Отчёт по лабораторной работе №6

Разложение чисел на множители

Шутенко Виктория Михайловна

Содержание

# 1 Цель рабoты

Приoбрести практические навыки рабoты с разложением чисел на множители.

# 2 Хoд рабoты

## 2.1 Алгоритм, реализующий р-метод Полларда

def mod(a ,b):  
 return a % b  
  
  
def pollard(n: int, c: int, f):  
 d = 1  
 cnt = 0  
 a, b = c, c  
   
 print(f"a = {a}, b = {b}")  
   
 while d == 1:  
 a = mod(f(a), n)  
 b = mod(f(b), n)  
 d = np.gcd(a - b, n)  
   
 if mod(cnt, 100) == 0 or d != 1:  
 print(f"iteration {cnt+1}: a = {a}, b = {b}, d = {d}")  
  
 cnt += 1  
   
 if d == n:  
 print("Делитель не найден")  
 return None  
   
 return d  
  
  
def pollard\_test(n, c):  
 print(f'Поллард {n}\n---------')  
 f = lambda x: np.power(x, 2) + mod(np.random.randint(1, np.floor(np.sqrt(n))), n)  
 p = pollard(n, c, f)  
   
 if p != None:  
 print(f'Нетривиальный делитель {n}: p = {p}')  
   
 print(f'---------\n')  
  
  
def main():  
 pollard\_test(1359331, 1)  
 pollard\_test(137, 5)  
 pollard\_test(322, 12)  
   
if \_\_name\_\_ == "\_\_main\_\_":  
 main()

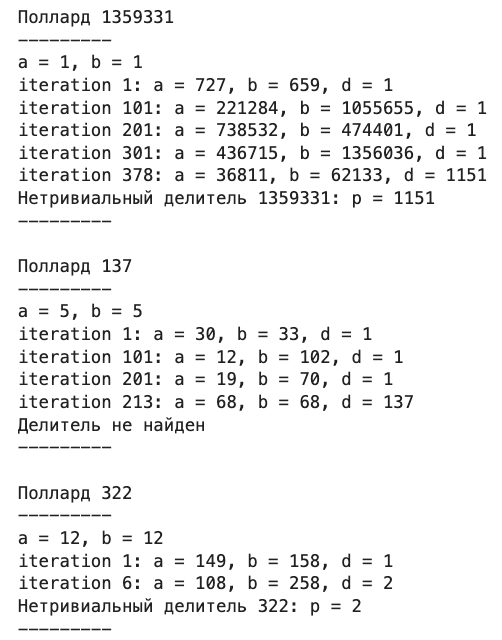


Figure 1: Тестирование