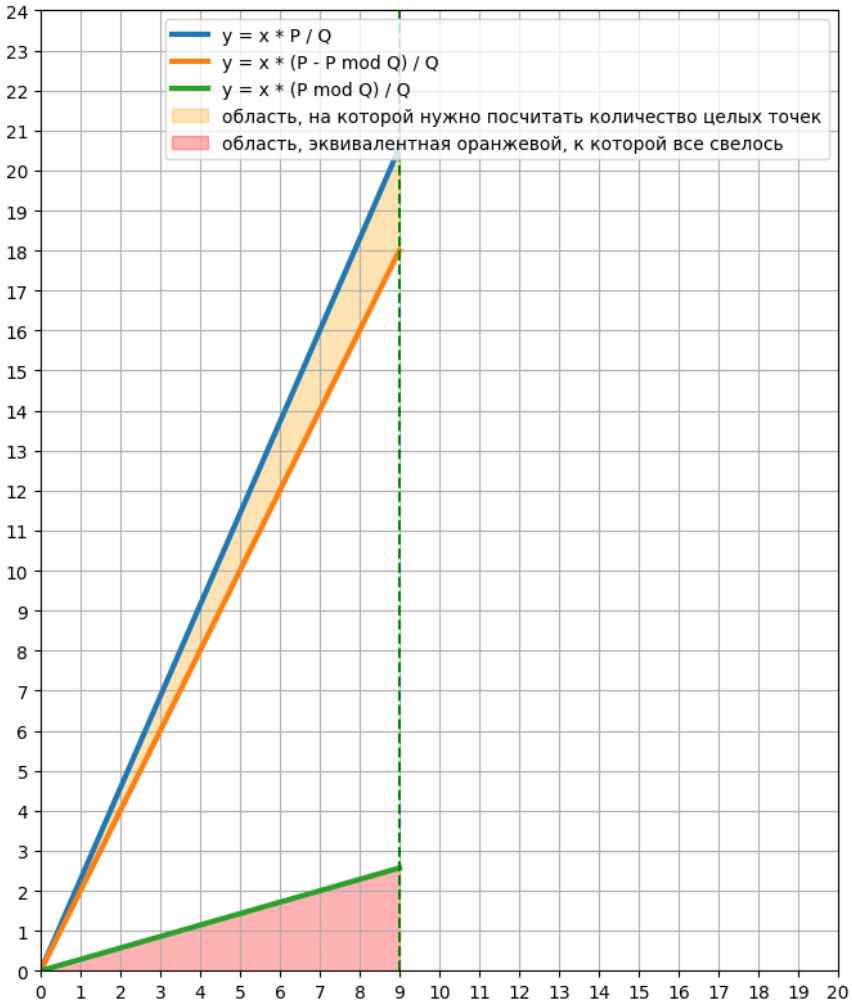

Рисунок 3.1 — Пример такого преобразования для $P = 16, Q = 7, r = 9$

Получается, нам осталось решить такую же задачу, но с функцией (3.12). Проведем прямую:

$$y = \frac{Q}{P \bmod Q} x, \tag{3.13}$$

$$0 \leqslant x \leqslant floor\left(\frac{P \bmod Q}{Q} r\right)$$

Посмотрим, что можно с ней сделать:

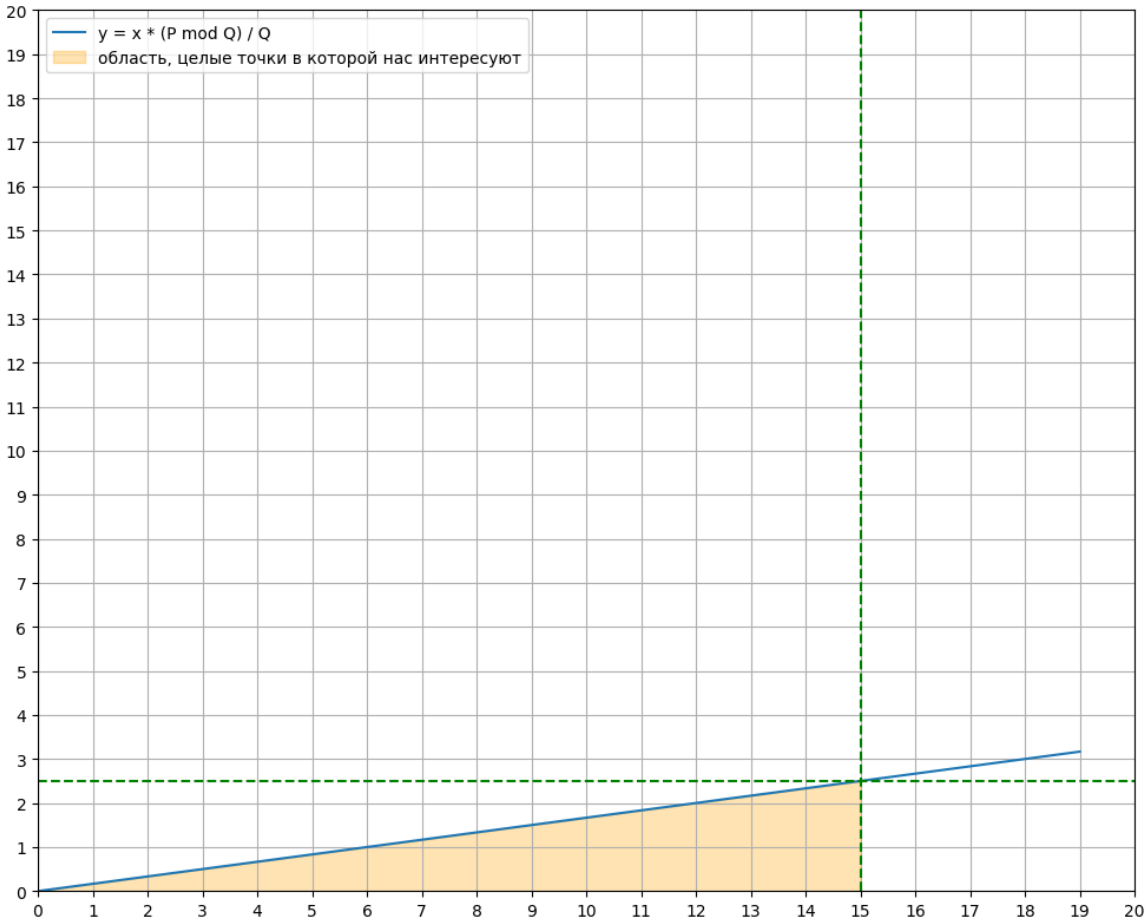

Рисунок 3.2 — Пример для $P = 1, Q = 6, r = 15$

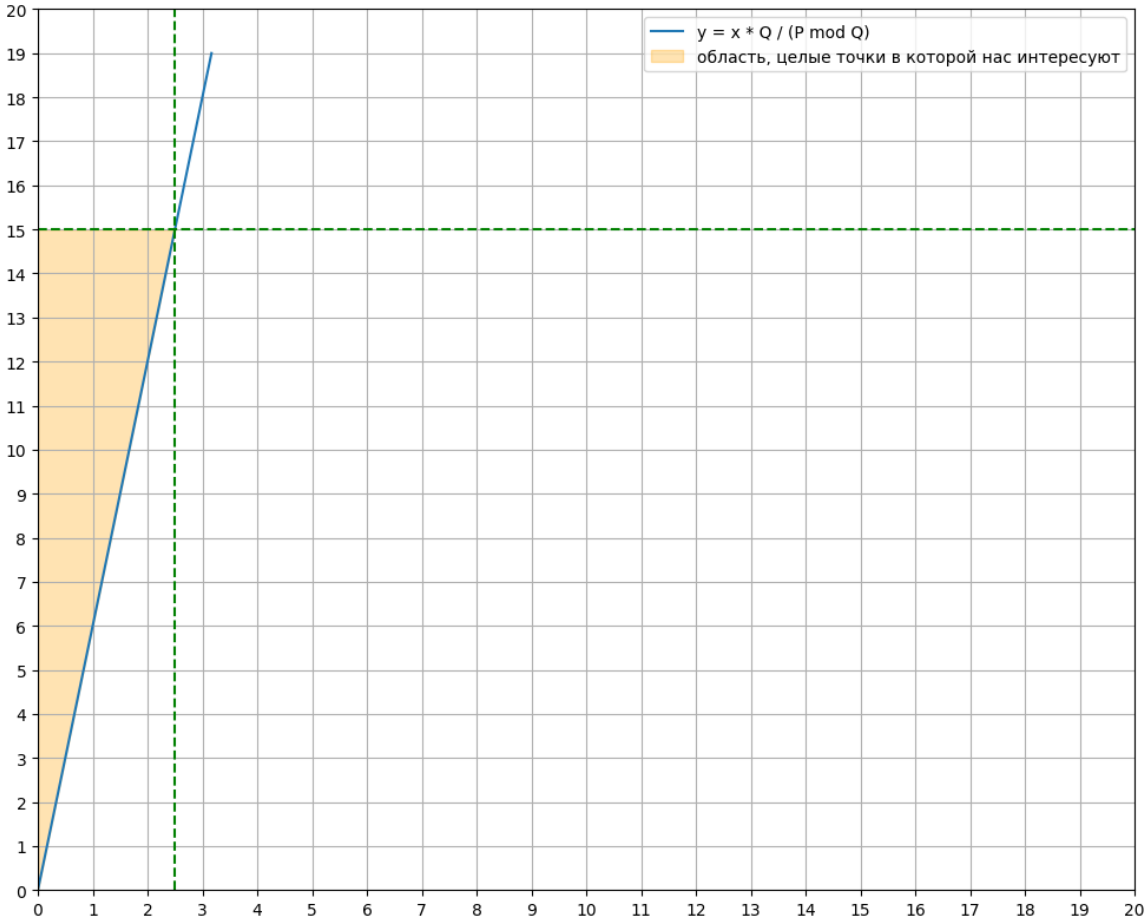

Рисунок 3.3 — Пример для $P = 1, Q = 6, r = \frac{15}{6}$

Так как такое преобразование — просто отражение прямой относительно $y = x$, это можно решить следующим образом:

1) Посчитать количество целых точек внутри такого прямоугольника:

$$\begin{cases} 0 \leqslant x \leqslant floor\left(\frac{P \bmod Q}{Q} r\right), \\ 0 \leqslant y \leqslant r \end{cases} \tag{3.14}$$

2) Рекурсивно посчитать суммарное количество точек на и под прямой (3.13)

3) Вычесть значение, посчитанное в шаге 2, из количества всех целых точек прямоугольника.

4) Так как мы в 3 шаге вычли и целые точки на прямой, которая входит в интересующее нас множество, нужно их вернуть. Просто прибавить количество целых точек на прямой , как в (3.6).

Как и писалось выше, мы получаем новую такую задачу, но с другой функ-

цией:

$$y = \frac{P_{new}}{Q_{new}} x \tag{3.15}$$
$$P_{new} = Q, Q_{new} = P \bmod Q$$

Отношение точно такое же, как и в алгоритме Евклида. Из этого следует, что за $\mathcal{O}(\log(\max(P, Q)))$ вызовов функция сведется к $y = 0$, после чего рекурсия завершится. Для (3.6) можно посчитать gcd один раз. Дальше, из-за соотношения в (3.15), каждый раз этот gcd будет одинаковым.

Из этого следует, что итоговая временная сложность алгоритма — $\mathcal{O}(\log(\max(P, Q)))$

ЗАКЛЮЧЕНИЕ

В данной работе был придуман алгоритм решения задачи (2.1), доказана его корректность и оценена время работы. Получившееся решение имеет очень много граничных случаев, которые в дальнейшем могут вызвать различные проблемы в реализации.

Также было придумано решение, доказана его корректность и оценено время работы для задачи про количество целых точек над и на прямой. В дальнейшем планируется обобщить решение для $y = \frac{P}{Q} * x + b, l \leqslant x \leqslant r$, и написать код с реализацией этого алгоритма.

Алгоритм Евклида

```cpp
#include <iostream>

int gcd (int a, int b) {
    while (b) {
        a %= b;
        swap (a, b);
    }
    return a;
}

int main() {
    int a, b;
    std::cin >> a >> b;
    std::cout << gcd(a, b) << '\n';
    return 0;
}
```

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Алгоритм Евклида. Доказательство коректности и времени работы алгоритма Евклида. Т.Кормен, Ч.Лейзерсон, Р.Ривест, К.Штайн - Алгоритмы. Построение и анализ. Издание 3-е, 2013, 978-980 с.