

Small Solutions of Quadratic Congruences Modulo Prime Powers

A Thesis submitted to
Department of Mathematics
Ramakrishna Mission Vivekananda Educational and Research Institute
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy
in
Mathematical Sciences

Submitted by
Anup Haldar
REG NO: B1950005

Under the supervision of
Prof. Stephan Baier
Professor, Department of Mathematics, RKMVERI



DEPARTMENT OF MATHEMATICS
RAMAKRISHNA MISSION VIVEKANANDA EDUCATIONAL AND
RESEARCH INSTITUTE
BELUR MATH, HOWRAH, 711202, INDIA
MONTH- JUNE,2025

ABSTRACT

Small solutions of quadratic congruences modulo prime powers

by

Anup Haldar

This thesis investigates the asymptotic behavior and equidistribution properties of small solutions to quadratic congruences and related problems in number theory. For a fixed prime $p > 5$, we study congruences of the form

$$x_1^2 + x_2^2 \equiv x_3^2 \pmod{p^m},$$

with bounded variables $\max\{|x_1|, |x_2|, |x_3|\} \leq p^\nu$ for $\nu > \frac{1}{2}$, proving the existence of solutions. We extend this result to congruences of the form

$$\alpha_1 x_1^2 + \alpha_2 x_2^2 + \alpha_3 x_3^2 \equiv 0 \pmod{q},$$

where $q = p^m$, $(\alpha_1 \alpha_2 \alpha_3, p) = 1$, and derive asymptotic formulas for the number of solutions within the box $\max\{|x_1|, |x_2|, |x_3|\} \leq N$. Under conditions $N \geq q^{\frac{1}{2} + \varepsilon}$ (when coefficients $\alpha_1, \alpha_2, \alpha_3$ are fixed) or $N \geq q^{\frac{11}{18} + \varepsilon}$ (when $\alpha_1, \alpha_2, \alpha_3$ are allowed to vary), we demonstrate the existence of solutions.

Further extending these results, we examine the solutions to quadratic forms

$$Q(x_1, x_2, x_3) \equiv 0 \pmod{q}$$

under non-degeneracy conditions. We establish asymptotic formulas for the number of solutions within bounded regions of the form

$$\max\{|x_1 - x_0|, |x_2 - y_0|, |x_3 - z_0|\} \leq N,$$

with $(x_3, p) = 1$, as $n \rightarrow \infty$ and $N \geq q^{\frac{1}{2} + \varepsilon}$.

We develop a novel method for evaluating general exponential sums with rational amplitude functions in multiple variables, extending previous results for single-variable cases. As an application, we obtain an asymptotic formula for the weighted

number of solutions to general n -variable quadratic congruences modulo p^m in small boxes, thus establishing equidistribution results.

Finally, we provide an asymptotic formula for the fourth power mean of a general s -dimensional hyper-Kloosterman sum, counting solutions to related congruence equations modulo p .

KEYWORDS: Quadratic congruences, Poisson summation, Evaluation of exponential sums, Parametrization of points, Diophantine equations, Asymptotic formulas, Equidistribution, Hyper-Kloosterman sums, Modular arithmetic, Parametrization of points, Multiple exponential sums, Non-degenerate quadratic forms, Weighted solutions, Rational amplitude functions, Character sums.