An introduction to number theory and Diophantine equations
Lecture Summaries
SWIM 2010

Lillian Pierce

Lecture 1: Famous Diophantine equations

- What is number theory?
- Natural numbers
- Prime numbers: multiplicative definition, interesting additive properties
- Types of numbers: natural numbers, integers, real numbers, rational number, irrational numbers
- Functions of numbers: Diophantine equations
- Real solutions to Diophantine equations lead to geometric problems
- Integer solutions to Diophantine equations lead to number theoretic problems
- The Gauss circle problem, the twin prime conjecture, the Goldbach conjecture

Lecture 2: A first look at binary quadratic forms

- definition of binary quadratic forms
- definition of the discriminant
- congruence properties of discriminant modulo 4
- definition of indefinite, positive definite, and negative definite forms
- construction of an infinite family of forms with fixed discriminant
- primitive forms, primitive values

Lecture 3: Fundamental questions

Problem 1. *Given an integer m and a discriminant D, find if there is a primitive representation of m by a quadratic form of discriminant D.*

Problem 2. *Enumerate the forms Q with discriminant D such that m has a primitive representation by Q.*

Problem 3. *For each Q of discriminant D such that m has a primitive representation by Q, determine all the representations of m by Q.*

- multiplication and inversion of 2×2 matrices
- linear changes of variables and $GL_2(\mathbb{Z})$
- equivalence of forms $Q \sim Q'$, via $GL_2(\mathbb{Z})$
- proper equivalence of forms $Q \approx Q'$, via $SL_2(\mathbb{Z})$

Lecture 4: Importance of equivalence

- Solution to Problem 1: Given m and $D \equiv 0, 1 \pmod 4$, there exists a primitive representation of m by some form of discriminant D if and only if there exists n such that $D \equiv n^2 \pmod{4m}$.
- Solution to Problem 2: m has a primitive representation by Q of discriminant D if and only if Q is properly equivalent to a form $\langle m, n, l \rangle$ for n in some residue class modulo $2m$ and for $l = (n^2 - D)/4m$.
- equivalence relations and equivalence classes
- key uses of equivalence and proper equivalence of forms

Lecture 5: Reduction of forms

- Reducing forms to "special" forms via linear changes of variables that reduce the coefficients
- fundamental inequalities for minima of forms
- definition of reduced forms
- there are finitely many reduced forms
- algorithm for reducing forms

Lecture 6: Reduced forms are representatives of equivalence classes

- every form is (properly) equivalent to exactly one reduced form
- equivalence classes split into either 1 or 2 proper equivalence classes
- definition of the class number
- computing the class number of a given discriminant
- computing all reduced forms of a given discriminant
- return to Problem 2: if there is one (proper) equivalence class of forms of discriminant D, we can enumerate the forms that represent a given integer.
- if there is one (proper) equivalence class of primitive forms of discriminant D, we can enumerate the forms that represent a given prime.
- what if there are more than two equivalence classes?

Lecture 7: Genus theory

- class numbers
- fundamental discriminants: definition and criteria
- equivalence modulo p for p prime
- Legendre symbol and quadratic residues
- definition of characters and the character system of a form
- definition of a genus
- the relation between the number of genera and the class number
- a fundamental ambiguity still remains if there is more than one class in each genus!
- algorithm to compute character system
- Open Problem Challenge: define a character system that disambiguates between classes in a single genus!