

Elliptic Curves - List 3

Task 1 (15 pts) Implement the square root algorithm explained on the lectures. The algorithm runs modulo a prime number $p > 2$.

Run the implementation for a random argument a being a square root modulo p for prime p of the form:

$$p = 2^t \cdot s + 1,$$

where s is an odd number greater than 2^{99} , and $t \geq 150$. For checking print p in the binary form. Check that the result returned by the algorithm is really a square root from $a \bmod p$.