

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего
образования

**«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»**

Кафедра теоретических основ
компьютерной безопасности и
криптографии

Решение сравнений с помощью алгоритма Евклида

ЛАБОРАТОРНАЯ РАБОТА

студента 4 курса 431 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Серебрякова Алексея Владимировича

Научный руководитель

доцент, к. п. н.

подпись, дата

А. С. Гераськин

Саратов 2022

Описание алгоритма

Решение с помощью алгоритма Евклида

Пусть x_0, x_1 — решения.

$$ax_0 = b \pmod{m}$$

$$-ax_1 = b \pmod{m}$$

$$a(x_0 - x_1) \equiv 0 \pmod{m}$$

$$m | a(x_0 - x_1)$$

$$\frac{m}{d} \mid \frac{a}{d}(x_0 - x_1); \frac{m}{d} = m', \frac{a}{d} = a'$$

$$(m', a') = 1 \Rightarrow m' \mid (x_0 - x_1) \Rightarrow x_1 = x_0 + km', k = r \circ d + s; 0 \leq s \leq d - s$$

Тогда $x_1 = x_0 + sm' + rm \Rightarrow$ получаем все эквивалентные решения.

Важно $[a] \cdot [x] = [1]$ в \mathbb{Z}_m

$$ax = 1 \pmod{m}, \text{НОД}(a, m) \mid 1$$

Алгоритм

Внести вычисление этих коэффициентов в алгоритм Евклида несложно, достаточно вывести формулы, по которым они меняются при переходе от пары (a, b) к паре $(b \% a, a)$ (знаком процента мы обозначаем взятие остатка от деления).

Итак, пусть мы нашли решение (x_1, y_1) задачи для новой пары $(b \% a, a)$:

$$(b \% a) \cdot x_1 + a \cdot y_1 = g,$$

и хотим получить решение (x, y) для нашей пары (a, b) :

$$a \cdot x + b \cdot y = g.$$

Для этого преобразуем величину $b \% a$:

$$b \% a = b - \left\lfloor \frac{b}{a} \right\rfloor \cdot a.$$

Подставим это в приведённое выше выражение с x_1 и y_1 и получим:

$$g = (b \% a) \cdot x_1 + a \cdot y_1 = \left(b - \left\lfloor \frac{b}{a} \right\rfloor \cdot a \right) \cdot x_1 + a \cdot y_1,$$

и, выполняя перегруппировку слагаемых, получаем:

$$g = b \cdot x_1 + a \cdot \left(y_1 - \left\lfloor \frac{b}{a} \right\rfloor \cdot x_1 \right).$$

Сравнивая это с исходным выражением над неизвестными x и y , получаем требуемые выражения:

$$\begin{cases} x = y_1 - \left\lfloor \frac{b}{a} \right\rfloor \cdot x_1, \\ y = x_1. \end{cases}$$

Код программы

```
#include <bits/stdc++.h>
#include <iostream>
```

```
using namespace std;
```

```
int validated_input()
{
    int s = 0;
    while (!(cin >> s))
```

```

    {
        cin.clear();
        cin.ignore(numeric_limits<streamsize>::max(), '\n');
        printf("! Неверный ввод. Повторите ввод, начиная с первого неверного элемента.\n");
    }

    return s;
}

int euclid_extended(int a, int b, int &x, int &y)
{
    int x1, y1;

    if (a == 0)
    {
        x = 0;
        y = 1;
        return b;
    }

    int d = euclid_extended(b % a, a, x1, y1);

    x = y1 - (b / a) * x1;
    y = x1;

    return d;
}

bool task(int a, int b, int c, int &x0, int &y0, int &g)
{
    g = euclid_extended(abs(a), abs(b), x0, y0);
    if (c % g != 0)
        return false;
    x0 *= c / g;
    y0 *= c / g;
    if (a < 0)
        x0 *= -1;
    if (b < 0)
        y0 *= -1;
    return true;
}

int norm(int x, int m){

    while (x < 0)
        x += m;

    return x % m;
}

int main()
{
    setlocale(0, "");

    int a, b, m, x, y, g, tmp;

    printf("\nРешение уравнения вида\n  $ax = b \pmod{m}$ \n");
    printf("можно свести к решению Диофантового уравнения вида\n  $ax + km = b$ \n");
    printf("которое в свою очередь может быть решено с помощью расширенного алгоритма Евклида.\n");

```

```

printf("\nВведите коэффициент a: ");
a = validated_input();

printf("\nВведите коэффициент b: ");
b = validated_input();

printf("\nВведите коэффициент m: ");
m = validated_input();
tmp = m;

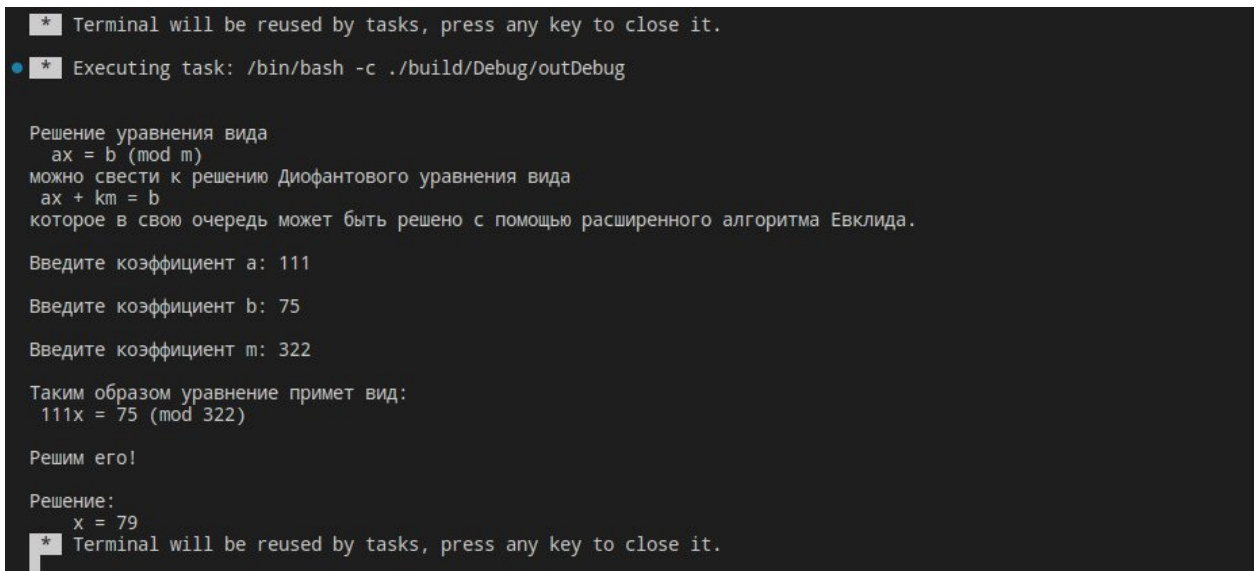
printf("\nТаким образом уравнение примет вид:\n %dx = %d (mod %d)\n", a, b, m);
printf("\nРешим его!\n");

task(a % tmp, m, b % tmp, x, y, g) ? printf("\nРешение:\n  x = %d\n", (norm(x,m))) : printf("\nРешения
нет!\n");

return 0;
}

```

Пример запуска программы



```

* Terminal will be reused by tasks, press any key to close it.
* Executing task: /bin/bash -c ./build/Debug/outDebug

Решение уравнения вида
  ax = b (mod m)
можно свести к решению Диофантового уравнения вида
  ax + km = b
которое в свою очередь может быть решено с помощью расширенного алгоритма Евклида.

Введите коэффициент a: 111
Введите коэффициент b: 75
Введите коэффициент m: 322

Таким образом уравнение примет вид:
  111x = 75 (mod 322)

Решим его!

Решение:
  x = 79
* Terminal will be reused by tasks, press any key to close it.

```

● * Executing task: /bin/bash -c ./build/Debug/outDebug

Решение уравнения вида

$$ax = b \pmod{m}$$

можно свести к решению Диофантового уравнения вида

$$ax + km = b$$

которое в свою очередь может быть решено с помощью расширенного алгоритма Евклида.

Введите коэффициент a: 9

Введите коэффициент b: 6

Введите коэффициент m: 12

Таким образом уравнение примет вид:

$$9x = 6 \pmod{12}$$

Решим его!

Решение:

$$x = 10$$

* Terminal will be reused by tasks, press any key to close it.