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

1117 mod 51 = (1116 \* 11) = 11

11 mod 51 = 11

112 mod 51 = 121 mod 51 = 19

114 mod 51 = (112 mod 51)2 mod 51 = 192 mod 51 = 4

118 mod 51 = (114 mod 51)2 mod 51 = 42 mod 51 = 16

1116 mod 51 = (118 mod 51)2 mod 51 = 162 mod 51 = 256 mod 51 = 1

1117 mod 51 = (1116 mod 51)\*(11 mod 51) = 1\*11 = 11

1. **Пример поиска случайного первообразного корня**

Пусть простое число p = 13

Простые делители (p-1) = 12 = 2\*3\*3

|  |  |  |  |
| --- | --- | --- | --- |
| 2(12/2) mod 13 = 12 | Подходит | 8(12/2) mod 13 = 12 | Не подходит |
| 2(12/3) mod 13 = 3 | 8(12/3) mod 13 = 1 |
| 3(12/2) mod 13 = 1 | Не подходит | 9(12/2) mod 13 = 1 | Не подходит |
| 3(12/3) mod 13 = 3 | 9(12/3) mod 13 = 9 |
| 4(12/2) mod 13 = 1 | Не подходит | 10(12/2) mod 13 = 1 | Не подходит |
| 4(12/3) mod 13 = 9 | 10(12/3) mod 13 = 3 |
| 5(12/2) mod 13 = 12 | Не подходит | 11(12/2) mod 13 = 12 | Подходит |
| 5(12/3) mod 13 = 1 | 11(12/3) mod 13 = 3 |
| 6(12/2) mod 13 = 12 | Подходит | 12(12/2) mod 13 = 1 | Не подходит |
| 6(12/3) mod 13 = 9 | 12(12/3) mod 13 = 1 |
| 7(12/2) mod 13 = 12 | Подходит |
| 7(12/3) mod 13 = 9 |

Первообразные: 6, 7, 11.

1. **Пример работы расширенного алгоритма Евклида**

x1\*a + y1\*b = нод(a,b), a =445, b =781, (a,b) = 1

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **итерация** | **q** | **a0** | **a1** | **x0** | **x1** | **y0** | **y1** |
| 0 | - | 445 | 781 | 1 | 0 | 0 | 1 |
| 1 | 0 | 781 | 445 | 0 | 1 | 1 | 0 |
| 2 | 1 | 445 | 336 | 1 | -1 | 0 | 1 |
| 3 | 1 | 336 | 109 | -1 | 2 | 1 | -1 |
| 4 | 3 | 109 | 9 | 2 | -7 | -1 | 4 |
| 5 | 12 | 9 | 1 | -7 | 86 | 4 | -49 |
| 6 | 9 | 1 | 0 | 86 | -781 | -49 | 445 |

**x1 = 86 y1 = -49**

**86 \* 445 + (-49) \* 781 = 1**