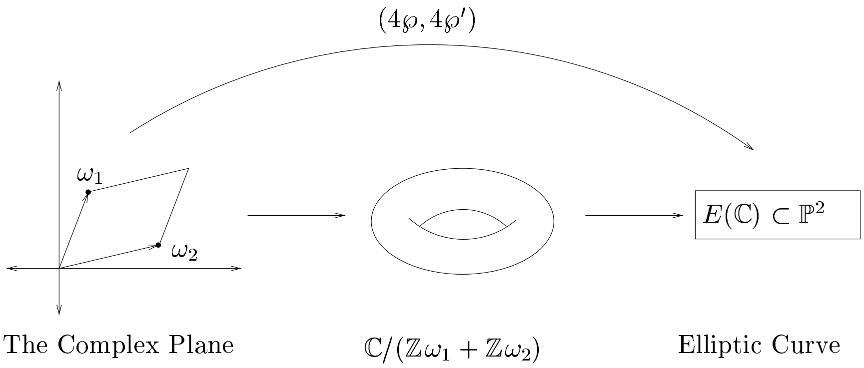

FIGURE 10.2. The Weierstrass $\wp$ Function and Elliptic Curves

10.2.5 Analytic Description of the Group Law

An alternative approach to the group law is via the Weierstrass $\wp$ function from complex analysis (see, e.g., [Ahl78,]). Let a and b be complex number with $4a^3 + 27b^2 \neq 0$. The Weierstrass $\wp$ function associated to a and b is a function $\wp : \mathbb{C} \to \mathbb{C} \cup \{\infty\}$ whose set of poles (points that map to ∞) are of the form $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, where $\omega_1, \omega_2 \in \mathbb{C}$ have the property that $\mathbb{R}\omega_1 + \mathbb{R}\omega_2 = \mathbb{C}$. Note that the quotient $\mathbb{C}/(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2)$ is homeomorphic to a torus. (In books, $\wp$ is usually viewed as being defined by $g_2 = -a/4$ and $g_3 = -b/16$.)

The connection with elliptic curves via $\wp$ is illustrated in Figure 10.2. If $x = 4\wp$ and $y = 4\wp'$, then $y^2 = x^3 + ax + b$, and $z \mapsto (4\wp(z), 4\wp'(z))$ extends to a complex analytic bijection

$$f : \mathbb{C}/(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2) \to E(\mathbb{C}).$$

Since $\mathbb{C}/(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2)$ is an abelian group, f induces a group structure on E. This group structure is the same as the one obtained above using divisors.

10.2.6 Geometric Description of the Group Law

Suppose $a, b \in \mathbb{R}$ and consider the elliptic curve defined by $y^2 = x^3 + ax + b$. Since $a, b \in \mathbb{R}$ it makes sense to draw a graph of the subset

$$E(\mathbb{R}) = \{(x, y) \in \mathbb{R} \times \mathbb{R} : y^2 = x^3 + ax + b\} \subset E(\mathbb{C}).$$

Qualitatively, there are two possibilities for this picture, depending on whether $x^3 + ax + b$ has 1 or 3 real roots. If $x^3 + ax + b$ has 1 real root, then $R(\mathbb{R})$ looks like a bow, and if the cubic has 3 real roots, then $E(\mathbb{R})$ looks like the union of an egg and a bow. See Figure 10.3 for graphs of $y^2 = x^3 + 1$ (one real root) and $y^2 = x^3 - 5x + 4$ (three real roots).

Geometrically, the group law on $E(\mathbb{R})$ is defined as illustrated in Figure 10.4. To compute $P + Q$ draw the line L detetermined by $P + Q$ (if

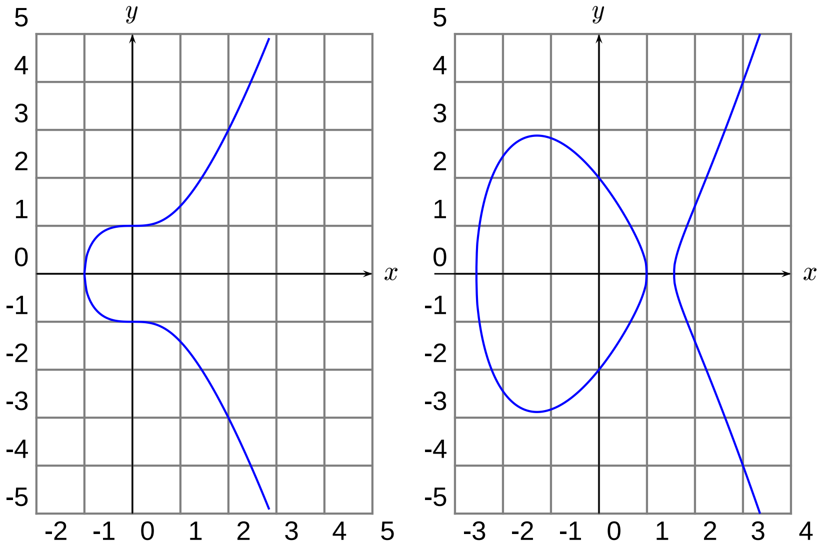

FIGURE 10.3. Real Points on $y^2 = x^3 + 1$ and $y^2 = x^3 - 5x + 4$

$P = Q$ let L be the tangent line to P). Let $R = (x, y)$ be the third point of intersection. Then the sum of $P + Q$ is $(x, -y)$. It is easy to see that the binary operation $E(\mathbb{R}) \times E(\mathbb{R}) \to E(\mathbb{R})$ determined by this process satisfies all the axioms of a group, except the associative law, which is much more tedious. (Note: One can rephrase all this geometry in a purely algebraic way, and then there is no need to restrict to real points.)

10.2.7 An Example

Let E be the elliptic curve defined by $y^2 = x^3 - 5x + 4$. Then $P = (0, 2)$, $Q = (1, 0)$, $R = (3, 4)$ and $R' = (3, -4)$ are elements of $E(\mathbb{C})$ and, as illustrated in Figure 10.4, $P + Q = R$. We verify this from the point of view of divisors and the Weierstrass $\wp$ function.

From the point of view of divisors, $P + Q = R$ is the assertion that

$$P - \mathcal{O} + Q - \mathcal{O} \sim R - \mathcal{O}.$$

To verify this, we exhibit a rational function f such that

$$(f) = P - \mathcal{O} + Q - \mathcal{O} - (R - \mathcal{O}) = P + Q - R - \mathcal{O},$$

i.e., so that f has simple zeros at P and Q and simples poles at R and $\mathcal{O}$. Let $f = \frac{2x+y-2}{x-3}$. Then

$$\begin{aligned}(2x + y - 2) &= P + Q + R' - 3\mathcal{O} \\ (x - 3) &= R + R' - 2\mathcal{O},\end{aligned}$$

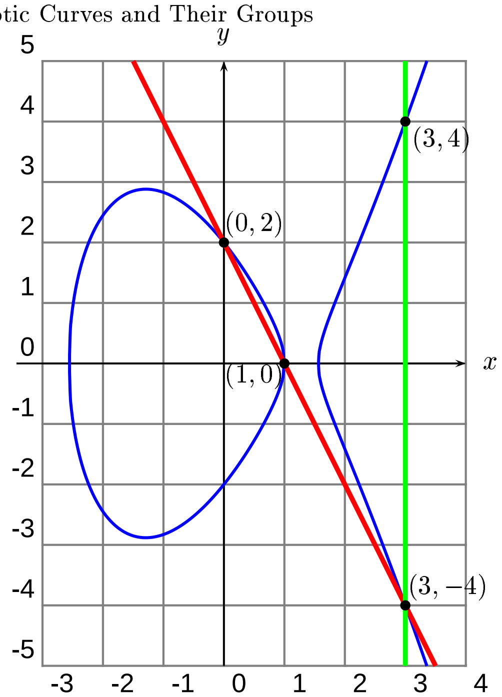

FIGURE 10.4. The Group Law: $(1, 0) + (0, 2) = (3, 4)$ on $y^2 = x^3 - 5x + 4$

so

$$(f) = P + Q + R' - 3\mathcal{O} - (R + R' - 2\mathcal{O}) = P + Q - R - \mathcal{O}$$

as required.

Let $\wp$ be the Weierstrass function associated to $y^2 = x^3 - 5x + 4$. The poles of $\wp$ are the elements of $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ where

$$\omega_1 = 2.3970980311644782804\ldots, \quad \omega_2 = i1.6043106621845101475\ldots.$$

Under the map $z \mapsto (4\wp(z), 4\wp'(z))$ we have

$$z_P = 0.58916472693707629\ldots + i0.8021553310922550\ldots \mapsto P$$
$$z_Q = 1.19854901558223914\ldots + i0.8021553310922588\ldots \mapsto Q$$
$$z_R = 1.78771374251931543\ldots \mapsto R$$

We have $z_P + z_Q = z_R + \omega_2$, so $z_P + z_Q = z_R \pmod{\Lambda}$, as expected.

10.3 Rational Points

Choose $a, b \in \mathbb{C}$ and consider the abelian group $E(\mathbb{C})$ associated to $y^2 = x^3 + ax + b$. As described in Section 10.2.5, $E(\mathbb{C})$ is isomorphic to $\mathbb{C}/(\mathbb{Z}\omega_1 +$

$\mathbb{Z}\omega_2$) for complex numbers ω_1 and ω_2. Viewing $\mathbb{C}$ as a two-dimensional real vector space with basis ω_1 and ω_2, we see that

$$E(\mathbb{C}) \cong \mathbb{C}/(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2) \cong (\mathbb{R}/\mathbb{Z}) \oplus (\mathbb{R}/\mathbb{Z}).$$

Thus, as an abstract abelian group, $E(\mathbb{C})$ does not depend on the elliptic curve E!

A *number field* is a field K that contains $\mathbb{Q}$ and is finite dimensional when viewed as a $\mathbb{Q}$-vector space. Think of K as being obtained from $\mathbb{Q}$ by "adjoining" to $\mathbb{Q}$ a root of a polynomial with coefficients in $\mathbb{Q}$. For example, $K = \mathbb{Q}$ is a number field, and we studied number fields of dimension 2 over $\mathbb{Q}$ in Chapter 9.

When $a, b \in K$ we say that the elliptic curve E associated to $y^2 = x^3 + ax + b$ is *defined over* K. Then the subset

$$E(K) = \{(x, y) \in K \times K : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\} \subset E(\mathbb{C})$$

is a subgroup.

The groups $E(K)$ are much more interesting than $E(\mathbb{C})$. For example, if E is the elliptic curve defined by $y^2 = x^3 - 5x + 4$ from Section 10.2.7, then

$$E(\mathbb{Q}) \cong \mathbb{Z} \times (\mathbb{Z}/2),$$

where a generator for the $\mathbb{Z}$-factor is the point $(0, -2)$ and a generator for the $\mathbb{Z}/2$ factor is $(1, 0)$.

For example, there is deep systematic theory that addresses the question of how to compute $E(K)$; in practice this theory usually produces the answer, but we don't know that it always will:

Open Problem 10.3.1. *Give a provably correct algorithm that takes as input a pair of numbers a, b such that $4a^3 + 27b^2 \neq 0$, and outputs the group $E(\mathbb{Q})$.*

Note that this is not a question of computational complexity. The question is to decide whether or not there even is an algorithm to compute $E(\mathbb{Q})$!

10.3.1 Rank and Torsion

Let E be an elliptic curve defined over a number field K.

Theorem 10.3.2 (Mordell). *The group $E(K)$ is finitely generated. That is, there are points $P_1, \ldots, P_s \in E(K)$ such that every element of $E(K)$ is of the form $n_1 P_1 + \cdots + n_s P_s$ for integers $n_1, \ldots n_s \in \mathbb{Z}$.*

The set of elements of $E(K)$ of finite order is a subgroup of $E(K)$ which we denote by $E(K)_{\mathrm{tor}}$. For example, if E is defined by $y^2 = x^3 - 5x + 4$, then

$$E(\mathbb{Q})_{\mathrm{tor}} = \{\mathcal{O}, (1, 0)\} \cong \mathbb{Z}/2.$$

TABLE 10.1. Exhibiting Every Possible Torsion Subgroup Over $\mathbb{Q}$

Curve	$E(\mathbb{Q})_{\mathrm{tor}}$
$y^2 = x^3 - 2$	$\{0\}$
$y^2 = x^3 + 8$	$\mathbb{Z}/2$
$y^2 = x^3 + 4$	$\mathbb{Z}/3$
$y^2 = x^3 + 4x$	$\mathbb{Z}/4$
$y^2 - y = x^3 - x^2$	$\mathbb{Z}/5$
$y^2 = x^3 + 1$	$\mathbb{Z}/6$
$y^2 = x^3 - 43x + 166$	$\mathbb{Z}/7$
$y^2 + 7xy = x^3 + 16x$	$\mathbb{Z}/8$
$y^2 + xy + y = x^3 - x^2 - 14x + 29$	$\mathbb{Z}/9$
$y^2 + xy = x^3 - 45x + 81$	$\mathbb{Z}/10$
$y^2 + 43xy - 210y = x^3 - 210x^2$	$\mathbb{Z}/12$
$y^2 = x^3 - 4x$	$(\mathbb{Z}/2) \times (\mathbb{Z}/2)$
$y^2 = x^3 + 2x^2 - 3x$	$(\mathbb{Z}/4) \times (\mathbb{Z}/2)$
$y^2 + 5xy - 6y = x^3 - 3x^2$	$(\mathbb{Z}/6) \times (\mathbb{Z}/2)$
$y^2 + 17xy - 120y = x^3 - 60x^2$	$(\mathbb{Z}/8) \times (\mathbb{Z}/2)$

The quotient $E(K)/E(K)_{\mathrm{tor}}$ is a free abelian group, so it is isomorphism to $\mathbb{Z}^r$ for some r. The integer r is called the *rank* of $E(K)$.

Theorem 10.3.3 (Mazur, April 16, 1976). *Let E be an elliptic curve over $\mathbb{Q}$. Then $E(\mathbb{Q})_{\mathrm{tor}}$ is isomorphic to one of the following 15 groups:*

$$\begin{aligned} \mathbb{Z}/n \qquad & \textit{for } n \leq 10 \textit{ or } n = 12, \\ (\mathbb{Z}/2) \times (\mathbb{Z}/2n) \qquad & \textit{for } n \leq 4. \end{aligned}$$

Table 10.1 lists elliptic curves with each possible torsion subgroups.

Conjecture 10.3.4. *There exist elliptic curves over $\mathbb{Q}$ of arbitrarily large rank.*

Probably nobody has a clue as to how to prove Conjecture 10.3.4. The "world record" is a curve of rank ≥ 24. It was discovered in January 2000 by Roland Martin and William McMillen of the National Security Agency. They weren't allowed to tell how they found the curve, and for several months they could only announce that they found a curve of rank ≥ 24, but they couldn't release the curve to the public. Here it is:

Proposition 10.3.5. *The elliptic curve*

$$y^2+xy+y = x^3-120039822036992245303534619191166796374x+504224992484910670010801799168082726759443756222911415116$$

over $\mathbb{Q}$ has rank at least 24. The following points $P_1, \ldots, P_{24}$ are independent points on the curve:

$$
\begin{aligned}
P_1 &= (2005024558054813068, -1648037158834308510823488252)\\
P_2 &= (-4690836759490453344, -3104988352578580151474452480 4)\\
P_3 &= (4700156326649806635, -6622116250158424945781859743)\\
P_4 &= (6785546256295273860, -1456180928830978521107520473)\\
P_5 &= (6823803569166584943, -1685950735477175947351774817)\\
P_6 &= (7788809602110240789, -6462981622972389783453855713)\\
P_7 &= (27385442304350994620556, 4531892554281655472841805111276996)\\
P_8 &= (54284682060285253719/4, -296608788157989016192182090427/8)\\
P_9 &= (-94200235260395075139/25, -3756324603619419619213452459781/125)\\
P_{10} &= (-3463661055331841724647/576, -439033541391867690041114047287793/13824)\\
P_{11} &= (-6684065934033506970637/676, -473072253066190669804172657192457/17576)\\
P_{12} &= (-956077386192640344198/2209, -2448326762443096987265907469107661/103823)\\
P_{13} &= (-27067471797013364392578/2809, -4120976168445115434193886851218259/148877)\\
P_{14} &= (-25538866857137199063309/3721, -7194962289937471269967128729589169/226981)\\
P_{15} &= (-102632501176025905189433 1/108241, -1000895294067489857736110963003267773/35611289)\\
P_{16} &= (9351361230729481250627334/1366561, -28697496057486357774753723393062048 32/1597509809)\\
P_{17} &= (10100878635879432897339615/1423249, -5304965776276966451066900941489387801/1697936057)\\
P_{18} &= (11499655868211022625340735/17522596, -15134357633415411882652302414268264 78043/73349586856)\\
P_{19} &= (110352253665081002517811734/21353641, -4617068333084066714055702545426477842 88/98675175061)\\
P_{20} &= (414280096426033094143668538257/285204544, 266642138924791310663963499787603019833872421/4816534339072)\\
P_{21} &= (36101712290699828042930087436/4098432361, -29952588557667645204633891535871116701422 92/262377541318859)\\
P_{22} &= (4544246340850352421546018316 5/5424617104, -3716041581470144108721590695554670156388869/399533898943808)\\
P_{23} &= (983886013344700707678587482584/141566320009, -126615818387717930449161625960397605741940953/5326475260234 6277)\\
P_{24} &= (1124614335716851053281176544216033/152487126016, -37714203831317877163580088877209977295481388540127/59545612760743936)
\end{aligned}
$$

Proof. See

`http://listserv.nodak.edu/scripts/wa.exe?A2=ind0005&L=nmbrthry&P=R182`

□

Given rational numbers a and b (with $4a^3 + 27b^2 \neq 0$) we have an associated group $E(\mathbb{Q})$, and a rank r. Even after several decades, mathematicians have given no examples of a, b for which they could show that $r > 24$, yet they still conjecture that r can be arbitrary large.

And they are probably right. Where does this intuition come from?