The equation $ax + by = k$ represents a straight line. The problem of solving this equation in integers x and y is equivalent to the problem of finding the lattice points situated on the straight line in question.

Suppose that the straight line has integral coefficients, or what is obviously the same, rational coefficients. Then, by Section 2, the straight line passes through an infinity of lattice points if it passes through one lattice point. This conclusion is not valid for equations with irrational coefficients a, b, k except when there exists a positive number p such that the numbers ap, bp, kp are all rationals. Thus the straight line $y = \sqrt{2}\,x$ only passes through one lattice point, namely the origin.

This can be generalized to three dimensions. Thus we can speak of lattice points and point lattices in space. The equation $ax + by + cz = k$ represents a plane in a Cartesian coordinate system with the coordinates x, y, z. The problem of solving this equation in integers x, y, z is equivalent to the problem of determining all lattice points in space which lie on the plane. More generally, one may consider the distribution of lattice points on a given curve in the plane or on a given surface in space. This leads to the problem of solving Diophantine equations in two or three unknowns of any degree.

4.

PARTIAL FRACTIONS

In elementary arithmetic the problem of combining several fractions with different denominators is solved by converting the fractions into equivalent fractions with a common denominator. The reverse process of converting a fraction with a composite denominator into a combination of fractions with prime denominators or powers of prime denominators is possible with the aid of Euclid's algorithm. Consider, for example, the problem of decomposing the fraction 7/30 into such fractions (called partial fractions). We first factor 30 into two factors, say 5 and 6. Euclid's algorithm applied to these two numbers gives $1 \times 6 - 1 \times 5 = 1$. Hence, dividing both sides by 30 yields $1/5 - 1/6 = 1/30$. Treating the denominator 6 in the same way, we get $1/6 = 1/2 - 1/3$. Hence $1/30 = 1/5 - 1/2 + 1/3$, and

$$7/30 = 7/5 - 7/2 + 7/30 = 1\ 2/5 - 3\ 1/2 + 2\ 1/3 = 2/5 - 1/2 + 1/3.$$

The procedure is somewhat modified when the denominator contains factors which are powers of primes. Consider for example the decomposition of 4/45 into partial fractions. Euclid's algorithm applied to 9 and 5 gives $2 \times 5 - 1 \times 9 = 1$; dividing both sides by 45 yields $2/9 - 1/5 = 1/45$. Hence

$$4/45 = 8/9 - 4/5 = 2/9 + 2/3 - 4/5.$$

A similar process exists for polynomials in x with coefficients in any field. In High School Algebra the reader has undoubtedly learned how to divide one polynomial $n(x)$ by a second polynomial $d(x)$ so as to get a quotient $q(x)$ and a remainder $r(x)$ of degree less than that of the divisor $d(x)$. Although this process is usually carried out for polynomials with rational coefficients, it is not difficult to show that it is equally valid for polynomials with coefficients in any field. If we accept this result, then Euclid's algorithm described in detail for rational integers can be used to compute a polynomial $g(x)$ which is the g.c.d. of $n(x)$ and $d(x)$ and which is unique except for unit factors, i.e., non-zero elements of the coefficient field. It follows that $g(x)$ is expressible as a linear combination of $n(x)$ and $d(x)$:

$$p(x) \times n(x) + q(x) \times d(x) = g(x).$$

In particular, if the polynomials $n(x)$ and $d(x)$ are prime to each other, i.e., have no polynomial factor in common, then Euclid's algorithm assures us of the existence of two polynomials $p(x)$ and $q(x)$ such that

$$p(x) \times n(x) + q(x) \times d(x) = c$$

where c is a constant of the field independent of x.

As in the case with rational numbers, the last equation makes it possible to decompose rational functions of x into sums of simple fractions with denominators which are irreducible over the coefficient field, or powers of such polynomials. Although this result is usually derived in algebra by the method of "undetermined coefficients", it is necessary to use some other method such as our present method to prove that an expression in partial fractions always exists.

If the denominator $d(x)$ is a product of distinct and repeated factors such as $[d_1(x)]^{m_1}[d_2(x)]^{m_2} \cdots [d_k(x)]^{m_k}$ with integral exponents m, any two distinct irreducible $d_i(x)$ are prime and so are their powers $[d_i(x)]^{m_i}$. By the method described above, we may factor $d(x)$ in a manner so that one factor is $[d_i(x)]^{m_i}$ while the other factor is all the rest. Applying Euclid's algorithm to each such product will ultimately lead to the decomposition of $d(x)/n(x)$ into partial fractions.

Example. Consider the decomposition of $(x^2+1)/(x-1)^2(x+1)$ in the field of rationals. By the algorithm

$$1 \times (x-1)^2 - (x-3)(x+1) = 4.$$

Multiplying both sides by (x^2+1) and dividing both sides by $(x-1)^2 \times (x+1)$ yields:

$$4(x^2+1)/(x-1)^2(x+1) = (x^2+1)/(x+1) - (x^3-3x^2+x-3)/(x-1)^2.$$

Each of the fractions on the right may be simplified further by long division. Eventually, we derive the identity:

$$(x^2+1)/(x-1)^2(x+1) = 1/2(x+1) + (x+1)/2(x-1)^2 =$$

$$1/2(x+1) + 1/2(x-1) + 1/(x-1)^2.$$

5.

APPROXIMATION OF NUMBERS BY RATIONALS

In computation it is frequently convenient to replace complicated rationals or irrationals by rationals with small terms. For some purposes the fraction 1/7 is simpler than the corresponding repeating decimal .142587; the value of π is sometimes taken as approximately 22/7. Let us agree to call such approximations "simpler" than the original numbers. Clearly, it is desirable to study the best approximations of numbers by such simpler rationals. There will be a series of such approximations according to the degree of accuracy required. An elegant way to arrive at such approximations is by means of Euclid's algorithm as will be shown.

Suppose we start with a rational approximation p/q to a real number which is of greater accuracy than is required; p/q being in reduced terms. It is desired to find a simpler fraction p'/q' which will be an approximation to p/q. The difference $(p/q-p'/q')$ has a denominator which can be no greater than qq', and the absolute value of the difference cannot be less than $1/qq'$. Let us then call p'/q' a "best approximation" to p/q if $(p/q-p'/q') = \pm 1/qq'$. This is evidently equivalent to the equation:

$$q'p - p'q = \pm 1.$$

The numbers p', q' are precisely those obtained in Euclid's algorithm. Consecutive simpler approximations can be found in the same way from p'/q', and from the subsequent fractions obtained.

As an example, let us express 29/73 in a simpler form. Euclid's algorithm yields: $5 \times 29 - 2 \times 73 = -1$. Here $p=2$, $q=5$, and the fraction 2/5 is a best approximation to 29/73.

The process described in the previous paragraph is equivalent to the representation of rational numbers by finite continued fractions. The successive approximations are simply the corresponding convergents with p/q equal to the nth. convergent and p'/q' equal to the $(n-1)$st. convergent. To see this more clearly, let

$$p/q = a_1 + 1/a_2 + 1/a_3 + \cdots + 1/a_n \equiv [a_1, a_2, \cdots, a_n]$$

be the continued fraction expansion of p/q. If in this expansion, the last term $1/a_n$ is omitted, it can be shown[2] that the remainder of the

[2] For this result and others quoted in this section, see Chapter X of G. H. Hardy's and E. M. Wright's "An Introduction to the Theory of Numbers", Oxford University Press, 1945.