Counting the solutions of a quadratic equation.

Roger Baker

§1 Introduction.

The ‘quadratic equation’ I have in mind takes the form

$$F(\boldsymbol{x}) := F(x_1, \dots, x_n) = m.$$

Here F is a nonsingular form with integer matrix,

$$F(\boldsymbol{x}) = \sum_{i,j=1}^{n} a_{ij} x_i x_j$$

with $D = \det[a_{ij}] \neq 0$. We can assume $m \geq 0$. Write $N(F, P)$ for the number of solutions in $P\mathcal{B} = (Pa_1, Pb_1] \times \cdots \times (Pa_n, Pb_n]$ where $\mathcal{B}$ is a given box; P tends to infinity. ‘Solution’ always means ‘solution in integers’.

By 1920, the English mathematicians G. H. Hardy and J. E. Littlewood had a method (often called the *circle method*) which gives an asymptotic formula for $N(F, P)$ in the case when $n \geq 5$ and F is *diagonal*, that is

$$F = b_1 x_1^2 + \cdots + b_n x_n^2.$$

(The method applies to $b_1 x_1^k + \cdots + b_n x_n^k$, but we must allow n to become larger as k increases, e.g. $n \geq 8$ for $k = 3$.) I recommend R. C. Vaughan, *The Hardy-Littlewood method*, 2nd edn., Cambridge, and H. Davenport, *Analytic methods for Diophantine equations and Diophantine inequalities*, 2nd edn., Cambridge, to learn more about the method.

§2 An outline proof.

Under the above hypothesis I will prove in the present lecture, in outline, that, if we let $m \to \infty$ and $P = m^{1/2}$,

$$N(F, P) = \sigma_\infty(F, \mathcal{B}) \sigma_m(F) P^{n-2} + O(P^{n-2-\delta}) \tag{1}$$

for a positive constant δ. The expression $O(G)$ for a positive G means 'any number, of absolute value $\leq CG$, where C is a constant'. Now (1) is an asymptotic formula if

$$\sigma_\infty = \sigma_\infty(F, \mathcal{B}) > 0 \quad \text{and} \quad \sigma_m(F) > c_F > 0.$$

The factor σ_∞ is connected with *real* solutions of $F = m$ in $P\mathcal{B}$. We have in fact

$$\sigma_\infty = \lim_{\epsilon \to 0} \frac{1}{2\epsilon} \int_{\substack{\boldsymbol{x} \in \mathcal{B} \\ |F(\boldsymbol{x})-1| \leq \epsilon}} 1 \, dx,$$

which can be shown to be positive if $F = 1$ for a *real* $\boldsymbol{x}$ interior to $\mathcal{B}$. For instance, $\mathcal{B} = \left(0, \frac{1}{4}\right]^5$, $F = x_1^2 + \cdots + x_5^2$ would yield $\sigma_\infty = 0$; and indeed in this case $N(F, P) = 0$. We call σ_∞ the *singular integral.*

The factor $\sigma_m(F)$ (the *singular series*) takes the form

$$\sigma_m(F) = \prod_p \sigma_p = \lim_{h \to \infty} \sigma_{p_1} \dots \sigma_{p_h},$$

where $p_1 < p_2 < \cdots$ is the sequence of primes. The numbers σ_p measure the relative frequency of solutions of the congruence

$$F(\boldsymbol{x}) \equiv m \pmod{p^k}.$$

To be precise, let $N(p^k)$ be the number of solutions of this congruence $\pmod{p^k}$, then

$$\sigma_p = \lim_{k \to \infty} p^{-(n-1)k} N(p^k).$$

For example, if $F(\boldsymbol{x}) = 3(x_1^2 + \cdots + x_5^2)$ and $m \not\equiv 0 \pmod 3$, then $N(3^k) = 0$, $\sigma_3 = 0$, $\sigma_m(F) = 0$. But this reflects the obvious fact that 'for congruence reasons', $N(F, P) = 0$.

It can be shown that, in our case $n \geq 5$, if each $N(p^\nu)$ is positive, then

$$\sigma_m(F) > c_F > 0$$

and we get our desired asymptotic formula if $\mathcal{B}$ is suitably 'large'. For simplicity, I take $\mathcal{B} = (0, b]^n$ below.

In the next lecture we will see how analytic number theorists have progressed in handling the harder cases $n = 4$ and $n = 3$. Much has happened (in particular) since the 1980s. While the Hardy-Littlewood method almost becomes unrecognizable, we do still see singular integrals and singular series appear.

Let us write $e(\theta)$ as an abbreviation for $e^{2\pi i\theta}$. The start of the process of proving (1) is the simple observation that

$$\int_0^1 e(k\alpha)d\alpha = \begin{cases} 0 & \text{if } k \in \mathbb{Z},\ k \neq 0 \\ 1 & \text{if } k = 0. \end{cases}$$

I leave this as an exercise; you have probably seen it in a discussion of Fourier series. Now write $S(\alpha)$ for the *Weyl sum*

$$S(\alpha) = \sum_{0<x<bP} e(\alpha x^2)$$

(the variable x is an integer). Now

$$\begin{aligned} (2) \qquad & \int_0^1 S(c_1\alpha)\dots S(c_n\alpha)e(-m\alpha)d\alpha \\ &= \sum_{x_1\in(0,bP]} \cdots \sum_{x_n\in(0,bP]} \int_0^1 e(\alpha(c_1x_1^2+\cdots+c_nx_n^2-m))d\alpha \\ &= N(F,P), \end{aligned}$$

by the observation just made.

It is convenient to write $Q = P^\nu$ where ν is a small positive constant, say $\nu = 1/100$, and replace the interval $[0,1]$ in (2) by

$$I = [P^{\nu-2}, 1+P^{\nu-2}].$$

This does not change the integral in (2) because the integrand has period 1.

When $1 \le a \le q \le Q$ and the gcd (a,q) is 1, let

$$\mathcal{M}(q,a) = \left\{\alpha : \left|\alpha - \frac{a}{q}\right| \le P^{\nu-2}\right\}.$$

The $\mathcal{M}(q,a)$ (*major arcs*) are intervals whose rational centers have relatively small denominator; it's easy to see that they don't overlap, for large P. Let $\mathcal{M}$ denote their union. Although it has very small measure, $\mathcal{M}$ contributes the 'lion's share' in (2): I will show that

$$(3) \qquad \int_{\mathcal{M}} S(c_1\alpha)\dots S(c_n\alpha)\, e(-m\alpha)d\alpha = c_\infty(F,\mathcal{B})c_m(F)P^{n-2} + O(P^{n-2-\delta}).$$

The complement $\mathfrak{m} = I\backslash\mathcal{M}$ (the *minor arcs*) contributes only a small amount:

$$\int_{\mathfrak{m}} S(c_1\alpha)\dots S(c_n\alpha)\, e(-m\alpha)d\alpha = O(P^{n-2-\delta}). \tag{4}$$

Combining (3), (4) gives the desired result.

The key to proving (3) is to give a good approximation to $S(c_j\alpha)$ in terms of better understood quantities. These are

$$v_j(\beta) = \frac{1}{2}\sum_{x=1}^{(c_jP)^2} x^{-1/2}e(\beta x)$$

and

$$S(q,a) = \sum_{x=1}^{q} e\left(\frac{ax^2}{q}\right).$$

Lemma *Let $1 \le a \le q \le Q$, $(a,q) = 1$, $\alpha \in \mathcal{M}(q,a)$. Then*

$$S(c_j\alpha) = q^{-1}S(q,c_ja)v_j\left(c_j\left(\alpha - \frac{a}{q}\right)\right) + O(Q^2).$$

The error $O(Q^2)$ is 'acceptable' in the sense that in any integrals where it appears, we can bound the value of the integral by $O(P^{n-2-\delta})$.

I won't prove the lemma. If we write $\alpha = \frac{a}{q} + \beta$, it depends on the fact that the simpler sum $\sum\limits_{x\le Y} e\left(\frac{c_jax^2}{q}\right)$ can be written

$$\begin{aligned}\sum_{x\le Y} e\left(\frac{c_jax^2}{q}\right) &= \sum_{r=1}^{q} e\left(\frac{c_jar^2}{q}\right) \sum_{\substack{x\le Y\\ x\equiv r \pmod q}} 1\\ &= Yq^{-1}S(q,c_ja) + O(q).\end{aligned}$$

That is, we distribute our summation into congruence classes.

The lemma leads to an acceptable approximation to $S(c_1\alpha)\dots S(c_n\alpha)$ of the form

$$q^{-n}S(q,c_1a)\dots S(q,c_na)V\left(\alpha - \frac{q}{a}\right)$$

where

$$V(\beta) = v_1(c_1\beta)\dots v_n(c_n\beta).$$

So we approximate to the integral in (3) by

$$\sum_{q\le Q}\ \sum_{\substack{a=1\\(a,q)=1}}^{q} q^{-n}\int_{\mathcal{M}(q,a)} S(q,c_1a)\dots S(q,c_na)e\left(-\frac{am}{q}\right)$$
$$V\left(\alpha-\frac{a}{q}\right)e\left(-\left(\alpha-\frac{a}{q}\right)m\right)d\alpha.$$

This factorizes as $\mathfrak{S}(m,P)J(m,P)$, where

$$\mathfrak{S}(m,P) = \sum_{q\le Q} q^{-n}\sum_{\substack{a=1\\(a,q)=1}}^{q} S(q,c_1a)\dots S(q,c_na)\,e\left(-\frac{ma}{q}\right) \tag{5}$$

and

$$J(m,P) = \int_{-P^{\nu-k}}^{P^{\nu-k}} V(\beta)e(-m\beta)d\beta.$$

Moreover, the series and the integral can be 'completed' with an acceptable error, so that $\mathfrak{S}(m,P)$ is approximated by

$$\sigma_\infty(F,m) = \sum_{q=1}^{\infty} q^{-n}\sum_{\substack{a=1\\(a,q)=1}}^{q} S(q,c_1a)\dots S(q,c_na)e\left(-\frac{ma}{q}\right) \tag{6}$$

and $J(m,P)$ is approximated by

$$J(m) = \int_{-\frac12}^{\frac12} v_1(c_1\beta)\dots v_n(c_n\beta)e(-m\beta)d\beta.$$

This integral in turn is acceptably close to $\sigma_\infty(F,\mathcal{B})P^{n-2}$. I have skipped over the interesting analysis that converts the infinite series in (6) to the infinite product $\prod_p \sigma_p$. This concludes our sketch of (3).

As for the minor arcs, one can show that each $S(c_j\alpha)$ is relatively small on $\mathfrak{m}$ compared with the obvious estimate

$$|S(c_j\alpha)| \le \sum_{x\in(0,bP]} 1 = O(P),$$

namely

$$S(c_j\alpha) = O(P^{1+\epsilon-\nu/2}) \quad (\alpha \in m) \tag{7}$$

for any $\epsilon > 0$. This estimate, depending on a so-called 'differencing' invented by H. Weyl in 1916, was the beginning of the theory of exponential sums, which plays a useful role in present-day analytic number theory. Now

$$\begin{aligned}
&\left| \int_{\mathcal{M}} S(c_1\alpha)\dots S(c_n\alpha)e(-m\alpha)d\alpha \right| \\
&\qquad \le \max_{\substack{\alpha\in m\\ 5\le j\le n}} |S(c_j\alpha)|^{n-4} \int_{\mathcal{M}} |S(c_1\alpha)\dots S(c_4\alpha)|d\alpha \\
&\qquad \le C_1 P^{(n-4)(1+\epsilon-\nu/2)} \int_0^1 |S(c_1\alpha)\dots S(c_4\alpha)|d\alpha \\
&\qquad \le C_2 P^{(n-4)(1+\epsilon-\nu/2)} \int_0^1 |S(\alpha)|^4 d\alpha.
\end{aligned} \tag{8}$$

Here C_1, C_2 are independent of P. The last step is a technical trick which I leave as an exercise.

By our original observation on integrals $\int_0^1 e(k\alpha)d\alpha$, the integral $\int_0^1 |S(\alpha)|^4 d\alpha$ is the number of solutions of

$$x_1^2 + x_2^2 - x_3^2 - x_4^2 = 0\ , \quad 1 \le x_j \le bP,$$

and it is fairly routine to show that this number of solutions is $O(P^{2+\epsilon})$. Thus the integral in (8) is

$$O(P^{n-2-\frac{\nu}{2}+n\epsilon})$$

giving our desired outcome with, say, $\delta = \nu/3$. This concludes our abbreviated tour of the proof of (1).

§3 Kloosterman's paper and Kloosterman sums.

In 1926 H. D. Kloosterman gave an asymptotic formula for $N(f,m)$ as $m \to \infty$. Here $N(F,m)$ is the total number of solutions of $f(\boldsymbol{x}) = m$, and F is diagonal and positive definite with only 4 variables. Now apart from an error of size $O\left(m^{\frac{1}{2}+\epsilon}\right)$ arising from solutions with some $x_j = 0$, $N(F,m)$ is given by $16N(F,P)$ where $P = m^{1/2}$, $\mathcal{B} = (0,1]^4$. For a solution of

$$c_1x_1^2 + \cdots + c_4x_4^2 = m\ ,\ 1 \le x_j \le P$$

gives rise to 16 solutions with arbitrary signs. Once we reduce the problem to studying $N(F,P)$, the signs of the c_j do not make much difference, but it is crucial that $m \neq 0$ or the method fails. The best exposition is T. Estermann, *A new application of the Hardy-Littlewood-Kloosterman method*, Proc. London Math. Soc. **12** (1962), 425–444.

The most striking aspect of Kloosterman's paper is the estimation and application of a new exponential sum, the *Kloosterman sum*

$$S(h,k,q) = \sum_{\substack{a=1 \\ (a,q)=1}}^{q} e\left(\frac{ha + k\bar{a}}{q}\right). \tag{9}$$

Here $\bar{a}$ is the inverse of $a \pmod q$, that is, $a\bar{a} \equiv 1 \pmod q$. It is a challenge to get an estimate

$$S(h,k,q) = O(q^{\theta})$$

for gcd $(q,h) = 1$, with $\theta < 1$. Kloosterman managed to get $\theta = 7/8$, and this sufficed for his paper. Others improved this, but the most remarkable step forward came when André Weil in the 1940s used deep methods of algebraic geometry to prove

$$|S(h,k,p)| \le 2\sqrt{p} \quad (p \nmid hk). \tag{10}$$

From (10), methods already available yielded

$$|S(h,k,q)| \le Cq^{1/2+\epsilon}(h,q) \tag{11}$$

where C depends only on ϵ. Incidentally there is now a rather elementary proof of (10). See W. M. Schmidt, *Equations Over Finite Fields, an Elementary Approach*, 2nd edn., Kendrick Press. There are nowadays many applications of Kloosterman sums in analytic number theory.

I now indicate Kloosterman's version of the circle method. Let $N = \left[m^{\frac{1}{2}+\epsilon}\right]$, where [ ] denotes integer part. It can be shown that $I = \left(\frac{1}{N+1}, 1 + \frac{1}{N+1}\right]$ is the disjoint union of the *Farey arcs*

$$I(q,a) = \left(\frac{a}{q} - \frac{1}{qq_0}, \frac{a}{q} + \frac{1}{qq_1}\right]$$

with $1 \leq a \leq q \leq N$, $(a,q)=1$, and

$$N < q_j \leq N+q, \;\; aq_0 \equiv 1 \pmod{q}, \;\; aq_1 \equiv -1 \pmod{q}.$$

Hence

$$N(F,P) = \sum_{q=1}^{N} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \int_{I(q,a)} S(c_1\alpha)\ldots S(c_4\alpha)e(-m\alpha)d\alpha$$

in the notation of Section 2. Writing

$$A_1(q,a) = \int_{I(q,a)} S(c_1\alpha)\ldots S(c_4\alpha)e(-m\alpha)d\alpha,$$

$$A_2(q) = \sum_{\substack{a=1 \\ (a,q)=1}}^{q} A_1(q,a),$$

we have

$$N(F,P) = \sum_{q=1}^{N} A_2(q).$$

What Estermann does is write $A_2(q)$ as a main term plus an acceptable error. From there, the analysis is similar to that following the factorization of our approximation to

$$\int_{\mathcal{M}} S(c_1\alpha)\ldots S(c_4\alpha)e(-m\alpha)d\alpha,$$

in Section 2. The minor arcs have 'vanished'. The key to the approximation to $A_2(q)$ is the 'cancellation among the a's' in estimating the error term; and this comes from (11).

Let $g(q,a,\beta)$ be the indicator function of $I(q,a) - a/q$,

$$g(q,a,\beta) = \begin{cases} 1 & \text{if } \frac{a}{q} + \beta \in I(q,a) \\ 0 & \text{otherwise.} \end{cases}$$

Clearly

$$A_2(q) = \int_{-q^{-1}m^{-1/2-\epsilon}}^{q^{-1}m^{-1/2-\epsilon}} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \prod_{j=1}^{4} S(c_j\alpha)e\left(-\frac{ma}{q}\right) e(-m\beta)g(q,a,\beta)d\beta.$$

Our approximation to the integrand takes the form

$$W(\beta)\sum_{\substack{a\le q\\(a,q)=1}}\prod_{j=1}^{4}S(q,c_ja)\ e\left(-\frac{ma}{q}\right)g(q,a,\beta)$$

for a function $W(\beta)$ similar to $V(\beta)\ e(-m\beta)$ in §2. If we now expand $g(q,\alpha,\beta)$ in a *finite Fourier series*,

$$g(q,a,\beta)=\sum_{h=1}^{q}c_he\left(\frac{h\bar{a}}{q}\right)\ ,\ c_h=c_h(\beta,q),$$

we are interested in approximating the sum

$$\sum_{h=1}^{q}c_h\sum_{\substack{a\le q\\(a,q)=1}}\prod_{j=1}^{4}S(q,c_ja)e\left(-\frac{ma+h\bar{a}}{q}\right).$$

This should be enough to convince you of the relevance of Kloosterman's sum, and tempt you to read Estermann's paper.

§4 Heath-Brown's version of the circle method.

D. R. Heath-Brown gave a powerful method for our problem in his *A new form of the circle method, and its application to quadratic forms* (J. reine angewandte Math. **481** (1996), 149–206). His method gives asymptotic formulae for

$$N(F,w)=\sum_{F(\boldsymbol{x})=m}w\left(\frac{\boldsymbol{x}}{P}\right)$$

(where either $P\to\infty$ if $m=0$, or $m\to\infty$ and $P=m^{1/2}$). The function w is smooth and has compact support E, $\mathbf{0}\notin E$, but otherwise w is at our disposal. The summation is over $\mathbb{Z}^n$, the integer points of $\mathbb{R}^n$, so it actually counts solutions of $F(\boldsymbol{x})=m$ in PE with weights attached. By taking w_1, w_2 above and below the indicator function of a box $\mathcal{B}$, $\mathbf{0}\notin\bar{\mathcal{B}}$, we recover an asymptotic formula for $N(F,P)$ with a rather weak error term estimate.

The previously inaccessible cases Heath-Brown covers are *homogeneous* equations, that is $m=0$, with $n=4$ (where we recall Kloosterman's approach fails) and even $n=3$. It is also worth emphasizing that restriction to diagonal F has disappeared.

The main terms for $m = 0$ are interesting. For $n = 4$ and D, the determinant of F, *not* a square we get

$$N(F, w) = \sigma_\infty(w) L(1, \chi) \sigma^*(F) P^2 + O(P^{3/2+\epsilon})$$

for every $\epsilon > 0$. Here $\sigma_\infty(w)$ is a constant analogous to the singular integral in Section 2, χ is the Jacobi symbol

$$\chi(k) = \left(\frac{D}{k}\right)$$

and $L(s, \chi)$ is the continuation of $\sum\limits_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ to the complex plane that first arose in studying primes in arithmetic progression. Dirichlet proved around 1840 that $L(1, \chi) > 0$.

Next,

$$\sigma^*(F) = \prod_p \left(1 - \frac{\chi(p)}{p}\right) \sigma_p,$$

where the σ_p are as in Section 1. For D a *square*, however, we get a different looking main term: if $n = 4$,

$$N(F, w) = \sigma_\infty(w) \sigma_*(F) P^2 \log P + O(P^2),$$

and rather similarly, for $n = 3$,

$$N(F, w) = \frac{1}{2} \sigma_\infty(w) \sigma_*(F) P \log P + O(P).$$

In both cases,

$$\sigma_*(F) = \prod_p \left(1 - \frac{1}{p}\right) \sigma_p.$$

It is unusual in the circle method to get a main term that is not merely a power of p.

The point of departure for these formulae is a new expression for δ_n,

$$\delta_n = \begin{cases} 1 & n = 0 \\ 0 & n \neq 0. \end{cases}$$

For $P > 1$, there is a positive constant c_P and an infinitely differentiable function $h(x, y)$ defined on $(0, \infty) \times \mathbb{R}$, such that

$$\delta_n = c_P P^{-2} \sum_{q=1}^{\infty} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} e\left(\frac{an}{q}\right) h\left(\frac{q}{P}, \frac{n}{P^2}\right).$$

The constant c_P is very close to 1: for any positive constant N,

$$c_P - 1 = O(P^{-N}).$$

Also, $h(x, y) = O(x^{-1})$ for all y, and $h(x, y) \neq 0$ implies $x \leq \max(1, 2|y|)$.

I am sorry I have no time to prove this. I admit it looks ugly compared with $\delta_n = \int_0^1 e(n\alpha)d\alpha$, but in analytic number theory we reckon a powerful tool is a beautiful tool. The variables a, q play the same role as in creating intervals around a/q in Sections 2, 3, but one must study the paper before this comparison emerges.

The next step involves the *Poisson summation formula*. Let f be any smooth function on $\mathbb{R}^n$ that drops off fairly rapidly at infinity, and write

$$\hat{f}(\boldsymbol{y}) = \int_{\mathbb{R}^n} f(\boldsymbol{x}) e(-\boldsymbol{x} \cdot \boldsymbol{y}) d\boldsymbol{y}$$

where $\int_{\mathbb{R}^n} d\boldsymbol{x}$ denotes integration with respect to Lebesgue measure on $\mathbb{R}^n$, and $\boldsymbol{x} \cdot \boldsymbol{y}$ is the inner product. We have

$$\sum_{\boldsymbol{k} \in \mathbb{Z}^n} f(\boldsymbol{k}) = \sum_{\boldsymbol{c} \in \mathbb{Z}^n} \hat{f}(\boldsymbol{c}).$$

This is an easy deduction from the L^2-theory of Fourier series on $\mathbb{R}^n/\mathbb{Z}^n$.

Let us write $G(\boldsymbol{x}) = F(\boldsymbol{x}) - m$. Then

$$N(F, w) = \sum_{\boldsymbol{x} \in \mathbb{Z}^n} w\left(\frac{\boldsymbol{x}}{P}\right) \delta_{G(\boldsymbol{x})}. \tag{12}$$

Rather as in Section 2, we split the values of $\boldsymbol{x}$ into their respective residue classes $\boldsymbol{b} \pmod q$. Leaving alone summation over $a = 1, \ldots, q$, $(a, q) = 1$, for the moment,

$$\sum_{\boldsymbol{x}} w\left(\frac{\boldsymbol{x}}{P}\right) e\left(\frac{aF(\boldsymbol{x})}{q}\right) h(P^{-1}q, P^{-2}G(\boldsymbol{x}))$$

$$= \sum_{\boldsymbol{b} \pmod q} e\left(\frac{aF(\boldsymbol{b})}{q}\right) \sum_{\boldsymbol{k}} f(\boldsymbol{k})$$

where, suppressing dependence of f on other variables,

$$f(\boldsymbol{y}) = w\left(\frac{\boldsymbol{b}+q\boldsymbol{y}}{P}\right)\, h(P^{-1}q, P^{-2}G(\boldsymbol{b}+q\boldsymbol{y})).$$

It is an easy exercise to show that

$$\hat{f}(\boldsymbol{c}) = q^{-n}e\left(\frac{\boldsymbol{b}\cdot\boldsymbol{c}}{q}\right) I_q(\boldsymbol{c}),$$

where

$$I_q(\boldsymbol{c}) = \int_{\mathbb{R}^n} w\left(\frac{\boldsymbol{x}}{P}\right)\, h\left(\frac{q}{P}, \frac{G(\boldsymbol{x})}{P}\right)\, e\left(-\frac{\boldsymbol{c}\cdot\boldsymbol{x}}{q}\right) d\boldsymbol{x}.$$

Hence an application of Poisson's formula leads to the following:

$$N(F,w) = c_P P^{-2}\sum_{\boldsymbol{c}\in\mathbb{Z}^n}\sum_{q=1}^{\infty} q^{-n}S_q(\boldsymbol{c})I_q(\boldsymbol{c}) \tag{13}$$

with

$$S_q(\boldsymbol{c}) = \sum_{\substack{a=1\\(a,q)=1}}^{q}\ \sum_{\boldsymbol{b}\pmod q} e\left(\frac{aF(\boldsymbol{b})+\boldsymbol{c}\cdot\boldsymbol{b}}{q}\right).$$

I leave the details as an exercise.

The $S_q(\boldsymbol{c})$ can also be found in Estermann's paper. The 'cancellation over a' is already built into $S_q(\boldsymbol{c})$ and hence into our formula (13). (Kloosterman sums appear in evaluating or estimating $S_q(\boldsymbol{c})$.)

Heath-Brown now has the lengthy task of showing that

$$c_P P^{-2}\sum_{q=1}^{\infty} q^{-n}S_q(\boldsymbol{0})I_q(\boldsymbol{0})$$

contributes the main term in the asymptotic formula, plus a remainder of smaller order, and that

$$c_P P^{-2}\sum_{\boldsymbol{c}\neq\boldsymbol{0}}\sum_{q=1}^{\infty} q^{-n}S_q(\boldsymbol{c})I_q(\boldsymbol{c})$$

is small compared with the main term. (Here I am assuming $\sigma_\infty(w)$ and all σ_p are positive, which implies $\sigma^*(F)$ or $\sigma_*(F)$ is positive.) In the hardest cases, $m = 0$, $n = 4$, D a square and $m = 0$, $n = 3$, it is crucial to use cancellation with respect to q in bounding the series $\sum\limits_{q=1}^{\infty} q^{-1}S_q(\boldsymbol{c})I_q(\boldsymbol{c})$. It is this '$q$ cancellation' that gives the method extra power compared with Kloosterman's approach.

In studying $I_q(\boldsymbol{c})$, Heath-Brown is building on work of van der Corput from the 1920s on integrals of simpler form,

$$\int_a^b g(x)e(f(x))dx,$$

where g and f are differentiable real functions. A simple case is $f(x) = \theta x$, $f'(x) = \theta > 0$, $g(x) = 1$:

$$\int_a^b e(\theta x) = \left[\frac{e(\theta x)}{2\pi i\theta}\right]_a^b,$$

$$\left|\int_a^b e(\theta x)dx\right| \leq \frac{1}{\pi\theta}.$$

Van der Corput got nearly the same bound assuming only that $g(x)/f'(x)$ is monotonic and $f'(x)/g(x) \geq m > 0$, namely

$$\left|\int_a^b g(x)e(f(x))dx\right| \leq \frac{4}{m}. \tag{14}$$

See Chapter 4 of E. C. Titchmarsh, *The Theory of the Riemann Zeta Function*, 2nd edn., Oxford. The idea behind (14) is the starting point in giving bounds for $I_q(\boldsymbol{c})$.

§5 Conclusion.

Some of the most exciting work in this area began in 1987 with the publication of a paper by H. Iwaniec, *Fourier coefficients of modular forms of half-integral weight*, Inventiones Math. **87**, 385–401. As W. Duke showed, Iwaniec had provided the key tool for the description of $N(Q, m)$ for a positive definite quadratic form Q in 3 variables (a *ternary* form), albeit with some restriction on the multiplicative structure of m. As the title of Iwaniec's paper suggests, one cannot study this without a background in modular forms, for which I suggest H. Iwaniec, *Topics in Classical Automorphic Forms*, American Math. Soc. After that, it might be useful to begin with V. Blomer, *Uniform bounds for Fourier coefficients of theta-series with arithmetic applications*, Acta Arithmetica **114** (2004), 1–21, for orientation. I can only say that Iwaniec's work leads to progress because he gives bounds for weighted sums of Kloosterman sums that are stronger than Weil's bound, i.e. there is cancellation between the Kloosterman sums.

The background to the application to $N(Q,m)$ is that a formula of Siegel gives a link between $N(Q,m)$ and representation of the integer m by forms in gen Q. The set of forms gen Q consists of positive definite forms that can be transformed into Q, and vice versa, by a linear change of variable over the ring of p-adic integers. We take one form Q' from each of the finitely many equivalence classes of forms in the genus (where equivalence refers to transformation over $\mathbb{Z}$) and define

$$r(m,\,\mathrm{gen}\,Q) = \sum_{Q' \in \,\mathrm{gen}\,Q} W(Q')N(Q',m)$$

for certain positive weights $W(Q')$ that I won't define here, $\sum\limits_{Q' \in \,\mathrm{gen}\,Q} W(Q') = 1$. So this is an *average* of $N(Q',m)$ over forms in gen Q. Siegel's formula can be written, for a suitable singular integral σ_∞,

$$r(m,\,\mathrm{gen}\,Q) = \sigma_\infty m^{1/2} L(1,\chi^*) \prod_p \left(1 - \frac{\chi_m(p)}{p}\right) \sigma_p$$

where $\chi_m^*(k) = \left(-\frac{Dm}{k}\right)$. So this is a 'perfect' asymptotic formula for an average over the genus of $N(Q',m)$. As long as we restrict m a little (the multiplicative part of m, left after removing the largest squarefree factor, should be coprime to a certain integer $K = K(Q)$), we can describe the difference

$$N(Q,m) - r(m,\,\mathrm{gen}\,Q)$$

in terms of the Fourier coefficients of a modular form, and using Iwaniec's idea, we can show this is $O\left(m^{\frac{1}{2}-\delta}\right)$ for a positive. We an also prove that if $\sigma_p > 0$ for each p, then

$$\prod_p \left(1 - \frac{\chi_m(p)}{p}\right) \sigma_p > m^{-\epsilon}.$$

So we actually do extract an asymptotic formula for $N(Q,m)$. The deepest mathematics I have described in these lectures lies in this section.