CHAPTER 23

Local Methods or p-Adic Applications

1. One of the most important applications of p-adic numbers to Diophantine equations deals with the

Problem

Let $\omega_1, \omega_2, \ldots, \omega_n$ be a basis of the integers in an algebraic number field $K = Q(\theta)$. Denote by $N(\omega)$ the norm of ω in the field. Then it is required to discuss the solution in rational integers x of the equation

$$N(x_1\omega_1 + x_2\omega_2 + \cdots + x_n\omega_n) = a, \tag{1}$$

where the x satisfy the $n - m$ equation

$$g_l(x) = 0, \quad (l = 1, 2, \ldots, n - m) \tag{2}$$

for given $m \leqslant n$, and the $g(x)$ are polynomials in x with rational coefficients.

The simplest problem is when $x_{m+1} = x_{m+2} = \cdots = x_n = 0$.

From algebraic number theory, it is known that the general solution of equation (1) is given by

$$x_1\omega_1^{(s)} + x_2\omega_2^{(s)} + \cdots + x_n\omega_n^{(s)} = c^{(s)}\varepsilon^{(s)}, \quad (s = 1, 2, \ldots, n), \tag{3}$$

where $\omega^{(s)}$ denotes the conjugates of ω, the c belong to a finite set of numbers in K and ε is a unit in K. We recall that every unit ε can be written in the form

$$\varepsilon = \zeta\eta_1^{u_1}\eta_2^{u_2}\ldots\eta_r^{u_r}, \tag{4}$$

where ζ is a root of unity in K, the η are a set of fundamental units, and the u are arbitrary rational integers. Also $r = r_1 + r_2 - 1$ where r_1, r_2 denote respectively the number of real fields and pairs of complex fields among the conjugates of K. On substituting for the x from equations (3) and (4) in (2), we have $n - m$ equations in the r unknowns u which occur as exponents in the powers of the units η. If $r \leqslant n - m$, we should expect there to be only a finite number of solutions if the equations resulting from (2) are independent. As these equations are best dealt with by p-adic methods, we give a brief résumé of p-adic number theory where p is a rational prime. For simplicity we define the p-adic numbers over the rational field Q. Let x be any number in Q. We define a valuation $|x|_p$ as follows. If $x = 0$, $|x|_p = 0$. If $x \neq 0$, x

can be written in the form $x = p^a x_1/x_2$, where x_1, x_2 are prime to p. Then $|x|_p = 1/p^a$. The valuation has the properties

1. $|x|_p \geqslant 0$, and $|x|_p = 0$ if and only if $x = 0$,
2. $|x_1x_2|_p = |x_1|_p|x_2|_p$,
3. $|x_1 \pm x_2|_p \leqslant |x_1|_p + |x_2|_p$.

This is the triangular inequality and may be sharpened to

$$|x_1 \pm x_2|_p \leqslant \max(|x_1|_p, |x_2|_p).$$

The p-adic field Q_p is defined as a field which contains the field Q and is such that if $X \in Q_p$, then

I. There is a valuation $|X|_p$ on Q_p which satisfies 1, 2 and 3 and coincides with $|x|_p$ when $X = x$ is an element of Q.

II. Limits are defined as for complex number theory, except that an absolute value $|x|$ there is replaced by $|x|_p$, and corresponding results exist for the p-adic field. Thus Cauchy's convergence principle holds, i.e. a sequence $X_1, X_2, \ldots$, tends to a limit if and only if $|X_m - X_n|_p < \varepsilon$ for $m, n > N(\varepsilon)$. This limit will be in Q_p and so the field Q_p is complete.

III. Every element of Q_p is a limit of a sequence of numbers of Q.

The discussion of convergence is now very simple since a series $\sum a_n$ converges if and only if $|a_n|_p \to 0$, and so there is no need for the concept of absolute convergence. The usual results on functions of a complex variable carry over to p-adic variables. There is, however, greater simplicity since if $|a_n|_p \to 0$, the series

$$f(x) = \sum_0^\infty a_n x^n$$

converges for $|x|_p \leqslant 1$.

We can define series which have the characteristic properties of the exponential and logarithmic functions.

Thus we have

$$e^x = 1 + x + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!} + \cdots \qquad \text{if } |x|_p < \frac{1}{p-1}$$

$$\log(1 + x) = x - \frac{x^2}{2} + \cdots + \frac{(-1)^{n-1}x^n}{n} + \cdots \quad \text{if } |x|_p < 1.$$

Similar results hold when x is a number in an algebraic number field K. If η is a unit in K, there exists a rational integer a such that if p is an odd prime, then $\eta^a \equiv 1 \pmod{p}$, but if $p = 2$, $\eta^a \equiv 1 \pmod 4$. Then $\eta^{av} = e^{v \log \eta^a}$ can be expanded as a power series in v with coefficients in K which converges for all p-adic integers v. Since $u = av + b$, $0 \leqslant b < a$, we have a expansions

for η^n. It follows at once that the product $\eta_1^{u_1}\eta_2^{u_2}\dots$ can be expressed as a finite number of power series *in* $v_1, v_2, \dots$ with coefficients in K which converge for all p-adic integers $v_1, v_2, \dots$.

2. We now show by a method due to Skolem how p-adic theory can be applied to the equations arising from (2). It is obvious that equations will have only a finite number of rational solutions if they have only a finite number of p-adic solutions. The equations (2) can be replaced by a finite number of equations

$$g_l(u_1, u_2, \dots, u_r) = 0, \quad (l = 1, 2, \dots, n - m). \tag{5}$$

where the $g(u)$ are power series converging for all p-adic integers u. The coefficients may be taken as rational numbers whose denominators are prime to p since we are considering a set of conjugate equations.

The finiteness of the number of p-adic solutions can be proved from the following theorems.

Theorem 1

Let $f(x) = \sum_0^\infty a_n x^n$ *where* $|a_n|_p \to 0$ *so that the series converges when* $|x|_p \leqslant 1$. *Then the equation* $f(x) = 0$ *has only a finite number of solutions for* $|x|_p \leqslant 1$, *i.e. for p-adic integers x.*

More generally we have a result given by Strassmann[1]

Theorem 2

Let $f_0(x), f_1(x), \dots$ *be polynomials whose coefficients are p-adic integers, and suppose that* $f_0(x)$ *has at least one coefficient* $\not\equiv 0 \pmod p$. *Then the equation*

$$\sum_{n=0}^{\infty} p^n f_n(x) = 0 \tag{6}$$

has only a finite number of solutions in p-adic integers.

There are extensions to several variables.

Theorem 3

Let $f_0(x, y), f_1(x, y), \dots, g_0(x, y), g_1(x, y), \dots$ *be polynomials whose coefficients are p-adic integers and suppose that*

$$\frac{\partial f_0}{\partial x}\frac{\partial g_0}{\partial y} - \frac{\partial f_0}{\partial y}\frac{\partial g_0}{\partial x} \not\equiv 0 \pmod p.$$

Then the simultaneous equations

$$\sum_0^\infty p^n f_n(x, y) = 0, \qquad \sum_0^\infty p^n g_n(x, y) = 0 \tag{7}$$

have only a finite number of p-adic solutions.

This also holds *if* f_0, g_0 are relatively prime mod p.

Skolem has proved many results by his methods. When the question is only to prove the existence of a finite number of integer solutions, the work may not be too complicated as can be seen from his[2,3] proof of

Theorem 4

Let $a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_n$ *be numbers in an algebraic number field K. Then the equation*

$$\sum_{i=1}^{n} a_i b_i^x = 0 \tag{8}$$

has only a finite number of rational integer solutions for x, if none of the quotients b_i/b_j *is a root of unity.*

When the numerical values of the fundamental units of the relevant algebraic number field play no part in an investigation, and only an estimate for the number of solutions is required, the details may not be troublesome as in Skolem's proof of Theorem 5

Theorem 5

If d is an integer > 1, *there is at most one rational integer solution of* $x^3 + dy^3 = 1$ *other than* $x = 1, y = 0$.

Let us suppose there are two solutions (x_1, y_1) and (x_2, y_2). Write $\theta = \sqrt[3]{d}$. Then $\eta_1 = x_1 + y_1\theta$, $\eta_2 = x_2 + y_2\theta$ are positive units with norm 1 in the field $Q(\theta)$. Since there are no roots of unity in the field and there is only one fundamental unit, we have

$$\eta_1^{u_1} = \eta_2^{u_2} \tag{9}$$

with rational integers, u_1, u_2. We may suppose that u_1, u_2 are not both $\equiv 0 \pmod 3$, for if so, we would have $\eta_1^{u_1/3} = \eta_2^{u_2/3}$. Hence we may suppose that $u_2 \not\equiv 0 \pmod 3$. Then u_1/u_2 is a 3-adic integer and so we have, say, the 3-adic equation

$$\eta_1^u = \eta_2.$$

Suppose first that $y_1 \equiv 0 \pmod 3$ and so $x_1 \not\equiv 0 \pmod 3$. Then η_1^u is defined in the 3-adic field over $Q(\theta)$ and so

$$x_1^u\left(1 + \frac{y_1}{x_1}\theta\right)^u = \eta_2,$$

and the left-hand side can be expanded as a binomial series. Equating the coefficient of θ^2 to zero, we have

$$\binom{u}{2}\left(\frac{y_1}{x_1}\right)^2 + \binom{u}{5}\left(\frac{y_1}{x_1}\right)^5 d + \binom{u}{8}\left(\frac{y_1}{x_1}\right)^8 d^2 + \dots = 0.$$

We show that the only solutions of this equation are $u = 0, 1$. For on dividing out by

$$2\binom{u}{2}\left(\frac{y_1}{x_1}\right)^2,$$

we have

$$\frac{1}{2} + \binom{u-2}{3}\frac{d}{4.5}\left(\frac{y_1}{x_1}\right)^3 + \binom{u-2}{6}\frac{d^2}{7.8}\left(\frac{y_1}{x_1}\right)^6 + \cdots = 0.$$

This gives an impossible congruence mod 3, since 4, 5, 7, 8, ... are 3-adic units.

Suppose next that $y_1 \not\equiv 0 \pmod 3$. Since

$$\eta_1^3 = x_1^3 + 3x_1^2y_1\theta + 3x_1y_1^2\theta^2 + y_1^3\theta^3$$
$$\equiv 1 + 3x_1^2y_1\theta + 3x_1y_1^2\theta^2 = 1 + 3\delta,$$

say, η_1^u is defined for $u \equiv 0 \pmod 3$. Write $u = 3v + u_0$, $u_0 = 0, 1, 2$.

Then $\eta_1^{3v+u_0} \equiv \eta_2 \pmod 3$, $\eta_1^{u_0} \equiv \eta_2 \pmod 3$.

Comparing coefficients of θ^2, we see that $u_0 = 0, 1$.
Take first $u_0 = 0$. Then

$$(1 + 3\delta)^v = x_2 + y_2\theta.$$

Denote by b_t the coefficient of θ^2 in δ^t. Then

$$\sum_{t=0}^{\infty} 3^t b_t \binom{v}{t} = 0,$$

or

$$3x_1y_1^2v + 3^2x_1^4y_1^2\binom{v}{2} + \cdots = 0.$$

Divide out by $3x_1y_1^2$, and we have, say,

$$v + 3B_2\binom{v}{2} + 3^2B_3\binom{v}{3} + \cdots = 0,$$

where the B are polynomials in x_1, y_1 with integer coefficients. This is impossible, for if 3^λ is the highest power of 3 dividing v, all the other terms are divisible by $3^{\lambda+1}$. For the general term is

$$3^{t-1}B_t\binom{v}{t} \equiv 3^{t-1}\frac{vB_t}{t}\binom{v-1}{t-1}$$

and $3^{t-2}/t$ is a 3-adic integer. This is obvious on putting $t = t_0 3^\mu$ where 3^μ is the highest power of 3 dividing t.

Suppose next $u_0 = 1$. Then

$$(x_1 + y_1\theta)\left(\sum_{t=0}^{\infty} 3^t\delta^t\binom{v}{t}\right) = x_2 + y_2\theta.$$

Denote by c_t the coefficient of θ in δ^t. Then

$$x_1\sum_{t=0}^{\infty} 3^t b_t\binom{v}{t} + y_1\sum_{t=0}^{\infty} 3^t c_t\binom{v}{t} = 0.$$

Dividing out by $3x_1^2y_1^2$, we have, say,

$$2v + 3c_1\binom{v}{2} + 3^2c_2\binom{v}{3} + \cdots = 0,$$

and this is impossible as before.

3. When it is required to find all the integer solutions of an equation, the process may not be very complicated if fundamental units are not involved as in the following theorem. This deals with a conjecture enunciated by Ramanujan and first proved by Nagell. Many other proofs have been given and these have been analysed and discussed by Hasse. He has given a simpler version of Nagell's[4] proof as well as a generalization. We give Hasse's[5] proof of

Theorem 6

The equation $x^2 + 7 = 2^n$ has only the positive integer solutions given by $x = 1, 3, 5, 11, 181$ corresponding to $n = 3, 4, 5, 7, 15$.

When n is even, $n = 4$ is the only solution since

$$(2^{n/2})^2 - x^2 = 7, \qquad 2^{n/2} \pm x = 7, \qquad 2^{n/2} \mp x = 1.$$

We may now suppose that n is odd, and we write the equation as

$$\frac{x^2 + 7}{4} = 2^y, \tag{10}$$

where y is odd and $y \geqslant 3$.

We factorize the equation in the field $Q(\sqrt{-7})$, in which the integers have the form $(m + n\sqrt{-7})/2$ where $m \equiv n \pmod 2$, and in which unique factorization holds. Since

$$2 = \left(\frac{1 + \sqrt{-7}}{2}\right)\left(\frac{1 - \sqrt{-7}}{2}\right),$$

we have

$$\frac{x + \sqrt{-7}}{2} \equiv \pm\left(\frac{1 \pm \sqrt{-7}}{2}\right)^y,$$

and so

$$\left(\frac{1 + \sqrt{-7}}{2}\right)^y - \left(\frac{1 - \sqrt{-7}}{2}\right)^y = \pm\sqrt{-7}. \tag{11}$$

We show that the positive sign is impossible in equation (11).
Write this as

$$a^y - b^y = a - b.$$

Then

$$a^2 \equiv (1 - b)^2 \equiv 1 \pmod{b^2},$$