August 5, 2016

A joint CIMPA-ICTP research school on
Lattices and applications to cryptography and coding theory
Saigon University, Ho Chi Minh City, Vietnam.
August 1st - 12th, 2016

http://ricerca.mat.uniroma3.it/users/valerio/hochiminh16.html

Lattices and geometry of numbers III

Michel Waldschmidt
Université Pierre et Marie Curie (Paris 6) France

http://www.imj-prg.fr/~michel.waldschmidt/

Update: 05/08/2016

Part III: August 5, 2016

Examples of lattices in number theory

- Minima of quadratic forms
- Sum of two squares
- Sum of four squares
- Primes of the form $x^2 + ny^2$
- Discriminant of a number field
- Units of a number field: Dirichlet's Theorem
- Geometry of numbers and transcendence

Minima of quadratic forms

Theorem 1 (Minkowski).
Given a positive definite quadratic form Q in n variables with real coefficients and determinant D, we have

$$\min\{Q(x) \mid x \in \mathbb{Z}^n \setminus \{0\}\} \leq \frac{4}{\pi}\Gamma(1+\frac{n}{2})^{2/n} D^{1/n}.$$

The coefficient

$$\frac{4}{\pi}\Gamma(1+\frac{n}{2})^{2/n} \quad \text{is} \quad 4V_n^{-2/n} \quad \text{with} \quad V_n = \frac{\pi^{n/2}}{\Gamma(1+\frac{n}{2})}.$$

Sums of two squares

Theorem 2 (Fermat).
A prime $p \equiv 1 \pmod 4$ is a sum of two squares.

Proof.
Assume G is a sublattice of $\mathbb{Z}^2$ of determinant p such that for all $(x_1, x_2) \in G$ we have $x_1^2 + x_2^2 \equiv 0 \pmod p$.
The disc $x_1^2 + x_2^2 < 2p$ has area $4\pi p^2 > 4p = 4 \det G$.
By Minkowski's Theorem for lattices, there is a point $(x_1, x_2) \neq \{0, 0\}$ of G in this disc. We have

$$0 < x_1^2 + x_2^2 < 2p \quad \text{and} \quad x_1^2 + x_2^2 \equiv 0 \pmod p,$$

hence $x_1^2 + x_2^2 = p$.

$\square$

A suitable lattice

For $u \in \mathbb{Z}$, consider the lattice $G_u = \mathbb{Z}(p,0) + \mathbb{Z}(u,1)$. The determinant is p. For $(x_1, x_2) \in G_u$ we have

$$x_1^2 + x_2^2 \equiv (u^2+1)x_2^2 \pmod{p}.$$

Since $p \equiv 1 \pmod{4}$, -1 is a quadratic residue modulo 4. Hence there exists $u \in \mathbb{Z}$ with $u^2 + 1 \equiv 0 \pmod{p}$.

Sums of four squares - Euler identity

Theorem 3 (Lagrange).

Any positive integer is a sum of four squares.

It suffices to prove the result for an odd prime number p, thanks to Euler identity.

$$\begin{aligned}(a_1^2+a_2^2+a_3^2+a_4^2)(b_1^2+b_2^2+b_3^2+b_4^2) = \\ (a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4)^2 + (a_1b_2 + a_2b_1 + a_3b_4 - a_4b_3)^2 \\ +(a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2)^2 + (a_1b_4 + a_2b_3 - a_3b_2 + a_4b_1)^2.\end{aligned}$$

R. C. Vaughan, *The Geometry of numbers.* `http://www.personal.psu.edu/rcv4/677C03.pdf`

Sums of four squares: Lagrange's Theorem

Lagrange's Theorem follows from the following special case: *Any odd prime number is a sum of four squares.*

Proof.

Assume G is a sublattice of $\mathbb{Z}^4$ of determinant p^2 such that for all $\underline{x} \in G$ we have $x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{p}$.
The sphere $x_1^2 + x_2^2 + x_3^2 + x_4^2 < 2p$ has volume
$2\pi^2 p^2 > 4p^2 = 2^4 \det G$.
By Minkowski's Theorem for lattices, there is a point $\underline{x} \neq 0$ of G in the disc. We have $0 < x_1^2 + x_2^2 + x_3^2 + x_4^2 < 2p$ and $x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{p}$, hence $x_1^2 + x_2^2 + x_3^2 + x_4^2 = p$. □

A suitable lattice

For u and v in $\mathbb{Z}$, consider the lattice
$G_{uv} = \mathbb{Z}(0,0,p,0) + \mathbb{Z}(0,0,0,p) + \mathbb{Z}(1,0,u,-v) + \mathbb{Z}(0,1,v,u)$.
The determinant is p^2. For $(x_1, x_2, x_3, x_4) \in G_{uv}$ we have

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv (u^2 + v^2 + 1)(x_1^2 + x_2^2) \pmod{p}.$$

It remains to select u and v in $\mathbb{Z}$ such that

$$u^2 + v^2 + 1 \equiv 0 \pmod{p}$$

(exercise).

Jay R. Goldman. *The Queen of Mathematics: A Historically Motivated Guide to Number Theory.* A K Peters/CRC Press, 1998. Chap. 22: Geometry of numbers.
`https://www2.math.ethz.ch/education/bachelor/seminars/hs2014/beweise-aus-dem-buch/`

Primes of the form $x^2 + ny^2$

Theorem 4 (Fermat).

An odd prime number p can be written $x^2 + 2y^2$ if and only if $p \equiv 1$ or $3 \mod 8$.
A prime number p can be written $x^2 + 3y^2$ if and only if $p \equiv 1 \mod 3$.

Theorem 5 (Gauss).

A prime number p can be written $x^2 + 27y^2$ if and only if $p \equiv 1 \mod 3$ and 2 is a cubic residue $\mod p$.

Reference: David A. Cox. Primes of the form $x^2 + ny^2$. John Wiley (1989).

Canonical embedding of a number field

Let k be a number field of degree n. Let r_1 be the number of real embeddings and $2r_2$ the number of complex embeddings. The canonical embedding of k is the injective map

$$\underline{\sigma} = (\sigma_1, \ldots, \sigma_{r_1+r_2}) : k \longrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}.$$

The image $\underline{\sigma}(\mathbb{Z}_k)$ of the ring of integers of k under $\underline{\sigma}$ is a lattice in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$.

Hence the ring of integers is a free $\mathbb{Z}$–module of rank n.

Discriminant of a number field

Let k be a number field of degree $n \geq 2$.

Consider an integral basis $\omega_1, \ldots, \omega_n$ of $\mathbb{Z}_k$. Let $\omega_i^{(1)}, \ldots, \omega_i^{(n)}$ be the n complex conjugates of ω_i $(i = 1, \cdots, n)$.

The discriminant d_k of k is the square of the determinant of the $n \times n$ matrix $\left(\omega_i^{(j)}\right)$.

The value of d_k depends only on k (not on the basis of $\mathbb{Z}_k$), it is a nonzero rational integer.

Further, if k is totally real, then it is a positive integer.

Lower bound for the discriminant

Here is the solution by Minkowski of a Conjecture of Kronecker.

Theorem 6.

The discriminant of a number field $\neq \mathbb{Q}$ is > 1, hence is divisible by at least one prime.

Proof.

For simplicity assume k is totally real. By Minkowski's linear form theorem for the product of linear forms, there exists a nonzero integer point $\underline{x}$ such that

$$\left| \prod_{j=1}^{n} \sum_{i=1}^{n} x_i \omega_i^{(j)} \right| \leq \frac{n! \sqrt{d_k}}{n^n}.$$

The left hand side is a nonzero integer. Hence

$$d_k \geq (n^n / n!)^2 > 1.$$

C.L. Siegel

Let $P \in \mathbb{Z}[X]$ be a monic irreducible polynomial of degree n and discriminant Δ having n real zeroes. Then

$$\Delta \geq \left(\frac{n^n}{n!}\right)^2.$$

Siegel, Carl Ludwig. *Lectures on the geometry of numbers.* Springer-Verlag, Berlin, 1989. See Lecture 3, §2.

Logarithmic embedding of a number field

The *logarithmic embedding* is the map $\lambda : k^\times \longrightarrow \mathbb{R}^{r_1+r_2}$ obtained by composing the restriction of $\underline{\sigma}$ to $k^\times$ with the map

$$(z_j)_{1\leq j\leq r_1+r_2} \longmapsto (\log|z_j|)_{1\leq j\leq r_1+r_2}$$

from $(\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2}$ to $\mathbb{R}^{r_1+r_2}$.

In other words

$$\lambda(\alpha) = (\log|\sigma_j(\alpha)|)_{1\leq j\leq r_1+r_2}.$$

Dirichlet's units Theorem

The image $\lambda(\mathbb{Z}_k^\times)$ of the group of units of k is a subgroup of the additive group $\mathbb{R}^{r_1+r_2}$, it is contained in the hyperplane H of equation

$$x_1 + \cdots + x_{r_1} + 2x_{r_1+1} + \cdots + 2x_{r_1+r_2} = 0,$$

and $\lambda(\mathbb{Z}_k^\times)$ is discrete in H. From these properties, one easily deduces that as a $\mathbb{Z}$–module, $\mathbb{Z}_k^\times$ is finitely generated of rank $\leq r$, where $r = r_1 + r_2 - 1$ is the dimension of H as a $\mathbb{R}$–vector space.

Theorem 7 (Dirichlet's units Theorem).

The image of the group of units $\lambda(\mathbb{Z}_k^\times)$ is a lattice in H. As a consequence, the group of units of an algebraic number field k is a finitely generated group of rank r.

http://www.numbertheory.org/ntw/lecture_notes.html

Geometry of numbers and transcendence

Thue–Siegel's Lemma - Dirichlet's box principle.
Siegel, C.L. *Über einige Anwendungen diophantischer Approximationen*. Abh. der Preuß Akad. der Wissenschaften. Phys.-math. K1. 1929, Nr. 1 (=Ges. Abh., **I,** 209-266).

K. Mahler: proof by geometry of numbers.

E. Bombieri– J. Vaaler *On Siegel's Lemma.* Invent. math. **73**, 11-32 (1983)

Siegel's lemma (1929)

Let a_{mn} be rational numbers, not all 0, bounded by B. The system of linear equations

$$\begin{cases} a_{11}x_1 + \cdots + a_{1N}x_N &= 0 \\ & \vdots \\ a_{M1}x_1 + \cdots + a_{MN}x_N &= 0 \end{cases}$$

where $N > M$, has a solution $x_1, \ldots, x_N$, where the x_i are rational integers, not all 0, bounded by

$$1 + (NB)^{M/(N-M)}.$$

Bombieri–Vaaler

Let

$$\sum_{n=1}^{N} a_{mn}x_n = 0 \qquad (m = 1, \ldots, M)$$

be a linear system of M linearly independent equations in $N > M$ unknowns with rational integer coefficients a_{mn}. There is a nontrivial solution in integers x_n with

$$\max_{1\le n\le N} |x_n| \le \left(D^{-1}\sqrt{|\det(A{}^tA)|}\right)^{1/(N-M)},$$

where A denotes the $M \times N$ matrix (a_{mn}), ${}^tA$ the transpose and where D is the greatest common divisor of the determinants of all $M \times M$ minors of A.

Bombieri–Vaaler

There are $N - M$ linearly independent integral solutions in integers $\underline{x}_\ell = (x_{1\ell}, \ldots, x_{N\ell})$ with

$$\prod_{\ell=1}^{N-M} \max_{1\le n\le N} |x_{n\ell}| \le \left(D^{-1}\sqrt{|\det(A{}^tA)|}\right).$$

Auxiliary functions in transcendence

Zero estimate

Interpolation determinants

Arakelov theory, slopes inequalities