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

13245 mod 267 = 242

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ шага** | А (основание) | Z (степень) | N (модуль) | X (результат) |
| 0 | 13 | 245 | 267 | 1 |
| 1 | 13 | 244 | 267 | 13 |
| 2 | 169 | 122 | 267 | 13 |
| 3 | 259 | 61 | 267 | 13 |
| 4 | 259 | 60 | 267 | 167 |
| 5 | 256 | 30 | 267 | 167 |
| 6 | 121 | 15 | 267 | 167 |
| 7 | 121 | 14 | 267 | 182 |
| 8 | 223 | 7 | 267 | 182 |
| 9 | 223 | 6 | 267 | 2 |
| 10 | 67 | 3 | 267 | 2 |
| 11 | 67 | 2 | 267 | 134 |
| 12 | 217 | 1 | 267 | 134 |
| 13 | 217 | 0 | 267 | 242 |

1. **Поиск первообразного корня**

Простое число p = 11

ȹ(p) = p - 1 = 10 = 2\*5

Количество первоообразных по модулю 11 = φ(φ(11)) = φ(10) = 4.

* Проверяем является ли 2 первообразным корнем по модулю 11:

210/5 mod 11 = 22 mod 11 = 4 mod 11 = 4;

210/2 mod 11 = 25 mod 11 = 32 mod 11 = 10.

Число 2 является первообразным по модулю.

* Проверяем является ли 3 первообразным корнем по модулю 11:

32 mod 11 = 9 mod 11 = 2;

35 mod 11 = 243 mod 11 = 1 – значит нет.

* Проверяем является ли 4 первообразным корнем по модулю 11:

42 mod 11 = 16 mod 11 = 5;

45 mod 11 = 1024 mod 11 = 1 – значит нет.

* Проверяем является ли 5 первообразным корнем по модулю 11:

52 mod 11 = 25 mod 11 = 3;

55 mod 11 = 3125 mod 11 = 1 – значит нет.

* Проверяем является ли 6 первообразным корнем по модулю 11:

62 mod 11 = 36 mod 11 = 3;

65 mod 11 = 7776 mod 11 = 10.

Число 6 является первообразным по модулю.

* Проверяем является ли 7 первообразным корнем по модулю 11:

72 mod 11 = 49 mod 11 = 5;

75 mod 11 = 16807 mod 11 = 10.

Число 7 является первообразным по модулю.

* Проверяем является ли 8 первообразным корнем по модулю 11:

82 mod 11 = 64 mod 11 = 5;

85 mod 11 = 32768 mod 11 = 10.

Число 8 является первообразным по модулю.

Нашлось уже 4 корня – 2, 6, 7, 8

* На всякий случай проверим 9:

92 mod 11 = 81 mod 11 = 4;

95 mod 11 = 59049 mod 11 = 1 – значит нет.

* На всякий случай проверим 10:

102 mod 11 = 100 mod 11 = 1 – значит нет.

Первообразные корни по модулю 11: 2, 6, 7, 8

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