Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования   
**Национальный исследовательский университет «МЭИ»**

**Лабораторная работа №10**

по курсу«**Методы и средства защиты информации**»

**«Кольца»**

Выполнил:

студент группы А-07-18

Востриков Р.В.

Вариант 8

Москва  
2020

**1. Задание**

Задание 1  
Составить программу для нахождения , где - натуральные числа и  может быть большим числом.

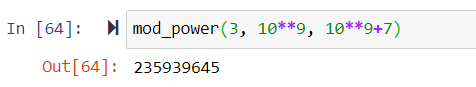
Задание 2  
Составить программу для нахождения минимального числа длины n кратного 3,4,5. Указание n может быть большим. Вывести последние 30 цифр такого числа.

**2. Описание результатов**

Задание 1

Была составлена программа на Python 3, на вход подаются целые числа a, b, p произвольной длины, результат.

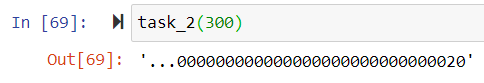
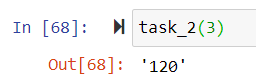
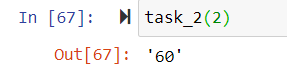
Пример работы программы для входных данных a = 3, b = 109, p =109+7:



Задание 2

Была составлена программа для нахождения минимального числа длины n кратного 3,4,5. Программа использует особенность реализации целых чисел в Python, позволяющей избежать переполнения.

Пример работы программы для n = 2, 3, 300 :



**3. Код программы (к заданию 1)**

def mod\_power(a, b, p):

from math import gcd

if gcd(a, p) != 1:

raise Exception("a и p должны быть взаимно простыми числами")

res = 1

while (b > 0):

if (b & 1): # <=> b % 2 == 1, но подходит для больших b

res = (res \* a) % p

b = b >> 1 # <=> b = b/2

a = (a \* a) % p;

return res;

**Код программы (к заданию 2)**

# нахождение наименьшего числа длины n, делящегося на divisor

def least\_multiple(divisor, n):

min = pow(10, n-1)

if min % divisor == 0:

return min

else:

return (min + divisor) - (min % divisor)

def task\_2(n):

# 𝑛 кратно 3, 4, 5 <=> 𝑛 кратно 60.

res = str(least\_multiple(60, n))

return res if len(res)<=30 else '...' + res[-30:]

**4. Вывод**

В лабораторной работе были разработаны алгоритмы для нахождения 𝑎𝑏 mod 𝑝 и минимального числа, кратного заданному длинны 𝑛. Для разработки алгоритмов были применены понятия теории групп.