

THREE MAT2000 PROJECTS

JOHN CHRISTIAN OTTEM

1. VARIANTS OF FERMAT'S LAST THEOREM

Fermat's Last theorem, proved by Andrew Wiles and Richard Taylor, states that for $n \geq 3$, any solution $(x, y, z) \in \mathbb{Z}^3$ of the Fermat equation

$$(1) \quad x^n + y^n = z^n$$

must be one of the 'trivial solutions' where $xyz = 0$.

This project will study and compare proofs for specific exponents, e.g.,

- (1) $n = 3$ (Euler)
- (2) $n = 4$ (Fermat)
- (3) n 's such that $\mathbb{Z}[\omega]$ is a unique factorization domain (Kummer).

Another possible direction is to explore Fermat's Last Theorem in other rings, e.g., $\mathbb{Z}[i]$, $\mathbb{Z}/n$, ..

2. HYPERSURFACES OVER FINITE FIELDS

Let $f(x_1, \dots, x_n)$ be a polynomial in n variables $x_1, \dots, x_n$ with integer coefficients and let k be a finite field. A natural question is: *How many solutions are there to the equation*

$$f(x_1, \dots, x_n) = 0$$

over the field k ?

The project will explore this question, and in particular how the number of solutions is reflected in the geometry of the hypersurface $X = \{f(x_1, \dots, x_n) = 0\} \subset k^n$.

Some possible directions:

- (i) Study the generating function $\sum_{n=1}^{\infty} a_n t^n$ where a_n is the number of solutions of f in $\mathbb{F}_{p^n}$; The Weil conjectures
- (ii) Gauss and Jacobi Sums; Fermat hypersurfaces
- (iii) Elliptic curves and cubic hypersurfaces
- (iv) The Chevalley–Warning theorem
- (v) Combinatorial applications (Cauchy–Davenport, Erdős–Ginzburg–Ziv,...).

3. DIOPHANTINE EQUATIONS

Many central questions in number theory involve *diophantine equations*, i.e., finding all integer solutions $x_1, \dots, x_n \in \mathbb{Z}$ of the equation

$$f(x_1, \dots, x_n) = 0$$

where f is a polynomial with integer coefficients.

This project will explore some of these intriguing questions, including:

- Equations of the form $y^2 = p(x)$
- The equations $1 + x + \dots + x^m = 1 + y + \dots + y^n$
- Geometric Diophantine Problems:
 - Is there a perfect cuboid? Does there exist a rectangular box where all edges, face diagonals, and the space diagonal have integer lengths?
 - Can four squares be found such that the sum of any pair is a perfect square?
 - Can four squares be found such that the difference of any pair is a perfect square?
 - Is there a point all of whose distances from the corners of the unit square are rational?

See R. Guy *Unsolved problems in number theory*.