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

80233 mod 299 = 201

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ шага** | А (основание) | E (степень) | M (модуль) | R (результат) |
| 0 | 80 | 233 | 299 | 1 |
| 1 | 121 | 116 | 299 | 80 |
| 2 | 289 | 58 | 299 | 80 |
| 3 | 100 | 29 | 299 | 80 |
| 4 | 133 | 14 | 299 | 226 |
| 5 | 48 | 7 | 299 | 226 |
| 6 | 211 | 3 | 299 | 84 |
| 7 | 269 | 1 | 299 | 83 |
| 8 | 3 | 0 | 299 | 201 |

1. **Поиск первообразного корня**

Простое число p = 43

ȹ(p) = p - 1 = 42 = 2\*3\*7

Количество первоообразных по модулю 43 = φ(φ(43)) = φ(42) = 12.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **g** | **g^42/2 mod 43** | **g^42/3 mod 43** | **g^42/7 mod 43** |  |
| 2 | 42 | 1 | 21 | - |
| 3 | 42 | 36 | 41 | + |
| 4 | 1 | 1 | 11 | - |
| 5 | 42 | 36 | 16 | + |
| 6 | 1 | 36 | 1 | - |
| 7 | 42 | 6 | 1 | - |
| 8 | 42 | 1 | 16 | - |
| 9 | 1 | 6 | 4 | - |
| 10 | 1 | 36 | 35 | - |
| 11 | 1 | 1 | 4 | - |
| 12 | 42 | 36 | 21 | + |
| 13 | 1 | 6 | 16 | - |
| 14 | 1 | 6 | 21 | - |
| 15 | 1 | 6 | 11 | - |
| 16 | 1 | 1 | 35 | - |
| 17 | 1 | 6 | 35 | - |
| 18 | 42 | 6 | 41 | + |
| 19 | 42 | 36 | 11 | + |
| 20 | 42 | 36 | 4 | + |
| 21 | 1 | 1 | 41 | - |
| 22 | 42 | 1 | 41 | - |
| 23 | 1 | 36 | 4 | - |
| 24 | 1 | 36 | 11 | - |
| 25 | 1 | 6 | 41 | - |
| 26 | 42 | 6 | 35 | + |
| 27 | 42 | 1 | 35 | - |
| 28 | 42 | 6 | 11 | + |
| 29 | 42 | 6 | 21 | + |
| 30 | 42 | 6 | 16 | + |
| 31 | 1 | 36 | 21 | - |
| 32 | 42 | 1 | 4 | - |
| 33 | 42 | 36 | 35 | + |
| 34 | 42 | 6 | 4 | + |
| 35 | 1 | 1 | 16 | - |
| 36 | 1 | 6 | 1 | - |
| 37 | 42 | 36 | 1 | - |
| 38 | 1 | 36 | 16 | - |
| 39 | 42 | 1 | 11 | - |
| 40 | 1 | 36 | 41 | - |
| 41 | 1 | 1 | 21 | - |
| 42 | 42 | 1 | 1 | - |

Первообразные корни по модулю 43: 3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33, 34.

1. **Расширенный алгоритм Евклида**

a = 264, b = 17

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **№ шага** | **q** | **a0** | **a1** | **x0** | **x1** | **y0** | **y1** |
| 0 | - | 264 | 17 | 1 | 0 | 0 | 1 |
| 1 | 15 | 17 | 9 | 0 | 1 | 1 | -15 |
| 2 | 1 | 9 | 8 | 1 | -1 | -15 | 16 |
| 3 | 1 | 8 | 1 | -1 | 2 | 16 | -31 |
| 4 | 8 | 1 | 0 | 2 | -17 | -31 | 264 |

Если y0 < 0, то

y0 = y0 + a = -31 + 264 = 233