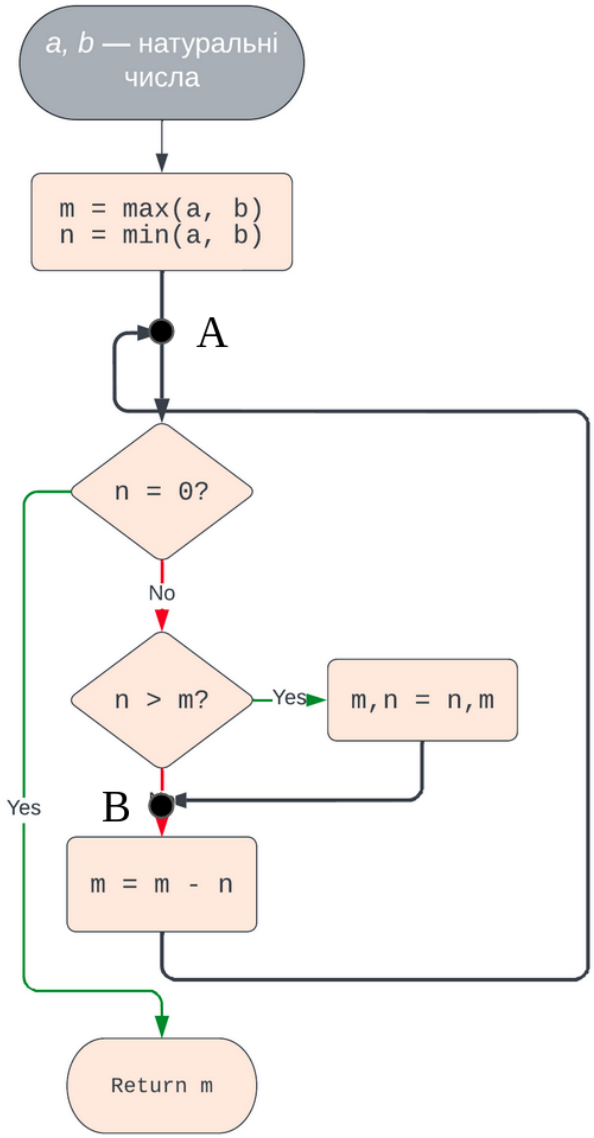
2️⃣

Homework #2

Отже, пропоную наступну схему алгоритма Євклида, показану нижче.

Також далі я буду використовувати символ $\mathbb{N}^+ = \mathbb{N} \cup \{0\}$ для зручності.



Для початку, доведемо часткову коректність алгоритму. Нехай маємо 3 “контрольні точки”: A, B та при виході з програми при виконанні умови $n = 0$. Маємо наступні “перевірочні” умови:

- **Точка** A. $\gcd(n, m) = \gcd(a, b);\ n, m \in \mathbb{N}^+$
- **Точка** B. $m, n \in \mathbb{N}; m > n$
- **Точка** C. $\gcd(a, b) = m$

Видно, що якщо всі вище зазначені умови виконуються, то і алгоритм буде працювати частково коректно, тобто для $\forall a, b \in \mathbb{N}$ буде виконуватись умова в точці C. Дійсно, якщо ми будемо повертатися до точки A після кожного проходу циклу і при цьому після деяких маніпуляцій з n, m (нам зараз не цікаво, яких саме) їх НСД не змінюється, то в разі, якщо якесь з чисел стане нулем, то $\gcd(a, b)$ буде ненулевим елементом з пари і тому умова C також буде виконуватись.

Отже, покажемо, що ці умови дійсно виконуються. Починаємо проходитись зверху-вниз від точки A. Нехай $a, b \neq 0$ (інакше вочевидь $\gcd(a, b) = \max(a, b)$ і програма працює правильно, бо $m = \max(a, b)$ за умовою ініціалізації).

Перше, що ми перевіряємо — це чи є $n > m$. Якщо так, то ми змінюємо місцями m та n. Ця операція гарантує, що до початку операції віднімання ми робимо значення m більшим або рівним до n. Тому дійсно умова на точці B виконується (те, що $m, n \in \mathbb{N}$ випливає з того, що ми або залишаємо m, n такими, які вони є, або змінюємо місцями, що не може зробити ці числа ненатуральними, коли вони були натуральними).

Далі ми віднімаємо від m значення n, отримуємо нове значення пари (m', n') і повертаємось до точки A. Умова того, що $\gcd(n', m') = \gcd(a, b)$ виконується і це було показано в передумові до завдання. Обидва числа залишились невід'ємними цілими (отже $n' = n \in \mathbb{N}^+$), бо ми від більшого (тобто m) відняли менше або рівне (тобто n), тому вираз $m' = m - n \in \mathbb{N}^+$.

Далі індуктивно можна показати, використовуючі те, що ми описали вище, що якщо умова A виконується для деяких $(m^{(i)}, n^{(i)})$ після i циклів, то для нових значень $(m^{(i+1)}, n^{(i+1)})$ після проходу циклу умова A також буде виконуватись. Таким чином, ми довели часткову коректність алгоритму.

Щоб довести повну коректність, достатньо показати, що програма завершить роботу $\forall a, b \in N$, бо часткову коректність вже доказано. Дійсно, помітимо, що після кожного проходу циклу в нас зменшується одне із чисел (вони можуть залишитися тими самими лише при умові, що при операції $m' = m - n$ число n буде дорівнювати 0, але це перевіряється перед початком віднімання, тому $n \neq 0$), тому оскільки в нас числа натуральні, то рано чи пізно одне з них стане

менше або дорівнювати нулю. Отже залишилось довести, що жодне з чисел не може стати менше за 0. Але це теж очевидно: оскільки ми при кожному шагу віднімаємо від більшого числа менше або рівне йому, то ми ніяк не можемо отримати число, менше за 0. Отже, повна коректність доведена.

Реалізацію на *Python* можна побачити нижче:

```
def gcd(a, b):
    m, n = max(a, b), min(a, b)
    while n != 0:
        if n > m:
            m, n = n, m
        m = m - n
    return m
```