Annals of Math 30 (1928) → 1542

Index under Pellians

ON THE MULTIPLE SOLUTIONS OF THE PELL EQUATION.*

By D. H. Lehmer.

1. Introduction. Most of the literature written on the Pell equation is concerned with the discovery and application of its fundamental solution. Less attention has been paid to the multiple solutions; in fact, no systematic discussion has been made of their many properties. The more fundamental of these have been established by means of the hyperbolic functions.† It is the purpose of this note to indicate a method by which a complete study of the multiple solutions of the Pell equation can be deduced from Lucas' theory of recurring series of the second order. A number of formulas and theorems of particular interest will be found in section 5 and 6. These are readily derived from the principle proved in section 4. The notation used is that of Lucas' classical memoir,‡ and numbers in square brackets [ ] refer to the equations of this article.

2. The general recurring series of the second order. Let a and b be the roots of the equation

(1) $$x^2 - Px + Q = 0$$

where P and Q are any integers prime to each other. We have then $a+b = P$, $ab = Q$.

Let

(2) $$(a-b)^2 = \Delta = \delta^2 = P^2 - 4Q$$

so that

(3) $$a = \frac{P+\delta}{2}, \qquad b = \frac{P-\delta}{2}.$$

Lucas considers two symmetric functions of a and b namely:

$$U_n = \frac{a^n - b^n}{a-b}, \qquad V_n = a^n + b^n$$

and shows that they are recurring series of the second order with (1) for scales of relation. That is, they differ only in the choice of initial values:

$$U_0 = 0, \quad U_1 = 1, \qquad V_0 = 2, \quad V_1 = P.$$

* Received February 9, 1928.

† Mathews: Theory of Numbers, pp. 93-95. D. H. Lehmer: Annals of Math., (2), vol. 27, pp. 471-476. Cf. also Cunningham: Brit. Assn. Rept. 1907, p. 462.

‡ Amer. Jour. of Math., vol. 1 (1877), pp. 184-240, 289-321.

In general let W_n be the nth term of the recurring series whose scale is (1) so that

$$W_{n+2} = P W_{n+1} - Q W_n \tag{4}$$

and is determined uniquely by the choice of certain values for W_0 and W_1. Then it is easy to verify that:

$$W_n = W_1 U_n - Q W_0 U_{n-1}. \tag{5}$$

In fact the series W_n thus defined satisfies the recurrence (4) and has for $n = 0$ and $n = 1$ the proper values namely W_0 and W_1. For example

$$V_n = P U_n - 2 Q U_{n-1}. \tag{6}$$

3. **The Pellian case.** Let us consider two functions X_n and Y_n satisfying the recurrences:

$$X_{n+2} = 2 X_1 X_{n+1} - X_n, \qquad Y_{n+2} = 2 X_1 Y_{n+1} - Y_n,$$

with $X_0 = 1$, $Y_0 = 0$, and $(X_1 Y_1)$ to be determined later. In the notation of section 2,

$$P = 2 X_1, \qquad Q = 1, \tag{7}$$

and (5) becomes:

$$X_n = X_1 U_n - U_{n-1}.$$

Comparing this with (6) and (7) and using (4) we have:

$$X_n = \frac{1}{2} V_n, \qquad Y_n = Y_1 U_n. \tag{8}$$

Consider the expression:

$$V_n^2 - \Delta U_n^2 = 4 Q^n. \qquad [46]$$

From (8), (2) and (7) we have

$$X_n^2 - \frac{X_1^2 - 1}{Y_1^2} Y_n^2 = 1. \tag{9}$$

Thus far X_1 and Y_1 have been left arbitrary. Now we impose the condition that

$$\frac{X_1^2 - 1}{Y_1^2} = D$$

where D is some integer, not a square. That is $(X_1 Y_1)$ are chosen so that

$$X_1^2 - D Y_1^2 = 1.$$

When this is done equation (9) becomes

$$X_n^2 - D Y_n^2 = 1, \tag{10}$$

which shows that $(X_n Y_n)$ are multiple solutions of the Pell equation. The initial values $(X_1 Y_1)$ are taken as the fundamental solution of (10) and may be found by well known methods. From (3) we have:

$$a = \frac{2X_1 + \sqrt{4X_1^2 - 4}}{2} = X_1 + \sqrt{D}\,Y_1,$$

$$b = \frac{2X_1 - \sqrt{4X_1^2 - 4}}{2} = X_1 - \sqrt{D}\,Y_1.$$

4. **Principle of substitution.** Summing up the results of the preceding section we have the following principle:

For every relation in Lucas' theory there exists one in terms of the multiple solutions of the Pell equation in which:

$$U_n, V_n, P, Q, \delta^2 = \Delta, a, b$$

are replaced by

$$Y_n/Y_1, 2X_n, 2X_1, 1, 4DY_1^2, X_1 + \sqrt{D}\,Y_1, X_1 - \sqrt{D}\,Y_1$$

respectively.

Thus the equations:

[6] $$V_n + \delta U_n = 2a^n, \qquad V_n - \delta U_n = 2b^n$$

become the familar relations:

$$X_n + \sqrt{D}\,Y_n = (X_1 + \sqrt{D}\,Y_1)^n,$$
$$X_n - \sqrt{D}\,Y_n = (X_1 - \sqrt{D}\,Y_1)^n.$$

The formulas for negative arguments:

[50] $$U_{-n} = -U_n/Q^n, \qquad V_{-n} = V_n/Q^n.$$

become:

$$Y_{-n} = -Y_n, \qquad X_{-n} = X_n.$$

The addition formulas:

[49] $$2U_{m+n} = U_m V_n + U_n V_m,$$
$$2V_{m+n} = V_m V_n + \Delta U_m U_n$$

become:

$$Y_{m+n} = Y_m X_n + Y_n X_m,$$
$$X_{m+n} = X_m X_n + D Y_m Y_n,$$

and so on.

5. **Algebraic theory of X_n and Y_n.** A very large number of relations may be written down by applying the principle of the foregoing section.

The following relations together with those preceding constitute the most important ones.

(11) [87] $$X_{2n} = 2X_n^2 - 1 = X_n^2 + DY_n^2,$$

[3] $$Y_{2n} = 2Y_n X_n,$$

[51] $$X_{m-n} = X_m X_n - DY_m Y_n,$$
$$Y_{m-n} = Y_m X_n - Y_n X_m,$$

$$Y_1 X_n = X_1 Y_n - Y_{n-1} = \frac{1}{2}(Y_{n+1} - Y_{n-1}) = Y_{n+1} - Y_n X_1,$$

$$X_{n+m} X_{n-m} + DY_{n+m} Y_{n-m} = X_{2n},$$
$$X_{n+m} X_{n-m} - DY_{n+m} Y_{n-m} = X_{2m},$$

[33] $$X_{n+m}^2 - X_n^2 = DY_m Y_{2n+m},$$

[32] $$Y_{n+m}^2 - Y_n^2 = Y_m Y_{2n+m},$$

[52] $$X_n + X_m = 2X_{(n+m)/2} X_{(n-m)/2},$$
$$Y_n + Y_m = 2Y_{(n+m)/2} X_{(n-m)/2},$$

[70] $$X_n = 2^{n-1} X_1^n + \frac{1}{2}\sum_{i=1}^{[\frac{n}{2}]}(-1)^i \frac{n}{i}\binom{n-i-1}{i-1}(2X_1)^{n-2i},$$

$$Y_{n+1} = Y_1 \sum_{i=0}^{[\frac{n}{2}]}(-1)^i \binom{n-i}{i}(2X_1)^{n-2i},$$

$$2^n X_n = \sum_{i=0}^{[\frac{n+1}{2}]}\binom{n}{2i} D^i (2Y_1)^{2i}(2X_1)^{n-2i},$$

$$2^{n-1} Y_n = Y_1 \sum_{i=0}^{[\frac{n-1}{2}]}\binom{n}{2i+1} D^i (2Y_1)^{2i}(2X_1)^{n-2i-1},$$

[44] $$\frac{X_n}{X_1} = (-1)^{\frac{n-1}{2}} + 2\sum_{i=0}^{\frac{n-1}{2}}(-1)^i X_{n-2i-1}, \qquad (n = 2k+1).$$

[42] $$\frac{Y_n}{Y_1} = -1 + 2\sum_{i=0}^{\frac{n-1}{2}} X_{n-2i-1}, \qquad (n = 2k+1),$$

[41] $$\frac{Y_n}{Y_1} = 2\sum_{i=0}^{\frac{n-2}{2}} X_{n-2i-1}. \qquad (n = 2k).$$

These are a very few of the hundreds of relations that exist between the functions X_n and Y_n. A glance at Lucas' memoir will indicate what is possible in this direction. Relations in terms of determinants, continued fractions, binomial coefficients, continued radicals, logarithms, cyclotomic functions, infinite series etc. are included in the algebraic theory of X_n, Y_n.

Every formula in X_n, Y_n or D may be generalised by replacing these quantities by X_{nr}, Y_{nr}/Y_r, and DY_r^2 respectively. By replacing X_n by $\cos n\theta$, Y_n by $\sin n\theta/\sin\theta$ and D by $\sin^2\theta$, every relation in X_n and Y_n may be transformed into a formula in circular functions. If X_n is replaced by $\cosh ny$, Y_n by $\sinh ny/\sinh y$, and D by $\sin^2 ny$ the hyperbolic functions may be studied in like manner.

6. **The arithmetic theory of X_n and Y_n.** The equations (8) show how intimate the connection is between the number-theoretic properties of (X_n, Y_n) and (U_n, V_n). These equations are sufficient for the most part to establish the following fundamental properties of X_n and Y_n. As Carmichael† has pointed out, Lucas was inaccurate in certain of his theorems by not allowing for the singularity of the prime 2 in his theory. Fortunately 2 is not such an exception in our discussion. The theorems marked with a * cannot be deduced immediately from Lucas' memoir. The present writer in a paper which he hopes to publish shortly has considered an extension of Lucas' theory by which he has been able to strengthen many of Lucas' classical theorems. Some of the theorems marked * indicate the effects of this extension on the theory of the Pell equation.

THEOREM 1. *X_n and Y_n are relatively prime.*

THEOREM 2. *If the G. C. D. of m and n is d then the G. C. D. of Y_m and Y_n is Y_d.*

THEOREM 3. *Y_m is a divisor of Y_n if and only if m is a divisor of n.*

COROLLARY: *Every Y_n is a multiple of Y_1.*

THEOREM 4. *X_m is a divisor of X_n if and only if n/m is an odd divisor of n.*

THEOREM 5. *If Y_ω is the first Y to contain the factor m then Y_n is divisible by m if and only if $n = k\omega$. (The number ω is called the rank of apparition of m in the series Y_n.)*

* THEOREM 6. *The number of terms less than Y_n and prime to Y_n, with the exception of the ever present common factor Y_1, is Euler's $\varphi(n)$.*

* THEOREM 7. *If p is a prime factor of D prime to Y_1, then $Y_1 \cdot Y_2 \cdot Y_3 \cdots Y_{p-1} \equiv -(X_1/p) \pmod p$ where (X_1/p) is Legendre's symbol.*

This theorem is an extension of Wilson's theorem. The converse of this theorem is true and gives a theoretical test for primality. Theorems 3, 6 and 7 exhibit properties of Y_n similar to those of the natural numbers. Also compare theorems 9 and 10.

† Annals of Math. (2), vol. 15, pp. 30–70.

* THEOREM 8. *If p is an odd prime not dividing DY_1, then its rank of apparition is some divisor of* $\frac{1}{2}\left\{p-\left(\frac{D}{p}\right)\right\}$.

This is the law of apparition of a prime p and is an extension of Fermat's theorem. In what follows p is a prime.

THEOREM 9. *If p divides Y_1 it divides Y_n. If p divides D, but not Y_1, then the rank of apparition of p is p, and p occurs to the first power as a divisor of Y_p.*

THEOREM 10. *If ω is the rank of apparition of p^α and if $\varkappa$ is any number prime to p, then $Y_{\varkappa\omega p^\lambda}$ contains the factor $p^{\alpha+\lambda}$ but no higher power of p.*

This is the law of repetition of the prime p. Unlike Lucas' law it holds for $p=2$.

* THEOREM 11. *If $m=\prod P_i^{\alpha_i}$ and if we define a function ψ_m by*

$$\psi_m=\frac{\prod p_i^{\alpha_i-1}\left[p_i-\left(\frac{D}{p_i}\right)\right]}{2^\varkappa}$$

where Legendre's symbol is taken as zero if p divides D and where $\varkappa$ is the number of distinct prime factors of m not dividing D, then $Y_{\psi_m}\equiv 0 \pmod{m}$. This corresponds to Euler's φ-function and his generalisation of Fermat's theorem. Compare Mathews† who replaces ψ_m by the L. C. M. of its factors.

*THEOREM 12. *If m is prime to D the primitive odd prime factors of Y_m are of the form $2km\pm 1$, and those of X_m are of the form $4km\pm 1$.*

*THEOREM 13. (a) *If p is a prime of the form $4n+1$, then $4X_{pr}/X_r$ and $4Y_{pr}/Y_r$ may both be put in the form t^2-Du^2.* (b) *If p is a prime of the form $4n-1$, then $4X_{pr}/X_r$ may be put in the form t^2+Dpu^2 and $4Y_{pr}/Y_r$ may be put in the form Dt^2+pu^2.*

This is an extension of Gauss' theorem about the cyclotomic function $4(x^p-1)/(x-1)$. Attention should be called to certain inaccuracies in Lucas' results on this topic.

Finally we give three typical theorems for determining the primality or non-primality of an integer N prime to $2DY_2$. The first is of theoretical interest only, the second‡ is a practical test for a general integer N. The third is not as impractical as it would first appear. Taken with equation (10) it becomes a very effective test for the numbers in question.

THEOREM 14. *If $(N\pm 1)/2$ is the rank of apparition of N, then N is a prime.*

---

† Mathews, loc. cit., p. 94.

‡ Compare the writer's note in the Bull. Amer. Math. Soc., vol. 34 (1928), p. 54.

*THEOREM 15. *If $Y_{N\pm 1} \equiv 0 \pmod{N}$ and if $Y_{(N\pm 1)/p} \equiv r \not\equiv 0 \pmod{N}$, and if the G. C. D. of N and r is ϱ, then the prime factors of N/ϱ are of the form $kp^{\alpha} \pm 1$ where α is the highest power to which the prime p occurs as a factor of $N \pm 1$.*

*THEOREM 16. *The number $2^n - 1$ with n odd is a prime if and only if it divides the numerator of the convergent of order 2^{n-1} to the square root of three.*

In case the reader may wish to verify many of the above theorems we subjoin a table giving the first 30 terms Y_n of the most fundamental series namely $D = 2$ and also their prime factors.

1542

n	Y_n	Non-primitive factors	Primitive factors
1	2	—	2
2	12	2^2	3
3	70	2	$5 \cdot 7$
4	408	$2^3 \cdot 3$	17
5	2378	2	$29 \cdot 41$
6	13860	$2^2 \cdot 3^2 \cdot 5 \cdot 7$	11
7	80782	2	$13^2 \cdot 239$
8	470832	$2^4 \cdot 3 \cdot 17$	577
9	2744210	$2 \cdot 5 \cdot 7$	$197 \cdot 199$
10	15994428	$2^2 \cdot 3 \cdot 29 \cdot 41$	$19 \cdot 59$
11	93222358	2	$23 \cdot 353 \cdot 5741$
12	543339720	$2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 17$	1153
13	3166815962	2	$79 \cdot 599 \cdot 33461$
14	18457556052	$2^2 \cdot 3 \cdot 13^2 \cdot 239$	$113 \cdot 337$
15	107578520350	$2 \cdot 5^2 \cdot 7 \cdot 29 \cdot 41$	$31^2 \cdot 269$
16	627013566048	$2^5 \cdot 3 \cdot 17 \cdot 577$	665857
17	3654502875938	2	$103 \cdot 137 \cdot 8297 \cdot 15607$
18	21300003689580	$2^2 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 197 \cdot 199$	13067
19	124145519261542	2	$37 \cdot 179057 \cdot 9369319$
20	723573111879672	$2^3 \cdot 3 \cdot 17 \cdot 19 \cdot 29 \cdot 41 \cdot 59$	$241 \cdot 5521$
21	4217293152016490	$2 \cdot 5 \cdot 7^2 \cdot 13^2 \cdot 239$	$4663 \cdot 45697$
22	24580185800219268	$2^2 \cdot 3 \cdot 23 \cdot 353 \cdot 5741$	$43 \cdot 89 \cdot 11483$
23	143263821649299118	2	$47 \cdot 229 \cdot 982789 \cdot 6771937$
24	835002744095575440	$2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 577 \cdot 1153$	$97 \cdot 13729$
25	4866752642924153522	$2 \cdot 29 \cdot 41$	$1549 \cdot 29201 \cdot 45245801$
26	28365513113449345692	$2^2 \cdot 3 \cdot 79 \cdot 599 \cdot 33461$	$22307 \cdot 66923$
27	165326326037771920630	$2 \cdot 5 \cdot 7 \cdot 197 \cdot 199$	$53 \cdot 146449 \cdot 7761799$
28	963592443113182178088	$2^3 \cdot 3 \cdot 13^2 \cdot 17 \cdot 113 \cdot 239 \cdot 337$	1535466241
29	5616228332641321147898	2	$44560482149 \cdot 63018038201$
30	32733777552734744709300	$2^2 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 19 \cdot 29 \cdot 31^2 \cdot 41 \cdot 59 \cdot 269$	$601 \cdot 2281$