and x, y are consecutive terms of the sequence 1, 1, 3, 13, ... where $u_n = 5u_{n-1} - u_{n-2} - 1$.

The equation

$$x^2 + y^2 - x - y + 1 = xyz, x > 0, y > 0,$$

Now $x \mid y^2 - y + 1$, $y \mid x^2 - x + 1$, and $x = y = 1$.

We conclude by noting that when the divisibility conditions (46) are not satisfied, the problem becomes a very difficult one. Thus for $z(1 + xy) = x^2 + 2y^2$, the only procedure seems to be to try if there is a solution for various values of z, e.g.,[7] when $z = 43$, $x = 30905$, $y = 663738$.

5. *The equation* $x^m - y^n = 1$

This equation seems to have been first noticed by Catalan who proposed in 1842 the

Conjecture

The only solution in integers $m > 1$, $n > 1$, $x > 1$, $y > 1$ *of the equation*

$$x^m - y^n = 1 \tag{61}$$

is

$$m = 3, \quad n = 2, \quad x = 2, \quad y = 3. \tag{62}$$

This still remains unproved. An alternative form of the conjecture is

If p *and* q *are prime numbers and* $x > 1$, $y > 1$, *a similar result holds for*

$$x^p - y^q = 1. \tag{63}$$

Very few really general results are known, and even when they are simple, their proofs are usually rather complicated and often out of place here. Some of the results give estimates for possible values of m, n, p, q.

Perhaps the most general result is Cassels'[12]

Theorem 4

If in equation (63), $p > q > 2$ *or* $q > p > 2$, *then* $q \mid x$, $p \mid y$.

Another proof has been given by Hyyrö[13]. The result when $p = 2$ is due to Nagell[14].

Most of the other results deal with the cases when some of the variables p, q, x, y are given. Thus Le Veque[15] established a result proved later by Cassels[16] as the

Theorem 5

Suppose that (x, y) *are given in* (61), *and* (62) *is excluded. Let* μ, ν *be the least positive solution of*

$$x^u \equiv 1 \pmod{Y}, \qquad y^v \equiv 1 \pmod{X},$$

where X, Y *are the products of the odd primes dividing* x, y *respectively. Then* $m = \mu$, $n = \nu$, *except that* $m = 2$, $n = 1$ *may occur if* $\mu = \nu = 1$ *and* $x + 1$ *is a power of* 2.

When m, n are given in equation (61), the equation has only a finite number of solutions but these are not easily found. This is a particular case of Siegel's Theorem in Chapter 25. The result also follows from Mahler's[16a] result.

Theorem 6

The greatest prime factor of $ax^m + by^n$, $ab \neq 0$, $(x, y) = 1$, $m \geqslant 2$, $n \geqslant 3$ *tends to infinity as* $\max(|x|), (|y|)$ *tends to infinity.*

Proofs for equation (61) when m, n are primes satisfying various conditions have been given by LeVeque by using the methods for dealing with Fermat's last theorem.

Suppose next in equation (63) that p and q are given odd primes. Then Hyyrö[17] has shown that all the solutions can be given explicitly in terms of the convergents to the simple continued fraction for $q^{1-1/p}p^{1-1/q}$.

There are many results for special values of m, n and some are now given.

The equation $y^2 + 1 = x^p$, p *an odd prime.*

This was proved impossible for $x > 1$ in 1850 by Lebesgue[18]. A slightly dissimilar proof was given by Cassels[16]. Clearly $y \equiv 0 \pmod 2$, $x \equiv 1 \pmod 2$. Then from

$$(1 + iy)(1 - iy) = x^p,$$

$$1 + iy = i^r(u + iv)^p \quad r = 0, 1, 2, 3.$$

$$x = u^2 + v^2.$$

The factor i^r can be absorbed in the pth power, and so we need only consider $r = 0$. Then

$$1 = u^p - \frac{p.p-1}{2!}u^{p-2}v^2 + \cdots \pm puv^{p-1},$$

Hence $u = \pm 1$, and from a congruence mod 4, since v is even, $u \equiv 1 \pmod 4$ and so $u = 1$. Then

$$\frac{p.p-1}{2!} - \frac{p.p-1.p-2.p-3}{4!}v^2 + \cdots \pm pv^{p-3} = 0. \tag{64}$$

Then, since v is even, the general term can be written for $k \geqslant 1$ as

$$(-1)^{k-1}\frac{p.p-1.}{2!}\frac{p-2.p-3.\ldots.p-2k+1.}{(2k-2)!}\frac{1.2v^{2k-2}}{2k-1.2k}. \tag{65}$$

To prove that equation (64) is impossible (which is obvious if $(p.p-1)/2$ is odd since v is even), we need only show that for $k > 1$ the term (65) is

divisible by a higher power of 2 than for $k = 1$. The first two parts of (65) are integers. Also 2 cannot occur in the reduced denominator of the third part since, for $k > 1$,

$$2^{2k-2} > 1 + 2k - 2 > k.$$

The equation $y^2 - 1 = x^p$

The special case $p = 3$ of the equation

$$y^2 - 1 = x^p \tag{66}$$

was considered by Euler. The only solutions are $x = 0, -1, 2$.

We may suppose now that p is a prime > 3. The first general results are due to Nagell[14,19]. He proved very simply that p must be $\equiv 1 \pmod 8$ and $y \equiv 0 \pmod p$. He showed that equation (66) leads to

$$y \pm 1 = 2x_1^p, \qquad y \mp 1 = 2^{p-1}x_2^p,$$

and so

$$x_1^p - 2^{p-2}x_2^p = \pm 1. \tag{67}$$

Since $y \equiv 0 \pmod p$, it is easy to see that $(x + 1, x^p + 1) = p$, and $(x^p + 1)/(x + 1) \equiv 0 \pmod p$ but $\not\equiv 0 \pmod{p^2}$.

When $p \equiv 1 \pmod 8$, Nagell[14] showed by cyclotomic considerations applied to equation (68) that a necessary condition for solvability is that $u + v \equiv 1 \pmod 8$, where $u + v\sqrt{p}$ is the fundamental unit > 1 in the field generated by $\sqrt{p}$. This condition is equivalent to his other one that 2 is a biquadratic residue of p. Since Nagell proved the impossibility of equation (66) when $p \equiv 3, 5, 7 \pmod 8$, he thus showed that equation (66) is impossible for a set of primes of density $\frac{1}{4} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8} = \frac{7}{8}$.

It may be noted that from (67), estimates (rather large ones) had been found for the magnitude of possible p, x_1, x_2 by Obláth[20], Hyyrö[17] and Inkeri[23].

Some thirty years after Nagell's results, Chao Ko[24] proved the impossibility of equation (66). We give his proof which for $p \equiv 3, 5, 7 \pmod 8$ is similar to Nagell's but not so simple.

It easily follows from (66) that

$$x + 1 = py_1^2, \qquad \frac{x^p + 1}{x + 1} = py_2^2, \tag{68}$$

where $y = py_1y_2$ is odd.

Suppose first that $p \equiv 5, 7 \pmod 8$, and so $p = 8n + a$, $a = 5, 7$. Then from (67), $x \equiv a - 1 \pmod 8$. Write (66) as

$$\begin{aligned} y^2 &\equiv (x^2 - 1 + 1)^{4n}x^a + 1 \\ &\equiv x^a + 1 \pmod{x^2 - 1}. \end{aligned}$$

Hence the quadratic character

$$\left(\frac{x^a + 1}{x - 1}\right) = \left(\frac{2}{x - 1}\right) = 1.$$

This is impossible since $x - 1 \equiv 3, 5 \pmod 8$.

Suppose next that

$$p = 8n + 3 = 24m + a, \quad a = 11, 19.$$

Now

$$\begin{aligned} y^2 &= (x^3 - 1 + 1)^{8m}x^a + 1, \\ &\equiv x^a + 1 \pmod{x^3 - 1}. \end{aligned}$$

Hence

$$\left(\frac{x^a + 1}{x^3 - 1}\right) = 1.$$

Suppose first that $a = 11$ and so $x \equiv 2 \pmod 8$. Since $x^{11} - x^2 = x^2(x^9 - 1)$,

$$1 = \left(\frac{x^2 + 1}{x^3 - 1}\right) = \left(\frac{x^3 - 1}{x^2 + 1}\right) = \left(\frac{-x - 1}{x^2 + 1}\right) = \left(\frac{x^2 + 1}{x + 1}\right) = \left(\frac{2}{x + 1}\right) = -1.$$

Take $a = 19$, $x \equiv 2 \pmod 8$, and then

$$1 = \left(\frac{x^{19} + 1}{x^3 - 1}\right) = \left(\frac{x + 1}{x^3 - 1}\right) = -\left(\frac{x^3 - 1}{x + 1}\right) = \left(\frac{2}{x + 1}\right) = -1.$$

There remains $p \equiv 1 \pmod 8$, and now from (68), $x \equiv 0 \pmod 8$.

From (68),

$$py_2^2 = x^{p-1} - x^{p-2} + \cdots - x + 1. \tag{69}$$

Let $q < p$ be a positive odd integer. Write $p = kq + a$, $0 < a < q$, and so $(a, q) = 1$.

Put

$$E(t) = \frac{(-x)^t - 1}{(-x) - 1},$$

and so $E(t) \equiv 1 \pmod 8$. By (68),

$$py_2^2 = \frac{x^p + 1}{x + 1} = \frac{x^{kq+a} + 1}{x + 1}.$$

Since $x^q + 1 = (x + 1)\,E(q)$, this becomes

$$\begin{aligned} py_2^2 &= \frac{((x + 1)\,E(q) - 1)^k x^a + 1}{x + 1} \\ &\equiv \frac{(-1)^k x^a + 1}{x + 1} \equiv E(a) \pmod{E(q)}, \end{aligned} \tag{70}$$

since $k \equiv a + 1 \pmod 2$. Now

$$(E(a), E(q)) = \frac{(-x)^{(a,q)} - 1}{-x - 1} = 1.$$

We show that the quadratic character $(E(a)/E(q)) = 1$. We apply the Euclidean algorithm

$$\begin{aligned} q &= k_1 a + r_1, \quad 0 < r_1 < a \\ a &= k_2 r_1 + r_2, \quad 0 < r_2 < r_1 \\ r_1 &= k_3 r_2 + r_3, \quad 0 < r_3 < r_2 \\ &\cdots\cdots\cdots \\ r_{s-1} &= k_{s+1} r_{s-1} + r_{s+1}, \quad 0 < r_s < r_{s-1} \\ r_s &= k_{s+2} r_{s+1}. \end{aligned}$$

Then since $E(k_1 a + r_1) - E(r_1) \equiv 0 \pmod{E(a)}$,

$$\left(\frac{E(a)}{E(q)}\right) = \left(\frac{E(q)}{E(a)}\right) = \left(\frac{E(k_1 a + r_1)}{E(a)}\right) = \left(\frac{E(r_1)}{E(a)}\right)$$
$$= \left(\frac{E(r_{s-1})}{E(r_s)}\right) = \left(\frac{1}{E(r_s)}\right) = 1.$$

From (70),

$$\left(\frac{pE(a)}{E(q)}\right) = 1, \qquad \left(\frac{p}{E(q)}\right) = 1.$$

Since $x \equiv -1 \pmod p$ from (67),

$$\left(\frac{p}{E(q)}\right) = \left(\frac{E(q)}{p}\right) = \left(\frac{q}{p}\right).$$

We have a contradiction if q is taken as an odd quadratic non-residue of p. This proves the result.

We conclude this section by mentioning the impossibility of the equations

$$\begin{aligned} y^3 &= x^p + 1, \quad |x| > 1, \quad \text{Nagell}^{[24]} \\ y^3 &= x^p - 1, \quad |x| > 2, \quad \text{Nagell}^{[24]} \\ y^4 &= x^p + 1, \quad \text{Selberg}^{[25]}. \end{aligned}$$

The last result is now a special case of Chao Ko's theorem.

REFERENCES

1. Leon Bernstein. Zur Lösung der diophantischen Gleichung $m/n = 1/x + 1/y + 1/z$ insbesondere im Fall $m = 4$. *J. reine angew. Math.*, **211** (1962), 1–10.
2. R. Obláth. Sur l'équation diophantienne $4/n = 1/x_1 + 1/x_2 + 1/x_3$. *Mathesis*, **59** (1949), 308–316.

3. K. Yamamoto. On the diophantine equation $4/n = 1/x + 1/y + 1/z$. *Mem. Fac. Sci. Kyushu University*, Ser. A, **19** (1965), 37–47.
3a. L. A. Rosati. Sull'equazione diofantea $4/n = 1/x_1 + 1/x_2 + 1/x_3$. *Boll. Union Mat. Ital.*, (3) **9** (1954), 59–63.
4. L. J. Mordell. On the number of solutions in positive integers of the equation $yz + zx + xy = n$. *Am. J. Math.*, **45** (1923), 1–4.
5. R. F. Whitehead. On the number of solutions in positive integers of the equation $yz + zx + xy = n$. *Proc. Lond. Math. Soc.*, (2), **21** (1923), xx.
6. L. J. Mordell. The congruence $ax^3 + by^3 + c \equiv 0 \pmod{xy}$, and integer solutions of cubic equations in three variables. *Acta Math.*, **88** (1952), 77–83.
7. E. S. Barnes. On the diophantine equation $x^2 + y^2 + c = xyz$. *J. Lond. Math. Soc.*, **28** (1953), 242–244.
8. K. Goldberg, M. Newman, E. G. Straus, and J. D. Swift. The representations of integers by binary quadratic rational forms. *Archiv Math.*, **5** (1954), 12–18.
9. W. H. Mills. A system of quadratic diophantine equations. *Pacific J. Math.*, **3** (1953), 209–220.
10. W. H. Mills. A method for solving certain diophantine equations. *Proc. Am. Math. Soc.*, **5** (1954), 473–475.
11. W. H. Mills. Certain diophantine equations linear in one unknown. *Can. J. Math.*, **8** (1956), 5–12.
12. J. W. S. Cassels. On the equation $a^x - b^y = 1$, II. *Proc. Camb. Phil. Soc.*, **56** (1960), 97–103. This contains a history of the conjecture and many references.
13. S. Hyyrö. Über die Gleichung $ax^m - by^n = z$ und das Catalansche Problem. *Ann. Acad. Sci. Fennicae*, Series A. 1, 355 (1964), 39–48.
14. T. Nagell. Sur l'impossibilité de l'équation indéterminée $z^p + 1 = y^2$. *Norsk Mat. Forenings Skrifter.*, 1 (1921), Nr. 4.
15. W. J. Le Veque. On the equation $a^x - b^y = 1$. *Am. J. Math.*, **74** (1952), 325–331.
16. J. W. S. Cassels. On the equation $a^x - b^y = 1$. *Am. J. Math.*, **75** (1953), 159–162.
16a. K. Mahler. On the greatest prime factor of $ax^m + by^n$. *Nieuw Arch. Wisk.*, (3) **1** (1953), 113–122.
17. S. Hyyrö. Über das Catalansche Problem. *Ann. Univer. Turku*, Series A, **79** (1964), 3–9.
18. V. A. Lebesgue. Sur l'impossibilité, en nombres entiers, de l'équation $x^m = y^2 + 1$. *Nouv. Ann., Math.*, (1) 9 (1850), 178–181.
19. T. Nagell. Sur une équation à deux indéterminées. *Norsk Vid. Selsk Forh.*, 7 (1934), 136–139.
20. R. Obláth. Sobre ecuaciones diofánticas imposibles de la forma $x^m + 1 = y^n$. *Riv. Mat. Hispano-Am.*, **14** (1), (1941), 122–140. This contains many references.
21. C. L. Siegel. Die Gleichung $ax^n - by^n = c$. *Math. Ann.*, **114** (1937), 57–68.
22. R. Obláth. Über die Zahl $x^3 - 1$. *Mathematica Zutphen.* **B8** (1939), 161–172.
23. K. Inkeri and S. Hyyrö. On the congruence $3^{p-1} \equiv 1 \pmod{p^2}$ and the diophantine equation $x^2 - 1 = y^n$. *Ann. Univer. Turku*, Series A, **50** (1961), 3–4.
24. Chao Ko. On the diophantine equation $x^2 = y^n + 1$, $xy \neq 0$. *Scientia Sinica* (Notes), **14** (1964), 457–460.
25. T. Nagell. Des équations indéterminées $x^2 + x + 1 = y^n$ et $x^2 + x + 1 = 3y^n$. *Norsk. Mat. Forenings Skr.* Series I, **2** (1921), 12–14.
26. S. Selberg. Sur l'impossibilité de l'équation indéterminée $z^p + 1 = y^2$. *Norsk. Mat. Tidskrift*, **14** (1932), 79–80.