(c) Find two values $x \in (\mathbb{Q}^+)^2$ such that $x \pm 210 \in (\mathbb{Q}^+)^2$. At the end of this chapter we shall prove that if there is one such x, then there are infinitely many. Equivalently (by Proposition 1), if there exists one right triangle with rational sides and area n, then there exist infinitely many.

6. (a) Show that condition (B) in Tunnell's theorem is equivalent to the condition that the number of ways n can be written in the form $2x^2 + y^2 + 8z^2$ with x, y, z integers and z odd, be equal to the number of ways n can be written in this form with z even.
   (b) Write a flowchart for an algorithm that tests condition (B) in Tunnell's theorem for a given n.

7. (a) Prove that condition (B) in Tunnell's theorem always holds if n is congruent to 5 or 7 modulo 8.
   (b) Check condition (B) for all squarefree $n \equiv 1$ or 3 (mod 8) until you find such an n for which condition (B) holds.
   (c) By Tunnell's theorem, the number you found in part (b) should be the smallest congruent number congruent to 1 or 3 modulo 8. Use the algorithm in Problem 2 to find a right triangle with rational sides and area equal to the number you found in part (b).

§2. A certain cubic equation

In this section we find yet another equivalent characterization of congruent numbers.

In the proof of Proposition 1 in the last section, we arrived at the equations $((X \pm Y)/2)^2 = (Z/2)^2 \pm n$ whenever X, Y, Z are the sides of a triangle with area n. If we multiply together these two equations, we obtain $((X^2 - Y^2)/4)^2 = (Z/2)^4 - n^2$. This shows that the equation $u^4 - n^2 = v^2$ has a rational solution, namely, $u = Z/2$ and $v = (X^2 - Y^2)/4$. We next multiply through by u^2 to obtain $u^6 - n^2u^2 = (uv)^2$. If we set $x = u^2 = (Z/2)^2$ (this is the same x as in Proposition 1) and further set $y = uv = (X^2 - Y^2)Z/8$, then we have a pair of rational numbers (x, y) satisfying the cubic equation:

$$y^2 = x^3 - n^2x.$$

Thus, given a right triangle with rational sides X, Y, Z and area n, we obtain a point (x, y) in the xy-plane having rational coordinates and lying on the curve $y^2 = x^3 - n^2x$. Conversely, can we say that any point (x, y) with $x, y \in \mathbb{Q}$ which lies on the cubic curve must necessarily come from such a right triangle? Obviously not, because in the first place the x-coordinate $x = u^2 = (Z/2)^2$ must lie in $(\mathbb{Q}^+)^2$ if the point (x, y) can be obtained as in the last paragraph. In the second place, we can see that the x-coordinate of such a point must have its denominator divisible by 2. To see this, notice that the triangle X, Y, Z can be obtained starting with a primitive Pythagorean triple X', Y', Z' corresponding to a right triangle with integral sides X', Y', Z' and area s^2n, and then dividing the sides by s to get X, Y, Z. But in a primitive

Pythagorean triple X' and Y' have different parity, and Z' is odd. We conclude that (1) $x = (Z/2)^2 = (Z'/2s)^2$ has denominator divisible by 2 and (2) the power of 2 dividing the denominator of Z is equal to the power of 2 dividing the denominator of one of the other two sides, while a strictly lower power of 2 divides the denominator of the third side. (For example, in the triangle in Fig. I.2 with area 5, the hypotenuse and the shorter side have a 2 in the denominator, while the other leg does not.) We conclude that a *necessary* condition for the point (x, y) with rational coordinates on the curve $y^2 = x^3 - n^2x$ to come from a right triangle is that x be a square and that its denominator be divisible by 2. For example, when $n = 31$, the point $(41^2/7^2, 29520/7^3)$ on the curve $y^2 = x^3 - 31^2x$ does not come from a triangle, even though its x-coordinate is a square. We next prove that these two conditions are *sufficient* for a point on the curve to come from a triangle.

Proposition 2. *Let (x, y) be a point with rational coordinates on the curve $y^2 = x^3 - n^2x$. Suppose that x satisfies the two conditions:* (i) *it is the square of a rational number and* (ii) *its denominator is even. Then there exists a right triangle with rational sides and area n which corresponds to x under the correspondence in Proposition* 1.

PROOF. Let $u = \sqrt{x} \in \mathbb{Q}^+$. We work backwards through the sequence of steps at the beginning of this section. That is, set $v = y/u$, so that $v^2 = y^2/x = x^2 - n^2$, i.e., $v^2 + n^2 = x^2$. Now let t be the denominator of u, i.e., the smallest positive integer such that $tu \in \mathbb{Z}$. By assumption, t is even. Notice that the denominators of v^2 and x^2 are the same (because n is an integer, and $v^2 + n^2 = x^2$), and this denominator is t^4. Thus, t^2v, t^2n, t^2x is a primitive Pythagorean triple, with t^2n even. By Problem 1 of §1, there exist integers a and b such that: $t^2n = 2ab$, $t^2v = a^2 - b^2$, $t^2x = a^2 + b^2$. Then the right triangle with sides $2a/t$, $2b/t$, $2u$ has area $2ab/t^2 = n$, as desired. The image of this triangle $X = 2a/t$, $Y = 2b/t$, $Z = 2u$ under the correspondence in Proposition 1 is $x = (Z/2)^2 = u^2$. This proves Proposition 2. □

We shall later prove another characterization of the points $P = (x, y)$ on the curve $y^2 = x^3 - n^2x$ which correspond to rational right triangles of area n. Namely, they are the points $P = (x, y)$ which are "twice" a rational point $P' = (x', y')$. That is, $P' + P' = P$, where "+" is an addition law for points on our curve, which we shall define later.

PROBLEMS

1. Find a simple linear change of variables that gives a one-to-one correspondence between points on $ny^2 = x^3 + ax^2 + bx + c$ and points on $y^2 = x^3 + anx^2 + bn^2x + cn^3$. For example, an alternate form of the equation $y^2 = x^3 - n^2x$ is the equation $ny^2 = x^3 - x$.

2. Another correspondence between rational right triangles X, Y, Z with area $\frac{1}{2}XY = n$ and rational solutions to $y^2 = x^3 - n^2x$ can be constructed as follows.

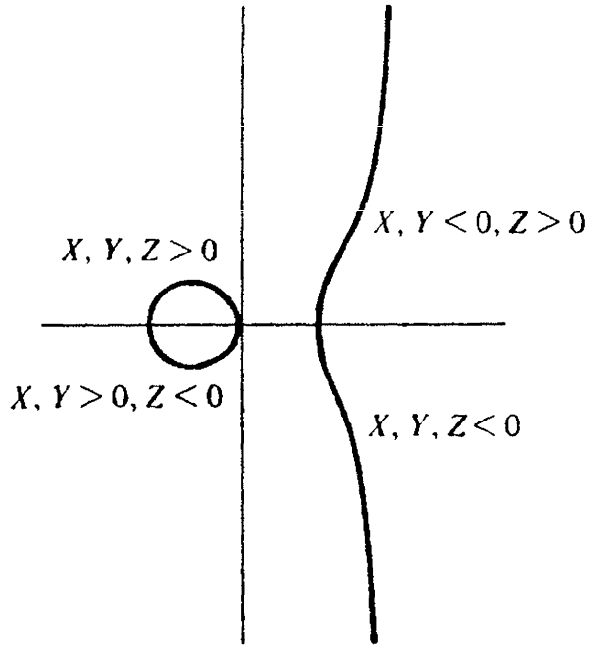

Figure I.5

§3. Elliptic curves

The locus of points $P = (x, y)$ satisfying $y^2 = x^3 - n^2x$ is a special case of what's called an "elliptic curve". More generally, let K be any field, and let $f(x) \in K[x]$ be a cubic polynomial with coefficients in K which has *distinct* roots (perhaps in some extension of K). We shall suppose that K does *not* have characteristic 2. Then the solutions to the equation

$$y^2 = f(x), \tag{3.1}$$

where x and y are in some extension K' of K, are called the *K'-points of the elliptic curve defined by* (3.1). We have just been dealing with the example $K = K' = \mathbb{Q}$, $f(x) = x^3 - n^2x$. Note that this example $y^2 = x^3 - n^2x$ satisfies the condition for an elliptic curve over any field K of characteristic p, as long as p does not divide $2n$, since the three roots $0, \pm n$ of $f(x) = x^3 - n^2x$ are then distinct.

In general, if $x_0, y_0 \in K'$ are the coordinates of a point on a curve C defined by an equation $F(x, y) = 0$, we say that C is "smooth" at (x_0, y_0) if the two partial derivatives $\partial F/\partial x$ and $\partial F/\partial y$ are not both zero at (x_0, y_0). This is the definition regardless of the ground field (the partial derivative of a polynomial $F(x, y)$ is defined by the usual formula, which makes sense over any field). If K' is the field $\mathbb{R}$ of real numbers, this agrees with the usual condition for C to have a tangent line. In the case $F(x, y) = y^2 - f(x)$, the partial derivatives are $2y_0$ and $-f'(x_0)$. Since K' is not a field of characteristic 2, these vanish simultaneously if and only if $y_0 = 0$ and x_0 is a multiple root of $f(x)$. Thus, the curve has a non-smooth point if and only if $f(x)$ has a multiple root. It is for this reason that we assumed distinct roots in the definition of an elliptic curve: an elliptic curve is smooth at all of its points.

In addition to the points (x, y) on an elliptic curve (3.1), there is a very important "point at infinity" that we would like to consider as being on the curve, much as in complex variable theory in addition to the points on the complex plane one throws in a point at infinity, thereby forming the "Riemann sphere". To do this precisely, we now introduce projective coordinates.

By the "total degree" of a monomial $x^i y^j$ we mean $i + j$. By the "total degree" of a polynomial $F(x, y)$ we mean the maximum total degree of the monomials that occur with nonzero coefficients. If $F(x, y)$ has total degree n, we define the corresponding *homogeneous polynomial* $\tilde{F}(x, y, z)$ of *three* variables to be what you get by multiplying each monomial $x^i y^j$ in $F(x, y)$ by z^{n-i-j} to bring its total degree in the variables x, y, z up to n; in other words,

$$\tilde{F}(x, y, z) = z^n F\left(\frac{x}{z}, \frac{y}{z}\right).$$

In our example $F(x, y) = y^2 - (x^3 - n^2 x)$, we have $\tilde{F}(x, y, z) = y^2 z - x^3 + n^2 x z^2$. Notice that $F(x, y) = \tilde{F}(x, y, 1)$.

Suppose that our polynomials have coefficients in a field K, and we are interested in triples $x, y, z \in K$ such that $\tilde{F}(x, y, z) = 0$. Notice that:

(1) for any $\lambda \in K$, $\tilde{F}(\lambda x, \lambda y, \lambda z) = \lambda^n \tilde{F}(x, y, z)$ (n = total degree of F);
(2) for any nonzero $\lambda \in K$, $\tilde{F}(\lambda x, \lambda y, \lambda z) = 0$ if and only if $\tilde{F}(x, y, z) = 0$. In particular, for $z \neq 0$ we have $\tilde{F}(x, y, z) = 0$ if and only if $F(x/z, y/z) = 0$.

Because of (2), it is natural to look at equivalence classes of triples $x, y, z \in K$, where we say that two triples (x, y, z) and (x', y', z') are equivalent if there exists a nonzero $\lambda \in K$ such that $(x', y', z') = \lambda(x, y, z)$. We omit the trivial triple $(0, 0, 0)$, and then we define the "projective plane $\mathbb{P}^2_K$" to be the set of all equivalence classes of nontrivial triples.

No normal person likes to think in terms of "equivalence classes", and fortunately there are more visual ways to think of the projective plane. Suppose that K is the field $\mathbb{R}$ of real numbers. Then the triples (x, y, z) in an equivalence class all correspond to points in three-dimensional Euclidean space lying on a line through the origin. Thus, $\mathbb{P}^2_{\mathbb{R}}$ can be thought of geometrically as the set of lines through the origin in three-dimensional space.

Another way to visualize $\mathbb{P}^2_{\mathbb{R}}$ is to place a plane at a distance from the origin in three-dimensional space, for example, take the plane parallel to the xy-plane and at a distance 1 from it, i.e., the plane with equation $z = 1$. All lines through the origin, except for those lying in the xy-plane, have a unique point of intersection with this plane. That is, every equivalence class of triples (x, y, z) with nonzero z-coordinate has a unique triple of the form $(x, y, 1)$. So we think of such equivalence classes as points in the ordinary xy-plane. The remaining triples, those of the form $(x, y, 0)$, make up the "line at infinity".

The line at infinity, in turn, can be visualized as an ordinary line (say,

the line $y = 1$ in the xy-plane) consisting of the equivalence classes with nonzero y-coordinate and hence containing a unique triple of the form $(x, 1, 0)$, together with a single "point at infinity" $(1, 0, 0)$. That is, we define the projective line $\mathbb{P}^1_K$ over a field K to be the set of equivalence classes of pairs (x, y) with $(x, y) \sim (\lambda x, \lambda y)$. Then $\mathbb{P}^2_K$ can be thought of as an ordinary plane $(x, y, 1)$ together with a projective line at infinity, which, in turn, consists of an ordinary line $(x, 1, 0)$ together with its point at infinity $(1, 0, 0)$.

More generally, n-dimensional projective space $\mathbb{P}^n_K$ is defined using equivalence classes of $(n + 1)$-tuples, and can be visualized as the usual space of n-tuples $(x_1, \ldots, x_n, 1)$ together with a $\mathbb{P}^{n-1}_K$ at infinity. But we shall only have need of $\mathbb{P}^1_K$ and $\mathbb{P}^2_K$.

Given a homogeneous polynomial $\tilde{F}(x, y, z)$ with coefficients in K, we can look at the solution set consisting of points (x, y, z) in $\mathbb{P}^2_K$ (actually, equivalence classes of (x, y, z)) for which $\tilde{F}(x, y, z) = 0$. The points of this solution set where $z \neq 0$ are the points $(x, y, 1)$ for which $\tilde{F}(x, y, 1) = F(x, y) = 0$. The remaining points are on the line at infinity. The solution set of $\tilde{F}(x, y, z) = 0$ is called the "projective completion" of the curve $F(x, y) = 0$. From now on, when we speak of a "line", a "conic section", an "elliptic curve", etc., we shall usually be working in a projective plane $\mathbb{P}^2_K$, in which case these terms will always denote the projective completion of the usual curve in the xy-plane. For example, the line $y = mx + b$ will really mean the solution set to $y = mx + bz$ in $\mathbb{P}^2_K$; and the elliptic curve $y^2 = x^3 - n^2x$ will now mean the solution set to $y^2z = x^3 - n^2xz^2$ in $\mathbb{P}^2_K$.

Let us look more closely at our favorite example: $F(x, y) = y^2 - x^3 + n^2x$, $\tilde{F}(x, y, z) = y^2z - x^3 + n^2xz^2$. The points at infinity on this elliptic curve are the equivalence classes $(x, y, 0)$ such that $0 = \tilde{F}(x, y, 0) = -x^3$, i.e., $x = 0$. There is only one such equivalence class $(0, 1, 0)$. Intuitively, if we take $K = \mathbb{R}$, we can think of the curve $y^2 = x^3 - n^2x$ heading off in an increasingly vertical direction as it approaches the line at infinity (see Fig. I.6). The points on the line at infinity correspond to the lines through the origin in the xy-plane, i.e., there is one for every possible slope y/x of such a line. As we move far out along our elliptic curve, we approach slope $y/x = \infty$, corresponding to the single point $(0, 1, 0)$ on the line at infinity. Notice that any elliptic curve $y^2 = f(x)$ similarly contains exactly one point at infinity $(0, 1, 0)$.

All of the usual concepts of calculus on curves $F(x, y) = 0$ in the xy-plane carry over to the corresponding projective curve $\tilde{F}(x, y, z) = 0$. Such notions as the tangent line at a point, points of inflection, smooth and singular points all depend only upon what is happening in a neighborhood of the point in question. And any point in $\mathbb{P}^2_{\mathbb{R}}$ has a large neighborhood which looks like an ordinary plane. More precisely, if we are interested in a point with nonzero z-coordinate, we can work in the usual xy-plane, where the curve has equation $F(x, y) = \tilde{F}(x, y, 1) = 0$. If we want to examine a point on the line $z = 0$, however, we put the triple in either the form $(x, 1, 0)$ or $(1, y, 0)$. In the former case, we think of it as a point on the curve $F(x, 1, z) = 0$

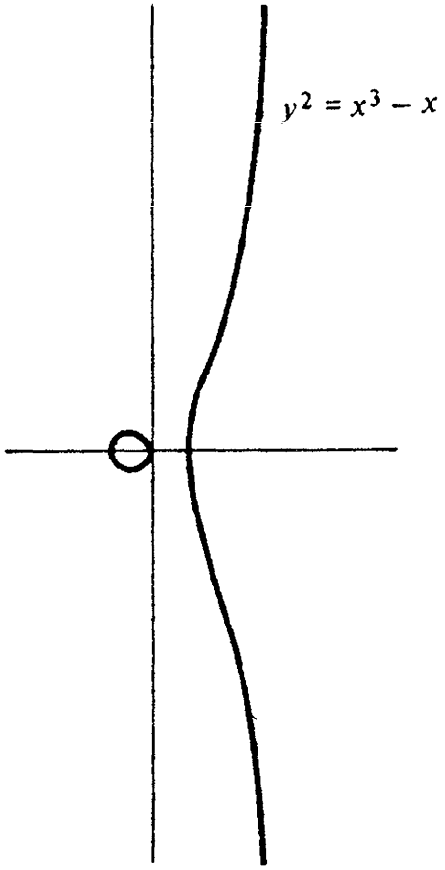

Figure I.6

in the xz-plane; and in the latter case as a point on the curve $F(1, y, z) = 0$ in the yz-plane.

For example, near the point at infinity $(0, 1, 0)$ on the elliptic curve $y^2z - x^3 + n^2xz^2$, all points have the form $(x, 1, z)$ with $z - x^3 + n^2xz^2 = 0$. The latter equation, in fact, gives us all points on the elliptic curve except for the three points $(0, 0, 1)$, $(\pm n, 0, 1)$ having zero y-coordinate (these are the three "points at infinity" if we think in terms of xz-coordinates).

Problems

1. Prove that if K is an infinite field and $F(x, y, z) \in K[x, y, z]$ satisfies $F(\lambda x, \lambda y, \lambda z) = \lambda^n F(x, y, z)$ for all $\lambda, x, y, z \in K$, then F is homogeneous, i.e., each monomial has total degree n. Give a counterexample if K is finite.

2. By a "line" in $\mathbb{P}_K^2$ we mean either the projective completion of a line in the xy-plane or the line at infinity. Show that a line in $\mathbb{P}_K^2$ has equation of the form $ax + by + cz = 0$, with $a, b, c \in K$ not all zero; and that two such equations determine the same line if and only if the two triples (a, b, c) differ by a multiple. Construct a 1-to-1 correspondence between lines in a copy of $\mathbb{P}_K^2$ with coordinates (x, y, z) and points in another copy of $\mathbb{P}_K^2$ with coordinates (a, b, c) and between points in the xyz-projective plane and lines in the abc-projective plane, such that a bunch of points are on the same line in the first projective plane if and only if the lines that correspond to them in the second projective plane all meet in the same point. The xyz-projective plane and the abc-projective plane are called the "duals" of each other.

11.5 The classification of Pythagorean triples

Let us return to our aim of classifying the primitive Pythagorean triples. The solution to this problem was given in the 3rd century AD by Diophantos of Alexandria, in Book II of his *Arithmetica*, and a more geometric version can also be found in Book X of Euclid's *Elements*.

Theorem 11.3

If u and v are coprime positive integers of opposite parity, with $u > v$, then the numbers

$$a = u^2 - v^2, \quad b = 2uv, \quad c = u^2 + v^2 \tag{11.3}$$

form a primitive Pythagorean triple. Conversely, every primitive Pythagorean triple (a, b, c) is given by (11.3) (possibly with a and b transposed) for such a pair u, v.

(This may be the way the Babylonians created their list of triples; for example, if $u = 81$ and $v = 40$ we get the triple $(a, b, c) = (4961, 6480, 8161)$.)

Proof

The numbers a, b and c in (11.3) are positive integers, and one can easily verify that

$$(u^2 - v^2)^2 + (2uv)^2 = (u^2 + v^2)^2$$

for all u and v, so (a, b, c) is a Pythagorean triple. Suppose that (a, b, c) is not primitive, so a, b and c are all divisible by some prime p. If $p = 2$ then a is even; since $a = u^2 - v^2$ it follows that u and v have the same parity, which is false. If p is odd then p divides $(a+c)/2 = u^2$, and hence divides u; it therefore divides $u^2 - a = v^2$ and hence divides v, contradicting the fact that u and v are coprime. In either case we have a contradiction, so (a, b, c) must be primitive.

For the converse, suppose that (a, b, c) is a primitive Pythagorean triple. Since $a^2 + b^2 = c^2$ we have $a^2 + b^2 \equiv c^2 \bmod (4)$. Now $x^2 \equiv 0$ or $1 \bmod (4)$ as x is even or odd, and the only solutions of the equation $[x] + [y] = [z]$ with $[x], [y], [z] = [0]$ or $[1]$ in $\mathbb{Z}_4$ are $[0] + [0] = [0]$, $[0] + [1] = [1]$ and $[1] + [0] = [1]$. Since a and b are not both even, it follows that one is odd and the other is even. Transposing a and b if necessary, we can assume that a is odd and b is even, say $b = 2d$ for some integer d. Then

$$4d^2 = b^2 = c^2 - a^2 = (c + a)(c - a),$$

so at least one of the factors $c \pm a$ is even, and since they differ by $2a$ they are both even. Thus

$$d^2 = \left(\frac{c+a}{2}\right)\left(\frac{c-a}{2}\right),$$

with both factors $(c \pm a)/2$ integers. These factors are coprime, since any common factor would also divide their sum (which is c) and their difference (which is a), and would therefore divide $\gcd(a, c)$, which is 1. Since their product is a perfect square, both of these factors must be perfect squares by Lemma 2.4, say

$$\frac{c+a}{2} = u^2 \quad \text{and} \quad \frac{c-a}{2} = v^2$$

for some positive integers u and v. Adding and subtracting these two equations, we then have $c = u^2 + v^2$ and $a = u^2 - v^2$, while the equations $b = 2d$ and $d^2 = u^2v^2$ imply that $b = 2uv$. Thus equations (11.3) are satisfied, and these show that u and v must be coprime, since any common factor would divide a, b and c. Since a is odd and positive, u and v must have opposite parity with $u > v$. □

This gives us a complete description of the primitive Pythagorean triples, and by taking integer multiples of these we immediately get a description of all the Pythagorean triples:

Corollary 11.4

The general form for a Pythagorean triple (a, b, c) is given by

$$a = m(u^2 - v^2), \quad b = 2muv, \quad c = m(u^2 + v^2)$$

(or possibly with a and b transposed), where u and v are coprime positive integers of opposite parity with $u > v$, and m is a positive integer.

There is an alternative approach, which classifies all *rational* solutions (a, b, c) of equation (11.2), including, of course, the Pythagorean triples. To avoid trivial solutions, let us assume that $b \neq 0$. This implies that $c \neq 0$, so dividing (11.2) by c^2 we get

$$x^2 + y^2 = 1, \tag{11.4}$$

where

$$x = \frac{a}{c} \quad \text{and} \quad y = \frac{b}{c}$$

are both rational numbers. Now (11.4) is the equation of a circle C of radius 1 in the xy-plane, centred at the origin $O = (0, 0)$. If $P = (x, y)$ is any point on C, other than the point $Q = (-1, 0)$, then the line PQ has gradient

$$t = \frac{y}{1+x},$$