**Лабораторная работа № 4  
Выполнил Казачинский Глеб, 3 курс 6 группа**

1. **def** gcdex(a, b):

2. **if** b == 0:

3. **return** a, 1, 0

4. **else**:

5. d, x, y = gcdex(b, a % b)

6. **return** d, y, x - y \* (a // b)

7.

8.

9. **def** fast\_p(x, n, m):

10. res = 1

11. **while** n:

12. **if** n % 2:

13. res = res \* x % m

14. x = (x \*\* 2) % m

15. n = n // 2

16. **return** res

17.

18.

19. p = 148250911826341

20. q = 202614773351219

21. e = 12776470783322290155855389671

22. X1 = 26926695734432769312536758139

23. Y2 = 7060854756795018940042464563

24.

25. n = p \* q

26. fi = (p - 1) \* (q - 1)

27.

28. gcd, x, y = gcdex(e, fi)

29.

30. d = 0

31. **if** gcd == 1:

32. d = x % fi

33. **print**('d: ', d)

34.

35. Y1 = fast\_p(X1, e, n)

36. **print**('Y1: ', Y1)

37.

38. X1\_ = fast\_p(Y1, d, n)

39. **print**('X1\_: ', X1\_)

40. **print**('X1 - X1\_ :', X1 - X1\_)

41.

42.

43. X2 = fast\_p(Y2, d, n)

44. **print**('X2: ', X2)

**Результаты:**

