Лабораторная работа №3

Яковлев В.Ю. 051003

Пример работы алгоритма быстрого возведения в степень

$$19^{45}\ mod\ 5 = 19\ mod\ 5 * 19^{44}\ mod\ 5 = 4 * 4^{44}\ mod\ 5 = 4 * 16^{22}\ mod\ 5 = 4 * 1^{22}\ mod\ 5 = 4 * 1 = 4$$

Пример поиска первообразных корней

Задано простое p = 7
Ищем простые делители p - 1 = 6 = 2*3
Проверяем от 1 до p – 1 числа, являются ли они первообразным корнем по модулю 7
$1^{6/2}\ mod\ 7$ *= 1* – не подходит

$2^{6/2}\ mod\ 7 = 1$ – не подходит

$3^{6/2}\ mod\ 7$ *= 6* $3^{6/3}\ mod\ 7 = 2$ – *оба подходят, значит 3 первообразный корень по модулю 7*

$4^{6/2}\ mod\ 7 = 1$ – не подходит

$5^{6/2}\ mod\ 7 = 6$ $5^{6/3}\ mod\ 7 = 5$ – *оба подходят, значит 5 первообразный корень по модулю 7*

$6^{6/2}\ mod\ 7 = 6$ $6^{6/3}\ mod\ 7 = 1$ – не подходит

3 и 5 – первообразные по модулю 7

Пример работы расширенного алгоритма Евклид

x*a + y*b = нод(a,b), a = 275, b = 84, (a,b) = 1

итерация	**a**	**b**	**x**	**y**
1	275	84	11	-36
2	84	23	-3	11
3	23	15	2	-3
4	15	8	-1	2
5	8	7	1	-1
6	7	1	0	1
7	1	0	1	0

x = 11; y = -36

11 * 275 – 33 * 84 = 1