A POLYNOMIAL-TIME REDUCTION OF THE QUADRATIC CONGRUENCE PROBLEM TO THE 3-SAT AND RELATED PROBLEMS

Renato Lui Geh
NUSP: 8536030
Computational Number Theory — Prof. Sinai Robins

Abstract. In this term paper for MAC6927 — Computational Number Theory, we explore the history behind the quadratic congruence problem (QCP) and other related number theory problems; show a polynomial-time reduction from the QCP to the 3-SAT quoting Adleman and Mander's 1978 article [MA78], implying that quadratic congruence is NP-complete; and show some open and solved problems in Number Theory that are directly (or indirectly) related to the QCP problem and its membership in NP.

References

[MA78] Kenneth Manders and Leonard Adleman. "NP-Complete Decision Problems for Binary Quadratics". In: *Journal of Computer and System Sciences* 16 (1978).