steps are as follows, assuming r, s, and hence v have no common prime divisor.

$$\begin{aligned} r^4 - s^4 = v^2 \quad &\Longrightarrow \quad r^2 = a^2 + b^2, \quad s^2 = 2ab, \quad v = a^2 - b^2 \\ &\qquad \text{for some nonzero integers } a, b \\ &\Longrightarrow \quad a = c^2 - d^2, \quad b = 2cd \\ &\qquad \text{for some nonzero integers } c, d \\ &\Longrightarrow \quad c = e^2,\ d = f^2 \text{ and } c^2 - d^2 \text{ are squares} \\ &\qquad \text{because } s^2 = 4cd(c^2 - d^2) \\ &\qquad \text{and } c, d, c^2 - d^2 \text{ have no common prime divisor} \\ &\Longrightarrow \quad e^4 - f^4 = g^2 \\ &\qquad \text{for an integer pair } (e, f) \text{ smaller than } (r, s) \end{aligned}$$

11.4.4 Justify the steps in this argument.

11.5 Rational Points on Cubics of Genus 0

It may be doubted that Fermat had a correct proof of Fermat's last theorem because most of his work deals with curves of low degree (≤ 4), and it is highly unlikely that he could have foreseen Frey's reduction of the nth-degree Fermat problem to a question about cubic curves. Admittedly, we do not know for certain what Fermat's methods were, and he did not talk in terms of finding rational points on curves. Nevertheless, this is the most natural way to interpret his solutions of Diophantine equations and to link them with earlier and later results in the same vein by Diophantus and Euler, respectively. We have already described methods for finding rational points on curves of degree 2 (in Section 1.3) and 3 (in Section 3.4). Now we shall reexamine them from the point of view of genus, which becomes increasingly important as curves of higher degree are considered. In this section we confine attention to genus 0.

One of the properties of a curve C of degree 2 that we observed in Section 1.3 is that a rational line L through a rational point P on C meets C in a second rational point, provided the equation of C has rational coefficients. Also, one obtains all rational points Q on C in this way by rotating L about C. There is another important consequence of this construction, not depending on the rationality of C or L. It is that by expressing the x and y coordinates of Q in terms of the slope t of L we obtain a *parameterization of C by rational functions* (recall that a rational function need not have rational coefficients).

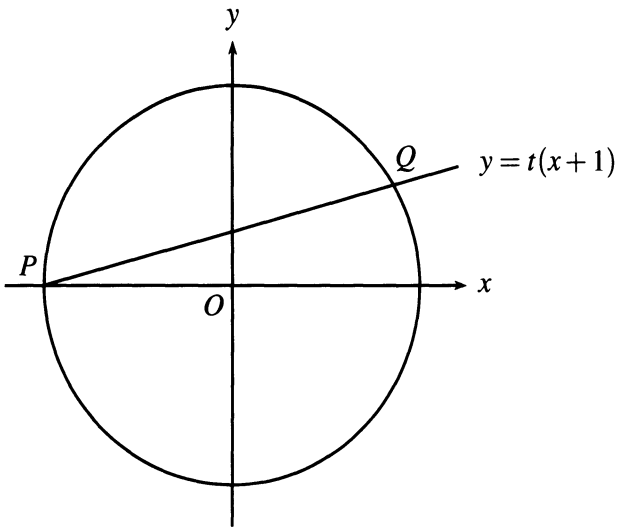

Figure 11.2: Parameterizing the circle

For example, this construction on the circle $x^2 + y^2 = 1$ in Section 1.3 gave the parameterization

$$x = \frac{1-t^2}{1+t^2}, \quad y = \frac{2t}{1+t^2}$$

(Figure 11.2). Genus 0 curves can be defined as those that admit parameterization by rational functions. I shall now show that genus 0 includes some cubic curves by applying a similar construction to the folium of Descartes.

The folium was defined in Section 7.3 as the curve with equation

$$x^3 + y^3 = 3axy. \tag{1}$$

The origin O is an obvious rational point on the folium; moreover O is a *double point* of the curve, as Figure 11.3 makes clear. The line $y = tx$ through O therefore meets the folium at one other point P, and varying t gives all other points P on the curve. By finding the coordinates of P as functions of t, we therefore obtain a parameterization.

To find P we substitute $y = tx$ in (1), obtaining

$$x^3 + t^3x^3 = 3axtx,$$

hence

$$x(1+t^3) = 3at$$

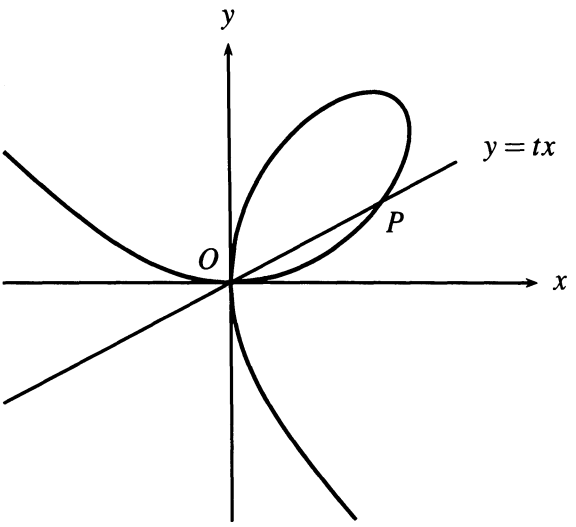

Figure 11.3: Parameterizing the folium

and

$$x = \frac{3at}{1+t^3}, \tag{2}$$

and therefore

$$y = \frac{3at^2}{1+t^3}. \tag{3}$$

(These parametric equations were pulled out of the air in Exercise 7.3.1.) A similar construction applies to any cubic with a double point, or more generally to any curve of degree $n+1$ with an n-tuple point; hence all such curves are of genus 0.

EXERCISES

It should be noted that a double point on a curve $p(x,y) = 0$ yields a *double root* of the equation $p(x,mx+c) = 0$ for the intersections of a line $y = mx+c$ through the double point.

11.5.1 Observe the double root of the equation obtained by substituting $y = tx$ in equation (1) above.

11.5.2 Explain, using the general double root property, why a line of rational slope through a rational double point on a cubic curve with rational coefficients necessarily meets the curve at another rational point.

We note also that, as in the construction for quadratic curves, *all* rational points on the folium are obtained by this method.

11.5.3 Show that if x and y are rational, then so is t in (2) and (3).

11.5.4 Deduce from Exercise 11.5.3 that the rational points on the folium are precisely those with rational t-values.

11.6 Rational Points on Cubics of Genus 1

We cannot yet give a precise definition of genus 1, but it so happens that this is the genus of all cubic curves that are not of genus 0. We know from Section 11.5 that cubics of genus 1 cannot have double points, and in fact they also cannot have cusps because both these cases lead to rational parameterizations. (For one case of a cusp, see Exercise 7.4.1.) What we have yet to exhibit are functions that do parameterize cubics of genus 1. Such functions, the *elliptic functions*, were not defined until the nineteenth century, and they were first used by Clebsch (1864) to parameterize cubics.

Many clues to the existence of elliptic functions were known before this, but at first they seemed to point in other directions. Initially, the mystery was how Diophantus and Fermat generated solutions of Diophantine equations. Newton's (1670s) interpretation of their results by the chord-tangent construction (Section 3.5) cleared up this first mystery—or would have if anyone had noticed it at the time. But before mathematicians really became conscious of the chord-tangent construction, they had to explain some puzzling relations between integrals of functions such as $1/\sqrt{ax^3+bx^2+cx+d}$, found by Fagnano (1718) and Euler (1768). Eventually Jacobi (1834) noticed that the chord-tangent construction explained this mystery too. Jacobi's explanation was cryptic and, even though elliptic functions were then known in connection with integrals they were not fully absorbed into number theory and the theory of curves until the appearance of Poincaré (1901).

The analytic origins of elliptic functions will be explained in the next chapter. In this section we shall prepare to link up with this theory by deriving the algebraic relation between collinear points on a cubic curve. [A much deeper treatment of the whole story appears in Weil (1984).]

We start with Newton's form of the equation for a cubic curve (Section 7.4):

$$y^2 = ax^3 + bx^2 + cx + d. \tag{1}$$

Figure 11.4 shows this curve when $y = 0$ for three distinct real values of x.

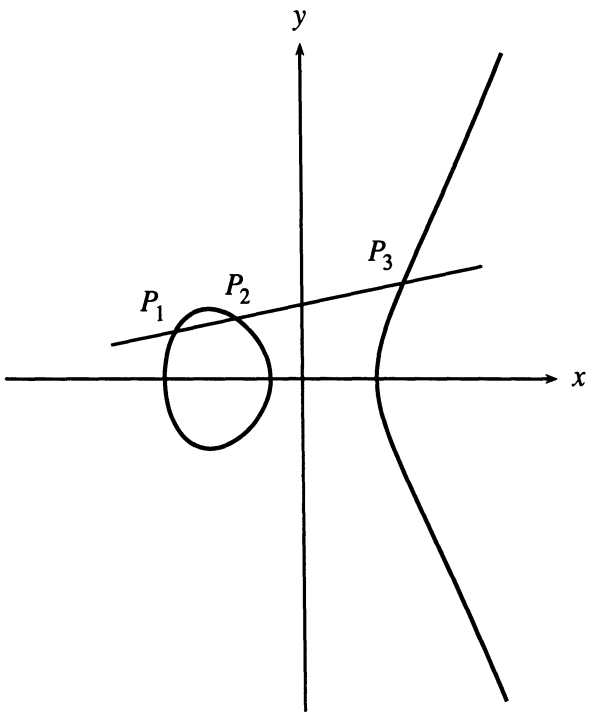

Figure 11.4: Collinear points on a cubic curve

In Section 3.5 we found that if a, b, c, d are rational, and if P_1, P_2 are rational points on the curve, then the straight line through P_1, P_2 meets the curve at a third rational point P_3. If the equation of this straight line is

$$y = tx + k, \tag{2}$$

then the result of substituting (2) in (1) is an equation

$$ax^3 + bx^2 + cx + d - (tx + k)^2 = 0 \tag{3}$$

for the x coordinates x_1, x_2, x_3 of the three points P_1, P_2, P_3. But if the roots of (3) are x_1, x_2, x_3 its left-hand side must have the form

$$a(x - x_1)(x - x_2)(x - x_3).$$

In particular, the coefficient of x^2 must be

$$-a(x_1 + x_2 + x_3).$$

Comparing this with the actual coefficient of x^2 in (3), we find

$$b - t^2 = -a(x_1 + x_2 + x_3),$$

hence

$$x_3 = -(x_1 + x_2) - \frac{b - t^2}{a}. \tag{4}$$

If $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, then $t = (y_2 - y_1)/(x_2 - x_1)$, and substituting this in (4) we finally obtain

$$x_3 = -(x_1 + x_2) - \frac{b - [(y_2 - y_1)/(x_2 - x_1)]^2}{a}, \tag{5}$$

giving x_3 as an explicit rational combination of the coordinates of P_1, P_2. If P_1, P_2 are rational points, then (5) shows that x_3 (and hence $y_3 = tx_3 + k$) is also rational, as we already knew.

What is unexpected is that (5) is also an *addition theorem* for elliptic functions. This has the consequence that the curve can be parameterized by elliptic functions $x = f(u)$, $y = g(u)$ such that (5) is precisely the equation expressing $x_3 = f(u_1 + u_2)$ in terms of $f(u_1) = x_1$, $f(u_2) = x_2$, $g(u_1) = y_1$, and $g(u_2) = y_2$. Thus the straight-line construction of x_3 from x_1 and x_2 can also be interpreted as *addition of parameter values*, u_1 and u_2 of x_1 and x_2. The first addition theorems were found by Fagnano (1718) and Euler (1768) by means of transformation of integrals. Euler realized there was a connection between such transformations and number theory, but he could never quite put his finger on it. Even earlier, Leibniz had suspected such a connection when he wrote:

> I ... remember having suggested (what could seem strange to some) that the progress in our integral calculus depended in good part upon the development of that type of arithmetic which, so far as we know, Diophantus has been the first to treat systematically.
>
> [Leibniz (1702), as translated by Weil (1984)]

Jacobi (1834) apparently saw the connection for the first time after receiving a volume of Euler's works on the transformation of integrals, but considerable clarification of elliptic functions was needed before Jacobi's insight became generally available. We describe some of the main steps in this process of clarification in Chapters 12 and 16.

EXERCISES

A proof that genus 1 curves *cannot* be parameterized by rational functions can be modelled on Fermat's proof that $r^4 - s^4 = v^2$ is impossible in positive integers. The reason is that the behavior of rational functions is surprisingly similar to that of rational numbers, with polynomials playing the role of integers, and degree being the measure of size. The most convenient curve to illustrate the idea is $y^2 = 1 - x^4$, which happens to be of genus 1.

11.6.1 Show that a parameterization of $y^2 = 1 - x^4$ by rational functions of u implies that there are polynomials $r(u)$, $s(u)$ and $v(u)$ with

$$r(u)^4 - s(u)^4 = v(u)^2.$$

Now to imitate the rest of Fermat's proof (or the simplified version in Exercise 11.4.4) one needs a theory of divisibility for polynomials. Like the theory for natural numbers, this can be based on the Euclidean algorithm. It follows the same basic lines as in Section 3.3, so we shall omit it.

One also needs the formula for "Pythagorean triples" of rational functions. This can be found by the geometric method of Section 1.3, carried out in the "rational function plane" where each "point" is an ordered pair $(x(u), y(u))$ of rational functions.

11.6.2 Convince yourself that "lines" and "slope" make sense in the rational function plane, and hence show that each point $\neq (0, -1)$ on the "unit circle"

$$x(u)^2 + y(u)^2 = 1$$

is of the form

$$x(u) = \frac{1 - t(u)^2}{1 + t(u)^2}, \quad y(u) = \frac{2t(u)}{1 + t(u)^2}$$

for some rational function $t(u)$.

11.6.3 Deduce from Exercise 11.6.2 a formula for "Pythagorean triples" of polynomials, like Euclid's formula for ordinary Pythagorean triples.

It is now possible to imitate Fermat's proof, showing that $r(u)^4 - s(u)^4 = v(u)^2$ is impossible for polynomials, and hence that $y^2 = 1 - x^4$ has no parameterization by rational functions. It follows that the same is true of certain cubic curves.

11.6.4 Substitute $x = (X + 1)/X$ and $y = Y/X^2$ in $y^2 = 1 - x^4$, and hence show

$$Y^2 = \text{cubic polynomial in } X.$$

Deduce that if this cubic curve in X, Y has a rational parameterization, then so has $y^2 = 1 - x^4$.

11.7 Biographical Notes: Fermat

Pierre Fermat (Figure 11.5) was born in Beaumont, near Toulouse, in 1601 and died in Castres, also near Toulouse, in 1665. His life is not known in detail—like his mathematics—but it seems to have been relatively uneventful. Fermat's father, Dominique, was a wealthy merchant and lawyer, his mother, Claire de Long, came from a prominent family, and they had two sons and two daughters. Pierre went to school in Beaumont, commenced university studies in Toulouse, and completed them with a law degree from Orléans in 1631. Thus Fermat's academic progress was far from meteoric, and not necessarily because he was distracted by mathematics either. As far as we know, his earliest mathematical work was the analytical geometry of 1629 and, in the opinion of Weil (1984), his number theory did not mature until Fermat was in his late thirties.

On the evidence available, Fermat seems to defy the usual clichés about mathematical genius: he didn't start young, didn't work with passionate intensity, and was generally unwilling to publish his results (though he did sometimes boast about them). It is true that few mathematicians of Fermat's era actually did mathematics for a living, but Fermat was the purest of amateurs. It seems that mathematics never caused any interruption to his professional life.

In fact, after getting his law degree in 1631 he married a distant cousin on his mother's side, Louise de Long, collected a generous dowry, and settled into a comfortable legal career. His position entitled him to be addressed as Monsieur de Fermat, hence the name Pierre de Fermat by which he is now known. He and Louise had five children, the oldest of whom, Clement-Samuel, edited his father's mathematical works [Fermat (1670)]. Probably the most dramatic, and terrifying, experience of Fermat's life was his contracting the plague during an outbreak of the disease in Toulouse in 1652 or 1653. He was at first reported to be dead but was among the lucky few who recovered.

During the 1660s Fermat was in ill health. A meeting with Pascal in 1660 had to be called off because neither was well enough to travel. As a result, Fermat missed his only chance to meet a major mathematician. He never traveled far from Toulouse and all his work was done by correspondence, mostly with members of Mersenne's circle in Paris. After 1662 his letters cease to refer to scientific work, but he was signing legal documents until three days before his death. He died in Castres while on the court cir-