The Parallel Worlds of Number Theory

Florian Breuer

15 August 2013

The Parallel Worlds of Number Theory
Inaugural lecture delivered on 15 August 2013

Prof Florian Breuer
Department of Mathematical Sciences
Faculty of Science
Stellenbosch University

Editor: SU Language Centre
Printing: SUN MeDIA
ISBN: 978-0-7972-1451-4

About the author

Florian Breuer was born in 1977 in Vienna, Austria, to German parents and moved to Stellenbosch at the age of 4, where he grew up and completed his undergraduate studies at Stellenbosch University in 1998. He then moved to Paris on a French Government Scholarship, where he completed his Ph.D. in 2002 at the Université Denis Diderot under supervision of Marc Hindry.

After postdoctoral positions at the National Center for Theoretical Sciences in Hsinchu, Taiwan (2003) and at the Max-Planck-Institut für Mathematik in Bonn, Germany (2004), he returned to Stellenbosch University as a Senior Lecturer in July 2004.

He was promoted to Associate Professor in October 2007, and to Professor in January 2013. He serves as the head of the Mathematics Division in the Department of Mathematical Sciences since 2012.

In 2007 Florian was awarded the *Meiring-Naudé Medal* by the Royal Society of South Africa, and in 2009 he spent six months at the University of Kassel, Germany and at the ETH-Zürich, Switzerland, with an Alexander-von-Humboldt-Fellowship for Experienced Researchers. In 2011 Florian was invited onto the editorial board of the *Journal of Number Theory* and in 2013 he was featured amongst the *Mail&Guardian's* "200 Young South Africans". Florian is particularly proud of the fact that for the last three years, a top first-year student has nominated him as his most inspiring lecturer at the First Year Academy's Prestige Dinner.

In his spare time, Florian is an award-winning landscape photographer. He lives in Stellenbosch and is married to Erica Breuer.

The Parallel Worlds of Number Theory

Dedicated to the memory of Klaus Breuer (1968–2013).

1 Introduction

Mathematics is like a fantastical, infinite and infinitely varied landscape which is seen and explored by the human mind. Different areas of Mathematics are like continents, so vast that only small parts of them can be explored in a lifetime. These continents differ substantially in character and in resistance to exploration, yet are connected to each other by various unexpected land bridges.

My own research concerns the continent of Number Theory. It is one of the very first areas of Mathematics to be explored, the earliest glimpses and rumours of it dating back to Babylonian times. Today, the exploration of Number Theory is one of the largest and most active endeavors in Mathematics, although it is unfortunately under-represented in the South African mathematical community.

The goal of this article is to give you a taste of Number Theory, and in particular of the curious phenomenon of the two *parallel worlds* of Number Theory – Number Fields and Function Fields – which resemble each other in character, yet differ in telling details.

The point of departure of Number Theory is the study of the whole numbers (integers) and their behaviour under the four basic operations of arithmetic: addition, subtraction, multiplication and division with remainder. Depending on the direction taken, this study can quickly leave behind the familiarity of basic arithmetic, and lead to more exotic concepts, often at the frontiers with other areas of Mathematics, such as Algebra, Analysis and Geometry. Today, I invite you to accompany me on a journey starting with the prime numbers and taking us to zeta functions and the Riemann Hypothesis, then skipping over to cyclotomy, elliptic functions, elliptic curves, Galois Theory and the André-Oort Conjecture. All this will take place in classical Number Theory, also known as the world of *Number Fields*.

At the same time, we will also trace an analogous path in the parallel world of *Function Fields*. We will start with the arithmetic of polynomials over a finite field, irreducible polynomials (primes), zeta functions and the Riemann Hypothesis (Hasse-Weil Theorem), then skip over to the theory of Drinfeld modules, Galois Theory and the André-Oort Conjecture for Drinfeld modular varieties.

2 Classical Number Theory

Let us start with the *prime numbers*: $2, 3, 5, 7, 11, 13, 17, \ldots$, which are integers greater than 1 and divisible only by themselves and by 1. These form the building blocks of all other integers, in that every non-zero integer can be factorised into a product of ± 1 and a finite list of prime numbers; moreover, these prime factors are unique (up to the order in which they are multiplied). This is known as the *Fundamental Theorem of Arithmetic*, and has been known since the time of the Ancient Greeks. As an example, the prime factorizations of 24 and 2013 are $24 = 2 \cdot 2 \cdot 2 \cdot 3 = 2^3 \cdot 3$ and $2013 = 3 \cdot 11 \cdot 61$, respectively.

How many prime numbers are there? The Greeks knew the answer to this, too, and their proof (most likely due to Euclid) is so beautiful that I repeat it here:

Theorem 1 (Euclid, ca. 300 B.C.E.) *There exist infinitely many prime numbers.*

Proof. Let $p_1, p_2, \ldots, p_n$ be any finite list of prime numbers. Now form the number $N := p_1 p_2 \cdots p_n + 1$. By construction, N leaves a remainder of 1 when divided by any p_i, hence is not divisible by any prime on our list. However, since $N > 1$, it must be divisible by at least one prime number, and this prime is not on our list. Therefore, any finite list of primes is necessarily incomplete. □

So how are the primes distributed amongst the integers? This question is more subtle, and it is not immediately clear what would qualify as an answer. If we compute the first thousand or ten thousand prime numbers, we notice that they are distributed seemingly at random, but tend to thin out as the numbers get larger. In fact, it looks very much like the probability that a given number n is prime is $1/\log(n)$ (Here $\log(x) = \ln(x)$ is the natural logarithm). Of course the distribution of primes numbers is entirely deterministic and not random at all, so we need a better answer.

The standard approach is to define the *prime counting function*

$$\pi(x) := \text{the number of primes } p \leq x, \qquad \text{for every real number } x.$$

Figure 1 shows two graphs of $y = \pi(x)$ at different scales.

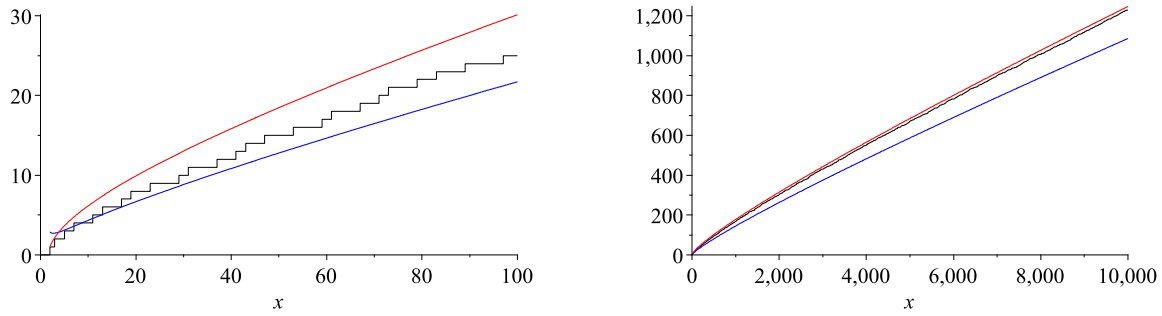

Figure 1: $y = \pi(x)$, $y = Li(x)$ and $y = \dfrac{x}{\log(x)}$ for $x \leq 100$ (left), and $x \leq 10,000$ (right).

Around 1792–1793 the teenaged C.F. Gauss had conjectured, based on his computations of prime numbers, that $\pi(x)$ behaves like the function $x/\log(x)$, and the following theorem was proved a century later by J. Hadamard and C.J. de la Vallée-Poussin.

Theorem 2 (Prime Number Theorem) *We have*

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\log(x)} = 1.$$

The relation in Theorem 2 is more succinctly written as

$$\pi(x) \sim \frac{x}{\log(x)}.$$

As we can see from the graphs of Figure 1, an even better approximation for $\pi(x)$ is the function

$$Li(x) := \int_2^x \frac{dt}{\log t},$$

which supports the idea that n is prime with "probability" $1/\log(n)$. This approximation was suggested by G.L. Dirichlet in 1838, and it is an exercise for our Mathematics 144 students to show that

$$Li(x) \sim \frac{x}{\log(x)}.$$

The proof of the Prime Number Theorem requires substantial input from Complex Analysis, applied to the Riemann zeta function, and this will be the next destination on our journey. But first, let us enter the magic mirror into the parallel world of Function Fields.

3 Polynomials Over a Finite Field

Our analogue of the ring $\mathbb{Z}$ of integers will be the ring $A = \mathbb{F}_q[T]$ of polynomials over a finite field $\mathbb{F}_q$ of q elements, where q is a power of some prime number p. These are expressions of the form

$$a = a_n T^n + a_{n-1} T^{n-1} + \cdots + a_1 T + a_0, \qquad a_0, a_1, \ldots, a_n \in \mathbb{F}_q,$$

where $n = \deg(a)$ is called the degree of a.

The layperson can set $q = p$ and think of these as "numbers" with digits $a_0, a_1, \ldots, a_n \in \mathbb{F}_p = \{0, \ldots, p-1\}$, but where the base has been replaced by the symbol T. The basic operations of arithmetic are performed as usual, except that all carries between digits are dropped.

As a result, adding 1 to itself p times yields 0 and we say that our ring A has *characteristic* p. This is the first major difference between A and the ring $\mathbb{Z}$ of integers, which we say has *characteristic 0*.

A polynomial is *monic* if its leading digit is $a_n = 1$; this is in analogy with the *positive* integers.

Our analogues for prime numbers in $\mathbb{Z}$ are monic polynomials in A of degree at least 1 which are *irreducible*, meaning polynomials which cannot be factorised into products of smaller polynomials. For example, the first few primes in $A = \mathbb{F}_3[T]$ are

$$T,\ T+1,\ T+2,\ T^2+1,\ T^2+T+2,\ T^2+2T+2.$$

As in the classical case, every non-zero polynomial in A can be factorised into a constant times a product of primes, unique up to ordering.

How many primes are there in A? Infinitely many – in fact, Euclid's proof of Theorem 1 also works in this case. As to their distribution, it again looks random, thinning out as the degree gets larger. In this case, however, we can get more precise information. We define the prime counting function for A as

$$\pi_A(n) := \text{The number of primes in } A \text{ of degree } n, \qquad \text{for any } n \geq 1.$$

Then one can prove

$$\begin{aligned} \pi_A(n) &\sim \frac{q^n}{n} \\ &= \frac{x}{\log_q(x)}, \end{aligned} \tag{1}$$

where $x = q^n$ is the total number of monic polynomials of degree n in A. So this is an exact analogue of the Prime Number Theorem. In this case, the proof of (1) is much simpler than the proof of the Prime Number Theorem for $\mathbb{Z}$. As we will see, this is related to the notion of *zeta functions*.

4 The Riemann Zeta Function

We now return to the world of classical Number Theory and consider the function defined by

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}. \tag{2}$$

This is called the Riemann zeta function, although it was first studied by L. Euler, who proved in 1735 that

$$\zeta(2) = 1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \cdots = \frac{\pi^2}{6},$$

and obtained similar expressions for $\zeta(s)$ for other positive even integers s. More importantly, Euler discovered in 1737 that

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}, \tag{3}$$

where the product runs over all prime numbers p. This is a simple consequence of unique factorisation, although to give a rigorous proof one must be a little careful with convergence issues. Speaking of convergence, the series (2) diverges for $s = 1$, since

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots + \frac{1}{n} \geq \log(n),$$

and so $\lim_{s\to 1^+} \zeta(s) = +\infty$. This, combined with the Euler Product (3), gives another proof of the fact that there are infinitely many prime numbers. In fact, with a little extra effort one can use this to show that the sum

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \cdots$$

of reciprocals of primes diverges, so in a sense there must be more prime numbers than there are squares (after all, the sum of reciprocals of squares converges to $\frac{\pi^2}{6}$). This immediately gives us $\pi(x) > \sqrt{x}$ for sufficiently large x. In fact this argument gives us, for any $\varepsilon > 0$, $\pi(x) > x^{1-\varepsilon}$ for all sufficiently large x.

We thus see that $\zeta(s)$ has much to tell us about the distribution of prime numbers.

In 1859 G.F.B. Riemann presented to the Prussian Academy of Sciences his one and only publication in Number Theory [30], which is nevertheless considered one of the greatest contributions to the field. His point of departure was to consider $\zeta(s)$ for *complex numbers* $s \in \mathbb{C}$, thus bringing to bear the full force of Complex Analysis on the study of prime numbers. The series in (2) converges to a holomorphic function for $\Re(s) > 1$, and Riemann showed how to extend $\zeta(s)$ to a meromorphic function on the whole complex plane, with only a simple pole at $s = 1$. Furthermore, he discovered that $\zeta(s)$ satisfies the functional equation

$$\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \pi^{-\frac{1-s}{2}}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s), \qquad \text{for all } s \in \mathbb{C}, \tag{4}$$

where

$$\Gamma(s) := \int_0^{\infty} e^{-t} t^{s-1}\, dt$$

is Euler's Gamma Function.

Thus we see that $\zeta(s)$ enjoys a certain symmetry about the *critical line* $\Re(s) = \frac{1}{2}$. The presence of $\Gamma\left(\frac{s}{2}\right)$ in (4) forces $\zeta(s)$ to be zero for negative even integers s, the so-called *trivial zeros*, and all other zeros must lie on, or be distributed symmetrically on either side of, the critical line $\Re(s) = \frac{1}{2}$. From the series (2) it is clear that $\zeta(s) \neq 0$ for $\Re(s) > 1$, and thus by symmetry also for $\Re(s) < 0$, except for the trivial zeros. All other zeros of ζ are thus confined to the *critical strip* $0 \leq \Re(s) \leq 1$; they are called the *critical zeros*.

Figure 2 shows a *phase plot* of $\zeta(s)$, on which we can clearly see the pole at $s = 1$, the trivial zeros on the left, and the first few critical zeros, all of which lie on the critical line.

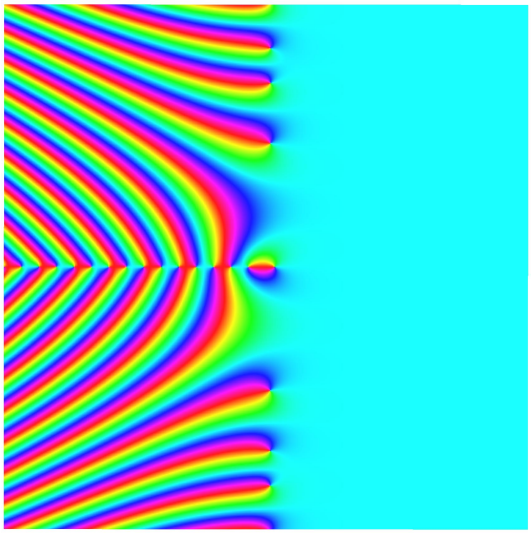

Figure 2: Phase plot of $\zeta(s)$

What does this tell us about prime numbers? Instead of the prime counting function $\pi(x)$, let us consider the following function, which is easier to study:

$$\psi(x) := \sum_{n \leq x} \Lambda(n), \quad \text{where} \quad \Lambda(n) := \begin{cases} \log p & \text{if } n = p^m \\ 0 & \text{otherwise.} \end{cases}$$

The Prime Number Theorem can be shown to be equivalent to

$$\psi(x) \sim x.$$

Riemann deduced an exact formula for $\psi(x)$, which (after some simplifications) can be written as

$$\psi(x) = x - \sum_{\rho} \frac{x^\rho}{\rho} - \log 2\pi - \frac{1}{2}\log(1 - x^{-2}), \tag{5}$$

where the sum ranges over all critical zeros ρ of $\zeta(s)$. This sum is only conditionally convergent, otherwise $\psi(x)$ would have to be continuous, which it is not. The terms of the sum must be added in order of increasing $|\rho|$. Since $|x^\rho| = x^{\Re(\rho)}$, we therefore get a valuable estimate of $\psi(x)$ (and hence of $\pi(x)$) if we knew that $\Re(\rho) < 1 - \varepsilon$ for all critical zeros ρ. In fact, Riemann conjectured that all the critical zeros ρ lie on the critical line; this is known as the

Riemann Hypothesis. *All critical zeros ρ of $\zeta(s)$ satisfy $\Re(\rho) = \frac{1}{2}$.*

This is the single most important unsolved problem in Mathematics today. There are hundreds, possibly thousands, of theorems that begin "Assume the Riemann Hypothesis is true, then ...". We will encounter examples of this towards the end of this article.

The Riemann Hypothesis is equivalent to the following strong form of the Prime Number Theorem:

$$\pi(x) = Li(x) + O(\sqrt{x}\log x). \tag{6}$$

In other words, the further left we can banish the zeros of $\zeta(s)$, the better estimates we can get for $\pi(x)$. Unfortunately, the best that is known at the moment is

$$\zeta(s) \neq 0 \quad \text{for all } \Re(s) \geq 1.$$

This was proved independently by Hadamard [18] and de la Vallée-Poussin [33] in 1896, which nevertheless allowed them to prove the Prime Number Theorem, albeit with much weaker error bounds than (6).

5 The Riemann Hypothesis for Function Fields

Let us define a zeta function for the polynomial ring $A = \mathbb{F}_q[T]$. For any $a \in A$ we set $|a| := q^{\deg(a)}$, and then define

$$\zeta_A(s) := \sum_{a \in A,\ a \text{ monic}} \frac{1}{|a|^s}.$$

In fact, since there are q^n monic polynomials of degree n, we see that

$$\zeta_A(s) = \sum_{n=0}^{\infty} q^n \cdot \frac{1}{q^{ns}} = 1 + \frac{q}{q^s} + \frac{q^2}{q^{2s}} + \cdots = \frac{1}{1 - q^{1-s}}, \tag{7}$$

by summing the geometric series. This expression makes sense for all $s \in \mathbb{C},\ s \neq 1$, and we find again a simple pole at $s = 1$. Unique factorisation in A again gives us the Euler product

$$\zeta_A(s) = \prod_P \left(1 - \frac{1}{|P|^s}\right)^{-1} = \prod_{n=1}^{\infty} \left(1 - \frac{1}{q^{ns}}\right)^{-\pi_A(n)}. \tag{8}$$

Combining (7) and (8), it is a simple exercise to deduce that

$$q^n = \sum_{d|n} d\,\pi_A(d),$$

and Möbius Inversion gives us the exact expression

$$\pi_A(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}. \tag{9}$$

Here μ is the *Möbius function*, defined for any integer $n \in \mathbb{Z}$ by

$$\mu(n) := \begin{cases} 1 & \text{if } n \text{ is the product of an even number of distinct prime numbers} \\ -1 & \text{if } n \text{ is the product of an odd number of distinct prime numbers} \\ 0 & \text{if } n \text{ has a repeated prime factor.} \end{cases}$$

The function $\mu(n)$ is highly erratic, but since the highest term in (9) is $\frac{q^n}{n}$, and the next term is no larger than $\frac{q^{n/2}}{n}$, we obtain the following strong form of the Prime Number Theorem for $A = \mathbb{F}_q[T]$:

$$\pi_A(n) = \frac{q^n}{n} + O(\frac{q^{n/2}}{n}), \tag{10}$$

which is even stronger than what we can get for $\mathbb{Z}$ assuming the Riemann Hypothesis.

So what about the Riemann Hypothesis for $\zeta_A(s)$? It is vacuously true, since $\zeta_A(s)$ does not have any zeros!

Does this mean that there is no interesting analogue of the Riemann Hypothesis in the function field world? Far from it, but we will need some more technical definitions (which will not be needed for the rest of this article).

Let K be a global function field, that is a finite extension of $\mathbb{F}_q(T)$. Choose any place ∞ of K, and define the ring

$$A := \{x \in K \mid x \text{ is regular at all places except } \infty\}.$$

This is a Dedekind domain with finite class number, and is a more sophisticated analogue of $\mathbb{Z}$ (or more generally, of the ring of integers in a number field). We can define the zeta function of this ring A by

$$\zeta_A(s) := \sum_{\mathfrak{a} \subset A} \frac{1}{|\mathfrak{a}|^s},$$

where the sum runs over all non-zero ideals $\mathfrak{a} \subset A$ and $|\mathfrak{a}| := \#(A/\mathfrak{a})$. Then $\zeta_A(s)$ again satisfies an Euler product, and it can be shown that it is a rational function of the form

$$\zeta_A(s) = \frac{P_A(q^{-s})}{1 - q^{1-s}},$$

where $P_A(x) \in \mathbb{Z}[x]$ is a polynomial of degree $2g$, where g is the genus of K.

From this one obtains the following exact expression for the prime counting function:

$$\begin{aligned} \pi_A(n) &:= \text{The number of prime ideals } \mathfrak{p} \subset A \text{ of norm } |\mathfrak{p}| = q^n \\ &= \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d} + \frac{1}{n} \sum_{d|n} \mu(d) \left(\sum_{i=1}^{2g} q^{(n/d)\rho_i} \right), \end{aligned} \tag{11}$$

where $\rho_1, \rho_2, \ldots, \rho_{2g}$ are the zeros of $\zeta_A(s)$.

Furthermore, the following analogue of the Riemann-Hypothesis was proved by A. Weil in 1948 [34].

Theorem 3 (Hasse-Weil) *All zeros ρ_i of $\zeta_A(s)$ satisfy $\Re(\rho_i) = \frac{1}{2}$.*

This applied to (11) again gives us

$$\pi_A(n) = \frac{q^n}{n} + O\left(\frac{q^{n/2}}{n}\right).$$

Weil then went on to conjecture a far-reaching generalisation of Theorem 3 to zeta functions associated to higher dimensional varieties. This conjecture was one of the main motivations of A. Grothendieck's foundations of modern Algebraic Geometry, and was eventually proved by P. Deligne in 1974. Grothendieck (1966) and Deligne (1978) were awarded Fields Medals for their work.

6 Lattices in $\mathbb{C}$

Let us now return to the classical world of characteristic 0, and start with something that at first sight appears to be purely Complex Analysis. A *lattice* $\Lambda \subset \mathbb{C}$ is a discrete additive subgroup of $\mathbb{C}$. There are two possibilities, depending on the rank of Λ.

$$\Lambda = \begin{cases} \mathbb{Z}\omega = \{n\omega \mid n \in \mathbb{Z}\} & \text{rank 1 case, or} \\ \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \{m\omega_1 + n\omega_2 \mid m, n \in \mathbb{Z}\} & \text{rank 2 case,} \end{cases}$$

for generators $\omega, \omega_1, \omega_2 \in \mathbb{C}$, where $\omega \neq 0$ and $\{\omega_1, \omega_2\}$ are linearly independent over $\mathbb{R}$.

We are interested in functions f on $\mathbb{C}$ which are periodic with respect to Λ, i.e. for which

$$f(z + \lambda) = f(z), \qquad \text{for all } z \in \mathbb{C} \text{ and } \lambda \in \Lambda.$$

In the rank one case, we find that every Λ-periodic function can be written in the form

$$f(z) = \tilde{f}(e_\Lambda(z)),$$

where $e_\Lambda(z) = e^{2\pi i z/\omega}$ and $\tilde{f}$ is a function on the multiplicative group $\mathbb{C}^* = \mathbb{C} \smallsetminus \{0\}$. If f is meromorphic, then $\tilde{f}$ is given by a suitably convergent Laurent series

$$\tilde{f}(w) = \sum_{n \in \mathbb{Z}} a_n w^n, \qquad a_n \in \mathbb{C},$$

which is just the *Fourier series* of f.

Thus the exponential function $e_\Lambda : \mathbb{C} \longrightarrow \mathbb{C}^*$ is fundamental to the study of periodic functions. It satisfies the functional equation

$$e_\Lambda(nz) = e_\Lambda(z)^n \qquad \text{for all } n \in \mathbb{Z},$$

which we capture in the following commutative diagram with exact rows.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Lambda & \longrightarrow & \mathbb{C} & \xrightarrow{e_\Lambda} & \mathbb{C}^* & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle n} & & \downarrow{\scriptstyle n} & & \downarrow{\scriptstyle [n]} & & \\ 0 & \longrightarrow & \Lambda & \longrightarrow & \mathbb{C} & \xrightarrow{e_\Lambda} & \mathbb{C}^* & \longrightarrow & 1 \end{array} \tag{12}$$

Here the first two vertical arrows represent multiplication by $n \in \mathbb{Z}$ and $[n] : \mathbb{C}^* \to \mathbb{C}^*$ is the homomorphism $x \mapsto x^n$.

The points of order n in $\mathbb{C}^*$ are the nth roots of unity:

$$\mathbb{C}^*[n] = \{w \in \mathbb{C}^* \mid w^n = 1\} = \{e_\Lambda(\lambda/n) \mid \lambda \in \Lambda\} \cong \Lambda/n\Lambda \cong \mathbb{Z}/n\mathbb{Z}$$

and they are of great relevance in Number Theory.

Let $\zeta_n \in \mathbb{C}^*[n]$ be a primitive nth root of unity, that is, a generator of the cyclic group $\mathbb{C}^*[n] \cong \mathbb{Z}/n\mathbb{Z}$. Denote by $\mathbb{Q}(\zeta_n)$ the nth *cyclotomic field*, obtained by adjoining ζ_n to $\mathbb{Q}$. Then $\mathbb{Q}(\zeta_n)$ is a Galois extension of $\mathbb{Q}$; moreover, its Galois group is Abelian, and we have the explicit isomorphism

$$\begin{array}{ccc} (\mathbb{Z}/n\mathbb{Z})^* & \xrightarrow{\sim} & \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \\ m \pmod n & \longmapsto & (\sigma_m : \zeta_n \mapsto \zeta_n^m). \end{array}$$

Moreover, every Abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field:

Theorem 4 (Kronecker-Weber) *Let $K/\mathbb{Q}$ be a finite Abelian extension. Then $K \subset \mathbb{Q}(\zeta_n)$ for some $n \in \mathbb{Z}$.*

7 Elliptic Functions and Elliptic Curves

Let us now consider the case of rank two lattices $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \subset \mathbb{C}$. Meromorphic functions which are periodic with respect to Λ are called *elliptic functions*, and were studied intensively in the 19th century. By Λ-periodicity, an elliptic function f is determined entirely by its behaviour on the *fundamental parallelogram*

$$\{x\omega_1 + y\omega_2 \in \mathbb{C} \mid 0 \leq x, y < 1\}$$

for the lattice, so f defines a function on the quotient $\mathbb{C}/\Lambda$, which is a torus (see Figure 3) – it can be visualised by glueing together opposite pairs of edges of a fundamental parallelogram.

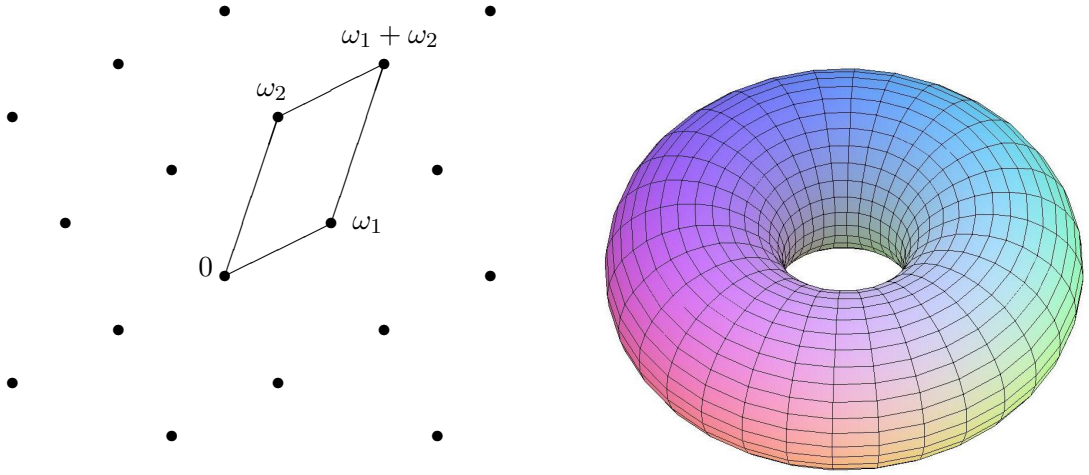

Figure 3: The lattice $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ with fundamental parallelogram (left), and the torus $\mathbb{C}/\Lambda$ (right)

It is easy to show that any non-constant elliptic function must have at least two poles in any fundamental parallelogram of Λ, so the simplest example is the *Weierstrass $\wp$-function*,

$$\wp_\Lambda(z) := \frac{1}{z^2} + \sum_{\lambda \in \Lambda \smallsetminus \{0\}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right),$$

which has a double pole at every point of Λ. A phase plot for $\wp_\Lambda(z)$ is shown in Figure 4.

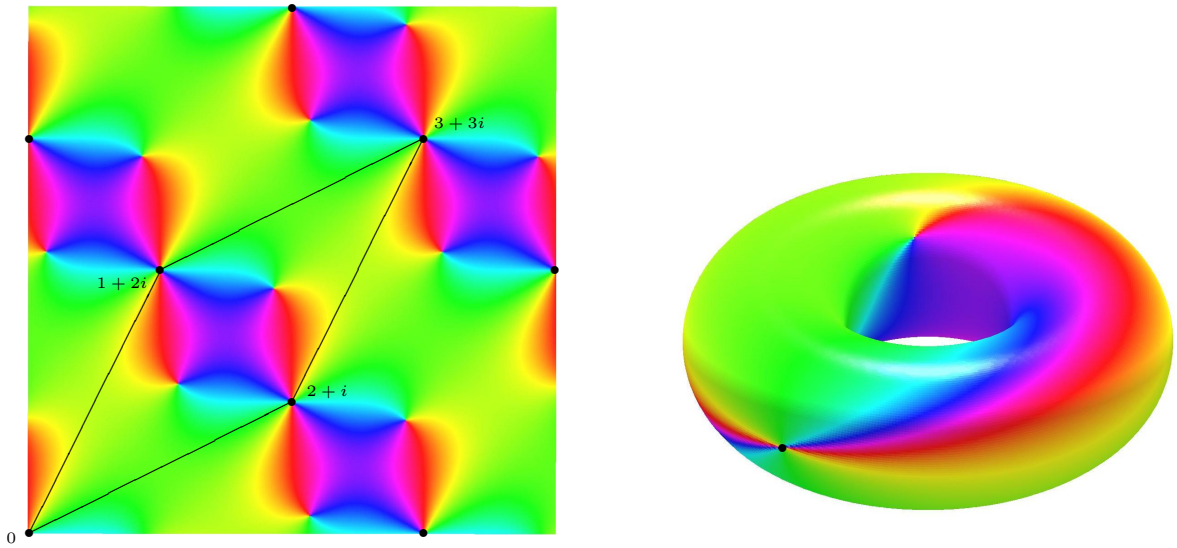

Figure 4: Phase plot of $\wp_\Lambda(z)$ on $\mathbb{C}$ (left) and on the torus $\mathbb{C}/\Lambda$ (right), with $\Lambda = \mathbb{Z}(1+2i)+\mathbb{Z}(2+i)$.

One can show that every elliptic function is a rational combination of $\wp_\Lambda(z)$ and its derivative $\wp'_\Lambda(z)$. Furthermore, these two functions are related by the following differential equation:

$$\wp'_\Lambda(z)^2 = 4\wp_\Lambda(z)^3 - g_2\wp_\Lambda(z) - g_3, \qquad \text{for all } z \in \mathbb{C} \setminus \Lambda \tag{13}$$

where

$$\begin{aligned} g_2 &= 60 \sum_{\lambda\in\Lambda\setminus\{0\}} \frac{1}{\lambda^4} \in \mathbb{C}, \\ g_3 &= 140 \sum_{\lambda\in\Lambda\setminus\{0\}} \frac{1}{\lambda^6} \in \mathbb{C} \end{aligned}$$

and

$$g_2^3 - 27g_3^2 \neq 0.$$

The constants g_2 and g_3 are called *Eisenstein series*, and depend on Λ. They are examples of *modular forms*, themselves very interesting from a number theoretic perspective, but beyond the focus of this article.

The differential equation (13) leads us to define an *Elliptic Curve* E as a projective algebraic curve whose affine equation is

$$E : y^2 = 4x^3 - g_2x - g_3, \tag{14}$$

for constants $g_2, g_3 \in \mathbb{C}$ satisfying $\Delta := g_2^3 - 27g_3^2 \neq 0$. The condition $\Delta \neq 0$ is equivalent to the curve being smooth.

The set of complex-valued points $E(\mathbb{C})$ consists of all solutions $(x, y) \in \mathbb{C}^2$ to (14), as well as one further point $\mathcal{O}$ at infinity. Now it follows from (13) that $E(\mathbb{C})$ is parametrised by $\wp_\Lambda$ and $\wp'_\Lambda$ as follows:

$$\begin{array}{rcl} \mathbb{C}/\Lambda & \xrightarrow{\sim} & E(\mathbb{C}) \\ z \pmod{\Lambda} & \longmapsto & \begin{cases} \big(\wp_\Lambda(z), \wp'_\Lambda(z)\big) & \text{if } z \notin \Lambda \\ \mathcal{O} & \text{if } z \in \Lambda. \end{cases} \end{array}$$

Thus an elliptic curve is isomorphic (as a Riemann surface) to a torus. Since the torus $\mathbb{C}/\Lambda$ is also an Abelian group, $E(\mathbb{C})$ inherits an Abelian group structure as well, with $\mathcal{O}$ as the identity element. Geometrically, this group structure is determined by the condition that for three points $P, Q, R \in E(\mathbb{C})$,

$$P + Q + R = \mathcal{O} \iff P,\ Q \text{ and } R \text{ are collinear;}$$

see Figure 5.

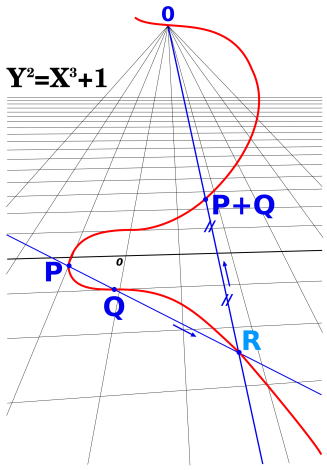

Figure 5: Addition law on an elliptic curve (Image credit: Beao/Wikipedia)

For every $n \in \mathbb{Z}$ we thus obtain a group homomorphism

$$\begin{array}{rcl} [n] : E(\mathbb{C}) & \longrightarrow & E(\mathbb{C}) \\ P & \longmapsto & [n]P := \underbrace{P + P + \cdots + P}_{n}. \end{array}$$

We summarise all this information in the following commutative diagram with exact rows, strongly reminiscent of (12):

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Lambda & \longrightarrow & \mathbb{C} & \xrightarrow{(\wp_\Lambda, \wp'_\Lambda)} & E(\mathbb{C}) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle n} & & \downarrow{\scriptstyle n} & & \downarrow{\scriptstyle [n]} & & \\ 0 & \longrightarrow & \Lambda & \longrightarrow & \mathbb{C} & \xrightarrow{(\wp_\Lambda, \wp'_\Lambda)} & E(\mathbb{C}) & \longrightarrow & 0 \end{array} \tag{15}$$

The right commutative square encodes a family of functional equations for $\wp_\Lambda$ known as *addition laws*; the version for $n = 2$ is

$$\wp_\Lambda(2z) = \frac{1}{4}\left(\frac{\wp''_\Lambda(z)}{\wp'_\Lambda(z)}\right)^2 - 2\wp_\Lambda(z) \qquad \text{if } 2z \notin \Lambda.$$

For any n, the subgroup $E[n]$ of points of order n is isomorphic to $\Lambda/n\Lambda \cong (\mathbb{Z}/n\mathbb{Z})^2$.

8 The Arithmetic of Elliptic Curves

Why are elliptic curves of interest to Number Theorists? We give here a small selection of interesting results.

Let K be a number field, i.e. a finite extension of $\mathbb{Q}$. Suppose E/K is an elliptic curve defined over K, i.e. defined by an equation like (14) with coefficients $g_2, g_3 \in K$. Then the addition law on E is defined by rational expressions with coefficients in K, and so the set $E(K)$ of K-valued points on E is a subgroup of $E(\mathbb{C})$. A fundamental result is the following.

Theorem 5 (Mordell-Weil) *The Abelian group $E(K)$ is finitely generated, i.e. $E(K) \cong E(K)_{\text{tor}} \times \mathbb{Z}^r$, where the torsion subgroup $E(K)_{\text{tor}}$ is finite.*

The integer $r \geq 0$ in the above theorem is called the *rank* of E/K (not to be confused with the rank of the lattice Λ, which is 2), and its behaviour is very mysterious. It is the subject of the *Birch and Swinnerton-Dyer Conjecture*, one of the Clay Millenium Problems, and it is conjectured that there exist elliptic curves over $\mathbb{Q}$ with arbitrarily high rank.

How large can the K-rational torsion subgroup $E(K)_{\text{tor}}$ be? It turns out that there are only finitely many options for each field K.

Theorem 6 (B. Mazur, 1978) *Let E be an elliptic curve over $\mathbb{Q}$. Then $E(\mathbb{Q})_{\text{tor}}$ is isomorphic to one of the following groups.*

$$\begin{array}{ll} \mathbb{Z}/N\mathbb{Z} & \text{where } N = 1, 2, 3, \ldots, 10 \text{ or } 12 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z} & \text{where } N = 1, 2, 3, 4. \end{array}$$

Moreover, all of these groups do occur.

Theorem 7 (L. Merel, 1996) *For every $d \in \mathbb{N}$, there exists a constant $B > 0$, depending only on d, such that, if E is an elliptic curve defined over a number field K of degree $[K : \mathbb{Q}] = d$, then $|E(K)_{\text{tor}}| < B$.*

The above theorem by Merel was known for a long time as the *Uniform Boundedness Conjecture*.

The n-torsion group $E[n]$ is defined over K and is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^2$. Adjoining the coordinates of these points to K gives a Galois extension $K(E[n])$ of K. Since the Galois action respects the $\mathbb{Z}/n\mathbb{Z}$-module structure of $E[n]$, this Galois group is isomorphic to a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$.

How large is this subgroup? That depends on the size of E's endomorphism ring. Since $[n]$ is an endomorphism for every $n \in \mathbb{Z}$, we find that $\mathbb{Z} \subset \mathrm{End}(E)$. Usually, that is all, but sometimes $\mathrm{End}(E)$ is larger and we say that E has complex multiplication (CM). In this case, the Galois action commutes with the additional endomorphisms, which forces $\mathrm{Gal}(K(E[n])/K)$ to be Abelian (and hence much smaller than $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$).

When E does not have complex multiplication, then this Galois group is much larger, and we have the following deep theorem by J.-P. Serre [32].

Theorem 8 (Serre, 1972) *Suppose E/K is an elliptic curve over a number field K, and that E does not have complex multiplication. Then there exists a constant $B > 0$ such that, for every $n \in \mathbb{Z}$, the Galois group of $K(E[n])/K$ is isomorphic to a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ of index at most B.*

As a consequence of Serre's Theorem, we can bound the growth of $E(K)_{\text{tor}}$ as we enlarge the number field K.

Theorem 9 (Breuer, 2010) *Let E/K be an elliptic curve defined over a number field K. Then there exists a constant $C > 0$ such that, for any finite extension L/K,*

$$\#E(L)_{\text{tor}} \leq C([L:K]\log\log[L:K])^{\gamma},$$

where $\gamma = 1$ if E has complex multiplication and $\gamma = \frac{1}{2}$ otherwise.

9 Drinfeld Modules

We now return to the world of function fields, where we wish to find an analogue of the theory of lattices in $\mathbb{C}$ and elliptic curves. First, we need a characteristic p analogue of the field of complex numbers, that is a field which is both complete and algebraically closed.

Starting with the ring $A = \mathbb{F}_q[T]$, we form its quotient field $F := \mathbb{F}_q(T)$ (the analogue of the field $\mathbb{Q}$ of rational numbers). On this field we define the absolute value

$$\left|\frac{f(T)}{g(T)}\right|_{\infty} := q^{\deg(f)-\deg(g)}, \qquad 0 \neq \frac{f(T)}{g(T)} \in F = \mathbb{F}_q(T),$$

and $|0|_{\infty} := 0$. This absolute value satisfies the following properties. For all $x, y \in F$,

1. $|x|_{\infty} = 0 \iff x = 0$,
2. $|xy|_{\infty} = |x|_{\infty}|y|_{\infty}$,
3. $|x+y|_{\infty} \leq \max(|x|_{\infty}, |y|_{\infty})$.

The third property is called the *strong triangle inequality* or *ultrametric inequality*, and it is stronger than the usual triangle inequality $|x+y| \leq |x| + |y|$. As a result, this absolute value induces a very different metric on F than the usual metric does on $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$. For example, in an ultrametric space all triangles are isosceles.

To construct an analogue of the real numbers $\mathbb{R}$, we complete F with respect to this absolute value, obtaining the field $F_{\infty} := \mathbb{F}_q((\frac{1}{T}))$ of formal Laurent series in $\frac{1}{T}$. The absolute value extends to this completion, and is given by $|x|_{\infty} = q^n$, where $n \in \mathbb{Z}$ with

$$x = a_n T^n + a_{n-1}T^{n-1} + \cdots, \qquad a_n \neq 0.$$

The field of complex numbers $\mathbb{C}$ is constructed as the algebraic closure of $\mathbb{R}$, so we take the algebraic closure $\overline{F_{\infty}}$ of F_{∞}. However, in contrast to $[\mathbb{C}:\mathbb{R}] = 2$, we find that $[\overline{F_{\infty}} : F_{\infty}] = \infty$, and as a result $\overline{F_{\infty}}$ is no longer complete. The absolute value extends to $\overline{F_{\infty}}$, and we complete it once more to obtain the field

$$\mathbb{C}_{\infty} := \widehat{\overline{F_{\infty}}},$$

which is both complete and algebraically closed. This is our analogue of the complex numbers, and there exists an entire theory of complex analysis for this field.

Since the function field analogue of $\mathbb{Z}$ is A, our philosophy is to replace $\mathbb{Z}$ by A wherever we can. For example, Abelian groups ($\mathbb{Z}$-modules) become A-modules.

We now define an *A-lattice* $\Lambda \subset \mathbb{C}_\infty$ *of rank* r to be a discrete A-submodule of $\mathbb{C}_\infty$ which is free of rank r. This means that

$$\Lambda = A\omega_1 + A\omega_2 + \cdots + A\omega_r,$$

where $\{\omega_1, \omega_2, \ldots, \omega_r\}$ is linearly independent over F_∞. Since $[\mathbb{C}_\infty : F_\infty] = \infty$, the field $\mathbb{C}_\infty$ has enough "space" to accommodate lattices of arbitrary rank $r \geq 1$, unlike the classical case which only admits lattices of rank 1 or 2.

When characterising the Λ-periodic functions on $\mathbb{C}_\infty$, one finds that these can be expressed in terms of the following *exponential function* associated to Λ:

$$e_\Lambda(z) := z \prod_{0 \neq \lambda \in \Lambda} \left(1 - \frac{z}{\lambda}\right)$$

The function $e_\Lambda : \mathbb{C}_\infty \to \mathbb{C}_\infty$ is *entire* (i.e. is given by an everywhere convergent power series), $\mathbb{F}_q$-linear, Λ-periodic, surjective and has simple zeros at every point of Λ and no other zeros. When Λ has rank 1 then e_Λ is the analogue of the usual exponential function, and when Λ has rank 2, it plays the role of the Weierstrass $\wp$-function.

We again encode the properties of e_Λ into a commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Lambda & \longrightarrow & \mathbb{C}_\infty & \xrightarrow{e_\Lambda} & \mathbb{C}_\infty & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle \phi_a} & & \\ 0 & \longrightarrow & \Lambda & \longrightarrow & \mathbb{C}_\infty & \xrightarrow{e_\Lambda} & \mathbb{C}_\infty & \longrightarrow & 0 \end{array} \tag{16}$$

Here for every $a \in A$ the first two vertical arrows represent multiplication by a. The right commutative square encodes the functional equation

$$e_\Lambda(az) = \phi_z(e_\Lambda(z)),$$

where

$$\phi_a(x) = \sum_{i=0}^{r \deg(a)} a_i x^{q^i}, \qquad a_i \in \mathbb{C}_\infty,\ a_{r\deg(a)} \neq 0$$

is an $\mathbb{F}_q$-linear polynomial of degree $q^{r\deg(a)} = |a|^r$.

The field $\mathbb{C}_\infty$ is automatically an A-module, since $A \subset \mathbb{C}_\infty$. However, it follows from (16) that ϕ induces a new A-module structure on $\mathbb{C}_\infty$, defined by

$$a \cdot z := \phi_a(z), \qquad z \in \mathbb{C}_\infty,\ a \in A.$$

This new A-module structure on $\mathbb{C}_\infty$ is called a *Drinfeld module* of rank r. Moreover, the submodule of a-division points is the A-module

$$\phi[a] := \{z \in \mathbb{C}_\infty \mid \phi_a(z) = 0\} = \{e_\Lambda(\lambda/a) \mid \lambda \in \Lambda\} \cong \Lambda/a\Lambda \cong (A/aA)^r,$$

which further cements the analogy with roots of unity (if $r = 1$) and elliptic curves (if $r = 2$).

Motivated by this, we define Drinfeld modules more generally as follows.

Let K be a field containing A. Denote by $\tau : x \mapsto x^q$ the q-Frobenius map. We denote by $K\{\tau\}$ the non-commutative ring of polynomials in τ with coefficients in K, subject to the

commutation relation $\tau a = a^q \tau$ for every $a \in K$. Equivalently, we can regard $K\{\tau\}$ as the ring of all polynomials of the form $\sum_{i=0}^{n} a_i x^{q^i}$ under point-wise addition and composition.

Then a *Drinfeld module* of rank r over K is a ring homomorphism

$$\begin{aligned} \phi : A &\longrightarrow K\{\tau\} \\ a &\longmapsto \phi_a = \sum_{i=0}^{r\deg(a)} a_i \tau^i, \end{aligned}$$

satsifying the conditions

1. $a_0 = a$, and
2. $a_{r\deg(a)} \neq 0$.

For $a \in A$, we define the A-module of a-division points on ϕ by

$$\phi[a] := \{x \in \overline{K} \mid \phi_a(x) = 0\};$$

it is isomorphic to $(A/aA)^r$.

Since $A = \mathbb{F}_q[T]$ is generated by T, a Drinfeld module ϕ is completely determined by

$$\phi_T = T + g_1\tau + \cdots + g_r\tau^r, \qquad g_i \in K,\ g_r \neq 0.$$

We note that the construction of ϕ associated to a lattice $\Lambda \subset \mathbb{C}_\infty$ of rank r indeed defines a Drinfeld module over the field $\mathbb{C}_\infty$ of rank r. Conversely, it can be shown that every Drinfeld module over $\mathbb{C}_\infty$ can be obtained this way.

The coefficients $g_1, g_2, \ldots, g_r$ depend on Λ and are examples of Drinfeld modular forms.

Drinfeld modules were introduced by V.G. Drinfeld [14] in 1974 as a tool for studying the Langlands correspondence for GL_2 over a function field. He was awarded a Fields Medal in 1990.

10 The Arithmetic of Drinfeld Modules

Let us start with the rank 1 case. Consider the Drinfeld module ϕ over $F = \mathbb{F}_q(T)$ defined by $\phi_T = T + \tau$; it is known as the *Carlitz module* and was already studied by L. Carlitz [12] in the 1930s. It corresponds to a rank 1 lattice of the form $A\varpi$, where $\varpi \in \mathbb{C}_\infty$ is transcendental over F; it is the analogue of $2\pi i \in \mathbb{C}$. Let $a \in A$, then the module of a-division points $\phi[a]$ is isomorphic to A/aA and, like the case of roots of unity, one can show that the field $F(\zeta_a)$, obtained by adjoining to F a generator ζ_a of $\phi[a]$, is Galois over F and its Galois group is canonically isomorphic to $(A/aA)^*$. Furthermore, we have an analogue of the Kronecker-Weber Theorem, due to D. Hayes [19], which states that every Abelian extension of F is contained in a field obtained by adjoining to F division points of the Carlitz module, elements of the algebraic closure $\bar{\mathbb{F}}_q$ of $\mathbb{F}_q$, and $(1/T)^n$-division points of the Carlitz module associated to the ring $\mathbb{F}_q[1/T]$.

Now consider the case of general rank $r \geq 1$.

Let K be a finite extension of $F = \mathbb{F}_q(T)$, and let ϕ be a rank r Drinfeld module over K. Do we have an analogue of the Mordell-Weil Theorem? Well, almost.

Theorem 10 (B. Poonen, 1995) *The A-module structure defined on K by a Drinfeld module is isomorphic to $\phi(K)_{\text{tor}} \times A^{\aleph_0}$, where $\phi(K)_{\text{tor}}$ is finite and $A^{\aleph_0}$ denotes the product of a countably infinite number of copies of A.*

The finite torsion module $\phi(K)_{\text{tor}}$ is an interesting object of study. The analogue of Merel's Theorem is still unsolved for rank $r > 1$.

Uniform Boundedness Conjecture. *For all integers $r, d \geq 1$, there exists a constant $B > 0$ such that $\#\phi(K)_{\text{tor}} \leq B$ for every Drinfeld module ϕ of rank r defined over a field K of degree $[K : F] = d$.*

In the case $r = 1$, this conjecture was proved by Poonen [28], and the case of $r = 2$ and $A = \mathbb{F}_2[T]$ was solved by A. Pál [25].

The field obtained by adjoining all of $\phi[a]$ to K is again Galois over K, and analogously to the elliptic curve case, its Galois group is isomorphic to a subgroup of $\mathrm{GL}_r(A/aA)$. In this case, the analogue of Serre's Theorem was proved by R. Pink and E. Rütsche [26].

Theorem 11 (Pink-Rütsche, 2009) *Let ϕ be a Drinfeld module defined over a finitely generated extension K of F, and suppose that $\mathrm{End}(\phi) = A$. Then there exists a constant $B > 0$ such that for every $a \in A$, $\mathrm{Gal}(K(\phi[a])/K)$ is isomorphic to a subgroup of $\mathrm{GL}_r(A/aA)$ of index at most B.*

As in the elliptic curve case, this allows us to bound the growth of the torsion module of a Drinfeld module.

Theorem 12 (Breuer, 2010) *Let ϕ be a Drinfeld module of rank r over a finitely generated extension K of F. Then there exists a constant $C > 0$ such that, for every finite extension L/K,*

$$\#\phi(L)_{\text{tor}} \leq C([L : K] \log\log[L : K])^{\gamma},$$

where $\gamma = [\mathrm{End}(\phi) : A]/r$.

Lastly, let $r > 1$ and let $K = \mathbb{F}_q(T, g_1, g_2, \ldots, g_{r-1})$, where $g_1, g_2, \ldots, g_{r-1}$ are algebraically independent over $\mathbb{F}_q(T)$. Consider the rank r Drinfeld module defined over K by

$$\phi_T = T + g_1\tau + \cdots + g_{r-1}\tau^{r-1} + \tau^r.$$

Up to isomorphism, every rank r Drinfeld module can be obtained from ϕ by substituting suitable values for the g_i's, so we call ϕ a *generic* Drinfeld module. For this particular Drinfeld module we obtain the following result, which was conjectured by S.S. Abhyankar [1].

Theorem 13 (Breuer, 2013) *For every $a \in A$, we have $\mathrm{Gal}(K(\phi[a]/K) \cong \mathrm{GL}_r(A/aA)$.*

11 The André-Oort Conjecture

Safely back in the Number Fields world, I want to touch upon one more theme, one which has been a focus of my own research: the concepts surrounding the André-Oort Conjecture.

We start with some definitions. Let E_1 and E_2 be two complex elliptic curves associated to the lattices Λ_1 and Λ_2, respectively. An *isogeny* $f : E_1 \to E_2$ is a morphism of algebraic

curves which maps the identity of E_1 to the identity of E_2. In terms of complex tori, it is induced by a map

$$\begin{array}{rcl} f : \mathbb{C}/\Lambda_1 & \longrightarrow & \mathbb{C}/\Lambda_2 \\ z \pmod{\Lambda_1} & \longmapsto & cz \pmod{\Lambda_2}, \end{array}$$

where $c \in \mathbb{C}$ with $c\Lambda_1 \subset \Lambda_2$. Its kernel is $\ker f = c^{-1}\Lambda_2/\Lambda_1$ and its *degree* is $\deg(f) = \#\ker f$.

An isomorphism $f : E_1 \to E_2$ is an isogeny with $\ker f = \{0\}$.

Suppose the elliptic curve E is defined by the affine equation

$$E : y^2 = 4x^3 - g_2 x - g_3, \qquad g_2, g_3 \in \mathbb{C},\ \Delta := g_2^3 - 27g_3^2 \neq 0.$$

Then its *j-invariant* is defined by

$$j(E) := \frac{1728\ g_2^3}{\Delta}$$

and two elliptic curves E_1 and E_2 are isomorphic if and only if their j-invariants are equal. Moreover, for every $j \in \mathbb{C}$, there exists an elliptic curve E with $j(E) = j$. Thus the complex plane $\mathbb{C}$ is a moduli space for elliptic curves.

More generally, the j-invariants of two isogenous elliptic curves are related in the following sense.

Theorem 14 *For every integer $N \geq 1$ there exists a polynomial $\Phi_N(X, Y) \in \mathbb{Z}[X, Y]$ with the following properties.*

1. *$\Phi_N(X, Y)$ is irreducible in $\mathbb{C}[X, Y]$.*
2. *$\Phi_N(X, Y) = \Phi_N(Y, X)$.*
3. *If P is a prime number, then $\Phi_P(X, Y) \equiv (X^P - Y)(X - Y^P) \bmod P$.*
4. *$\Phi_N(j(E_1), j(E_2)) = 0$ if and only if there exists an isogeny $E_1 \to E_2$ with kernel ismorphic to $\mathbb{Z}/n\mathbb{Z}$.*

This polynomial $\Phi_N(X, Y)$ is called the Nth *modular polynomial*.

We see that the ring of endomorphisms of an elliptic curve E associated to a lattice Λ is

$$\mathrm{End}(E) = \{c \in \mathbb{C} \mid c\Lambda \subset \Lambda\},$$

and it is not hard to show that when E has complex multiplication (CM), i.e. $\mathbb{Z} \subsetneq \mathrm{End}(E)$, then $\mathrm{End}(E)$ is an order in a quadratic imaginary field.

The j-invariant of a CM elliptic curve has interesting Number Theoretic properties.

Theorem 15 *Let E be an elliptic curve with complex multiplication by an order $R = \mathrm{End}(E)$ in the quadratic imaginary field K. Then*

1. *$j(E)$ is an algebraic integer,*
2. *$K(j(E))$ is the* ring class field *of R, i.e. $K(j(E))/K$ is an Abelian extension of K, with Galois group isomorphic to the generalised ideal class group* $\mathrm{Pic}(R)$ *of R.*

Moreover, given a quadratic imaginary field K, then every Abelian extension of K can be obtained by adjoining the j-invariants and torsion points of elliptic curves with complex multiplication by orders in K. This is a generalisation of the Kronecker-Weber Theorem, and is generally known as *Kronecker's Jugendtraum*.

So CM j-invariants are very interesting numbers. One may ask about the distribution of CM-valued points on algebraic varieties, and this leads to the André-Oort Conjecture, the precise statement of which is beyond the scope of this survey. We can, however, show one very interesting special case. A point $(x, y) \in \mathbb{C}^2$ is called a *CM point* if both x and y are j-invariants of CM elliptic curves.

Theorem 16 (S.J. Edixhoven, Y. André, 1995) *Let $X \subset \mathbb{C}^2$ be an irreducible algebraic curve. Then X contains infinitely many CM points if and only if*

1. *X is a horizontal or vertical line with CM constant coordinate, or*
2. *X is the locus of $\Phi_N(X, Y) = 0$ for some $N \in \mathbb{Z}$.*

This theorem was first proved by Edixhoven [15], assuming the Generalized Riemann Hypothesis for quadratic imaginary fields, and then unconditionally by André [2] using methods from Diophantine approximation.

This theorem can also be made effective:

Theorem 17 (F. Breuer, L. Kühne) *Let d_1, d_2 and m be positive integers. Then there exists a constant B such that the following holds. Let $X \subset \mathbb{C}^2$ be an irreducible algebraic curve of degree d_1 and d_2 in the two coordinates and defined over a number field K of degree $[K : \mathbb{Q}] = m$. Suppose that X is not one of the two types given in Theorem 16. Then any CM point on X has height at most B.*

The *height* of a point is a measure of its complexity. We will not give its precise definition here, but we note that there are only finitely many points of height below any given bound.

I first proved Theorem 17 in 2001 assuming the Generalized Riemann Hypothesis for quadratic imaginary fields [4]. In a recent breakthrough, Kühne found an unconditional proof [22].

12 The André-Oort Conjecture for Drinfeld modules

Finally, we will have a look at the Function Field analogues of the concepts presented in the previous section.

Let ϕ and ψ be two Drinfeld modules. Then a *morphism* $f : \phi \to \psi$ is an element $f \in \mathbb{C}\{\tau\}$ such that

$$f\phi_a = \psi_a f, \qquad \text{for all } a \in A.$$

A non-zero morphism is called an *isogeny*, and can only exist if ϕ and ψ have the same rank.

An isomorphism is an isogeny with trivial kernel, i.e. an element $f \in \mathbb{C}_\infty$ with

$$f\phi_a f^{-1} = \psi_a, \qquad \text{for all } a \in A.$$

Suppose now that ϕ is a Drinfeld module of rank $r = 2$, then ϕ is determined by

$$\phi_T = T + g\tau + \Delta\tau^2, \qquad g, \Delta \in \mathbb{C}_\infty,\ \Delta \neq 0.$$

We define its *j-invariant* by

$$j(\phi) := \frac{g^{q+1}}{\Delta}.$$

As in the case of elliptic curves, two Drinfeld modules are isomorphic if and only if they have the same j-invariant. Furthermore, for every $j \in \mathbb{C}_\infty$ there exists a Drinfeld module ϕ with $j(\phi) = j$, and so $\mathbb{C}_\infty$ is a moduli space for rank 2 Drinfeld modules.

We also have an analogue of modular polynomials, due to S. Bae [3].

Theorem 18 *For every monic $N \in A$ there exists a polynomial $\Phi_N(X, Y) \in A[X, Y]$ with the following properties.*

1. *$\Phi_N(X, Y)$ is irreducible in $\mathbb{C}_\infty[X, Y]$.*
2. *$\Phi_N(X, Y) = \Phi_N(Y, X)$.*
3. *If $P \in A$ is prime, then $\Phi_P(X, Y) \equiv (X^{|P|} - Y)(X - Y^{|P|}) \bmod P$.*
4. *There exists an isogeny $\phi \to \psi$ of rank 2 Drinfeld modules with kernel isomorphic to A/NA if and only if $\Phi_N(j(\phi), j(\psi)) = 0$.*

A generalisation of Theorem 18 to higher rank can be found in my joint work with H.-G. Rück [10, 11].

The endomorphism ring of a Drinfeld module ϕ is

$$\mathrm{End}(\phi) := \{f \in \mathbb{C}_\infty\{\tau\} \mid f\phi_a = \phi_a f,\ \forall a \in A\},$$

which is in fact the centraliser of ϕ_A in $\mathbb{C}_\infty\{\tau\}$. Once again, one can show (by considering the lattice in $\mathbb{C}_\infty$ corresponding to ϕ) that $\mathrm{End}(\phi)$ is an order in an extension $K/\mathbb{F}_q(T)$ of degree dividing r, and in which the absolute value $|\cdot|_\infty$ extends to a unique absolute value in K (this is called an *imaginary* extension). When this degree is r, i.e. when $\mathrm{End}(\phi)$ is as large as possible, we say that ϕ has *complex multiplication* (CM).

Adjoining the isomorphism invariants (of which there are several if $r > 2$, see [29] for a definition) of a CM Drinfeld module ϕ to K again produces the ring class field associated to $\mathrm{End}(\phi)$. Moreover, every Abelian extension of a global function field can be obtained by adjoining invariants and torsion points of CM Drinfeld modules, so an analogue of Kronecker's Jugendtraum is true in this case, too.

The following analogue of Theorem 16 was the subject of my Ph.D. thesis, and appeared in [5]. A point $(x, y) \in \mathbb{C}_\infty^2$ is called a *CM point* if both x and y are j-invariants of rank 2 Drinfeld modules with CM.

Theorem 19 (Breuer, 2002) *Suppose that q is odd. Let $X \subset \mathbb{C}_\infty^2$ be an irreducible algebraic curve. Then X contains infinitely many CM points if and only if*

1. *X is a horizontal or vertical line with CM constant coordinate, or*
2. *X is the locus of $\Phi_N(X, Y) = 0$ for some $N \in A$.*

Furthermore, given positive integers d_1, d_2, m, there exists a constant $B > 0$ with the following property. Suppose that $X \subset \mathbb{C}_\infty^2$ is an irreducible algebraic curve of degree d_1 and d_2 in the two coordinates and defined over a field K of degree $[K : \mathbb{F}_q(T)] = m$. If X is not of the form (1) or (2) above, then any CM point on X has height at most B.

Theorem 19 was generalised to more general rings A (still of odd characteristic) in [6], and in [21] my Ph.D. student A. Karumbidza proved a generalisation of Theorem 19 to Drinfeld modules of rank 3 (so $\mathbb{C}_\infty^2$ is replaced by the product of two Drinfeld modular surfaces).

In 2003 I made the following conjecture which was the main focus of my research during the following decade.

Conjecture 20 (André-Oort Conjecture for Drinfeld modular varieties) *Let X be an irreducible subvariety of a moduli space of rank r Drinfeld modules. Then $X(\mathbb{C}_\infty)$ contains a Zariski-dense set of CM points if and only if X is a locus of Drinfeld modules with additional endomorphisms.*

I succeeded in proving this conjecture in the cases where X is a curve, and when X is any subvariety containing a Zariski-dense set of CM points which all lie in one Hecke orbit, see [8]. More recently, P. Hubschmid [20] succeeded in proving Conjecture 20 in almost full generality.

13 Concluding remarks

I hope that the reader has enjoyed this brief journey to some of the sights of Number Theory, and can appreciate the astonishing similarities between Number Fields and Function Fields. It is indeed a magic mirror from which the reflection of classical Number Theory gazes back at us, familiar, yet subtly different.

If the reader wishes to see more, and in more depth, I strongly recommend the excellent book [31] by M. Rosen.

References

[1] S.S. Abhyankar, Resolution of singularities and modular Galois theory. *Bull. Amer. Math. Soc. (N.S.)* **38** (2001), no. 2, 131–169.

[2] Y. André, Finitude des couples d'invariants modulaires singuliers sur une courbe algébrique plane non modulaire. *J. reine angew. Math.* **505** (1998), 203–208.

[3] S. Bae, On the modular equation for Drinfeld modules of rank 2. *J. Number Theory* **42** (1992), 123–133.

[4] F. Breuer, Heights of CM points on complex affine curves. *Ramanujan J.* **5** (2001), no. 3, 311–317.

[5] F. Breuer, The André-Oort conjecture for products of Drinfeld modular curves. *J. reine angew. Math.* **579** (2005), 115–144.

[6] F. Breuer, CM points on products of Drinfeld modular curves. *Trans. Amer. Math. Soc.* **359** (2007), 1351–1374.

[7] F. Breuer, Torsion bounds for elliptic curves and Drinfeld modules. *J. Number Theory* **130** (2010), 1241–1250.

[8] F. Breuer, Special subvarieties of Drinfeld modular varieties. *J. reine angew. Math.* **668** (2012), 35–57.

[9] F. Breuer, Galois groups associated to generic Drinfeld modules and a conjecture of Abhyankar. Manuscript, 2013.

[10] F. Breuer and H.-G. Rück, Drinfeld modular polynomials in higher rank. *J. Number Theory* **129** (2009), 59–83.

[11] F. Breuer and H.-G. Rück, Drinfeld modular polynomials in higher rank II. Manuscript, 2012.

[12] L. Carlitz, A class of polynomials. *Trans. Amer. Math. Soc.* **43** (1938), no. 2, 167–182.

[13] P. Deligne, La conjecture de Weil. I, *Publ. Math. I.H.É.S.* **43** (1974) 273–307

[14] V.G, Drinfeld, Elliptic modules (Russian). *Math. Sbornik* **94** (1974), 594–627. Translated in *Math. USSR. S.* **23** (1974), 561–592.

[15] S.J. Edixhoven, Special points on the product of two modular curves. *Compositio Math.* **114** (1998), 315–328.

[16] H.M. Edwards, *Riemann's Zeta Function*, Academic Press, New York, 1974. Reprinted by Dover, New York, 2001.

[17] Euclid, *The Elements, Book IX*.

[18] J. Hadamard, Sur la distribution des zeros de la fonction $\zeta(s)$ et ses consequences arithmétiques. *Bull. Soc. Math. France* **24** (1896), 199–220.

[19] D.R. Hayes, Explicit class field theory for rational function fields. *Trans. Amer. Math. Soc.* **189** (1974), 77–91.

[20] P. Hubschmid, The André-Oort Conjecture for Drinfeld modular varieties. *Compositio Math.* **149** (2013), no. 4, 507–567.

[21] A.C. Karumbidza, *An analogue of the André-Oort Conjecture for products of Drinfeld modular surfaces.* Ph.D. thesis, Stellenbosch University, March 2013.

[22] L. Kühne, An effective result of Andr-Oort type. *Ann. of Math.* (2) **176** (2012), no. 1, 651–671.

[23] B. Mazur, Modular curves and the Eisenstein ideal. *Inst. Hautes tudes Sci. Publ. Math.* **47** (1977), 33–186.

[24] L. Merel, Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.* **124** (1996), no. 1-3, 437–449.

[25] A. Pál, On the torsion of Drinfeld modules of rank two. *J. reine angew. Math.* **640** (2010), 1–45.

[26] R. Pink and E. Rütsche, Adelic openness for Drinfeld modules in generic characteristic. *J. Number Theory* **129** (2009), no. 4, 882–907.

[27] B. Poonen, Local height functions and the Mordell-Weil theorem for Drinfeld modules. *Compositio Math.* **97** (1995), no. 3, 349–368.

[28] B. Poonen, Torsion in rank 1 Drinfeld modules and the uniform boundedness conjecture. *Math. Ann.* **308** (1997), no. 4, 571–586.

[29] I.Y. Potemine, Minimal terminal $\mathbb{Q}$-factorial models of Drinfeld coarse moduli schemes. *Math. Phys. Anal. Geom.* **1** (1998), 171–191.

[30] G.F.B. Riemann, Über die Anzahl der Primzahlen unter einer gegebenen Grösse. *Gesammelte Werke*, Teubner, Leipzig, 1892. An English translation is found in [16].

[31] M. Rosen, *Number Theory in Function Fields,* Graduate Texts in Mathematics **210**, Springer-Verlag, New York, 2002.

[32] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.* **15** (1972), 259–331.

[33] C.J. de la Vallée-Poussin, Sur la fonction $\zeta(s)$ de Riemann et le nombre des nombres premiers inférieurs a une limite donnée. *Mém. Courronnés et Autres Mém. Publ. Acad. Roy. Sci., des Lettres Beaux-Arts Belg.* **59** (1899-1900), 1–74.

[34] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent,* Hermann, Paris, 1948.