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

Приведён пример работы итеративного алгоритма, когда с каждой итерацией накапливается значение , сам показатель степени на каждой итерации целочисленно делится на 2, проверяется остаток от деления показателя степени на 2. Если он равен 1, то текущий результат домножается на . Повторяется до тех пор, пока показатель степени станет равен 0.

Пусть основание a = 8, показатель b = 22 = 101102, модуль n = 47

|  |  |  |  |
| --- | --- | --- | --- |
| a^(2^i) | Показатель степени b | Результат | Итерация i |
| 8 | 22 | 1 | 0 |
| (8 \* 8) mod 47 = 17 | 11 | (1 \* 17) mod 47 = 17 | 1 |
| (17 \* 17) mod 47 = 7 | 5 | (17 \* 7) mod 47 = 25 | 2 |
| (7 \* 7) mod 47 = 2 | 2 | 25 (2 - чётное, ничего не делать) | 3 |
| (2 \* 2) mod 47 = 4 | 1 | 1. 4) mod 47 = 6 | 4 |

1. **Пример поиска случайного первообразного корня**

Пусть p = 11

p – 1 = 10 = 2 \* 5

|  |  |  |  |
| --- | --- | --- | --- |
| g | g^(10/5) mod 11 | g^(10/2) mod 11 | Первообразный? |
| 2 | 4 | 10 | Да |
| 3 | 9 | 1 | Нет |
| 4 | 5 | 1 | Нет |
| 5 | 3 | 1 | Нет |
| 6 | 3 | 10 | Да |
| 7 | 5 | 10 | Да |
| 8 | 9 | 10 | Да |
| 9 | 4 | 1 | Нет |
| 10 | 1 | 10 | Нет |

Итого первообразные корни: 2, 6, 7, 8

1. **Пример работы расширенного алгоритма Евклида**

**x1\*a + y1\*b = нод(a,b), a = 373, b = 773, (a,b) = 1**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **итерация** | **q** | **a0** | **a1** | **x0** | **x1** | **y0** | **y1** |
| 0 | - | 373 | 773 | 1 | 0 | 0 | 1 |
| 1 | 0 | 773 | 373 | 0 | 1 | 1 | 0 |
| 2 | 2 | 373 | 27 | 1 | -2 | 0 | 1 |
| 3 | 13 | 27 | 22 | -2 | 27 | 1 | -13 |
| 4 | 1 | 22 | 5 | 27 | -29 | -13 | 14 |
| 5 | 4 | 5 | 2 | -29 | 143 | 14 | -69 |
| 6 | 2 | 2 | 1 | 143 | -315 | -69 | 152 |
| 7 | 2 | 1 | 0 | -315 | 773 | 152 | -373 |

**x1 = -315 y1 = 152**

**-315\*373 + 152 \* 773 = 1**