1. **Быстрое возведение в степень по модулю**

35 mod 7, т.е. a = 3, z =5, n = 7

|  |  |  |  |
| --- | --- | --- | --- |
| **а (основание степени)** | **Z(степень)** | **X(результат)** | **итерация** |
| 3 | 5 | 1 | 0 |
| 2 | 2 | 3 | 1 |
| 4 | 1 | 3 | 2 |
| 2 | 0 | 5 | 3 |

Ответ: 35 mod 7 = 5.

1. **Поиск первообразного корня**p=11, p – 1 = 10 = 2\*5 – простые делители: 2 и 5.

|  |  |  |  |
| --- | --- | --- | --- |
| **g** | **g^10/2 mod 11** | **g^10/5 mod 11** | **Является первообразным?** |
| 2 | 10 | 4 | Да |
| 3 | 1 | 9 | Нет |
| 4 | 1 | 5 | Нет |
| 5 | 1 | 3 | Нет |
| 6 | 10 | 3 | Да |
|  |  |  |  |
| 7 | 10 | 5 | Да |
| 8 | 10 | 9 | Да |
| 9 | 1 | 4 | Нет |
|  |  |  |  |
| 10 | 10 | 1 | Нет |

2, 6, 7, 8 – первообразные корни.

p=17, p – 1 = 16 = 2^4 – простой делитель: 2.

|  |  |  |
| --- | --- | --- |
| **g** | **g^16/2 mod 17** | **Является первообразным?** |
| 2 | 1 | Нет |
| 3 | 16 | Да |
| 4 | 1 | Нет |
| 5 | 16 | Да |
| 6 | 16 | Да |
|  |  |  |
| 7 | 16 | Да |
| 8 | 1 | Нет |
| 9 | 1 | Нет |
|  |  |  |
| 10 | 16 | Да |
| 11 | 16 | Да |
|  |  |  |
| 12 | 16 | Да |
| 13 | 1 | Нет |
| 14 | 16 | Да |
| 15 | 1 | Нет |
| 16 | 1 | Нет |

3, 5, 6, 7, 10, 11, 12, 14 – первообразные корни

1. **Расширенный алгоритм Евклида**

a = 101, b = 23

**a\*x + b\*y= НОД(a,b), a = 101, b = 23, НОД(101, 23) = 1**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **№ шага** | **q** | **a0** | **a1** | **x0** | **x1** | **y0** | **y1** |
| 0 | - | 101 | 23 | 1 | 0 | 0 | 1 |
| 1 | 4 | 23 | 9 | 0 | 1 | 1 | -4 |
| 2 | 2 | 9 | 5 | 1 | -2 | -4 | 9 |
| 3 | 1 | 5 | 4 | -2 | 3 | 9 | -13 |
| 4 | 1 | 4 | 1 | 3 | -5 | -13 | 22 |
| 5 | 4 | 1 | 0 | -5 | 23 | 22 | -101 |

**НОД(101, 23) = a0 = 1**

**x = x0 = -5**

**y = y0 = 22**

**a\*x + b\*y = 101\*(-5) + 23 \* 22 = -505 + 506 = 1 = НОД(101, 23)**