**Примеры работы алгоритмов:**

**Быстрое возведение в степень**

Вычислим значение выражения: 1515 mod 11.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Шаг | Основание | Показатель | Модуль | Результат |
| 0 | 15 | 15 | 11 | 1 |
| 1 | 15 | 15 – 1 = 14 | 11 | (1 \* 15) mod 11 = 4 |
| 2 | (15\*15) mod 11=5 | 14 : 2 = 7 | 11 | 4 |
| 3 | 5 | 7 – 1 = 6 | 11 | (4 \* 5) mod 11 = 9 |
| 4 | (5 \* 5) mod 11 = 3 | 6 : 2 = 3 | 11 | 9 |
| 5 | 3 | 3 – 1 = 2 | 11 | (9 \* 3) mod 11 = 5 |
| 6 | (3 \* 3) mod 11 = 9 | 2 : 2 = 1 | 11 | 5 |
| 7 | 9 | 1 – 1 = 0 | 11 | (5 \* 9) mod 11 = 1 |

**Расширенный алгоритм Евклида**

Подберём такие значения a и b, что 2311a + 1459b = НОД(2311; 1459) = 1.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Шаг | X | Y | B | A | X div Y | След. X | След. Y | След. B | След. A |
| -1 | 2311 | 1459 | 0 | 1 | - | - | - | 1 | 0 |
| 0 | 2311 | 1459 | 1 | 0 | 1 | 1459 | 852 | -1 | 1 |
| 1 | 1459 | 852 | -1 | 1 | 1 | 852 | 607 | 2 | -1 |
| 2 | 852 | 607 | 2 | -1 | 1 | 607 | 245 | -3 | 2 |
| 3 | 607 | 245 | -3 | 2 | 2 | 245 | 117 | 8 | -5 |
| 4 | 245 | 117 | 8 | -5 | 2 | 117 | 11 | -19 | 12 |
| 5 | 117 | 11 | -19 | 12 | 10 | 11 | 7 | 198 | -125 |
| 6 | 11 | 7 | 198 | -125 | 1 | 7 | 4 | -217 | 137 |
| 7 | 7 | 4 | -217 | 137 | 1 | 4 | 3 | 415 | -262 |
| 8 | 4 | 3 | 415 | -262 | 1 | 3 | 1 | -632 | 399 |
| 9 | 3 | 1 | -632 | 399 | 3 | 1 | 0 |  |  |

Проверка: 2311 \* 399 – 1459 \* 632 = 922089 – 922088 = 1.

**Поиск случайного первообразного корня**

Найдём все первообразные корни простого числа 11.

Найдём все простые числа, меньшие 11: 2, 3, 5, 7.

Найдём простые сомножители числа 10: 2, 5.

Переберём все числа от 2 до 10:

2) 210/2 mod 11 = 32 mod 11 = 10;

25/10 mod 11 = 4 mod 11 = 4.

Число 2 является первообразным корнем.

3) 310/2 mod 11 = 35 mod 11 = 1;

Число 3 не является первообразным корнем.

4) 410/2 mod 11 = 45 mod 11 = 1;

Число 4 не является первообразным корнем.

5) 510/2 mod 11 = 55 mod 11 = 1;

Число 5 не является первообразным корнем.

6) 610/2 mod 11 = 65 mod 11 = 10;

65/10 mod 11 = 62 mod 11 = 3.

Число 6 является первообразным корнем.

7) 710/2 mod 11 = 75 mod 11 = 10;

75/10 mod 11 = 72 mod 11 = 5.

Число 7 является первообразным корнем.

8) 810/2 mod 11 = 85 mod 11 = 10;

85/10 mod 11 = 82 mod 11 = 9.

Число 8 является первообразным корнем.

9) 910/2 mod 11 = 95 mod 11 = 1;

Число 9 не является первообразным корнем.

10) 1010/2 mod 11 = 105 mod 11 = 1;

Число 10 не является первообразным корнем.