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

539 mod 17 = (532 mod 17 \* 54 mod 17 \* 52 mod 17 \* 51 mod 17) mod 17 = 10

|  |  |  |  |
| --- | --- | --- | --- |
| а1(основание степени) | Z(степень) | х(результат) | Шаги выполнения |
| 5 | 1 | 5mod 17 = 5 | 0 |
| 5 mod 17 | 2 | (5 \* 5)mod 17 = 8 | 1 |
| 52 mod 17 | 2 | (8 \* 8)mod 17 = 13 | 2 |
| 54 mod 17 | 2 | (13 \* 13)mod 17 = 16 | 3 |
| 58 mod 17 | 2 | (16 \* 16)mod 17 = 1 | 4 |
| 516 mod 17 | 2 | (1 \* 1)mod 17 = 1 | 5 |

5 mod 17 = 5; 52 mod 17 = 8; 54 mod 17 = 13; 532 mod 17 = 1

(5 \* 8 \* 13 \* 1) mod 17 = ((1 \* 13) mod 17 \* (5 \* 8) mod 17) mod 17 = (13 mod 17 \* 40 mod 17) mod 17 = (13 \* 6) mod 17 = 10

1. **Пример поиска всех первообразных корней**

Задано простое p = 59

Ищем простые делители p-1 = 58 = 2\*29

Число g является первообразным корнем по модулю 59, если:

g^29 != 1 (mod 59), g^2 != 1(mod 59).

Количество первоообразных корней по модулю 59 = φ(φ(59)) = φ(58) =

= 58 \* (1 – 1/2) \* (1 – 1/29) = 28.

Считаем все первообразные корни:

g = 2:

* 2^29 mod 59 = 58 != 1
* 2^2 mod 59 = 4 != 1
* Первообразный корень

g = 3:

* 3^29 mod 59 = 1
* Не первообразный корень

g = 4:

* 4^29 mod 59 = 1
* Не первообразный корень

g = 5:

* 5^29 mod 59 = 1
* Не первообразный корень

g = 6:

* 6^29 mod 59 = 58 != 1
* 6^2 mod 59 = 36 != 1
* Первообразный корень

g = 7:

* 7^29 mod 59 = 1
* Не первообразный корень

g = 8:

* 8^29 mod 59 = 58 != 1
* 8^2 mod 59 = 5 != 1
* Первообразный корень

g = 9:

* 9^29 mod 59 = 1
* Не первообразный корень

g = 10:

* 10^29 mod 59 = 58 != 1
* 10^2 mod 59 = 41 != 1
* Первообразный корень

g = 11:

* 11^29 mod 59 = 58 != 1
* 11^2 mod 59 = 3 != 1
* Первообразный корень

g = 12:

* 12^29 mod 59 = 1
* Не первообразный корень

g = 13:

* 13^29 mod 59 = 58 != 1
* 13^2 mod 59 = 51 != 1
* Первообразный корень

g = 14:

* 14^29 mod 59 = 58 != 1
* 14^2 mod 59 = 19 != 1
* Первообразный корень

g =15:

- 15^29 mod 59 = 1

* Не первообразный корень

g =16:

* 16^29 mod 59 = 1
* Не первообразный корень

g =17:

* 17^29 mod 59 = 1
* Не первообразный корень

g = 18:

* 18^29 mod 59 = 58 != 1
* 18^2 mod 59 = 29 != 1
* Первообразный корень

g =19:

* 19^29 mod 59 = 1
* Не первообразный корень

g =20:

* 20^29 mod 59 = 1
* Не первообразный корень

g =21:

* 21^29 mod 59 = 1
* Не первообразный корень

g =22:

* 22^29 mod 59 = 1
* Не первообразный корень

g = 23:

* 23^29 mod 59 = 58 != 1
* 23^2 mod 59 = 57 != 1
* Первообразный корень

g = 24:

* 14^29 mod 59 = 58 != 1
* 14^2 mod 59 = 45 != 1
* Первообразный корень

g =25:

* 25^29 mod 59 = 1
* Не первообразный корень

g =26:

* 26^29 mod 59 = 1
* Не первообразный корень

g =27:

* 27^29 mod 59 = 1
* Не первообразный корень

g =28:

* 28^29 mod 59 = 1
* Не первообразный корень

g =29:

* 29^29 mod 59 = 1
* Не первообразный корень

g = 30:

* 30^29 mod 59 = 58 != 1
* 30^2 mod 59 = 15 != 1
* Первообразный корень

g = 31:

* 31^29 mod 59 = 58 != 1
* 31^2 mod 59 = 17 != 1
* Первообразный корень

g = 32:

* 32^29 mod 59 = 58 != 1
* 32^2 mod 59 = 21 != 1
* Первообразный корень

g = 33:

* 33^29 mod 59 = 58 != 1
* 33^2 mod 59 = 27 != 1
* Первообразный корень

g = 34:

* 34^29 mod 59 = 58 != 1
* 34^2 mod 59 = 35 != 1
* Первообразный корень

g = 35:

* 35^29 mod 59 = 1
* Не первообразный корень

g = 36:

* 36^29 mod 59 = 1
* Не первообразный корень

g = 37:

* 37^29 mod 59 = 58 != 1
* 37^2 mod 59 = 12 != 1
* Первообразный корень

g = 38:

* 38^29 mod 59 = 58 != 1
* 38^2 mod 59 = 28 != 1
* Первообразный корень

g = 39:

* 39^29 mod 59 = 58 != 1
* 39^2 mod 59 = 46 != 1
* Первообразный корень

g = 40:

* 40^29 mod 59 = 58 != 1
* 40^2 mod 59 = 7 != 1
* Первообразный корень

g = 41:

* 41^29 mod 59 = 1
* Не первообразный корень

g = 42:

* 42^29 mod 59 = 58 != 1
* 42^2 mod 59 = 53 != 1
* Первообразный корень

g = 43:

* 43^29 mod 59 = 58 != 1
* 43^2 mod 59 = 20 != 1
* Первообразный корень

g = 44:

* 44^29 mod 59 = 58 != 1
* 44^2 mod 59 = 48 != 1
* Первообразный корень

g = 45:

* 45^29 mod 59 = 1
* Не первообразный корень

g = 46:

* 46^29 mod 59 = 1
* Не первообразный корень

g = 47:

* 47^29 mod 59 = 58 != 1
* 47^2 mod 59 = 26 != 1
* Первообразный корень

g = 48:

* 48^29 mod 59 = 1
* Не первообразный корень

g = 49:

* 46^29 mod 59 = 1
* Не первообразный корень

g = 50:

* 50^29 mod 59 = 58 != 1
* 50^2 mod 59 = 22 != 1
* Первообразный корень

g = 51:

* 51^29 mod 59 = 1
* Не первообразный корень

g = 52:

* 52^29 mod 59 = 58 != 1
* 52^2 mod 59 = 49 != 1
* Первообразный корень

g = 53:

* 53^29 mod 59 = 1
* Не первообразный корень

g = 54:

* 54^29 mod 59 = 58 != 1
* 54^2 mod 59 = 25 != 1
* Первообразный корень

g = 55:

* 55^29 mod 59 = 58 != 1
* 55^2 mod 59 = 16 != 1
* Первообразный корень

g = 56:

* 56^29 mod 59 = 58 != 1
* 56^2 mod 59 = 9 != 1
* Первообразный корень

g = 57:

* 57^29 mod 59 = 1
* Не первообразный корень

g = 58:

* 58^29 mod 59 = 1
* Не первообразный корень

Итого 28 корней: 2, 6, 8, 10, 11, 13, 14, 18, 23, 24, 30, 31, 32, 33, 34, 37, 38, 39, 40, 42, 43, 44, 47, 50, 52, 54, 55, 56.

1. **Пример работы расширенного алгоритма Евклида**

**x1\*a + y1\*b = нод(a,b), a = 292, b = 221, (a,b) = 1**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **итерация** | **q** | **a0** | **a1** | **x0** | **x1** | **y0** | **y1** |
| 0 | - | 292 | 221 | 1 | 0 | 0 | 1 |
| 1 | 1 | 221 | 71 | 0 | 1 | 1 | -1 |
| 2 | 3 | 71 | 8 | 1 | -3 | -1 | 4 |
| 3 | 8 | 8 | 7 | -3 | 25 | 4 | -33 |
| 4 | 1 | 7 | 1 | 25 | -28 | -33 | 37 |
| 5 | 7 | 1 | 0 | -28 | 221 | 37 | -292 |

**x1 = -28; y1 = 37**

**(-28) \* 292 + 37 \* 221 = -8176 + 8177 = 1**