Sums Over Lattices: The Basics of the Weierstrass Function

by Gerardo Con Diaz

Harvard University

Freshman Seminar 24g: Fermat's Last Theorem
January 22, 2004

Introduction

Lattices are, put simply, sets of points on a euclidean space arranged in a grid-like structure. Their study has been of great importance to the study of elliptic curves, one of the major recent research interests for number theorists. The study of lattices leads to the study of the functions defined over them.

The object of this paper is to give a basic introduction to one of these functions, the Weierstrass $\wp$ function, and exhibit some of its more basic characteristics at a less technical level than the one used by standard texts on elliptic curves. It assumes little or no background in algebra and complex analysis and is aimed to the beginning mathematics student or the curious reader. To provide this introduction, we will begin by setting the basic theorems of algebra needed to study lattices. Then we will deduce some very interesting relations between lattices and n-dimensional toruses and we will conclude by introducing the Weierstrass function and describing its basic properties.

Algebraic Background

To understand the way lattices are structured, it is useful to apply some algebraic tools. Perhaps the most fundamental of all of them is the group, a set that works just like the real positive numbers in the sense that it has a form of multiplication operation, an identity and inverses. Formalized, this last statement reads:

Definition 1. *A group is a set G with an associative composition law $\cdot$, an identity element $e \in G$ and such that every element in G has an inverse.*

In other words, a group is a set $G, \text{an element}\, e \in G$ and an operation $\cdot$ such that for all $a, b, c \in G$,

- $a \cdot b \in G$
- $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- $e \cdot a = a \cdot e = a$

and such that for each $a \in G$, there is an $i \in G$ such that $a \cdot i = i \cdot a = a$.

To understand how groups work, we must first understand how their major elements work. As we can expect from the analogy with the positive real numbers, the identity is unique and the inverse of a given element is unique, too. This is what the following propositions say:

Proposition 2. *The identity e of a group G is unique.*

Proof:

If e and e' are both identities of G, then we have $e = e e' = e' e = e'$. □

Proposition 3. *The inverse of an element is unique.*

Proof:

If i and i' are both inverses of a, then $i = i a = i(a i') = (i a) i' = i'$.□

Since inverses are unique, then for a given $a \in G$, we will denote its inverse by a^{-1}. The following proposition works as a cancellation law for group operations. It is interesting how this property is preserved even if our elements are abstractions:

Proposition 4. *If a, b, c are elements of a group G and $a b = a c$, then $b = c$.*

Proof:

If $a b = a c \text{then}\, a^{-1} a b = a^{-1} a c$, and thus $b = c$. □

In addition, sometimes we might have groups within other groups. When this happens, we say that we have a subgroup:

Definition 5. *A subset H of a group G is called a subgroup of G if it satisfies the following:*

- *For all $a, b \in H$, $a \cdot b \in H$*
- *$e \in H$*
- *If $a \in H, \text{then}\, a^{-1} \in H$.*

Before we move on, we need another definition. Notice that in the definition of group, we did not require that the elements commute (this is, that $a \cdot b = b \cdot a$ for all $a, b \in G$). When this happens, the group has a special name:

Definition 6. *A group G is called abelian if all its elements commute with each other.*

Perhaps the most simple group to imagine is the group of the positive real numbers under multiplication. The number 1 would be the identity and the inverses would be taken as the regular multiplicative inverses. However, more delicate groups arise in mathematics, and we will see some of them in later sections.

While studying groups, sometimes it is useful to relate them through functions that preserve their structure. What this last statement means is that it is useful to study functions that do not alter the way we "multiply." This idea is formalized through the concept of homomorphism that we give in the following definition:

Definition 7. *Let G and G' be two groups. A function $f: G \to G'$ is called a homomorphism if*

$$f(a \cdot b) = f(a) \cdot f(b),$$

where the first composition happens in G and the second one in G'.

Notice that the multiplication in G and G' need not be the same. We will see in a later example, a case in which the multiplication in G is addition of integers and multiplication in G' is complex number multiplication.

This definition gives us the idea that a homomorphism is a function that preserves the most fundamental elements of a group. As a matter of fact, the following proposition shows us that this is true:

Proposition 8. *A homomorphism $f: G \to G'$ maps the identity of G to the identity of G', and $f(a^{-1}) = f(a)^{-1}$.*

Proof:

Let e_G and $e_{G'}$ be the identities of G and G' respectively. Then

$$f(e_G) = f(e_G \cdot e_{G'}) = f(e_G) \cdot f(e_G)$$

and thus $f(e_G) = e_{G'}$. Thus,

$$e_{G'} = f(a \cdot a^{-1}) = f(a) \cdot f(a^{-1})$$

and so $f(a^{-1}) = f(a)^{-1}$. □

The preservation of group structure given by a homorphism can provide more control if the map is bijective:

Definition 9. *A bijective homomorphism is called an isomorphism. Furthermore, if there is an isomorphism between two groups, these groups are said to be isomorphic.*

Thus, isomorphisms preserve more than just basic structure. As the following example will show, they also preserve the "shape":

Example 10. Fix $a \in \mathbb{C}$ such that $|a| > 1$ and define $G = \{..., a^{-3}, a^{-2}, a^{-1}, 1, a, a^2, a^3, ...\}$. Then the map

$$f: \mathbb{Z} \to G$$

$$f(i) \longmapsto a^i$$

is a homomorphism:

$$f(m+n) = a^{m+n} = a^n a^m = f(m) f(n).$$

Furthermore, notice that f is clearly surjective and since the norm of a is more than 1, then the map is injective since all the elements in G have different norms. This proves that f is an isomorphism. □

An important result that the following theorem will address is particularly important. It basically states that given a homomorphism between groups, there is a way to construct an isomorphism:

Theorem 11. *Let $f\colon G \rightarrow G'$ be a homomorphism, and define $H = \{x \in G |\ f(x) = e_{G'}\}$. If we define the quotient group $G/H := \{a \cdot h | a \in G, h \in H\}$, then G/H and $f(G)$ are isomorphic.*

Proof:

This theorem is a re-statement of the first isomorphism theorem. We will not prove this theorem here, but a very well-done proof is in Artin's Algebra listed in the bibliography. □

This last theorem is particularly powerful. It allows to contruct an isomorphism given any homomorphism! This construction will be the aim of the next section, when we will see that the quotient of $\mathbb{R}^n$ and a lattice is isomoprhic to an n-dimensional torus.

We will conclude this section by sketching some properties of euclidean spaces and giving some important definitions. Let's examine $\mathbb{R}^n$, a group of special importance to our paper. An important concept arises in the study of sets like $\mathbb{R}^n$. For our practical porpuses, we will study it with a lower level of generality than usual, since our exposition does not require more:

Definition 12. *If $m \leq n$, a list of m vectors $\{l_1, l_2, ..., l_m\} \in \mathbb{R}^n$ is called linearly independent if*

$$\sum_{i=1}^{m} a_i l_i = 0 \Rightarrow a_i = 0 \,\text{for all}\, i \in \{1, 2, ..., m\}.$$

Definition 13. *A list $L = \{l_1, ..., l_m\}$ of n linearly independent vectors in $\mathbb{R}^n$ is called a basis of $\mathbb{R}^n$. The elements of L are then called a basis of $\mathbb{R}^n$ and the list is said to span $\mathbb{R}^n$.*

This choice of names becomes clear with the following theorem:

Theorem 14. *Under the notation above, for any $x \in \mathbb{R}^n$, there exist unique constants $a_1, ..., a_n$ such that*

$$x = \sum_{i=1}^{n} a_i l$$

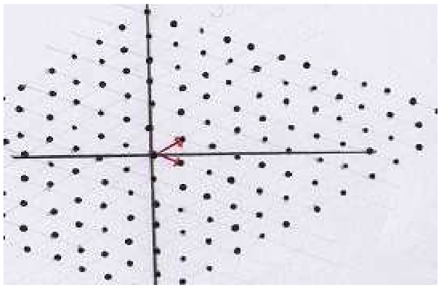
Proof:

This will be admitted without proof to avoid being distracted from the objective of the paper. To see a very clean, well presented proof, see Axler's book Linear Algebra Done Right. □

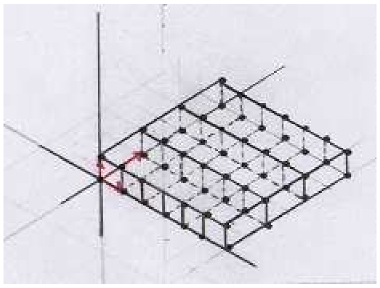
Lattices

We will now introduce the concept of a lattice. Informally, the lattices are the points that define a regular, not necessarily rectangular grid in $\mathbb{R}^n$.

For example, a two dimensional lattice is similar to the following:



And a three-dimensional lattice looks somewhat like this:



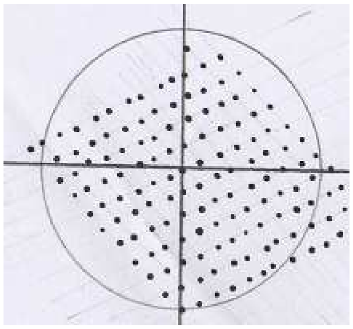
However, a one dimensional lattice in $\mathbb{R}$ is a set of even points on the line as the next diagram shows:

Notice the colored vectors in each lattice. They are called its generators. The following definition formalizes this:

Definition 15. *Let $l_1, ..., l_n$ be n linearly independent vectors in $\mathbb{R}^n$. An n-dimensional lattice $\mathcal{L}$ is the set of all linear combinations of the form*

$$\sum_{i=1}^{n} a_i l_i, \text{where}\, a_i \in \mathbb{Z}\, \text{for all}\, i.$$

In other words, given two vectors, you add and substract them in all possible ways and the endpoints of each of the resulting vectors gives you a lattice. The even distribution of the lattice over n-dimensional space is partly described by saying that the intersection of the lattice and any ball centered at the origin is a finite set and that it partitions $\mathbb{R}^n$ into a set of disjoint subsets, as the following drawing shows:



We will now prove these properties:

Proposition 16. *An n-dimensional lattice in $\mathbb{R}^n$ is discrete.*

Proof:

Let $B_r(0)=\{v\in\mathbb{R}^n\,|\,|v|\le r\}$ be an n-dimensional ball of radius r centered at the origin. Let $l_1,l_2,\ldots,l_n$ be the generators of a lattice $\mathcal{L}$. Since the l_i are linearly independent and there is n of them, $\mathbb{R}^n$ is spanned by the generators of $\mathcal{L}$.

Now, for a given $v\in\mathbb{R}$, write $v=\lambda_1 l_1+\ldots+\lambda_n l_n$ and define a function $f\colon\mathbb{R}^n\to\mathbb{R}^n$ such that

$$f(v)=(\lambda_1,\ldots,\lambda_n).$$

It follows that $f(B_r(0))$ is a bounded subset of $\mathbb{R}^n$, so there exists some positive K such that

$$|f(v)|\le K.$$

Hence, for each $v=\lambda_1 l_1+\ldots+\lambda_n l_n\in B_r(0)\bigcap\mathcal{L}$, we have

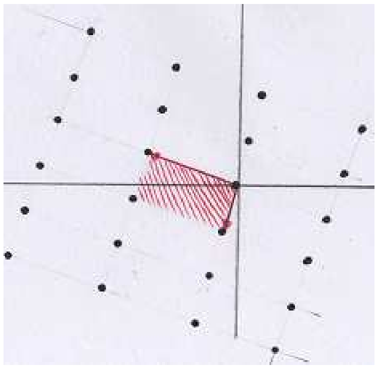
$$|(\lambda_1,\ldots,\lambda_n)|\le K.$$

And this implies that

$$|\lambda_i|\le|(\lambda_1,\ldots,\lambda_n)|\le K.$$

However, the last inequality has only finitely many integer solutions and so $B_r(0)\bigcap\mathcal{L}$ is finite. □

Now, to prove that $\mathbb{R}^n$ is partitioned into a set of disjoint sets, we need to figure out how these sets look like. A second look at a two dimensional lattice proposes a very good candidate, as the following drawing shows on the shadowed area:



This is formalized through the following definition:

Definition 17. *Given an n-dimensional lattice $\mathcal{L}\subset\mathbb{R}^n$ with the set of generators $\{l_i\}_{i=1}^n$, the fundamental domain of $\mathcal{L}$ is defined as the set*

$$T=\left\{\sum_{i=1}^n a_i l_i\,\middle|\,0\le a_i<1\,\text{for all}\,i\right\}.$$

And now, with this definition in mind, definition in mind, we prove the partitioning:

Proposition 18. *The sets $\{T+l|l\in\mathcal{L}\}$ define equivalence classes over $\mathbb{R}^n$ under the relationship $x\sim y$ if and only if there exists $l\in\mathcal{L}$ such that $x,y\in\mathcal{L}$.*

Proof:

Write $A=\sum_{i=1}^n\alpha_i l_i$, where the l_i's are the generators of $\mathcal{L}$ and define $A_i=[\![\alpha_i]\!]$ and $a_i=\alpha_i-A_i$, where the brackets indicate integer part.

It follows that

$$A = \sum_{i=1}^{n} A_i l_i + \sum_{i=1}^{n} a_i l_i.$$

But the first term of the right hand side is an element of $\mathcal{L}$ and the second one is in T, and so there exists an $l \in \mathcal{L}$ such that $A \in T + l$. However, since the assignment $x \to (\llbracket x \rrbracket, x - \llbracket x \rrbracket)$ is bijective, this choice of l is unique. □

Now we are ready to explore the relationships with toruses and lattices. We will begin by formally defining a torus. We will arrive to this definition by first studying some simpler cases:

Definition 19. *The circle group S is the set of all complex numbers of modulus 1.*

This will be our "building block" for toruses. The following proposition is immediate:

Proposition 20. *S is a group under regular complex multiplication with identity $1 \in S$.*

Now we derive a simple yet very interesting relationship:

Theorem 21. *The quotient group $\mathbb{R}/\mathbb{Z}$ is isomorphic to S.*

Proof:

Define a function φ: $\mathbb{R} \to S$ by $\varphi(x) = e^{2\pi i x}$. Then, viewing $\mathbb{R}$ as a group under addition and S as a group under complex multiplication, we easily see that φ is a homomorphism. Furthermore, it is clear that φ is surjective and, finally, since $\varphi(\mathbb{Z}) = \{1\}$, it follows that there is an isomorphism between $\mathbb{R}/\mathbb{Z}$ and S, and we are done. □

The techniue used in the past proof is the basis for the proof of the statement's generalization. To arrive to this stronger result, consider the definition of a torus:

Definition 22. *For $n \in \mathbb{Z}^+$, define the n-dimensional torus $\mathcal{T}^n$ as the cartesian product*

$$\mathcal{T}^n = S \times S \times \ldots \times S$$

of n copies of S.

For example a 2-dimensional torus can be represented as shown in the following drawing:

The expected generalization of the past theorem with this new definition is as expected:

Theorem 23. *If $\mathcal{L}$ is an n-dimensional lattice in $\mathbb{R}^n$, then $\mathbb{R}^n/\mathcal{L}$ is isomorphic to $\mathcal{T}^n$.*

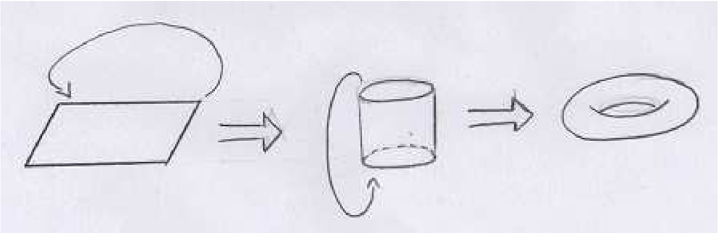
Proof:

Let $\{l_i\}_{i=1}^n$ be the generators of $\mathcal{L}$. Since this same set spans $\mathbb{R}^n$, then we can define a map $\varphi: \mathbb{R} \to \mathcal{T}^n$ such hat

$$\varphi(a_1 l_1 + \ldots + a_n l_n) = (e^{2\pi i a_1}, \ldots, e^{2\pi i a_n}).$$

As before, it is clear that φ is a surjective homomorphism and since $\varphi(\mathcal{L}) = (1, \ldots, 1)$, it follows that $\mathbb{R}^n/\mathcal{L}$ is isomoprhic to $\mathcal{T}^n$. □

To illustrate this some more, consider the following process that represents the transformation of a fundamental domain of a lattice in $\mathbb{R}^2$ into a torus:



Sums over lattices

Now we will study the properties of the sums taken over the points of a given lattice to learn that the function $\wp$, as we will define it later, provides us with an alternative to create a relatively controllable, absolutely convergent series.

We will consider by considering the first sums we think of that involve all the points of a lattice:

Proposition 24. *For any lattice $\mathcal{L} \in \mathbb{C}$, the series $\sum_{l\in\mathcal{L}} l^{-n}$ is not absolutely convergent if $n \in \{1, 2\}$ and is absolutely convergent if $n \in \{3, 4, 5, \ldots\}$.*

Proof:

Let R_k be the parallelogram in $\mathbb{C}$ whose vertices form the set $\{\pm 2kl_1, \pm 2kl_2\}$, where $k \in \mathbb{Z}$ is fixed and the l_i's are the generators of the lattice. A counting argument shows that the sides of this parallelogram contain exactly $16k$ points of the form $2al_1 + 2bl_2$, where a and b are integers with absolute value less than or equal to k. Let S_k be this set and let $S = \bigcup_{i=1}^{\infty} S_i$.

Now let D_1 be the largest distance from the origin to a point in R_1 and let d_1 be the shotest distance similarly defined. Then, for all $z \in S_1$,

$$d_1 \leq |z| \leq D_1.$$

Thus, for all $z \in S_2$, we hace

$$2d_1 \leq |z| \leq 2D_1.$$

And so on so that for all $z \in S_k$,

$$kd_1 \leq |z| \leq kD_1.$$

Hence,

$$\sum_{z\in S_1} |z|^{-n} \geq \frac{16\cdot 1}{(1\cdot D_1)^n}$$

$$\sum_{z\in S_2} |z|^{-n} \geq \frac{16\cdot 2}{(2\cdot D_1)^n}$$

$$\sum_{z\in S_3} |z|^{-n} \geq \frac{16\cdot 3}{(3\cdot D_1)^n}$$

And so

$$\sum_{z\in S} |z|^{-n} \geq \frac{16}{D_1^n} \sum_{i=1}^{\infty} \frac{1}{i^{n-1}}$$

but the series on the right diverges for $n \in \{1, 2\}$, and, since

$$\sum_{z\in\mathcal{L}} |z|^{-n} > \sum_{z\subset S} |z|^{-n},$$

it follows that the sum in our proposition diverges for $n \geq 2$.

Now, for $n \geq 3$, a similar argument shows that

$$\sum_{z\in S_k} |z|^{-n} \leq \frac{16k}{(k\cdot d_1)^n}.$$

And so

$$\sum_{z\in S} |z|^{-n} \leq \frac{16}{d_1^n} \sum_{i=1}^{\infty} \frac{1}{i^{n-1}},$$

which converges for $n \geq 3$. Finally, notice that, by counting each point in S enough times,

$$4\sum_{z\in S} |z|^{-n} > \sum_{z\in\mathcal{L}} |z|^{-n}$$

and so the series to the right converges for $n \geq 3$, and we are done. □

The past proposition answers the question of how convergent series can be defined on lattices. Now, in an attempt to take this further, it is normal to ask when more complicated functions can be constructed following a similar method. The following definition is a good way to start answering this question:

Definition 25. *Let $\mathcal{L}$ be a lattice. For $n \geq 3$, define a function P_n: $\mathbb{C}/\mathcal{L} \to \mathbb{C}$ such that*

$$P_n(z) = \sum_{l \in \mathcal{L} - \{0\}} (z-l)^{-n}.$$

The following proposition, which will be admitted without proof it follows a similar method to one shown later on, provides insight on the convergence of P_n:

Proposition 26. *For $n \geq 3$ and any positive constants K and k, the series given by $P_n(z)$ is absolutely convergent for all z such that $|z| \leq K$ and $|z-l| \geq k$ for all $l \in \mathcal{L}$.*

Notice that what this proposition means is that the series converges in any bounded region that does not contain lattice points. However, this is not the case for n=2. Trying to describe circumstance in which there is convergence, we introduce the Weierstrass $\wp$ function:

Definition 27. *Let $\mathcal{L} \in \mathbb{C}$ be a lattice and let $\mathcal{L}'$ be the lattice excluding the zero point. We define its associated Weierstrass $\wp$ function by*

$$\wp(z) = \sum_{l \in \mathcal{L}'} \left(\frac{1}{(z-l)^2} - \frac{1}{l^2} \right).$$

By defining such a function, we are "taking away a little" of each term to give the absolute convergence described in the following theorem:

Theorem 28. *The defining series for $\wp(z)$ is absolutely convergent for all $z \in \mathbb{C}$ such that $|z| \leq K$ and $|z-l| \geq k$ for all $l \in \mathcal{L}$.*

Proof:

Let S' be the set of all $l \in \mathcal{L}'$ such that $|l| \leq 2K$. Furthermore, let S be the set of all $l \in \mathcal{L}$ such that $|l| > 2K$. Clearly, S' is finite and

$$\sum_{l \in \mathcal{L}'} \left(\frac{1}{(z-l)^2} - \frac{1}{l^2} \right) = \sum_{l \in S'} \left(\frac{1}{(z-l)^2} - \frac{1}{l^2} \right) + \sum \left(\frac{1}{(z-l)^2} - \frac{1}{l^2} \right).$$

Now, since S' is finite, the first term of the right hand side is well defined for our choice of z and it defines a meromorphic function with discontinuities at each lattice pole. Disregard this term for a moment and notice that, for $l \in S$,

$$\left| \frac{z}{l} \right| < \frac{K}{2K} = \frac{1}{2}$$

and

$$\frac{1}{(z-l)^2} = \frac{1}{l^2} \left[\frac{1}{(1-\frac{z}{l})^2} \right],$$

so using the power series expansion for $\frac{1}{1-x}$ and Merten's theorem for multiplying series,

$$\frac{1}{(z-l)^2} = \frac{1}{l^2} \left[1 + \frac{2z}{l} + 3\left(\frac{z}{l}\right)^2 + 4\left(\frac{z}{l}\right)^3 + \ldots \right],$$

which gives

$$\frac{1}{(z-l)^2} - \frac{1}{l^2} = \frac{z}{l^3} \left[2 + 3\left(\frac{z}{l}\right) + 4\left(\frac{z}{l}\right)^2 + \ldots \right].$$

Taking absolute values, this gives

$$\left|\frac{1}{(z-l)^2}-\frac{1}{l^2}\right|<\frac{K}{|l|^3}\sum_{i=2}^{\infty}\frac{i}{2^{i-2}}$$

But the series on the right hand side is convergent, so let T be its limit. By taking the sum over S, we get

$$\sum_{l\subset S}\left|\frac{1}{(z-l)^2}-\frac{1}{l^2}\right|<\mathrm{KT}\sum_{l\subset S}\frac{1}{|l|^3}.$$

But the right hand side converges, so the series defined by $\wp(z)$ is absolutely convergent for any z not in the lattice. □

From this, the following corollary is immediate:

Corollary 29. *$\wp(z)$ is differentiable on $\mathbb{C}/\mathcal{L}$ and*

$$\wp'(z)=-2\sum\frac{1}{(z-l)^3}.$$

This shows that $\wp'$ is analytic everywhere except on the points of the lattice and, furthermore, for the generators l_1 and l_2 of $\mathcal{L}$, we have, for all z in the region of convergence,

$$\wp'(z+2l_i)=\wp'(z).$$

Integrating, it follows that, for some constants $C_1,C_2\in\mathbb{C}$,

$$\wp(z+2l_i)=\wp(z)+C_i.$$

Setting $z=-l_i$ in the last equation gives

$$\wp(l_i)=\wp(-l_i)+C_i.$$

But since $\wp$ is absolutely convergent at a point $l\in\mathbb{C}$ then $-l\in\mathbb{C}$ and the sum

$$\wp(-z)=\frac{1}{z^2}+\sum_{l\in\mathcal{L}}\left(\frac{1}{(z-(-l)^2}-\frac{1}{(-l)^2}\right)$$

is merely a rearrangement of $\wp(z)$ and so it equals it. Thus $C_i=0$ and so $\wp$ is doubly periodic.

The Weierstrass $\wp$ Function

We will conclude after showing some very interesting properties of the function $\wp$ defined in the last section. To do this, recall that $\wp$ was defined over a complex lattice and consider the following:

Theorem 30. *The integral*

$$-\int\int \wp(u)\,\mathrm{du}\,\mathrm{du}$$

defines an absolutely convergent series.

Proof:

Notice that

$$-\int \wp(u)\mathrm{du} = -\int \frac{1}{u^2}\mathrm{du} - \int \sum_{l \in \mathcal{L}-\{0\}} \{\frac{1}{(u-l)^2} - \frac{1}{l^2}\}$$

and the latter, by the uniform convergence of the sum, gives

$$-\int \wp(u)\mathrm{du} = \frac{1}{u} + \sum_{l \in \mathcal{L}-\{0\}} \{\frac{1}{u-l} - \frac{u}{l^2} + C_l\}.$$

However, the rightmost sum is not always convergent, but writing $C_l = \frac{1}{l}$ gives

$$-\int \wp(u)\mathrm{du} = \frac{1}{u} + \sum_{l \in \mathcal{L}-\{0\}} \{\frac{1}{u-l} - \frac{u}{l^2} + \frac{1}{l}\}$$

And the latter expression is clearly absolutely convergent for all $u \notin \mathcal{L}$.

Integrating once again we get

$$-\int\int \wp(u)\,\mathrm{du}\,\mathrm{du} = \ln u + \sum_{l \in \mathcal{L}-\{0\}} \{\ln(1-\frac{u}{l}) + \frac{u}{l} + \frac{u^2}{w^2}\}$$

Fix $R > 0$. Now let

$$L_1 = \{l \in \mathcal{L} - \{0\} \,\mathrm{such\,that}\, |l| \leq 2R\}$$

and

$$L_2 = \{l \in \mathcal{L} - \{0\} \,\mathrm{such\,that}\, |l| > 2R\}.$$

Hence

$$-\int\int \wp(u)\,\mathrm{du}\,\mathrm{du} = \ln u + \sum_{l \in L_1} \{\ln(1-\frac{u}{l}) + \frac{u}{l} + \frac{u^2}{w^2}\} + \sum_{l \in L_2} \{\ln(1-\frac{u}{l}) + \frac{u}{l} + \frac{u^2}{w^2}\}$$

but the leftmost sum is finite for $u \neq l$ and, by expanding the logarithm, the rightmost sum can be written as

$$\sum_{l \in L_2} \{\ln(1-\frac{u}{l}) + \frac{u}{l} + \frac{u^2}{w^2}\} = \sum_{l \in L_2} \{-\frac{1}{3}(\frac{u}{l})^3 - \frac{1}{4}(\frac{u}{l})^4 - ...\}$$

and the latter is absolutely convergent for $u \neq l$ under the restriction $l \in L_2$.

This completes the proof. □

Consider the following definition:

Definition 31. *For a given lattice $\mathcal{L}$, define its invariants*

$$g_2 = 2^2 \cdot 3 \cdot 5 \sum_{l \in \mathcal{L}-\{0\}} \frac{1}{l^4},$$

$$g_3 = 2^2 \cdot 5 \cdot 7 \sum_{l \in \mathcal{L}-\{0\}} \frac{1}{l^6}.$$

It is clear that both g_2 and g_3 are finite for a given lattice. The need for this definition becomes clearwith the following theorem, whose solution we will just sketch:

Theorem 32. *If $\wp$, g_2* and *g_3 are defined over the same lattice $\mathcal{L}$, then there exist functions constants $c_{i,j}$ such that $i \in \{1,2\}$, $j \in \{3,4,...\}$ and*

$$\wp(u) = \frac{1}{u^2} + \frac{g_2}{2^2 \cdot 5}u^2 + \frac{g_3}{2^2 \cdot 7}u^4 + \sum_{j \geq 3} c_{1,j}u^{2j}$$

and

$$\wp'(u) = -\frac{2}{u^3} + \frac{g_2}{10}u + \frac{g_3}{7}u^3 + \sum_{j \geq 3} c_{2,j}u^{2j-1}.$$

Proof:

The solution to this problem involves the introduction of several new functions outside of the scope of this paper. However, the proof is worth sketching since the way these functions are related is truly subtle and beautiful.

One defines the function

$$\sigma(u) = e^{-\iint \wp(u)\mathrm{du}\mathrm{du}}$$

and gets

$$\wp(u) = -\frac{d^2}{\mathrm{du}^2}\ln \sigma(u).$$

Furthermore, it can be shown, by manipulation of the definition of σ, that

$$\sigma(u) = u - \frac{1}{2}\sum_{l \in \mathcal{L}-\{0\}} \frac{1}{l^4}u^5 - \frac{1}{3}\sum_{l \in \mathcal{L}-\{0\}} \frac{1}{l^6}u^7 - ...$$

which implies that

$$\sigma(u) = u - \frac{g_2}{2^4 \cdot 3 \cdot 5}u^5 - \frac{g_3}{2^3 \cdot 5 \cdot 7}u^7 - \sum_{j \geq 4}\sum_{l \in \mathcal{L}-\{0\}} \frac{1}{l^{2j}}u^{2j+1}$$

and that

$$\frac{\sigma'(u)}{\sigma(u)} = \frac{1}{u} - \frac{g_2}{2^2 \cdot 3 \cdot 5}u^3 - \frac{g_3}{2^2 \cdot 5 \cdot 7}u^5 - \sum_{j \geq 4}\sum_{l \in \mathcal{L}-\{0\}} \frac{1}{l^{2j}}u^{2j-1}.$$

From this, it follows that

$$\wp(u) = -\frac{d^2}{\mathrm{du}^2}\ln(\sigma u) = -\frac{d}{\mathrm{du}}\{\frac{\sigma'(u)}{\sigma u}\} = \frac{1}{u^2} + \frac{g_2}{2^2 \cdot 5}u^2 + \frac{g_3}{2^2 \cdot 7}u^4 + ...$$

and, finally,

$$\wp'(u) = -\frac{2}{u^3} + \frac{g_2}{10}u + \frac{g_3}{7}u^3 + ... \square$$

An essential characteristic of the Weierstrass function is described in the following theorem:

Theorem 33. *If $\wp$, g_2 and g_3 are generated from the same lattice then*

$$[\wp'(u)]^2 = 4[\wp(u)]^3 - g_2\wp(u) - g_3.$$

Proof:

Again, this proof will be outlined. From the past theorems, we get that

$$[\wp'(u)]^2 = \frac{4}{u^6} - \frac{2g_2}{5} \cdot \frac{1}{u^2} + \frac{3g_3}{2^2 \cdot 7} + f_1(u^2)$$

and

$$[\wp(u)]^3 = \frac{1}{u^6} + \frac{3g_2}{2^2 \cdot 5} \cdot \frac{1}{u^2} + \frac{3g_3}{2^2 \cdot 7} + f_2(u^2)$$

where f_1 and f_2 are absolutely convergent powerseries of u whose term with lowest degree has degree at least 2.

After some manipulation of the latter expressions, we get that

$$[\wp'(u)]^2 - 4[\wp(u)]^3 + g_2\wp(u) + g_3 = f_3(u^2),$$

where f_3 is defined as f_1 and f_2.

However, the left hand side is doubly periodic so, by Liouville's theorem, since by definition f_3 is differentiable everywhere, both hand sides are equal to a constant, and so $f_3(u^2) = 0$ and the desired equation is attained. □

Conclusion

We have just exposed the most basic property of the Weierstrass $\wp$ function, the differential equation that relates it to elliptic curves. The following theorem gives us a very close relationship suggesting a link between the $\wp$ function and elliptic curves:

Theorem 34. *(Weierstrass Normal Form) Every nonsingular cubic curve in the complex projective plane is projectively equivalent to a curve which in affine coordinates takes the Weierstrass normal form*

$$y^2 = 4x^3 - g_2x - g_3.$$

where g_2 and g_3 are complex constants.

This theorem gives us a link between the *form* of an elliptic curve and a specific $\wp$ function, thus associating a $\wp$ function to the curve. Since the function is associated with a lattice (specifically with the quotient of the complex plane with a lattice), this gives us an association between elliptic (more generally, cubic) curves and quotients groups between the complex plane and lattices.

However, this relationship goes beyond this point and relates the group structures of certain groups. Elliptic curves can be viewed as groups where the composition operation between its points is a way of constructing a third point.

As a matter of fact, let C be an elliptic curve and let $\oplus$ be its composition operation. With a proper choice of identity, the following is true:

Proposition 35. *Under the last paragraph's terminology, if $(x_3, y_3) = (x_1, y_1) \oplus (x_2, y_2)$, then*

$$x_3 = \frac{1}{4}(\frac{y_1 - y_2}{x_1 - x_2})^2 - (x_1 + x_2)$$

and

$$y_3 = \frac{y_1 - y_2}{x_1 - x_2}x_3 + \frac{x_1y_2 - x_2y_1}{x_1 - x_2}$$

And, it can be proven using Liouville's theroem that the function

$$h(u) = \wp(u + v) - \frac{1}{4}(\frac{\wp'(u) - \wp'(v)}{\wp(u) - \wp(v)})^2$$

equals zero. By differentiating it, we find that the triplets (x_1, x_2, x_3) and (y_1, y_2, y_3) satisfy the same equations as the triplets $(\wp(u), \wp(v), \wp(u+v))$ and $(\wp'(u), \wp'(v), \wp'(u+v))$, and the following elegant relationship, which comes after formally identifying these triplets:

Theorem 36. *The group structure of an elliptic curve has the property*

$$(\wp(u), \wp'(u)) \oplus (\wp(v), \wp'(v)) = (\wp(u+v), \wp'(u+v)).$$

And with this, the group structure of an elliptic curve can be viewed in terms of the associated Weierstrass function.

However, more relationships can be deduced between this function and its derivative, the associated elliptic curve has a more intricate relationship than the one shown in this paper. However, a more thorough understanding of these connections requires tools that take many years to develop.

Bibliography

Artin, Michael. ‘‘Algebra.” New Jersey: Prentice Hall. 1991.

Axler, Sheldon. ‘‘Linear Algebra Done Right.” New York: Springer. 1997.

Hancocock, Harris. ‘‘Theory of Elliptic Funtions.” New York: John Wiley and Sons. 1910.

Priestly, Hilary. ‘‘Introduction to Complex Analysis.” United States: Oxford University Press. 1990.

Stewart, Ian. ‘‘Algebraic Number Theory and Fermat’s Last Theorem.” Massachussetts: A K Peters Editorial. 2002.