As a group, the torus is the product of two copies of a circle, i.e., its points can be parametrized by ordered pairs of angles (α, β). (More precisely, if the torus was obtained from the lattice $L = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$, then we write an element in $\mathbf{C}/L$ in the form $a\omega_1 + b\omega_2$ and take $\alpha = 2\pi a$, $\beta = 2\pi b$.) Thus, we can think of an elliptic curve over the complex numbers as a generalization to two real dimensions of the circle in the real plane. In fact, this analogy goes much farther than one might think. The "elliptic functions" (which tell us how to go back from a point $(x, y) \in E$ to the complex number z for which $(x, y) = (\wp(z), \wp'(z))$) turn out to have some properties analogous to the familiar function *Arcsin* (which tells us how to go back from a point on the unit circle to the real number that corresponds to that point when we "wrap" the real number line around the circle). In the algebraic number theory of elliptic curves, one finds a deep analogy between the coordinates of the "n-division points" on an elliptic curves (the points P such that nP is the identity O) and the n-division points on the unit circle (which are the n-th roots of unity in the complex plane). See the references at the end of the section for more information on this, and for the definition of the Weierstrass $\wp$-function and proofs of its properties.

Elliptic curves over the rationals. In Equation (1), if a and b are rational numbers, it is natural to look for rational solutions (x, y), i.e., to consider the elliptic curve over the field $\mathbf{Q}$ of rational numbers. There is a vast theory of elliptic curves over the rationals. It turns out that the abelian group is finitely generated (the Mordell theorem). This means that it consists of a finite "torsion subgroup" (the points of finite order) plus the subgroup generated by a finite number of points of infinite order. The number of generators needed for the infinite part is called the *rank* r; it is zero if and only if the entire group is finite. The study of the rank r and other features of the group of an elliptic curve over $\mathbf{Q}$ is related to many interesting questions in number theory and algebraic geometry. For example, a question asked since ancient times — "Given a positive integer n, when does there exist a right triangle with rational sides whose area is n?" — turns out to be equivalent to the question "Is the rank of the elliptic curve $y^2 = x^3 - n^2x$ greater than zero?" The case $n = 6$ and the $3-4-5$ right triangle lead to the point P in Example 2, which is a point of infinite order on the curve $y^2 = x^3 - 36x$. For more information on this subject, we again refer the reader to the references at the end of the section.

Points of finite order. The *order* N of a point P on an elliptic curve is the smallest positive integer such that $NP = O$; of course, such a finite N need not exist. It is often of interest to find points P of finite order on an elliptic curve, especially for elliptic curves defined over $\mathbf{Q}$.

Example 3. Find the order of $P = (2, 3)$ on $y^2 = x^3 + 1$.

Solution. Using (5), we find that $2P = (0, 1)$, and using (5) again gives $4P = 2(2P) = (0, -1)$. Thus, $4P = -2P$, and so $6P = O$. Thus, the order of P is 2, 3 or 6. But $2P = (0, 1) \neq O$, and if P had order 3, then $4P = P$, which is not true. Thus, P has order 6.