Сложности (проект)

Игорь Мельников

Ноябрь 2021

1 Введение

В данной работе приведены доказательство кореектности и анализ работы ZPP алгоритма, безошибочно проверяющего простоту числа. Алгоритм будет построен, при помощи пары алгоритмов из RP и co-RP. В качестве таких алгоритмов берем алгоритмы Миллера–Рабина и Эйдлмана–Хуана проверки простоты числа. Данные алгоритмы вероятностные и допускают ошибки в разные стороны. Так алгоритм Миллера–Рабина может принять составное число за простое, в то время как алгоритм Эйдлмана–Хуана может принять простое число за составное. Для безошибочной проверки простоты числа мы будет действовать следующим образом - запускать алгоритмы Миллера–Рабина и Эйдлмана–Хуана до тех пор, пока их ответы не совпадут. Так же мы докажем, что алгоритм построенный таким образом будет принадлежать классу ZPP.