Contents

Translator's introduction

Dirichlet's *Vorlesungen über Zahlentheorie* is one of the most important mathematics books of the 19th century: the link between Gauss and the number theory of today. The German editions of the book are often called Dirichlet-Dedekind, because Dedekind wrote up Dirichlet's lectures and added supplements to the second and later editions. This translation includes Supplements I–IX, partly because they fill some gaps in the main text but also because they showcase some famous results Dirichlet modestly omitted, such as his theorem on primes in arithmetic progressions and his "pigeonhole" solution of Pell's equation. I have omitted the very lengthy Supplements X and XI, where Dedekind launches into ideal theory, because Dedekind wrote a more compact version of his main results which has already been translated (Dedekind (1996)), and also because they have a more abstract flavour than the rest of the book, which Dirichlet was at pains to make as concrete as possible. Thus, for the first time since 1863, when the first edition of the *Vorlesungen* appeared, it is possible to concentrate fully on Dirichlet's work.

The book is an exceptionally clear synthesis of the number theory of his time, from absolute fundamentals to the frontiers of research. It includes the classic results of Fermat, Euler, Lagrange and Gauss – the staples of any introduction to number theory today – but also a lucid and thorough treatment of Dirichlet's class number formula for quadratic forms. For this reason, Dirichlet is still an outstanding guide to number theory, since there are no modern authors who attempt to explain everything from basic arithmetic to L-functions in the same book.[1]

Of course, the book is also of great historical interest, documenting Dirichlet's role as the expositor who made Gauss's *Disquisitiones Arithmeticae* understandable to ordinary mortals. Dedekind's footnotes (which have been collected from both the second and fourth editions in this translation) show the sections of the *Disquisitiones* that are redone in the *Vorlesungen*, and allow a ready comparison of the two books. When combined with the historical remarks made by Gauss himself, they give a bird's eye view of number theory from approximately 1640 to 1840 – from Fermat's little theorem to L-functions – the period which produced the problems and ideas which are still at the center of the subject.

To assist the reading of Dirichlet's book, the historical picture is outlined in the remainder of this introduction. It helps to know in advance what the main problems of number theory were in his time, and what the basic principles were understood to be. As we shall see, the results considered important by Gauss were much the same as those we consider important today, but our present view of them owes more to Dirichlet.

[1] However, Mathews (1892) is still in print and still a useful guide to 19th century number theory. It largely follows Dirichlet and uses his notation.

Number theory before Gauss

It is easy to summarise the number theory which influenced Gauss, because so little was known before him. Most of it is contained in the works of Euclid, Diophantus, Fermat, Euler, Lagrange and Legendre. Certainly, the quality and depth of their work in number theory was extraordinary, but nevertheless the quantity was slight, no doubt because of the difficulty of the subject and its then unrecognised connections with other parts of mathematics. An excellent study of number theory before Gauss which emphasises connections to other areas, and to modern number theory, is Weil (1984). Here we shall be brief and describe only the roots of the subject.

Euclid laid the foundations of number theory in Books VII – IX of the *Elements*. He found the basic theorem about divisibility, that if a prime p divides ab then p divides a or p divides b, with the help of the euclidean algorithm for finding the gcd. He also gave a glimpse of things to come by proving that there are infinitely many primes. The importance of these achievements was not recognised for 2000 years – probably because of the huge mathematical complexities in the distribution of primes – and in fact the work of the number theorists just mentioned was more influenced by Diophantus than Euclid.

The *Arithmetica* of Diophantus gave number theorists a new and more tractable body of problems, by asking for integer and rational solutions of equations. A typical question (*Arithmetica*, Book III, 19) was: what are the integers x and y such that $x^2 + y^2 = 65$? Diophantus pointed out that this question can be simplified by factorising 65 as 5×13 and finding the solutions of the smaller equations

$$x_1^2 + y_1^2 = 5 \quad \text{and} \quad x_2^2 + y_2^2 = 13.$$

This is because

$$(x_1^2 + y_1^2)(x_2^2 + y_2^2) = (x_1x_2 - y_1y_2)^2 + (x_1y_2 + x_2y_1)^2 = x^2 + y^2,$$

so a pair of squares x^2, y^2 summing to 65 may be obtained from pairs x_1^2, y_1^2 and x_2^2, y_2^2 summing to 5 and 13 respectively.

Fermat was the first mathematician to see the full depth and generality of the seemingly artless problems of Diophantus. In particular, he realised that the real question behind *Arithmetica* III, 19, was: *which primes are sums of two squares?* And he was ready with the answer: those of the form $4n + 1$. However, he did not explain why, so proving this claim became the task of his successors in number theory, Euler and Lagrange.

Euler gave the first published proof in 1749, but it was not very transparent, and Lagrange (1773) clarified the problem greatly by placing it in a theory of *binary quadratic forms*. The general binary form is $ax^2+2bxy+cy^2$ for integers a, b, c, and the general problem is to decide which integers n occur as values of $ax^2+2bxy+cy^2$. Lagrange attacked this problem by considering how the form changes with a change of variables:

$$x' = \alpha x + \beta y,$$
$$y' = \gamma x + \delta y.$$

If the coordinates α, β, γ, δ are integers with $\alpha\delta-\beta\gamma = \pm 1$ then the pair (x', y') runs through all integer pairs when (x, y) does, hence the new form $a'x'^2+2b'x'y'+c'y'^2$ takes the same values as the old, and can be considered *equivalent* to it. One can then study all binary quadratic forms by studying their "simplest" equivalents, and

Lagrange found a precise and practical way to do this. In the process, he discovered a crucial concept for all deeper investigations along these lines, the *class number*.

Lagrange computed the "simplest" equivalent of a form $ax^2 + 2bxy + cy^2$ with the help of special transformations such as

$$x' = x \pm y,$$
$$y' = y.$$

This one converts the form to $ax'^2 + (2b \pm 2a)x'y' + (a + c \pm 2b)y'^2$, and when combined with the similar conversion to $(a + c \pm 2b)x'^2 + (2b \pm 2c)x'y' + cy'^2$ it gives a way to simplify the coefficients by a process like the euclidean algorithm. However it is not clear, without completing the simplification process, how to recognise inequivalent forms. A quick but incomplete answer is given by the *determinant of the form* $D = b^2 - ac$.

Two forms with different determinants are definitely not equivalent, but two forms with the same determinant may or may not be — it depends on the value of D. For example, it turns out that all forms with $D = -1$ are equivalent to $x^2 + y^2$, and indeed Lagrange used this fact to give a new proof of Fermat's theorem about primes of this form. He was similarly able to explain a second result claimed by Fermat — that the primes of the form $x^2 + 2y^2$ are those of the linear forms $8n + 1$ and $8n + 3$ — by showing that all forms with $D = -2$ are equivalent to $x^2 + 2y^2$.

On the other hand, there are two inequivalent forms with $D = -5$, $x^2 + 5y^2$ and $2x^2 + 2xy + 3y^2$, and this explains a situation Fermat did *not* understand. The linear forms one expects for $D = -5$ are $20n + 1$, $20n + 3$, $20n + 7$ and $20n + 9$, but they are not all realised by primes of the form $x^2 + 5y^2$. In fact they are "shared" between the two quadratic forms with $D = -5$; with the values $20n + 1$ and $20n + 9$ being taken by $x^2 + 5y^2$, and $20n + 3$ and $20n + 7$ being taken by $2x^2 + 2xy + 3y^2$.

The number of inequivalent forms with a given discriminant D is the class number. Thus the class number is 1 for $D = -1$, and it is 2 for $D = -5$. After Lagrange, the importance of the class number was clear, but understanding it was a problem of unexpected difficulty. There was no sign of a formula giving the class number as a function of D. Even Gauss, as we shall see, did not get far beyond computing class numbers for particular values of D.

Quadratic forms threw up another problem that was too hard for 18th century mathematicians: *the law of quadratic reciprocity*. In investigating the prime values of quadratic forms, it turns out to be important to know which primes p are squares modulo a given prime q. Euler and Legendre observed that the answer seems to depend only the "reciprocal" property: whether q is a square mod p. To be precise, they conjectured that

- when p and q are both $\equiv 3 \pmod 4$, p is a square mod q if and only if q is *not* a square mod p,
- otherwise, p is a square mod q if and only q is a square mod p.

This is the law of quadratic reciprocity. Legendre (1785) proposed a proof, but it depended on the unproved assumption that an arithmetic progression $an + b$, where $\gcd(a, b) = 1$ and $n = 1, 2, 3, \ldots$, contains infinitely many primes.

One of the great achievements of Gauss was to prove quadratic reciprocity, in several different ways, without Legendre's assumption. The assumption about primes in arithmetic progressions lies even deeper, at the level of the class number formula.

Gauss and the *Disquisitiones*

Gauss published the *Disquisitiones* in 1801, when he was 24, and it is clear from his many citations that he had already mastered the works of Euler, Lagrange and Legendre. The first three sections of his book cover their main results, using a streamlined approach which fills some major gaps. Gauss begins by introducing the concept of congruence in Section I, then proves several theorems about congruence modulo a prime p in Sections II and III:

- Lagrange's theorem that a congruence of degree n has $\leq n$ roots mod p (article 43)
- Fermat's little theorem that $a^{p-1} \equiv 1 \pmod{p}$ when $a \not\equiv 0 \pmod{p}$ (article 50)
- The existence of primitive roots mod p, a conjecture of Euler which had not previously been proved (article 55)
- Euler's theorem that -1 is a square mod any p of the form $4n+1$ (article 64)
- "Wilson's theorem," actually first proved by Lagrange, that $(p-1)! \equiv -1 \pmod{p}$ (article 76)

Another innovation in the elementary part of the *Disquisitiones* is the first statement of unique prime factorisation (article 16). Gauss quite properly credits Euclid with the underlying result — that if a prime p divides ab then p divides a or p divides b — but is at pains to give an entirely different proof. He reaches unique prime factorisation directly (if unexpectedly) by induction, whereas Euclid uses the less direct (but useful) euclidean algorithm for the gcd. In fact, Gauss keeps his distance from the euclidean algorithm even when discussing the gcd, finding it by the less efficient method of prime factorisation (article 18), and saying only that "we know from elementary considerations how to solve these problems when the resolution of the numbers A, B, C, etc. into factors is not given."

These early sections contain many new proofs and and new theorems. However, they are not particularly hard, and indeed they basically clarify and systematise known material. The level of originality and difficulty rises sharply in Section IV, where Gauss gives the first proof of quadratic reciprocity. The law of quadratic reciprocity was Gauss's favourite theorem, and he gave several other proofs of it – which is just as well, because his first proof was horrendous. It provoked Dirichlet to thoroughly reorganise the methods and theorems of elementary number theory, if only to make the path to quadratic reciprocity easier.

The massive Section V (nearly three quarters of the *Disquisitiones*) was an even greater obstacle. As Lagrange (1773) discovered, the theory of quadratic forms is complicated by the existence of inequivalent forms with the same discriminant; in other words, by the existence of class numbers other than 1. Gauss surprisingly deferred the problem of *computing* the class number in favour of an attack on the *structure* of quadratic forms with the same discriminant. Instead of trying to find how many inequivalent forms there were, he studied how the equivalence classes of forms interact with each other algebraically. Following faint hints in the work of Lagrange and Legendre, Gauss defined a subtle operation on the set of equivalence classes of forms with given discriminant called *composition of forms*.

A simple example is the Diophantus identity

$$(x_1^2 + y_1^2)(x_2^2 + y_2^2) = (x_1x_2 - y_1y_2)^2 + (x_1y_2 + x_2y_1)^2 = x^2 + y^2,$$

which shows x^2+y^2 being in some sense "composed with itself" and producing itself again. Under this operation of composition, $I = x^2 + y^2$ is the "identity element," because $I^2 = I$. No other form is involved here because I is equivalent to all forms with determinant -1.

A less trivial example brings together the two inequivalent forms with determinant -5, $A = x^2 + 5y^2$ and $B = 2x^2 + 2xy + 3y^2$. Lagrange (1773) observed that

$$(2x_1^2 + 2x_1y_1 + 3y_1^2)(2x_2^2 + 2x_2y_2 + 3y_2^2) = x^2 + 5y^2,$$

where

$$x = 2x_1x_2 + x_1y_2 + y_1x_2 - 2y_1y_2 \quad \text{and} \quad y = x_1y_2 + y_1x_2 + y_1y_2,$$

hence when B is "composed with itself" the result is A; in symbols, $B^2 = A$. Similar identities show that $AB = B$ and $A^2 = A$, so here we have a group of order 2 with identity element A. When properly defined, composition of forms always turns out to be a group operation on equivalence classes of forms with a given discriminant. The result is what is now called the *class group*, and Gauss essentially succeeded in finding its structure.

This was an amazing achievement, but the world was not ready for it, because *the group concept did not yet exist!* Even with hindsight, it is a herculean task to clean up Gauss's work enough to make the group concept visible. For example, his proof that composition of forms is associative involves 37 equations, most of which Gauss asks the reader to derive. This put the class group on the shelf for nearly 70 years, until Kronecker (1870) gave a simple and elegant proof of Gauss's structure theorem by axiomatising the concept of finite abelian group. In the meantime, Dirichlet had successfully attacked the class number problem directly.

Quadratic forms and quadratic integers

One reason Gauss had trouble with quadratic forms is that he rejected an alternative which had already been used by Lagrange and Euler – the theory of *quadratic integers*. It is true that the theory of quadratic integers was not on a sound footing in Gauss's time, and this may also have deterred Dirichlet from using it in the *Vorlesungen*, but later work by Kummer and Dedekind showed it is the best way to go. We therefore mention it briefly here, since subtle properties of quadratic forms correspond to quite down-to-earth properties of quadratic integers. It is likely that Gauss was guided by these properties in writing the *Disquisitiones*, but chose to "translate" them into properties of quadratic forms for the sake of rigour. According to Kummer (1846), Dirichlet

> recounted and showed to me, specifically from oral and written remarks of Gauss, that Gauss had already used in his own private work something like ideal factors at the time he was completing the section on composition of forms in the *Disquisitiones Arithmeticae*, but that he was never able to put it on a firm foundation; he says in particular, in a note to his article on the decomposition of polynomials into linear factors, that: 'If I wanted to proceed with the use of imaginaries in the way that earlier mathematicians have done, then one of my earlier researches which is very difficult could have been done in a very simple way.'

What then are these "imaginaries" and "ideal factors"?

The simplest "imaginaries" are the *Gaussian integers* $a+b\sqrt{-1}$ where $a, b \in \mathbb{Z}$. They are so called because they were first studied by Gauss (1831), who showed that they have a "division algorithm" like that for $\mathbb{Z}$: if α and $\beta \neq 0$ are Gaussian integers then there is a "quotient" μ and "remainder" ρ such that

$$\alpha = \mu\beta + \rho \quad \text{with} \quad 0 \leq |\rho| < |\beta|.$$

In fact, this result is geometrically obvious if one views $|\rho|$ as the distance from α to the nearest multiple $\mu\beta$ of β in the plane of complex numbers. It follows from the division algorithm that the Gaussian integers admit a euclidean algorithm and hence (by an argument like Euclid's for ordinary integers) unique prime factorisation.

The Gaussian integers mirror the properties of the quadratic form $x^2 + y^2$. For example, the composition formula

$$(x_1^2 + y_1^2)(x_2^2 + y_2^2) = (x_1x_2 - y_1y_2)^2 + (x_1y_2 + x_2y_1)^2 = x^2 + y^2,$$

comes from the Gaussian integer factorisations

$$\begin{aligned} x_1^2 + y_1^2 &= (x_1 + y_1\sqrt{-1})(x_1 - y_1\sqrt{-1}) \\ \text{and} \quad x_2^2 + y_2^2 &= (x_2 + y_2\sqrt{-1})(x_2 - y_2\sqrt{-1}), \end{aligned}$$

when the factors are recombined as

$$\begin{aligned} (x_1 + y_1\sqrt{-1})(x_2 + y_2\sqrt{-1}) &= x_1x_2 - y_1y_2 + (x_1y_2 + x_2y_1)\sqrt{-1} \\ \text{and} \quad (x_1 - y_1\sqrt{-1})(x_2 - y_2\sqrt{-1}) &= x_1x_2 - y_1y_2 - (x_1y_2 + x_2y_1)\sqrt{-1}. \end{aligned}$$

Moreover, unique prime factorisation in the Gaussian integers reflects the fact that all forms with determinant -1 are equivalent to $x^2 + y^2$.

In fact, any determinant D corresponds to a ring of quadratic integers which has unique prime factorisation just in case the class number for D is 1. For example, the integers for determinant -5 are those of the form $a + b\sqrt{-5}$ for $a, b \in \mathbb{Z}$, and one finds that

$$2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

are *non*unique prime factorisations of the number 6. Thus the class number (2 in this case) is a measure of the deviation from unique prime factorisation in a suitable ring of quadratic integers.

Knowing this, we can see that unique prime factorisation in the ordinary integers is a gift we cannot take for granted. As Kummer (1844) said:

> it is greatly to be lamented that this virtue of the real numbers [that is, the ordinary integers] to be decomposable into prime factors, always the same ones for a given number, does not belong to the complex numbers [more general integers]; were this the case, the whole theory, which is still laboring under such difficulties, could easily be brought to a conclusion.

Perhaps Gauss was first to state the theorem of unique prime factorisation for $\mathbb{Z}$ because he was also first to realise the theorem failed for more general integers. Gauss's response to the difficulty was composition of forms; Kummer's was the creation of "ideal" prime factors – generalised "numbers" which behaved more simply than forms. But before embarking on either course, one needed to evaluate the class number to see whether unique prime factorisation had actually failed. This is where Dirichlet comes into the story.

Euler and the zeta function

Dirichlet's evaluation of the class number is probably his deepest and most original work, nevertheless it did not come entirely out of the blue. Its roots are in the zeta function and its product formula discovered by Euler (1748). The zeta function $\zeta(s)$ is defined for $s > 1$ by the series

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots,$$

and the product formula is

$$\zeta(s) = \frac{1}{(1-1/2^s)}\frac{1}{(1-1/3^s)}\frac{1}{(1-1/5^s)}\frac{1}{(1-1/7^s)}\frac{1}{(1-1/11^s)}\cdots,$$

where the general term on the right hand side is $1/(1-1/p_n^s)$ and p_n is the n^{th} prime.

The product formula is proved by expanding the general term in the product as a geometric series

$$\frac{1}{(1-1/p_n^s)} = 1 + \frac{1}{p_n^s} + \frac{1}{p_n^{2s}} + \frac{1}{p_n^{3s}} + \cdots,$$

and observing that the product of all these series is the sum of 1 and the terms

$$\frac{1}{(p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k})^s}$$

where each product $p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k}$ of primes occurs exactly once. It follows, by unique prime factorisation, that the term $1/n^s$ occurs exactly once for each integer $n > 1$, and hence the sum is precisely $\zeta(s)$.

As mentioned above, we initially define $\zeta(s)$ only for $s > 1$. This is because the series

$$1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots$$

has an infinite sum for $s = 1$. However, there is a profit to be made even from this setback. If the number of primes is finite, the product

$$\zeta(s) = \frac{1}{(1-1/2^s)}\frac{1}{(1-1/3^s)}\frac{1}{(1-1/5^s)}\frac{1}{(1-1/7^s)}\frac{1}{(1-1/11^s)}\cdots,$$

is finite even for $s = 1$, and hence so is the sum

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots$$

This is a contradiction, hence the number of primes must be infinite.

Thus Euler's product formula encapsulates the two great ideas of Euclid: uniqueness of prime factorisation and the infinite number of primes. Dirichlet's great achievement was to generalise these two ideas: he found a formula for the class number (and hence measured how far quadratic integers deviate from unique prime factorisation), and showed that the number of primes in arithmetic progressions is infinite. The latter theorem is not in the main text of Dirichlet's book, but is in Dedekind's Supplement VI, which actually uses the class number formula for one step. The theorem can also be found in many modern books on number theory, for example Rademacher (1964) or Serre (1973). As Cohn (1962) p.174 puts it, Dirichlet's theorem on primes is now seen as the "historical consummation" of his class number formula, and it is easier to present in a textbook. For more on the

connection between it and the class number formula, see Cohn (1962) or Scharlau and Opolka (1985).

The class number formula

The search for a class number formula probably began with Gauss, but the first formula in print was proposed by Jacobi (1832). He conjectured it on the evidence of some results of Cauchy in the theory of circle division, and his own brilliant extrapolation (or "induction" as they called it then) from numerical results. Jacobi's formula was correct, but by no means proved by him. In a memorial speech for Jacobi, Dirichlet later said

> I believe it should be mentioned, regarding the previously unknown origin of this result, that Jacobi's communication is a noteworthy example of shrewd induction, even though it is not possible to base a rigorous proof on circle division; it appears necessary to use essentially different principles, involving integral calculus and the theory of series, which were only later introduced into the subject. (Dirichlet (1852), p.241.)[2]

The integral calculus and series methods were developed by Dirichlet (1837, 1839), and explained in Chapter 5 of his book. They were not *entirely* new, having been foreshadowed by the zeta function, and in fact the idea of using zeta-like series to evaluate class numbers had been incompletely explored by Gauss (1834, 1837) in unpublished work. But Dirichlet probably had the idea independently, and he brought it to fruition with characteristic thoroughness and rigour.

Because of the depth and complexity of Dirichlet's proof, it is hard to preview it for the first-time reader. It draws on many earlier sections of his book, particularly those on squares modulo m and equivalence of forms, and it also inherits a lot of notation from these earlier sections. However, the following ideas are perhaps the most important, and it should help to bear them in mind when reading Chapter 5. To make it easier to look them up, we list the sections where they occur in Dirichlet's book. The first idea actually comes from Gauss's *Disquisitiones*, article 154, and it shows why quadratic reciprocity is important in the theory of quadratic forms.

1. When $ax^2 + 2bxy + cy^2$ is a quadratic form with $b^2 - ac = D$, and m is a value of $ax^2 + 2bxy + cy^2$ for relatively prime x and y, then D is a square mod m (§60).
2. It follows that the representable numbers may be associated with a value D, rather than with a particular form. This leads, in §88, to a kind of sharing of the numbers m represented by forms of determinant D between the members of a complete system of $h(D)$ inequivalent forms, where $h(D)$ is the class number. (A simple example of this, mentioned above, is the sharing

[2]There is an interesting modern parallel to this situation, observed by Andrew Wiles in his address to the International Congress of Mathematicians in Zürich in August 1994. At the time, Wiles was still laboring to fix the gap in his proof of Fermat's last theorem — another result once thought to be provable by circle division. He had come to the conclusion that he needed to prove a class number formula, and he recalled that when this happened to Jacobi it took another seven years for Dirichlet to find the proof. So it did, but Wiles was luckier. Only a month later he found what he needed, with the help of Richard Taylor.

of primes between the two inequivalent forms x^2+5y^2 and $2x^2+2xy+3y^2$ with $D=-5$.)

3. The precise statement of the way the values m are shared between the inequivalent forms $ax^2+2bxy+cy^2$, $a'x^2+2b'xy+c'y^2$, ... with determinant D is what Dirichlet calls the *fundamental equation* (§88)

$$\sum\left(\frac{ax^2+2bxy+cy^2}{\sigma}\right)^{-s}+\sum\left(\frac{a'x^2+2b'xy+c'y^2}{\sigma}\right)^{-s}+\cdots=\kappa\sum\frac{2^\mu}{m^s},$$

where σ, κ and μ are certain constants required for correct accounting, the sums are over certain x, y and m, and $s>1$ to ensure convergence.

4. The right hand side of the fundamental equation can be transformed into an infinite product over certain primes, essentially by the argument for the Euler product formula (§89).
5. As with the Euler formula, something interesting happens as s tends to the critical value 1. If the fundamental equation is multiplied by $s-1$, each side tends to a finite limit as s tends to 1. Moreover, each term on the left hand side tends to the *same* limit (§95), depending only on D. The limit can be evaluated by geometric considerations (area of an ellipse when $D<0$, area of a hyperbolic sector when $D>0$). Since there are $h(D)$ terms on the left hand side, this side tends to $h(D)\times$ this geometric limit.
6. The limiting value of the right hand side can also be evaluated, by analytic means, and hence we have an expression for the class number $h(D)$. In particular, Jacobi's class number formula is confirmed (§104).

Dirichlet works through the case of $D=-1$ in §97, since it is a particularly beautiful example of the emergence of a class number from geometry and analysis. The $h(-1)$ terms on the left hand side of the transformed fundamental equation each tend to the area of a circle, and the series on the right tends to a multiple of $1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+\cdots$, with the result that

$$h(-1)\frac{\pi}{4}=1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+\cdots.$$

Because the series is the well-known one for $\frac{\pi}{4}$, this confirms that $h(-1)=1$.

Acknowledgements

I would like to thank Helmut Koch for suggesting that I translate Dirichlet's *Vorlesungen*, and my son Michael for converting my handwritten translation to LaTeX.

References

H. Cohn (1962): *A Second Course in Number Theory*, John Wiley and Sons. Reprinted by Dover, 1980, under the title *Advanced Number Theory*.

R. Dedekind (1996): *Theory of Algebraic Integers*, Cambridge University Press.

P. G. L. Dirichlet (1837): Beweis der Satz, dass jede unbegrentze arithmetische progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftliche Factor sind, unendliche viele Primzahlen enthält. *Abh. der Königlichen Preuss. Akad. der Wiss.*, 45–81. Also in Dirichlet *Mathematische Werke*, volume I, 313–342.

P. G. L. Dirichlet (1839): Recherches sur diverses applications de l'analyse infinitésimal à la théorie des nombres. *J. reine angew. Math.*, **19**, 324–369. Also in his *Mathematische Werke*, volume I, 411–496.

P. G. L. Dirichlet (1852): Gedächtnisrede auf Carl Gustav Jacob Jacobi. *Abh. der Königlichen Preuss. Akad. der Wiss.* Also in Dirichlet *Mathematische Werke*, volume II, 227–252.

L. Euler (1748): *Introductio in analysin infinitorum. Opera Omnia*, series 1, volume VIII. English translation, *Introduction to the Analysis of the Infinite*, Springer-Verlag, 1988.

C. F. Gauss (1831): Theoria residuorum biquadraticorum. *Comm. Soc. Reg. Sci. Gött. Rec.*, **7**. Also in Gauss *Werke*, volume 2, 67–148.

C. F. Gauss (1834, 1837): De nexu inter multitudinem classium, in quas formae binariae secundi gradus distribuuntur, earumque determinantem. Gauss *Werke*, volume 2, 269–291.

C. G. J. Jacobi (1832): Observatio arithmetica de numero classium divisorum quadraticorum formae $yy + Azz$, designante A numerum primum formae $4n + 3$. *J. reine angew. Math.*, **9**, 189–192.

L. Kronecker (1870): Auseinandersetzung einige Eigenschaften der Klassenzahl idealer complexer Zahlen. *Monatsber. Königl. Akad. Wiss. Berlin*, 881–889. Also in his *Werke* volume I, 271–282.

E. E. Kummer (1844): De numeris complexis, qui radicibus unitatis et numeris realibus constant. *Gratulationschrift der Univ. Breslau zur Jubelfeier der Univ. Königsberg*. Also in Kummer *Collected Papers*, volume 1, 165–192.

E. E. Kummer (1846): Letter to Kronecker, 14 June 1846. In Kummer *Collected Papers*, volume 1, 98.

J. L. Lagrange (1773): Recherches d'arithmétique. *Nouv. mém. de l'acad. sci. Berlin*, 265ff. Also in his *Œuvres*, volume 3, 695–795.

A. -M. Legendre (1785): Recherches d'Analyse Indéterminée, *Mem. de Mat. et Phys. de l'Acad. Roy. des Sci.*, 465–559.

G. B. Mathews (1892): *Theory of Numbers*, G. Bell and Sons. Reprinted by Chelsea 1980.

H. Rademacher (1964): *Lectures on Elementary Number Theory*, Blaisdell Publishing Company.

W. Scharlau and H. Opolka (1985): *From Fermat to Minkowski. Lectures on the Theory of Numbers and Its Historical Development*, Springer-Verlag.

J. -P. Serre (1973): *A Course in Arithmetic*, Springer-Verlag.

A. Weil (1984): *Number Theory. An Approach Through History*, Birkhäuser.

Clayton, Victoria, Australia — John Stillwell

April 1999