1. **Пример работы алгоритма быстрого возведения в степень** (без модульной арифметики, студент должен привести пример с модульной арифметикой)

95 mod 7

a = 9, z = 7, x = 1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| А1 (основание степени)bb | Z(степень) | X(результат) | Модуль | Шаги выполнения |
| 9 | 5 | 1 | 7 | 0 |
| 9 | 4 | 2 | 7 | 1 |
| 4 | 2 | 2 | 7 | 2 |
| 2 | 1 | 2 | 7 | 3 |
| 2 | 0 | 4 | 7 | 4 |

1. **Пример поиска случайного первообразного корня**

p=15, p – 1 = 14 = 2\*7

|  |  |  |  |
| --- | --- | --- | --- |
| **g** | **g^14/2 mod 15** | **g^14/7 mod 15** | **Является первообразным** |
| 2 | 8 | 2 | да |
| 3 | 3 | 9 | да |
| 4 | 4 | 1 | нет |
| 5 | 5 | 10 | да |
| 6 | 6 | 9 | да |
| 7 | 13 | 4 | да |
| 8 | 2 | 4 | да |
| 9 | 9 | 6 | да |
| 10 | 10 | 10 | да |
| 11 | 11 | 1 | нет |
| 12 | 3 | 9 | да |
| 13 | 7 | 4 | да |
| 14 | 14 | 1 | нет |

2, 3, 5, 6, 7, 8, 9, 10, 12, 13 – первообразные корни

1. **Пример работы расширенного алгоритма Евклида**

a = 11, b = 29

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Итерация** | **q** | **a0** | **a1** | **x0** | **x1** | **y0** | **y1** |
| 0 | - | 11 | 29 | 1 | 0 | 0 | 1 |
| 1 | 0 | 29 | 11 | 0 | 1 | 1 | 0 |
| 2 | 2 | 11 | 7 | 1 | -2 | 0 | 1 |
| 3 | 1 | 7 | 4 | -2 | 3 | 1 | -1 |
| 4 | 1 | 4 | 3 | 3 | -5 | -1 | 2 |
| 5 | 1 | 3 | 1 | ­-5 | 8 | 2 | -3 |
| 6 | 3 | 1 | 0 | 8 | -29 | -3 | 11 |