May 03, 2021

Dirichlet's class number formula.

→ Dirichlet's class number formula, in its simplest and most striking form, was conjectured by Jacobi in 1832 and proved in full by Dirichlet in 1839.

→ Peter Gustav Lejeune Dirichlet (Düren, Germany 1805 – Gotinga (Göttingen) 1859).

→ Carl Gustav Jacob Jacobi (Postdam, Germany – 1851, Berlin).

There are two stages in Dirichlet's work:

→ In the first stage, the class number of quadratic forms of given (fundamental) discriminant d is related to the value of $L(1, \chi)$, where χ is the real primitive character $(d|n)$ (Kronecker).

→ In the second stage, the value of $L(1,\chi)$ is expressed in terms of a finite sum.

We shall give the substance of Dirichlet's work.

Notation: We shall use the notation

$$ax^2 + bxy + cy^2 \qquad (a,b,c \in \mathbb{Z})$$

for a binary quadratic form.

(Dirichlet's notation: $ax^2 + 2bxy + cy^2$)

→ Discriminant: The discriminant d of $f(x,y) = ax^2 + bxy + cy^2$ is given by $d = b^2 - 4ac$.

→ d is an integer, not a square, which is congruent to 0 or $1 \pmod 4$.

→ a fundamental discriminant is one which has the property that all forms of that discriminant have $(a,b,c) = 1$.

The forms of given (fundamental) discriminat d fall into classes of mutually equivalent forms under linear substitutions of the type

$$(1) \qquad x = \alpha x' + \beta y', \qquad y = \gamma x' + \delta y'$$

with integral coefficients $\alpha, \beta, \gamma, \delta$ satisfying $\alpha\delta - \beta\gamma = 1$.

→ We call these unimodular substitutions.

That is, two forms f ang g are equivalent $f \sim g$ if $\exists \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbb{Z})$ such that $f(\alpha x' + \beta y', \gamma x' + \delta y') = g(x', y')$.

For instance: $f(x,y) = x^2 + 4xy + 2y^2$ is equivalent to $g(x',y') = -x'^2 + 4x'y' - 2y'^2$.

Take $\alpha = -3$, $\beta = 2$, $\gamma = 1$, $\delta = -1$: $\begin{pmatrix} -3 & 2 \\ 1 & -1 \end{pmatrix}$

$$f(-3x' + 2y', x' - y') = (-3x' + 2y')^2 + 4(-3x' + 2y')(x' - y') + 2(x' - y')^2 = g(x', y').$$

→ $\sim$ is an equivalence relation.

→ Lagrange: Every class contains at least one form whose coefficients satisfy the inequality

$$|b| \leq |a| \leq |c|. \quad (*)$$

Theorem: The number of classes, for a given discriminant d, is finite.

Proof: 1) For $d > 0$ it follows from $(*)$ that

$$|ac| \geq b^2 = d + 4ac > 4ac.$$

Hence we have,

$$ac < 0$$

$$4a^2 \leq 4|ac| = -4ac = d - b^2 \leq d,$$

$$|a| \leq \frac{\sqrt{d}}{2},$$

$$|b| \leq |a| \leq \frac{\sqrt{d}}{2}.$$

a and b thus have only a finite set of possible values, and therefore so does c.

2) For $d < 0$ it follows from $(*)$, since $a > 0$ and $c > 0$, that $|b| \leq a \leq c$, $4a^2 \leq 4ac = -d + b^2 \leq |d| + a^2$, $\Rightarrow |b| \leq a \leq \sqrt{\frac{|d|}{3}}$ so that c, too, has only a finite number of possible values. $\blacksquare$

* If $d<0$, the forms of discriminant d are definite. Half of them are positive definite and half are negative definite. The latter being obtained from the former by replacing a, b, c by $-a, -b, -c$.
It is sufficient to consider the positive definite forms, which is equivalent to saying that we restrict ourselves to forms with $a>0$.

* If $d>0$, each of the forms of discriminant d is indefinite. It is therefore equivalent to some form with $a>0$.

→ We can select a representative from each class of equivalenct forms with $a>0$.

→ We denote the number of classes of forms (positive definite if $d<0$) by $h(d)$.

There is always at least one form of discriminant d, namely, the principal form

$$(2) \quad \begin{cases} x^2-\frac{1}{4}dy^2 & \text{if } d\equiv 0 \pmod 4, \\ x^2+xy-\frac{1}{4}(d-1)y^2 & \text{if } d\equiv 1 \pmod 4. \end{cases}$$

Hence $h(d)$ is a positive integer.

→ An automorph is the unimodular substitution that transform a form into itself.

→ There are always two trivial automorphs, namely, the identity $x = x'$, $y = y'$ and the negative identity $x = -x'$, $y = -y'$.

* If $d < 0$, there are in general no others, but there are two exceptions to this: when $d = -3$ or $d = -4$. In both cases there is only one class of forms, representared by the principal form.

- If $d = -3$, the principal form is $x^2 + xy + y^2$, and this has the additional automorphs

$$x = -y', \quad y = x' + y', \quad \text{and} \quad x = x' + y', \quad y = -x'$$

and their negatives

$$x = y', \quad y = -x' - y' \quad \text{and} \quad x = -x' - y', \quad y = x'$$

- If $d = -4$, the principal form is $x^2 + y^2$, and this has the additional automorph,

$$x = y', \quad y = -x'$$

and its negative $x = -y'$, $y = x'$.

We denote by w the number of automorphs, so that

$$w = \begin{cases} 2 & \text{if } d < -4. \\ 4 & \text{if } d = -4 \\ 6 & \text{if } d = -3. \end{cases}$$

The position is quite different when $d>0$. Each form has infinitely many actomorphs, and these are determined by the solutions of Pell's equation

(4) $$t^2 - du^2 = 4.$$

For the form with coefficients a, b, c, the automorphs are given by

(5) $$\begin{cases} \alpha = \frac{1}{2}(t - bu) & \beta = -cu \\ \gamma = au & \delta = \frac{1}{2}(t + bu) \end{cases}$$

The trivial actomorphs corresponds to the trivial solutions $t = \pm 2$, $u=0$ of Pell's equation.

The equation (4) has infinitely many solutions, and if t_0, u_0 is that solution with $t_0>0$, $u_0>0$ for which u_0 is least, then all solutions are given by

(6) $$\frac{1}{2}(t + u\sqrt{d}) = \pm\left[\frac{1}{2}(t_0 + u_0\sqrt{d})\right]^n.$$

where n is an integer (positive or negative)

That (5) actually does give an actomorph is easily verified by factorizing the form $ax^2+bxy+cy^2$.
We have

(7) $$ax^2 + bxy + cy^2 = a(x-\theta y)(x-\theta' y)$$

where

(8) $$\theta = \frac{-b+\sqrt{d}}{2a}, \quad \theta' = \frac{-b-\sqrt{d}}{2a}$$

and the effect of the unimodular substitution with the coefficients (5) is expressed by

(9) $$\begin{cases} x-\theta y = \frac{1}{2}(t-u\sqrt{d})(x'-\theta y') \\ x-\theta' y = \frac{1}{2}(t+u\sqrt{d})(x'-\theta' y'). \end{cases}$$

We now turn to the question of the total number of representations of a positive integer n by a representative set of forms of given (fundamental) discriminant d.

* If $d<0$, so that the forms are positive definite, the number of representations of n by any form is finite.

We denote by $R(n)$ the total number of representations by the various forms of a representative set.

* If $d>0$ there are infinitely many representations, since any one representation gives rise to an infinity of others by the application of the automorphs of the form

We shall select one representation from each such set, and call it primary.

→ The number of primary representation is finite.

If x, y and X, Y are two representations of the same integer that are related by an automorph, then by (9) we have

$$\frac{x-\theta' y}{x-\theta y} = \frac{\frac{1}{2}(t+u\sqrt{d})}{\frac{1}{2}(t-u\sqrt{d})} \cdot \frac{X-\theta' Y}{X-\theta' Y}$$

let $\varepsilon = \frac{1}{2}(t_0+u_0\sqrt{d})>1$. Then, by (6),

$$\frac{1}{2}(t+u\sqrt{d}) = \pm\varepsilon^{m}, \quad \frac{1}{2}(t-u\sqrt{d}) = \pm\varepsilon^{-m},$$

for some integer m. There is just one choice of m (for given X and Y) which will ensure that

(10) $$1 \le \frac{X-\theta' Y}{X-\theta y} \le \varepsilon^{2},$$

then by choice of the ambigous sign we can futher ensure that

(11) $$X-\theta y > 0$$

A representation that satisfies these two conditions ((10) - (11)). will be called primary.

→ The number of primary representations of a given integer n by a given form is finite, since the product of the linear forms $X-\theta y$ and $x-\theta' y$ is n/a by (7), and their quotient is bomded both ways by (10).

* For $d>0$ we denote by $R(n)$ the number of primary representations of n by a representative set of forms of discriminant d.

(12) If $n>0$ and $(d,n)=1$ then

$$R(n) = w \sum_{m|n} \left(\frac{d}{m}\right),$$

Where w is given by (3) if $d<0$ and $w=1$ if $d>0$.

Here $\left(\frac{d}{m}\right)$ is the Kronecker's symbol:

Let $m>0$. Then $\left(\frac{d}{m}\right)$ is always given a meaning by means of the following:

$$\left(\frac{d}{p}\right)=0 \text{ if } p|d,$$

$$\left(\frac{d}{2}\right) = \begin{cases} 1 & \text{if } d\equiv 1 \pmod 8 \\ -1 & \text{if } d \equiv 5 \pmod 8 \end{cases}$$

$$\left(\frac{d}{p}\right) = \text{Legendre's symbol if } p>2 \text{ and } p\nmid d.$$

$$\left(\frac{d}{m}\right) = \prod_{r=1}^{v} \left(\frac{d}{p_r}\right) \text{ for } m = \prod_{r=1}^{v} p_r \quad (\text{i.e., } 1 \text{ for } m=1).$$

→ $\left(\frac{d}{m}\right)=0$ if $(d,m)>1$.

→ If $(d,m)=1 \Rightarrow \left(\frac{d}{m}\right)=\pm 1$.

(12) is proved by expressing $R(n)$ in terms of the number of solutions of the congruence $z^2 \equiv d \pmod{4n}$, and then evaluating this number in terms of quadratic character symbols.

→ The basic idea in the first stage of Dirichlet's work is to determine, from the expression (12) for $R(n)$, the averge value of $R(n)$ as n varies.

(The sum in (12) runs over all the square-free positive divisors m of n).

We have a theorem.

Theorem.

If for $N>1$, we set

$$H(N) = \sum_{\substack{1 \le n \le N \\ (n,d)=1}} R(n),$$

(the number of primory representations, by forms belonging to the representative system, of all of the natural numbers up to N that are relatively prime to d), then

$$\lim_{N \to \infty} \frac{H(N)}{N}$$

exists, and we have

$$\lim_{N \to \infty} \frac{H(N)}{N} = w \, \frac{\phi(|d|)}{|d|} \sum_{m=1}^{\infty} \left(\frac{d}{m}\right) \frac{1}{m}.$$

Proof.

$$\frac{H(N)}{w} = \sum_{\substack{1 \le n \le N \\ (n,d)=1}} \sum_{m \mid n} \left(\frac{d}{m}\right) = \sum_{1 \le n \le N} \sum_{m \mid n} \left(\frac{d}{m}\right)\left(\frac{d}{\frac{n}{m}}\right)^2$$

this follows from the fact that, if m/n and $m>0$, we have

$$\left(\frac{d}{m}\right)\left(\frac{d}{\frac{n}{m}}\right)^2 = \begin{cases} \left(\frac{d}{m}\right) & \text{for } (n,d)=1, \\ 0 & \text{for } (n,d)>1 \end{cases}$$

for in the former case $\left(\frac{n}{m}, d\right)=1$ and in the latter case either $(m,d)>1$ or $\left(\frac{n}{m}, d\right)>1$.

Consequently, $m \geq 1$ and $K \geq 1$, we have

$$\frac{H(N)}{w} = \sum_{mK \leq N} \left(\frac{d}{m}\right)\left(\frac{d}{K}\right)^2,$$

If $mK \leq N$, then either $m \leq \sqrt{N}$, so that we have $K \leq \frac{N}{m}$; or else $m > \sqrt{N}$, so that we have $K \leq \sqrt{N}$, $\sqrt{N} < m \leq \frac{N}{K}$.

Then

$$\frac{H(N)}{w} = \sum_{mK \leq N} \left(\frac{d}{m}\right)\left(\frac{d}{K}\right)^2$$

$$= \sum_{m \leq \sqrt{N}} \left(\frac{d}{m}\right) \sum_{K \leq \frac{N}{m}} \left(\frac{d}{K}\right)^2 + \sum_{K \leq \sqrt{N}} \left(\frac{d}{K}\right)^2 \sum_{\sqrt{N} \leq m \leq \frac{N}{K}} \left(\frac{d}{m}\right). \quad (a)$$

Now, for $\xi > 0$,

$$\sum_{K \leq \xi} \left(\frac{d}{K}\right)^2$$

is the number of positive integers up to ξ that are relatively primes to d, that is, the number of positive integers $\leq \xi$ belonging to a certain collection of $\phi(|d|)$ residue classes mod $|d|$.

Consequntly, we have

$$\left|\sum_{k\le\xi}\left(\frac{d}{k}\right)^2-\frac{\phi(|d|)}{|d|}\xi\right|\le\phi(|d|)\le|d|. \qquad (b)$$

It follows further, since $\left(\frac{d}{n}\right)$ is not a principal character that for $1\le\xi\le\eta$

$$\left|\sum_{\xi<m\le\eta}\left(\frac{d}{m}\right)\right|\le\frac{\phi(|d|)}{2}<|d|. \qquad (c)$$

(If χ is not the principal character, then we have

$$\left|\sum_{a=u}^{v}\chi(a)\right|\le\frac{h}{2},\qquad v\ge u\ge 1,$$

h = number of values that $|\chi(a)|$ are 1.)

From (a), (b), and (c), we obtain

$$\left|\frac{H(N)}{w}-\frac{\phi(|d|)}{|d|}N\sum_{m\le\sqrt{N}}\left(\frac{d}{m}\right)\frac{1}{m}\right|$$

$$=\left|\sum_{km\le N}\left(\frac{d}{m}\right)\left(\frac{d}{k}\right)^2-\frac{\phi(|d|)}{|d|}N\sum_{m\le\sqrt{N}}\left(\frac{d}{m}\right)\frac{1}{m}\right|$$

$$=\left|\sum_{m\le\sqrt{N}}\left(\frac{d}{m}\right)\left(\sum_{k\le\frac{N}{m}}\left(\frac{d}{k}\right)^2-\frac{\phi(|d|)}{|d|}\frac{N}{m}\right)+\sum_{k\le\sqrt{N}}\left(\frac{d}{k}\right)^2\sum_{\sqrt{N}<m\le\frac{N}{k}}\left(\frac{d}{m}\right)\right|$$

$$\le\sum_{m\le\sqrt{N}}|d|+\sum_{k\le\sqrt{N}}|d|\le 2|d|\sqrt{N}$$

$$\Rightarrow \left| \frac{H(N)}{N} - w\frac{\phi(|d|)}{|d|} \sum_{m \leq \sqrt{N}} \left(\frac{d}{m}\right)\frac{1}{m} \right| \leq \frac{2|d|w}{\sqrt{N}}.$$

But, remember that

The the L function corresponding to the character mod a is defined by the Dirichlet's series

$$L(s,\chi) = \sum_{m=1}^{\infty} \frac{\chi(m)}{m^s} \qquad s>1$$

$\rightarrow \displaystyle\sum_{m=1}^{\infty} \frac{\chi(m)}{m^s} = L(s,\chi)$ is absolutely convergent for $s>1$.

$\rightarrow$ If χ is not a principal character, then the series

$$\sum_{m=1}^{\infty} \frac{\chi(m)}{m^s} = L(s,\chi)$$

converges uniformly for $s \geq 1$.

Notice that $\displaystyle\sum_{m=1}^{\infty} \left(\frac{d}{m}\right)\frac{1}{m} = L(1,\chi)$

since this series converges, then as $N \rightarrow \infty$

$$\lim_{N\to\infty} \frac{H(N)}{N} = w\frac{\phi(|d|)}{|d|} \sum_{m=1}^{\infty} \left(\frac{d}{m}\right)\frac{1}{m}. \qquad ▨$$