11:06 a.m. December 30, 2010

On the analytic theory of quadratic forms

by C. L. Siegel (translated loosely by Bill Casselman from the preface of *Annals of Mathematics* **35**, pages 527–606)

Among the best known results of number theory belongs the result first proven by Fermat, that every prime of the form $4n+1$ and no prime of the form $4n+3$ is a sum of two squares. From this one immediately deduces that the equation $x^2+y^2=p$, with p prime, has integral solutions when the congruence $x^2+y^2 \equiv p \pmod q$ is solvable for every modulus q. Thus is raised the more general question of the solubility of an equation in integers in terms of the solubility in q-adic numbers.

If one poses the general problem of solving

$$(1) \qquad ax^2+bxy+cy^2=d$$

by considering the corresponding congruences

$$(2) \qquad ax^2+bxy+cy^2 \equiv d \pmod q,$$

the example $5x^2+11y^2=1$ shows that the second doesn't imply the first. If one avoids the question of solubility in integers but just looks for rational solutions, a well known and important theorem of Legendre asserts that the solution of (2) in every $\mathbb{Q}_q$ implies that of (1) in $\mathbb{Q}$. This theorem of Legendre was generalized by Hasse to deal with the problem of representing a quadratic form of dimension n in terms of one of dimension m. Hasse's theorem says this is possible if it is possible modulo every prime and also over $\mathbb{R}$. For $m=2$, $n=1$ comes out of this Legendre's theorem, if one observes that the solubility over $\mathbb{R}$ follows from that modulo the primes because of quadratic reciprocity. Another special case of Hasse's result, that when $m=n$, had already been asserted by Minkowski, but without a detailed proof.

In order to obtain a quantitative extension of the Legendre-Hasse theorem, that is to say to obtain information about the number of solutions and not just their existence, consider the following points. Suppose Q and Q_1 two quadratic forms with non-zero determinant. If they are equivalent—that is to say, if one is an integral transform of the other—then representations of R in terms of Q correspond exactly to transformations of Q_1 to R. The same is true when we replace integral transformations by integral q-adic transformations. But it can happen that two forms are equivalent over each $\mathbb{Z}_q$ and also over $\mathbb{R}$ without being equivalent over $\mathbb{Z}$. As examples we have $5x^2+11y^2$ and x^2+55y^2. For our purposes we must take both Q and Q_1 into account. The **genus** of Q is the set of all quadratic forms equivalent over each $\mathbb{Z}_q$ and also over $\mathbb{R}$. There are a finite number of equivalences in each genus, say with representatives Q_i.

From Legendre-Hasse it follows that if R is representable by Q everywhere locally, then it is representable by one of the Q_i. The principal result of this paper is a quantitative version of this fact. I'l formulate it here for positive definite forms. Let (Q_i, R) be the number of ways to represent R by Q_i. Let $A(Q_i, Q_i)$ be the cardinality of the integral orthogonal group of Q_i. It turns out that the ratio

$$(3) \qquad \left(\frac{A(Q_1,R)}{A(Q_1,Q_1)}+\cdots+\frac{A(Q_n,R)}{A(Q_n,Q_n)}\right) : \left(\frac{1}{A(Q_1,Q_1)}+\cdots+\frac{1}{A(Q_n,Q_n)}\right)$$

can be determined solely in terms of local information, and more particularly with the number $A_q(Q,R)$ of solutions of ${}^tX\,Q\,X = R \pmod q$. In fact the limit

$$(4) \qquad A_q(Q,R)/q^{mn-\frac{n(n+1)}{2}},$$

as q is eventually divisible by all integers, exists as long as $n < m$, and the ratio of this limit to the number in (3) is a constant κ that depends only on m. n, and the determinants $|Q|$ and $|R|$. This factor can be defined in the following way: consider the $n(n + 10/2$ independent entries in the matrix R as Cartesian coordinates in $n(n+1)/2$-space. Each region G of the space corresponds through the equation ${}^tX\,QX = R$ to a region G' of mn-space. If $v(G)$ and $v(G')$ are the volumes of these regions and one lets G approach R let

$$\lambda = \lim \frac{v(G')}{v(G)} .$$

The we set $\kappa = \lambda/2$ for $m = n + 1$, $\kappa = \lambda$ for $m > n + 1$.

The number λ is in some sense the expected value of $A(Q, R)$ ... As q passes through larger and larger powers of a pixed p the ratio

$$A_q(Q, R)/q^{mn-\frac{n(n+1)}{2}}$$

becomes a constant $\alpha_p(Q, R)$ ... The limit value of A_q may be represented as the product over primes p of limits over powers of p of solutions. Assigning $\mathbb{R}$ to a prime by convention, the principal result says that

$$(5) \quad \frac{\frac{A(Q_1,R)}{A(Q_1,Q_1)}+\cdots+\frac{A(Q_n,R)}{A(Q_n,Q_n)}}{\frac{1}{A(Q_1,Q_1)}+\cdots+\frac{1}{A(Q_n,Q_n)}} = \prod_p \alpha_p(Q, R) .$$

If $m = n + 1$ put a factor of $1/2$ on the right.

... If p does not divide $2|Q||R|$ then $\alpha_p(Q, R)$ is just

$$A_p(Q, R)/q^{mn-\frac{n(n+1)}{2}} .$$

The formula (5) holds also in the so far excluded case $m = n$, if one adds a factor of $1/2$ to the definition of α_p. if $Q = R$ one has on the left the reciprocal of the denominator and one obtains from (5) a relation that was derived earlier, although in a much more complicated and not quite correct fashion, by Minkowski. Also implicit in this is the class number formula of Dirichlet and the formula due to Eisenstein for the weight of the genus of a ternary quadratic form, if the genus contains just one class, and on obtains a formula for $A(Q, R)$ itself. This in particular holds when Q is the sum of m squares with $m \leq 8$. From the formulas (5) can be deduced those of Lagrange, Gauss, Jacobi, Eisenstein, Smith, and Minkowski. Hardy has also proven this formula for $5 \leq m \leq 8$, using the successful methods developed by him and Littlewood.