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. **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