1. **Пример работы алгоритма быстрого возведения в степень**

**N = 5**

**37 mod 5 = 3\*36 mod 5 = 3\*(4)3 mod 5 = 2\*(4)2 mod 5** = (**2\*1) mod 5 =** 2

|  |  |  |  |
| --- | --- | --- | --- |
| а1(основание степени) | Z(степень) | х(результат) | Шаги выполнения |
| 3 | 7 | 1 | 0 |
| 3 | 6 | (1\*3) mod 5 =3 | 1 |
| (3\*3) mod 5 = 4 | 3 | 3 | 2 |
| 4 | 2 | (3\*4) mod 5 = 2 | 3 |
| (4\*4) mod 5 = 1 | 1 | 2 | 4 |
| 1 | 0 | (2\*1) mod 5 = 2 | 5 |

1. **Пример поиска случайного первообразного корня**

Задано простое p = 11

Ищем простые делители p-1 = 10 = 2\*5

Проверяем все числа от 2 до p-1:

210/2 mod 11 = 10; 210/5 mod 11 = 4. Число **2** является первообразным по модулю 11.

310/2 mod 11 = 1; 310/5 mod 11 = 9. Число 3 не является первообразным по модулю 11.

410/2 mod 11 = 1; 410/5 mod 11 = 5. Число 4 не является первообразным по модулю 11.

510/2 mod 11 = 1; 510/5 mod 11 = 3. Число 5 не является первообразным по модулю 11.

610/2 mod 11 = 10; 610/5 mod 11 = 3. Число **6** является первообразным по модулю 11.

710/2 mod 11 = 10; 710/5 mod 11 = 5. Число **7** является первообразным по модулю 11.

810/2 mod 11 = 10; 810/5 mod 11 = 9. Число **8** является первообразным по модулю 11.

910/2 mod 11 = 1; 910/5 mod 11 = 4. Число 9 не является первообразным по модулю 11.

1010/2 mod 11 = 10; 1010/5 mod 11 = 1. Число 10 не является первообразным по модулю 11.

1. **Пример работы расширенного алгоритма Евклида**

**x1\*a + y1\*b = нод(a,b), a = 100, b = 9, (a,b) = 1**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **итерация** | **q** | **a0** | **a1** | **x0** | **x1** | **y0** | **y1** |
| 0 | - | 100 | 9 | 1 | 0 | 0 | 1 |
| 1 | 11 | 9 | 1 | 0 | 1 | 1 | -11 |
| 2 | 9 | 1 | 0 | 1 | -9 | -11 | 99 |

**x1 = 1 y1 = -11**

**1 \* 100 + (-11) \* 9 = 1**