

```

1 # Лабораторная работа №6
2 # Тема: Разложение чисел на множители
3 # Выполнила: Исламова Сания Маратовна
4 # Группа: НПИмд-01-24
5
6 print("n = "); n = parse(BigInt, readline())           # 1
7 # Выводим приглашение "n = " и сразу считываем введённое число как BigInt.
8 # BigInt нужен, потому что в задании числа могут быть очень большими (сотни цифр),
9 # а обычный Int переполнится. readline() читает строку из терминала.
10
11 let                                         # 2
12 # Создаём локальный блок let – это важно!
13 # Благодаря let все переменные внутри (a, b, i, f) будут локальными,
14 # и Julia не будет ругаться на «global variable» и не выдаст UndefVarError.
15 # Это самый чистый и правильный способ в скрипте.
16
17 a = b = 1                                     # 3
18 # Согласно лабораторной (стр. 25): «Положить  $a \leftarrow c$ ,  $b \leftarrow c$ », а  $c = 1$ .
19 # Поэтому оба указателя («черепаха» a и «заяц» b) стартуют с значения 1.
20
21 i = 1                                         # 4
22 # Счётчик итераций. Начинаем с 1, потому что в таблице из методички
23 # первая строка после заголовка – это  $i = 2$  (уже после первого шага).
24
25 f(x) = (x*x + 5) % n                         # 5
26 # Определяем полиномиальную функцию  $f(x) = x^2 + 5 \pmod{n}$ .
27 # Именно +5 требует методичка (пример на стр. 25).
28 # % n – это взятие остатка по модулю n, чтобы числа не росли бесконечно.
29
30 println(" i\t a\t b\t d")                      # 6
31 # Печатаем шапку таблицы точно как в лабораторной.
32 # \t – табуляция для выравнивания столбцов.
33
34 while true                                      # 7
35 # Запускаем бесконечный цикл – будем выходить из него вручную через break,
36 # когда найдём нетривиальный делитель.
37
38     a = f(a); b = f(f(b)); i += 1                # 8
39     # Один шаг алгоритма Полларда:
40     # • «черепаха» a делает один шаг:  $a \leftarrow f(a)$ 
41     # • «заяц» b делает два шага:  $b \leftarrow f(f(b))$ 
42     # • увеличиваем счётчик итераций
43
44     d = gcd(abs(a - b), n)                        # 9
45     # Вычисляем НОД от  $|a-b|$  и n – это ключевая идея метода Полларда.
46     # Если последовательности зациклятся в каком-то подмодуле,
47     # то  $|a-b|$  будет кратно одному из простых делителей n.
48
49     println("$i\t $a\t $b\t $d")                  # 10
50     # Печатаем текущую строку таблицы: номер итерации, значения a, b и d.
51     # Интерполяция $ позволяет подставить значения переменных прямо в строку.
52
53 if 1 < d < n                                  # 11
54     println("\nНетривиальный делитель: $d и $(n ÷ d)")
55     # Если найден нетривиальный делитель (не 1 и не всё n),
56     # выводим результат и завершаем работу.
57     #  $n \div d$  – это целочисленное деление (в Julia  $\div = \backslash\text{div} + \text{TAB}$ )
58
59     break                                         # 12
60     # Выходим из цикла – задача решена.

```

```
61      end
62    end
63 end
64 # Конец блока let – все локальные переменные автоматически уничтожаются.
```