AN EXTENDED THEORY OF LUCAS' FUNCTIONS.*

By D. H. Lehmer.

Introduction. In this paper we extend the arithmetic theory of Lucas' functions† U_n, V_n defined by

$$U_n = (a^n - b^n)/(a - b), \qquad V_n = a^n + b^n, \tag{1.1}$$

where a and b are the roots of

$$x^2 - Px + Q = 0, \tag{1.2}$$

P and Q being coprime integers, to the case in which P is replaced by $R^{1/2}$, where R is any integer prime to Q.

This change of hypothesis introduces a duality between R and the discriminant $\Delta = R - 4Q$ of (1.2). In Lucas' theory Δ cannot be of the form $4n+2$ or $4n+3$.

In section 1 we develop the generalities necessary to our theory, and obtain from the extended laws of apparition and repetition‡ a new generalisation of Fermat's theorem and Euler's totient function. It is in this section that the similarities between the old and the new theories are most apparent. The rest of the paper is devoted to problems which cannot be completely answered by previous investigations. In sections 2 certain exceptional series U, V are discussed and Wilson's theorem is generalised. Section 3 is devoted to a certain irreducible binary form G_n representing numbers whose factors are of the forms $kn \pm 1$. The connection between G_n and Sylvester's§ ψ_n is established. In section 4, a, b are replaced by a^r, b^r. The invariants of this transformation are discussed, and from the inverse transformation a new extension of the theory of quadratic and higher residues is reached. Finally in section 5, the theory is applied to the identification of large primes. Practical as well as theoretical tests are given and illustrated.

---

* Received August 14, 1929; in revised form December 26, 1929.

† Lucas, *Amer. Jour. of Math.*, 1 (1878), pp. 184–239, 289–321. Dickson, *Amer. Math. Monthly*, 12 (1905), pp. 86–89. Birkhoff and Vandiver, *Annals of Math.*, (2), 5 (1904), pp. 173–180. Carmichael, *Annals of Math.*, (2), 15 (1913–14), pp. 30–70. Dickson, *History of the Theory of Numbers*, vol. 1, ch. 17.

‡ Lucas, *loc. cit.*, pp. 209, 289, 294.

§ *Amer. Jour. of Math.*, 2 (1879), pp. 357–381. *Coll. Papers* 3, p. 325.

SECTION 1. GENERALITIES.

1. **Fundamental formulas.** Consider the equation

$$x^2 - R^{1/2}x + Q = 0 \tag{1.3}$$

where R and Q are coprime integers. Let a and b be the roots of (1.3). Then

$$\begin{aligned} a+b &= R^{1/2}, \qquad ab = Q, \\ a-b &= \delta = \Delta^{1/2} = (R-4Q)^{1/2}, \\ 2a &= R^{1/2}+\delta = R^{1/2}+(R-4Q)^{1/2}, \\ 2b &= R^{1/2}-\delta = R^{1/2}-(R-4Q)^{1/2}. \end{aligned} \tag{1.4}$$

We discuss the two functions defined by

$$U_n = (a^n - b^n)/(a-b), \qquad V_n = a^n + b^n, \tag{1.5}$$

where n is an integer $\geqq 0$. Hence

$$U_{n+2} = R^{1/2}U_{n+1} - QU_n, \qquad V_{n+2} = R^{1/2}V_{n+1} - QV_n. \tag{1.6}$$

It follows that U_{2n+1}, V_{2n} are integers, while U_{2n}, V_{2n+1} are integral multiples of $R^{1/2}$. Thus for $R=5$, $Q=-3$

n	0,	1,	2,	3,	4,	5,
U_n	0,	1,	$5^{1/2}$,	8,	$11\cdot 5^{1/2}$,	79,
V_n	2,	$5^{1/2}$,	11,	$14\cdot 5^{1/2}$,	103,	$145\cdot 5^{1/2}$,

n	6,	7,	8,	9,	10.
U_n	$112\cdot 5^{1/2}$,	797,	$1133\cdot 5^{1/2}$,	8056,	$11455\cdot 5^{1/2}$.
V_n	1034,	$1469\cdot 5^{1/2}$,	10447,	$14854\cdot 5^{1/2}$,	105611.

We shall need the following identities given by Lucas.

$$V_n^2 - \Delta U_n^2 = 4Q^n. \tag{1.7}$$

$$2U_{n+m} = U_nV_m + V_nU_m, \qquad 2V_{n+m} = V_mV_n + \Delta U_nU_m. \tag{1.8}$$

$$2Q^mU_{n-m} = U_nV_m - V_nU_m, \qquad 2Q^mV_{n-m} = V_nV_m - \Delta U_nU_m. \tag{1.9}$$

$$U_{2n} = U_nV_n, \qquad V_{2n}^2 = V_n - 2Q^n. \tag{1.10}$$

$$U_{ms} = \sum_{r=0}^{(s-1)/2} \frac{s}{r}\binom{s-r-1}{r-1} Q^{mr}\delta^{s-2r-1}U_m^{s-2r}, \tag{1.11}$$

where s is odd.

With every pair of series U, V having constants $(R^{1/2}, Q)$ there are associated three other pairs of series having constants $(-R^{1/2}, Q)$, $((-R)^{1/2}, -Q)$, $(-(-R)^{1/2}, -Q)$, whose corresponding terms do not differ in absolute value from the terms of the original pair U, V. For most purposes of this paper, the 4 pairs are equivalent. We shall take as representative the pair in which $R^{1/2}$ is real and positive. A factor $R^{1/2}$ of U_n or V_n may in general be dropped, as we shall be interested chiefly in the integral coefficient of $R^{1/2}$. The series $\overline{U}, \overline{V}$ obtained from U, V by suppressing $R^{1/2}$ in the latter, obey the following recurrences,

$$\overline{U}_n = [1+(R-1)\,i^{n-1}\sin \pi n/2]\,\overline{U}_{n-1} - Q\,\overline{U}_{n-2},$$
$$\overline{V}_n = [1+(R-1)\,i^{n}\quad\cos \pi n/2]\,\overline{V}_{n-1} - Q\,\overline{V}_{n-2}.$$

DEFINITION. $R^{1/2} \equiv 0 \pmod m$ *states that* $R^{1/2}$ *is divisible by* m *when and only when* $R \equiv 0 \pmod{m^2}$.

2. **Fundamental theorems.** The proofs of the following 5 fundamental theorems on divisibility parallel those of the corresponding Lucas theory, and may be omitted.*

THEOREM 1.1. *U_n and V_n are both prime to Q.*

THEOREM 1.2. *The G. C. D. of U_n and V_n is 1 or 2.*

THEOREM 1.3. *U_n is divisible by 2 in the following cases only*

1)	$R = 4k,$	$Q = 2l+1,$	$n = 2h,$
2)	$R = 4k+2,$	$Q = 2l+1,$	$n = 4h,$
3)	$R = 4k\pm 1,$	$Q = 2l+1,$	$n = 3h.$

V_n is divisible by 2 in the following cases only

1)	$R = 4k,$	$Q = 2l+1,$	
2)	$R = 4k+2,$	$Q = 2l+1,$	$n = 2h,$
3)	$R = 4k\pm 1,$	$Q = 2l+1,$	$n = 3h.$

THEOREM 1.4. *If the G. C. D. of m and n is ρ then the G. C. D. of U_n and U_m is U_ρ.*

THEOREM 1.5. *If n is divisible by m, then U_n is divisible by U_m. If n/m is an odd integer, then V_n is divisible by V_m.*

3. **Law of repetition.** THEOREM† 1.6. *If 2α is a positive integer such that q^α is the highest power of a prime q dividing U_m, and if k is any*

* For Theorems 1.1, 1.2, 1.3, and 1.4 see Carmichael, *loc. cit.*, pp. 35-37. For Theorem 1.5 see Lucas, *loc. cit.*, p. 199.

† This theorem is analogous to Carmichael's Theorem X, p. 42. The proof given above is however shorter and illustrates the advantages of using Lucas' algebraic relations.

integer not divisible by q, then for any integer λ, U_{kmq^λ} is divisible by $q^{\alpha+\lambda}$, and if $q^\alpha \nmid 2$, this is the highest power of q dividing U_{kmq^λ}.

Proof. Case 1, q odd. The term involving the lowest power of U_m in (1.11) is $s Q^{m(s-1)/2} U_m$. Put $s = q$, then $q^{\alpha+1}$ is the highest power of q dividing U_{mq}. Put $s = k$, k odd, then U_{mk} contains the factor q to the same power as U_m. Let k be even, $k = 2^\mu k'$, where k' is odd. Then by (1.10)

$$U_{mk} = U_{mk'} V_{mk'} V_{2mk'} V_{4mk'} \cdots V_{mk/2}.$$

By Theorem 1.2 none of the V's on the right have an odd factor in common with U_{mk}. Hence U_{mk} contains the same power of q as $U_{mk'}$, or U_m.

Case 2, $q = 2$. Again by (1.11) U_{mk} contains the same power of 2 as U_m. From Theorem 1.3 V_{mk} is even, if U_{mk} is even, but by Theorem 1.2 their G. C. D. $\leqq 2$. Hence if U_{mk} is divisible by 2^α, where $\alpha > 1$, then by (1.10), $2^{\alpha+1}$ is the highest power of 2 in U_{2mk}.

The theorem now follows by λ applications of the above reasoning.

4. **The law of apparition.** The preceding theorem gives a complete account of the divisibility of U_n by the given prime q, provided we know the term U_ω in which q appears to the first time as a factor in the series U, and also the power to which q appears. The number ω (if it exists), we call *the rank of apparition of q*. If $q = 2$, the number ω is given by Theorem 1.3; in fact $\omega = 2$, 3, or 4, according as $R = 4k$, $2k+1$, or $4k+2$. Consider next odd primes. *In this paper the symbol p designates an arbitrary odd prime.* If we subtract and add the p-th powers of both sides of the last pair of equations (1.4) we get

$$(1.12)\qquad \begin{aligned} 2^{p-1} U_p &= \sum_{k=0}^{(p-1)/2} \binom{p}{2k+1} R^{(p-2k-1)/2} \Delta^k, \\ 2^{p-1} V_p &= \sum_{k=0}^{(p-1)/2} \binom{p}{2k} R^{(p-2k)/2} \Delta^k. \end{aligned}$$

On account of the divisibility of the binomial coefficients by p we have

$$(1.13)\qquad \begin{aligned} U_p &\equiv \Delta^{(p-1)/2} \equiv \left(\frac{\Delta}{p}\right) \equiv \varepsilon \pmod p, \\ V_p &\equiv R^{1/2} R^{(p-1)/2} \equiv R^{1/2}\left(\frac{R}{p}\right) \equiv \sigma R^{1/2} \pmod p. \end{aligned}$$

Put $n = p$ and $m = 1$ in (1.9), then

$$(1.14)\qquad 2Q U_{p-1} = U_p V_1 - U_1 V_p, \qquad 2Q V_{p-1} = V_p V_1 - \Delta U_p U_1.$$

Since $U_1 = 1$, $V_1 = R^{1/2}$, (1.13) gives

(1.15) $2\,Q\,U_{p-1}/R^{1/2} \equiv \sigma - \varepsilon$; $\quad 2\,Q\,V_{p-1} \equiv R\sigma - \Delta\varepsilon = 2\,\varepsilon + R\,(\sigma - \varepsilon)$, $(\mathrm{mod}\ p)$.

From (1.8) we have

$$2\,U_{p+1} = U_1\,V_p + V_1\,U_p, \qquad 2\,V_{p+1} = V_1\,V_p + \Delta\,U_1\,U_p$$

and therefore

$$2\,U_{p+1}/R^{1/2} \equiv \sigma + \varepsilon, \quad 2\,V_{p+1} \equiv R\sigma + \Delta\varepsilon = R\,(\sigma + \varepsilon) - 4\,Q\varepsilon \pmod{p}.$$

From (1.10) we have

$$U_{2p}/R^{1/2} \equiv \sigma\varepsilon, \qquad V_{2p} \equiv R\sigma^2 - 2\,Q \pmod{p}.$$

Since R is prime to Q we cannot have $\varepsilon = \sigma = 0$. Hence there are 8 possible cases for which we tabulate the above congruences.

TABLE I.

Case	ε	σ	$2QU_{p-1}/R^{1/2}$	U_p	$2\,U_{p+1}/R^{1/2}$	$U_{2p}/R^{1/2}$	V_{p-1}	$V_p/R^{1/2}$	$2\,V_{p+1}$	V_{2p}
1	1	1	0	1	2	1	2	1	$2R-4Q$	$R-2Q$
2	1	-1	2	1	0	-1	$2-R/Q$	-1	$-4Q$	$R-2Q$
3	1	0	1	1	1	0	$2-R/2Q$	0	$R-4Q$	$-2Q$
4	-1	1	-2	-1	0	-1	$-2+R/Q$	1	$4Q$	$R-2Q$
5	-1	-1	0	-1	-2	1	-2	-1	$4Q-2R$	$R-2Q$
6	-1	0	-1	-1	-1	0	$-2+R/2Q$	0	$4Q-R$	$-2Q$
7	0	1	-1	0	1	0	$R/2Q$	1	R	$R-2Q$
8	0	-1	1	0	-1	0	$-R/2Q$	-1	$-R$	$R-2Q$

From inspection of this table we deduce the following fundamental theorem which further generalizes Lucas' extension of Fermat's theorem.

THEOREM 1.7. *If RQ is not divisible by the odd prime p, then*

$$U_{p-\sigma\varepsilon} \equiv 0 \pmod{p}.$$

Put $R = p$ so that $\sigma = 1$, then U becomes of Lucas' type and we have Lucas' theorem*

$$U_{p-\varepsilon} \equiv 0 \pmod{p}.$$

Further let Δ be a perfect square prime to p so that $\varepsilon = 1$, then a and b are integers and

$$U_{p-1} = (a^{p-1} - b^{p-1})/(a - b) \equiv 0 \pmod{p}$$

or setting $c = a/b$ we have $c^{p-1} - 1 \equiv 0 \pmod{p}$ which is Fermats theorem.

THEOREM 1.8. *If ω is the rank of apparition of p, then U_n is divisible by p if and only if $n = k\omega$*

* *Loc. cit.*, pp. 295–297.

Proof. This theorem follows at once from Theorem 1.4 since U_ϱ is not divisible by p if $\varrho < \omega$. Theorems 1.7 and 1.8 give the following law of apparition.

THEOREM 1.9. *If p is an odd prime not dividing QR, then its rank of apparition ω is some divisor of $p - \sigma\varepsilon$. If p divides Q no term of the series is divisible by p. If p^2 divides R, then $\omega = 2$. If R contains the factor p but not p^2, $\omega = 2p$. If p divides Δ, then $\omega = p$.*

THEOREM* 1.10. *If ω is odd, then V_n is not divisible by p for any value of n. If ω is even $(2k)$, then $V_{(2n+1)k}$ is divisible by p for every n, but no other terms of the series contain a factor p.*

Theorem 1.9 gives a good restriction on the value of ω. A definite formula for ω is not to be expected any more that a formula for the exponent to which a given number c belongs modulo p. In certain special cases ω can be given in advance but this will be discussed in section 5. The problem of determining the power to which p appears as a factor of U_ω is a generalization of the classical problem of Fermat's quotient $(c^{p-1} - 1)/p$. A complete solution of this simpler problem has not been discovered.† In the following special case we have however the

THEOREM 1.11. *If p divides Δ so that $\omega = p$, and if $p > 3$, then U_p is not divisible by p^2.*

Proof. By (1.12)

$$2^{p-1} U_p \equiv p R^{(p-1)/2} + \left(\frac{p}{3}\right) R^{(p-3)/2} \Delta \pmod{p^2}.$$

But p divides both Δ and $\left(\frac{p}{3}\right)$. Hence

$$2^{p-1} U_p \equiv p R^{(p-1)/2} \pmod{p^2}.$$

Since R and Δ have no odd common factor and p is prime to R, the theorem follows. If p is 3, (1.12) becomes $4 U_3 = 3R + \Delta$. Hence U_3 is divisible by 9 if and only if $\Delta = 3k$ where k is prime to 3 and $R = 3n - k$.

5. Generalization of Euler's totient function. We define $T(m)$ m an arbitrary integer by

$$(1.16) \quad T(m) = 2 \prod_{i=1}^{\nu} q_i^{\alpha_i - 1} \left\{ q_i - \left(\frac{R\Delta}{q_i}\right) \right\}, \quad \text{where} \quad m = \prod_{i=1}^{\nu} q_i^{\alpha_i}.$$

Here $\left(\frac{R\Delta}{p}\right)$ is Legendre's symbol or zero according as p does or does not divide $R\Delta$, while the symbol $\left(\frac{R\Delta}{2}\right)$ is defined to be $0, -1$ or -2 according as $R = 4k, 2k+1$ or $4k+2$.

* Carmichael, *loc. cit.*, p. 47.

† Dickson, *History of the Theory of Numbers*, vol. 1, ch. 4.

THEOREM 1.12. *If (R, Q) are the constants of the series U, then for any number m prime to Q*

$$U_{T(m)} \equiv 0 \pmod{m}.$$

Proof. In fact $\left\{p - \left(\frac{R\Delta}{p}\right)\right\} = p - \sigma\varepsilon$. Hence by the laws of apparition and repetition $U_{T(m)} \equiv 0 \pmod{p_i^{\alpha_i}}$. Also by Theorem 1.3 $U_{T(m)} \equiv 0 \pmod{2^\alpha}$ and the theorem follows.

It can be shown that if $S(m)$ designates the L. C. M. of the factors of $T(m)$, then $U_{S(m)} \equiv 0 \pmod{m}$. Thus the rank of apparition of m is at most $S(m)$. In fact the rank of apparition of m may be $< S(m)$. For example, $R = 5$, $Q = -3$, $m = 103$, $S(m) = 104$, but $\omega = 8$.

6. **The divisors of U_n.** In the preceding discussion the prime p was considered as given. Now let us suppose that ω is given and that it is required to determine the primes p which correspond to ω.

DEFINITIONS: *A prime factor of U_n is called primitive if its rank of apparition in the series U is n. Otherwise it is called non-primitive. A primitive factor of U_n is called intrinsic if it divides the index n. Otherwise it is called extrinsic.**

From the law of apparition we have the following

THEOREM 1.13. *The non-primitive factors of U_n are primitive factors of U_{d_i} where d_i are the proper divisors of n. The odd extrinsic factors of U_n are of the forms $kn \pm 1$.*

COROLLARY. *The odd extrinsic factors of V_n are of the forms $2kn \pm 1$.* This follows at once from (1.10).

SECTION 2. PERIODIC AND DEGENERATE SERIES.

1. **Periodic series.** The present extension of Lucas' theory gives rise to a set of periodic series only 2 of which are of Lucas' type.† In what follows we show that there are 12 periodic series U.

If a series U is periodic, it is bounded. Hence the congruence $U_{p-\sigma\varepsilon} \equiv 0 \pmod{p}$ becomes an equality for p sufficiently large. Hence $U_r = 0$ for some $r \neq 0$. But $U_r = 0$ implies that $a^r = b^r$ and $a \neq b$ and since $(a+b)^2$ and ab are coprime integers it follows that a and b are roots of unity. The condition $ab = Q$ implies that these roots of unity are reciprocals or negative reciprocals. Hence we have only 2 cases.

Case 1, $Q = 1$. Let‡ $a = e(k/m)$, then $b = e(-k/m)$ and since $a \neq b$, $k \neq 0$. Then $R = (a+b)^2 = 4\cos^2(2k\pi/m)$. Hence $R = 1$, 2, or 3

* Compare Sylvester, *loc. cit.*, p. 362.

† Carmichael, *loc. cit.*, excludes this pair of series.

‡ Throughout this paper the notation $e(k/m)$ will be used for $e^{\frac{2\pi ik}{m}}$.

are the only possible cases, each of which is satisfied by integral values of k and m. The case $R = 0$ is excluded by our fundamental hypothesis that R and Q are coprime.

Case 2, $Q = -1$. If $a = e(k/m)$, then $b = -e(-k/m)$. The condition $a \neq b$ becomes $k/m \neq 1/2$. Then $R = -4\sin^2(2k\pi/m)$. Hence $R = -1, -2, -3$.

We have then 6 periodic series U. It will be of interest later to consider as distinct the series arising from the 2 values of $R^{1/2}$. In this way we get 12 series U which are periodic. Their constants are listed below, where t is the number of terms in the period. The corresponding series V are also periodic and have the same values of t.

TABLE 2.

N	Q	$R^{1/2}$	Δ	a	b	t
1_0	1	1	-3	$e(1/6)$	$e(-1/6)$	6
1_1	1	-1	-3	$e(1/3)$	$e(-1/3)$	3
1_2	-1	i	3	$e(1/12)$	$-e(-1/12)$	12
1_3	-1	$-i$	3	$e(-1/12)$	$-e(1/12)$	12
2_0	1	$2^{1/2}$	-2	$e(1/8)$	$e(-1/8)$	8
2_1	1	$-2^{1/2}$	-2	$-e(-1/8)$	$-e(1/8)$	8
2_2	-1	$i2^{1/2}$	2	$e(1/8)$	$-e(-1/8)$	8
2_3	-1	$-i2^{1/2}$	2	$e(-1/8)$	$-e(1/8)$	8
3_0	1	$3^{1/2}$	-1	$e(1/12)$	$e(-1/12)$	12
3_1	1	$-3^{1/2}$	-1	$-e(-1/12)$	$-e(1/12)$	12
3_2	-1	$i3^{1/2}$	1	$-e(1/6)$	$e(-1/6)$	6
3_3	-1	$-i3^{1/2}$	1	$e(-1/6)$	$-e(1/6)$	6

Conversely if a series is bounded, it is periodic. For if p is a prime larger than the absolute value of any term in the series U_n, then $U_{p-\sigma\epsilon} = 0$. Hence the series is periodic, since the roots are roots of unity.

2. **Degenerate series.** A series U or V is said to be degenerate, when $\Delta = 0$. Then $R = 4Q$, $a = b = R^{1/2}/2 = Q$, and $(a^n - b^n)/(a-b)$ becomes the derivative of a^n with respect to a and hence $U_n = n a^{n-1}$, $V_n = 2a^n$. Since R and Q are coprime, $R = \pm 4$, $Q = \pm 1$. This gives 4 series

N	$R^{1/2}$	Q	U_n	V_n
4_0	2	1	n	2
4_1	-2	1	$n(-1)^{n-1}$	$2(-i)^n$
4_2	$2i$	-1	$n i^{n-1}$	$2i^n$
4_3	$-2i$	-1	$n(-i)^{n-1}$	$2(-i)^n$

in all of which V is periodic and the absolute values of the terms in U give the series of natural numbers.

THEOREM 2.1. *If the k-th differences of U_n are zero for some value of k and for every value of n, then either U_n is identically zero or else U is the series of natural numbers.*

Proof. If $\Delta \neq 0$, the k-th difference of U_n, $a^n(a-1)^k - b^n(b-1)^k = 0$, implies $a-1 = b-1$ which contradicts the hypothesis $\Delta \neq 0$.

Hence if a series exists satisfying the hypothesis of our theorem it must be one of the degenerate series. If $a = b$, the k-th difference of U_n becomes the derivative of $a^n(a-1)^k$ with respect to a or

$$a^{n-1}(a-1)^{k-1}[n(a-1)+ka].$$

This must be zero for k, $k+1$, etc. which can happen only if $a = 0$ or $a = 1$. If $a = 0$, U_n is identically zero, and if $a = 1$, $U_n = n$.

3. **Degenerate series modulo m.** A series is said to be degenerate modulo m if R, Q, or Δ is congruent to zero (mod m). If m is an odd prime p, we have already seen (in section 1) the effect of degeneracy on the apparition of p in the series U.

The cases R or Q congruent to zero present little of interest, U_n and V_n being congruent (mod m) to powers of R and Q respectively.

In case $\Delta \equiv 0 \pmod m$ we see that if m is odd, R and Q are both prime to m. If m is even, $R \equiv m \pmod 4$ and Q is prime to m. The case $\Delta \equiv 0$ gives the following extension of Wilson's theorem.

THEOREM 2.2. *Let $\bar{U}_n = U_n$ if n is odd and $\bar{U}_n = U_n/R^{1/2}$ if n is even, then*

$$\prod_{k=1}^{p-1} \bar{U}_k \equiv -\left(\frac{2}{p}\right) \sigma^{(p+1)/2} \pmod p.$$

Proof. Let m be any odd divisor of Δ. Then (1.12) (mod m) becomes

$$U_k \equiv k 2^{1-k} R^{(k-1)/2} \pmod m. \tag{2.1}$$

For $m = p$,

$$\prod_{k=1}^{p-1} \bar{U}_k \equiv \prod_{k=1}^{(p-3)/2} U_{2k+1} \prod_{k=1}^{(p-1)/2} U_{2k} R^{-1/2}$$

$$\equiv \prod_{k=1}^{(p-3)/2} (2k+1) 2^{-2k} R^k \prod_{k=1}^{(p-1)/2} 2k \cdot 2^{1-2k} R^{k-1}$$

$$\equiv (p-1)! \, 2^{-(p-1)(p-2)/2} R^{(p-1)(p-3)/4} \equiv -\left(\frac{2}{p}\right)\left(\frac{R}{p}\right)^{(p-3)/2} \pmod p,$$

which gives the theorem. We note that in Lucas' theory in which R is a square we have simply

$$\prod_{k=1}^{p-1} \bar{U}_k \equiv (-1)^{(p^2+7)/8} \pmod{p}.$$

In case of a composite modulus m we have two generalizations of the preceding theorem depending on the parity of m.

THEOREM 2.3. *If m is an odd divisor of Δ, and k runs over the $\varphi(m)$ numbers less than m and prime to m, then*

$$\prod \bar{U}_k \equiv \eta_1 \left\{\frac{2}{m}\right\} \left\{\frac{R}{m}\right\}^{(m+1)/2} \pmod{m},$$

where the symbol $\left\{\frac{t}{m}\right\} \equiv t^{\varphi(m)/2} \pmod{m}$ and where $\eta_1 = -1$ or 1 according as m is or is not a power of an odd prime p.

Proof. The set k can be separated into two subsets: k_1 and k_2 containing respectively the odd and even numbers of k and each having $\varphi(n)/2$ elements. Then

$$\prod \bar{U}_k = \prod U_{k_1} \cdot \prod \bar{U}_{k_2}.$$

From (2.1)

$$\begin{aligned}\prod \bar{U}_k &= \prod k_1 \prod k_2 \prod 2^{1-k_1} \prod 2^{1-k_2} \prod R^{(k_1-1)/2} \prod R^{(k_2-2)/2} \\ &\equiv \prod k \cdot 2^{-\Sigma(k_1-1)-\Sigma(k_2-1)} R^{1/2[\Sigma(k_1-1)+\Sigma(k_2-2)]} \pmod{m}.\end{aligned}$$

According to a theorem first stated by Gauss, $\prod k \equiv \eta \pmod{m}$,

where $\eta = -1$, when $m = 4, p^\alpha, 2p^\alpha$

and $\eta = 1$, in all other cases.

Since m is odd the values of η are as described in the theorem. Also*

$$\Sigma k_1 + \Sigma k_2 = \Sigma k = \frac{m}{2} \cdot \varphi(m).$$

Hence we have

$$\prod \bar{U}_k \equiv \eta_1 2^{-m\varphi(m)/2+\varphi(m)} R^{\varphi(m)(m-3)/4} \equiv \eta_1 \left\{\frac{2}{m}\right\} \left\{\frac{R}{m}\right\}^{(m+1)/2} \pmod{m},$$

which gives the theorem.

Finally if m is even we have the following

THEOREM 2.4. *If $\Delta \equiv 0 \pmod{m}$ and k runs over the $\varphi(m)$ numbers less than m and prime to m, then for m even*

* A. L. Crelle, *Jour. für Math.*, 29, pp. 80–84.

$$\prod U_k \equiv \eta_2 \left\{\frac{Q}{m}\right\}^{(m-2)/2} \pmod m$$

where $\eta_2 = -1$, *if* $m = 4$ *or* $2p^\alpha$ *and unity in all other cases.*

Proof. Since m is even, the product $\prod U_k$ extends over odd values of k only, and (2.1) can be replaced by $U_k \equiv k Q^{(k-1)/2}$. Then

$$\prod U_k \equiv \prod k \prod Q^{(k-1)/2} \equiv \eta_2 Q^{\Sigma(k-1)/2} \equiv \eta_2 \left\{\frac{Q}{m}\right\}^{(m-2)/2} \pmod m.$$

Section 3. The Binary Form G_n.

Thus far we have considered U_n and V_n as functions of n. In this section we are primarily concerned with U_n and V_n considered as functions of R and Q. From the definition of U_n and V_n we have

$$(3.1)\qquad \begin{aligned} U_n(R, Q) &= \sum_{i=0}^{[(n-1)/2]} (-1)^i \binom{n-i-1}{i} R^{(n-2i-1)/2} Q^i, \\ V_n(R, Q) &= R^{n/2} + \sum_{i=1}^{[n/2]} (-1)^i \binom{n-i-1}{i-1} \frac{n}{i} R^{(n-2i)/2} Q^i. \end{aligned}$$

Hence $U_n(R, Q)$ and $V_n(R, Q)$ are binary forms. In Lucas' theory the corresponding forms are not homogeneous.

1. **A transformation.** If we consider U_n and V_n as functions of Δ and Q, we obtain binary forms different from $U_n(R, Q)$ and $V_n(R, Q)$ given above. However these forms are related as follows. Let $F(x, y) \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} f(x, y)$ mean that F is the same function of x and y as f is of $\alpha x + \beta y$ and $\gamma x + \delta y$. Then

Theorem 3.1. *If* n *is odd*

$$(3.2)\qquad (R - 4Q)^{1/2} U_n(R, Q) \begin{pmatrix} 1 & -4 \\ 0 & -1 \end{pmatrix} \qquad V_n(R, Q),$$

$$(3.3)\qquad V_n(R, Q) \begin{pmatrix} 1 & -4 \\ 0 & -1 \end{pmatrix} R^{1/2} U_n(R, Q).$$

If n *is even*

$$(3.4)\qquad (R - 4Q)^{1/2} U_n(R, Q) \begin{pmatrix} 1 & -4 \\ 0 & -1 \end{pmatrix} R^{1/2} U_n(R, Q),$$

$$(3.5)\qquad V_n(R, Q) \begin{pmatrix} 1 & -4 \\ 0 & -1 \end{pmatrix} \qquad V_n(R, Q).$$

Proof. The roots of the equation $x^2 - R^{1/2}x + Q = 0$ are a and b. Let a' and b' be the corresponding roots of $x^2 - \Delta^{1/2}x - Q = 0$. Then

$a = a'$ and $b = -b'$. Consequently $\Delta U_n(R, Q) = a'^n + b'^n$ or $a'^n - b'^n$ according as n is odd or even. This proves (3.2) and (3.4). Similarly $V_n(R, Q) = a'^n \pm b'^n$ according as n is odd or even. This gives (3.3) and (3.5).

This transformation which interchanges R and Δ and changes the sign of Q is not possible in Lucas' theory unless Δ is a perfect square, that is, when a and b are integers.

2. **Definition of G_n.** The divisors of U_n have been classified in section 1 as primitive and non-primitive, the latter being primitive divisors of U_{d_i} where d_i are the proper divisors of n. This being true for every value of R and Q the product of these non-primitive divisors appears algebraically in $U_n(R, Q)$. The quotient of division of U_n by the product of its non-primitive divisors we shall denote by G_n. As a function of R and Q, G_n is a binary form.

3. **Inversion formulas.** It follows from the definition of G_n, that

$$U_n = \prod G_{\delta_i} \tag{3.6}$$

where δ_i are the divisors of n (including n itself). Dedekind* observed that if any 2 functions satisfy (3.6) they may be inverted

$$G_n = \frac{U_n \prod U_{n/p_1 p_2} \cdots}{\prod U_{n/p_1} \prod U_{n/p_1 p_2 p_3} \cdots} \tag{3.7}$$

where p_i are the distinct prime factors of n. We find it sometimes convenient to use the following inversion of (3.6)†

$$G_n = \frac{U_n \prod U_{b_i} \cdots}{\prod U_{a_i} \prod U_{c_i} \cdots} \tag{3.8}$$

where a_i are the proper divisors (less than n) of n, b_i the proper divisors of a_i and so on.

4. **The fundamental property of G_n.** Since G_n is the product of the primitive factors of U_n we have by Theorem (1.13) the following fundamental property.

THEOREM 3.2. *The odd extrinsic prime factors of the numbers represented by the binary form $G_n(R, Q)$ are of the forms $kn \pm 1$*

---

* *Jour. für Math.*, 54 (1857), p. 21.

† *Amer. Jour. of Math.*, 51 (1930), p. 296.

In accordance with the fundamental hypothesis of section 1 we consider only numbers properly represented, i. e. with R and Q coprime.

5. **The law of repetition for G_n.** It is clear from the definition of G_n that the law governing the appearance of a given prime in the sequence $G_1, G_2, G_3, \cdots$, is identical with the law of apparition for U_n given in section 1. Hence we consider the reappearence of this prime in the sequence of G's.

In discussing the properties of G_n relative to divisibility the cases $n = 1, 2, 3, 4$ and 6 are of no interest since any number is representable by these linear forms. These cases are therefore excluded.

First let p be odd and let ω be its rank of apparition. If p divides G_r, then r is of the form $k\omega$, since otherwise $U_r \neq 0 \pmod{p}$. Furthermore k is divisible by p, for $G_{k\omega}$ is a divisor of $U_{k\omega}/U_\omega$ which by Theorem 1.6 does not contain the factor p unless k is divisible by p. Let $k = p^\lambda k'$, $k' > 1$ and prime to p, then $G_{\omega p^\lambda}$ is a divisor of $U_{\omega p^\lambda k'}/U_{\omega p^\lambda}$ which by Theorem 1.6 does not contain the factor p, since k' is prime to p. We therefore consider the case $r = \omega p^\lambda$. If first neither $\omega = p$ nor $\omega = 2p$, from (3.6)

$$U_{\omega p^\lambda}/U_{\omega p^{\lambda-1}} = \prod G_d = G_{\omega p^\lambda} \prod\prod G_{\omega' p^\lambda},$$

where d ranges over these divisors of ωp^λ which contain the factor p^λ and where ω' are the proper divisors of ω. The product $\prod G_{\omega' p^\lambda}$ is not divisible by p since none of the subscripts are multiples of ω. By Theorem 1.6 the ratio on the left is divisible by p, but not by p^2, hence the same is true of $G_{\omega p^\lambda}$.

If $\omega = p$ we have from (3.7)

$$G_{p^\lambda} = U_{p^\lambda} / U_{p^{\lambda-1}}$$

and if $\omega = 2$ or $2p$ we have

$$G_{2p^\lambda} = U_{2p^\lambda} U_{p^{\lambda-1}} / U_{p^\lambda} U_{2p^{\lambda-1}}.$$

In either case G is divisible by p, but not by p^2.

Finally consider the prime 2, which will appear in U_2, U_3, or U_4. By similar reasoning it is easy to show that the numbers G_{2^λ} or $G_{3 \cdot 2^\lambda}$ may be even while all other G's are odd. Moreover these even G's will not be divisible by 4. Hence we have the following theorem.

THEOREM 3.3. *If $n \neq 1, 2, 3, 4,$ or 6, and if ω is the rank of apparition of an odd prime p in the series U, then the numbers G_n are divisible by p if and only if $n = \omega p^\lambda$. If $\lambda > 0$, G_n is not divisible by p^2; if $\lambda = 0$, $G_n = G_\omega$ may be divisible by p^2 unless $\omega = p > 3$, or $\omega = 2p > 6$. The*

numbers G_n (for Q odd) are even if and only if $n = 2^\lambda$ or $n = 3 \cdot 2^\lambda$. No G_n is divisible by 4.

6. The intrinsic divisors of G_n. Let d be a divisor common to G_n and n, let p be any odd prime factor of d, and let ω be the rank of apparition of p. By the preceding theorem n must be of the form ωp^λ. Now $\omega \leqq p+1$ and consequently p is the largest prime factor of n. That is d contains no other odd prime factor, than the largest dividing n itself. But by the preceding theorem G_n does not contain the factor p^2. Therefore if d is odd, $d = p$. Suppose now that d is even. Then by Theorem 3.3, $n = 2^\lambda$ or $3 \cdot 2^\lambda$. In either case d may be a power of 2, but since we consider $n > 4$, d is 2 itself. In order that d be of the form $3 \cdot 2^\mu$ we must have $n = 3^\nu \omega$. If then $n = 3 \cdot 2^\lambda = 3^\nu \omega$, we have only one value of n, namely 12, for which G_n and n are both divisible by 6. These results may be summarised as follows.

THEOREM 3.4. *If n is not of the form 2^λ or $3 \cdot 2^\lambda$, $\lambda \geqq 0$, then the only intrinsic factor of the binary form $G_n(R, Q)$, is the largest prime factor of n. If $n = 2^\lambda$ or $3 \cdot 2^\lambda$, $\lambda > 2$, then 2 is the only intrinsic factor of $G_n(R, Q)$. If $n = 12$, G_{12} may have 2, 3, or 6 for intrinsic factors.*

7. G_n as a function of a and b. If we substitute for R and Q their values in terms of a and b in $G_n(R, Q)$, we obtain a binary form* $F_n(a, b)$. This same form may be obtained from the function $(a^n - b^n)/(a - b)$, or simply $a^n - b^n$ for $n \neq 1$, by removing all its irreducible algebraic factors of degrees $< \varphi(n)$. If we put $a = x$ and $b = 1$, $F_n(a, b)$ becomes the well known irreducible factor of $x^n - 1$, whose roots are the $\varphi(n)$ primitive n-th roots of unity.† Let $a = z$ and $b = 1/z$. Then $F_n(a, b)$ is a polynomial in z of degree $2\varphi(n)$ which is in fact $F_n(z^2, 1)$. The substitution

$$(z + 1/z)^2 = R \tag{3.9}$$

transforms $F_n(z^2, 1)$ into $G_n(R, 1)$. The roots of $F_n(z^2, 1) = 0$ are the square roots of the primitive n-th roots of unity. Hence from (3.9) the roots of $G_n(R, 1) = 0$ are of the form

$$[e(k/2n) + e(-k/2n)]^2 = e(k/n) + e(-k/n) + 2 = 4\cos^2(\pi k/n). \tag{3.10}$$

The above expression yields $\frac{1}{2}\varphi(n)$ distinct roots, and this being the degree of $G_n(R, 1)$, it follows that this polynomial has distinct roots, which are given without repetition by (3.10), where k runs over $\frac{1}{2}\varphi(n)$ integers $< n/2$ and prime to n.

---

* This form is a generalization of Carmichael's F_n. For $n = 1$ however we have $F_1 = 1$, while his $F_1 = a - b$.

† Kronecker, *Jour. de Math.*, (1), 19 (1854), pp. 177–192.

8. **The forms H_n.** If we express that irreducible factor, of degree $\varphi(2n)$ of $V_n = a^n + b^n$ in terms of R and Q, we obtain a binary form $H_n(R, Q)$ which can be obtained directly from V_n in the same way as G_n is obtained from U_n. The forms H_n however are contained in the G's, since the above mentioned irreducible factors of $a^{2n} - b^{2n}$ and $a^n + b^n$ are identical. That is

$$H_n = G_{2n}. \tag{3.11}$$

From Theorem 1.5 it follows that if n is odd

$$V_n = \prod H_{\delta_i} \tag{3.12}$$

where δ_i ranges over the divisors of n.

THEOREM 3.5. *If n is odd there exists a linear transformation between G_{2n} and G_n of the form*

$$G_{2n}(R, Q) \begin{pmatrix} 1 & -4 \\ 0 & -1 \end{pmatrix} G_n(R, Q). \tag{3.13}$$

Proof. If we invert (3.12) and apply the transformation (3.3) to each factor we get

$$H_n = \frac{V_n \prod V_{n/p_1 p_2} \cdots}{\prod V_{n/p_1} \prod V_{n/p_1 p_2 p_3} \cdots} \begin{pmatrix} 1 & -4 \\ 0 & -1 \end{pmatrix} \frac{R^{1/2} U_n \prod R^{1/2} U_{n/p_1 p_2} \cdots}{\prod R^{1/2} U_{n/p_1} \prod R^{1/2} U_{n/p_1 p_2 p_3} \cdots}. \tag{3.14}$$

It can be shown* that the numerator and denominator of the right hand member of (3.7) contain the same number of factors. Hence $R^{1/2}$ cancels in the right hand member of (3.14) and we are left with G_n. That is $H_n \begin{pmatrix} 1 & -4 \\ 0 & -1 \end{pmatrix} G_n$. This result together with (3.11) proves the theorem.

9. **Sylvester's polynomials $\Psi_n(u, 1)$.** Sylvester† has defined a set of polynomials $\Psi_n(u, 1)$ having the fundamental property of G_n. They arise from the polynomials $F_n(x, 1)$ by the reciprocal substitution $x + x^{-1} = y$ and have roots of the form $2\cos(2k\pi/n) = e(k/n) + e(-k/n)$ where k as before runs over the $\frac{1}{2}\varphi(n)$ numbers prime to n and $< n/2$. Hence

$$\Psi_n(x, y) \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix} G_n(x, y). \tag{3.15}$$

* Bachmann, *Kreistheilung*, Leipzig (1872), pp. 9, 10.

† Loc. cit.

This transformation furnishes another proof of the fundamental property for the Ψ's. The present extension is necessary for the complete equivalence of Sylvester's theory and this part of Lucas' theory.*

If n is odd it is easy to show that the roots of $G_n(x, 1) = 0$ are the square roots of the roots of $\Psi_n(x, 1) = 0$ or

$$G_n(x^2, 1) = \Psi_n(x, 1)\,\Psi_n(-x, 1) \qquad (n \text{ odd}).$$

Transformations (3.13) and (3.15) give

$$\Psi_n(-x, 1) = \Psi_{2n}(x, 1). \qquad (n \text{ odd}).$$

Hence

$$G_n(x^2, y^2) = \Psi_n(x, y)\,\Psi_{2n}(x, y) \qquad (n \text{ odd}). \tag{3.16}$$

If $n = 2^\lambda l$ with l odd and $\lambda > 0$

$$G_{2^\lambda l}(x^2, y^2) = \prod \left(x - 2y \cos \frac{2\pi k}{2^{\lambda+1} l}\right)\left(x - 2y \cos \frac{2\pi(2^\lambda l - k)}{2^{\lambda+1} l}\right)$$
$$= \prod \left(x - 2y \cos \frac{2\pi t}{2^{\lambda+1} l}\right)$$

where t runs over the numbers less than $2^\lambda l$ and prime to $2^{\lambda+1} l$. Hence

$$G_{2^\lambda l}(x^2, y^2) = \Psi_{2^{\lambda+1} l}(x, y). \tag{3.17}$$

10. G_n **for special values of** R **and** Q. So far we have considered R and Q as variables. If we fix R and Q and let n vary, we obtain a sequence of integers whose factors are the primitive factors of the numbers U. Thus if $R = 9$ and $Q = 2$, then G_n is the maximum irreducible factor of $2^n - 1$. If n is a prime, we get the Mersenne numbers, if n is a power of 2, the Fermat numbers. More generally if $R = (y+1)^2$ and $Q = y$, G_n is the maximum irreducible factor of $y^n - 1$. If R and Q assume values rendering the series U degenerate, we have

THEOREM 3.6. *If* $R = 4$ *and* $Q = 1$, $G_n(4,1)$ *has the value* q *or* 1, *according as* n *is or is not a power of a prime* q.†

Proof. In this case $\Delta = 0$, so that the series U is the degenerate series‡ for which $U_n = n$. Hence if $n = q^\alpha$, $G_n = U_{q^\alpha}/U_{q^{\alpha-1}} = q$.

If $n = \prod_{i=1}^{\nu} q_i^{\alpha_i}$, $\nu > 1$, then

$$U_n = n = \prod G_{\delta_i} = \prod G_{d_i} \prod_{i=1}^{\nu} \prod_{\lambda=1}^{\alpha_i} G_{q_i^{\lambda_i}} \tag{3.18}$$

---

* Notwithstanding Lucas' statement to the contrary. *Comptes Rendus*, 90 (1880), p. 855.

† Using the function $\Lambda(n)$ (Landau, *Handbuch*, I, p. 333) we can state this theorem as follows: $G_n(4, 1) = e^{\Lambda(n)}$.

‡ The series 4_0 and 4_2 give the same value of G_n for $n \neq 2$.

where d_i extends over those divisors of n which have more than one prime factor. But $G_{q_i^{\lambda_i}} = q_i$, and since each q_i appears α_i times in the above double product, the latter $= n$. Hence $\prod G_{d_i} = 1$. Since G_n is a factor of $\prod G_{d_i}$ its absolute value is unity. Moreover from (3.7), G_n is positive being a ratio of positive integers. Hence in this case $G_n = 1$.

THEOREM 3.7. *For $R = 0$, $Q = 1$, $G_n(0, 1) = (-1)^{\varphi(n)/2} q$ or $(-1)^{\varphi(n)/2}$ according as n is or is not twice the power of a prime q. In other words the product of the roots of G_n is unity or q according as n is or is not $2q^\alpha$.*

Proof. Case 1, n odd. $U_n(0, 1) = 1$, hence by (3.7), $|G_n(0, 1)| = 1$. The sign of $G_n(0, 1)$ is $(-1)^\gamma$, where $\gamma = \varphi(n)/2$ is the degree of G_n.

Case 2, $n = 2k$, k odd. By Theorem 3.5

$$G_{2k}(0, 1) = G_k(-4, -1) = (-1)^\gamma G_k(4, 1).$$

Hence by Theorem 3.6, $G_{2k}(0, 1) = (-1)^\gamma q$ or 1 according as k is or is not a power of a prime q.

Case 3, $n = 2^\lambda k$, $\lambda > 1$. By (3.15) and (3.17)

$$G_{2^\lambda k}(0, 1) = \Psi_{2^\lambda k}(-2, 1) = G_{2^{\lambda-1} k}(4, 1).$$

Hence by Theorem 3.5, $G_{2^\lambda k}(0, 1) = 2$ or 1 according as k is or is not a power of 2.

11. **Discriminant of G_n.** The preceding theorems can be applied to the determination of the general formula for the discriminant of G_n. We need the following

LEMMA. *Let D_f be the discriminant of the symmetric polynomial*

$$f(x) = x^{2k} + ax^{2k-1} + bx^{2k-2} + \cdots + bx^2 + ax + 1 = \prod_{i=1}^{k} (x - r_i)(x - r_i^{-1})$$

and let D_g be the discriminant of $g(y)$ obtained from $f(x)$ by setting $x + x^{-1} = y$. Then

$$D_f = D_g^2 \prod_{i=1}^{k} (s_i^2 - 4)$$

where s_i are the roots of $g(y) = 0$.

The proof, which is straight forward, is omitted to save space. Let $f(x) = F_n(x, 1)$ and $g(x) = \Psi_n(x, 1)$ then in this case

$$\prod (s_i^2 - 4) = \prod (s_i + 2)(s_i - 2)$$
$$= \Psi_n(-2, 1)\Psi_n(2, 1) = G_n(0, 1) G_n(4, 1),$$

in view of (3.16). By Theorems 3.6 and 3.7 this product is 4, when $n = 2^\lambda$, $(-1)^\gamma p$ when $n = p^\alpha$ or $2p^\alpha$ and 1 in all other cases. The discriminant of F_n is known to be*

$$(3.19) \qquad (-1)^{\varphi(n)/2} \frac{n^{\varphi(n)}}{\prod q_i^{\varphi(n)/(q_i-1)}}.$$

Using this result together with our lemma and (3.15), we have the

THEOREM 3.8. *The discriminant of G_n is given by*

$$\begin{cases} 2^{(\lambda-1)2^{\lambda-2}-1} & \text{if } n = 2^\lambda, \quad \lambda > 2, \\ p^{[\alpha p^\alpha-(\alpha+1)p^{\alpha-1}-1]/2} & \text{if } n = p^\alpha \text{ or } 2p^\alpha, \\ \dfrac{n^{\varphi(n)/2}}{\prod_{i=1}^{\nu} q_i^{\varphi(n)/2(q_i-1)}} & \text{if } n = \prod_{i=1}^{\nu} q_i^{\alpha_i}, \quad \nu > 1, \quad n \neq 2p^\alpha. \end{cases}$$

12. **An unsolved problem.** It is interesting to inquire whether there exist binary forms, not linear transforms of G_n, which possess the fundamental property of G_n, that is, whose extrinsic divisors are all of the forms $kn \pm 1$. Although we have not yet obtained a proof of the existence of such forms, we have general rules for obtaining forms which appear to possess this property. For example the forms

$$x^3 + 16x^2y - 57xy^2 - y^3,$$
$$x^3 - 18x^2y + 69xy^2 - y^3$$

have extrinsic factors of the forms $14k \pm 1$ and $18k \pm 1$ respectively, but are not linear transforms of G_7 or G_9. There seem to be infinitely many such forms associated with each value of n.

A detailed account of the quadratic partitions of G_n, and methods of factoring G_n will be given elsewhere.

ERRORS IN SYLVESTER'S TABLE OF Ψ_n.

n	For	Read	n	For	Read
9	-1	$+1$	23	$36u^2$	$36u^7$
10	$+1$	-1	25	$-5u$	$+5u$
14	$+2u$	$-2u$	29	$28u^3$	$28u^2$
18	$+1$	-1	30	$u^8-9u^6+\cdots+1$	$u^4+u^3-4u^2-4u+1$
19	$10u^3$	$-20u^3$	31	$-4u$	$-8u$
22	$+1$	-1	33	-1	$+1$
22	$-3u$	$+3u$	36	$9u^3$	$9u^2$

* Rados, *Jour. für Math.*, 131 (1906), pp. 49–55. See also E. T. Lehmer, *Bull. Amer. Math. Soc.*, 36 (1930), pp. 291–298.

The author regrets the lack of illustrative material in this section (especially a table of $G_n(R, Q)$), which was omitted to save space.

SECTION 4. DERIVED AND ANTI-DERIVED SERIES.

1. Derived series. If in a given series U we select every r-th term and divide each of these by U_r, we obtain a new series

$$0,\ 1,\ U_{2r}/U_r,\ U_{3r}/U_r, \cdots, U_{nr}/U_r\ \cdots.$$

We shall call this series the derived series of order r, and denote it by $U^{(r)}$. It is obvious* that $U^{(r)}$ is a recurring series of the second order with constants

$$R^{(r)} = V_r^2, \qquad Q^{(r)} = Q^r, \qquad \Delta^{(r)} = \Delta U_r^2, \qquad \delta^{(r)} = \delta U_r,$$
$$a^{(r)} = a^r, \qquad b^{(r)} = b^r, \qquad U_n^{(r)} = U_{nr}/U_r, \qquad V_n^{(r)} = V_{nr}.$$

These may be looked upon as substitutions which enable us to generalize all the formulas we have developed involving Q, R, Δ etc. If $r = 1$, it is obvious that no change takes place in the series on derivation. The operation of derivation is commutative. If $r = 2k$, V_{2k} is an integer, hence $U^{(2k)}$ is of Lucas' type.

A given series and its derived series have certain properties in common. These we proceed to examine.

THEOREM 4.1. *If ω is the rank of apparition of an odd prime p in the series U, then its rank of apparition $\omega^{(r)}$ in the series $U^{(r)}$ is*

$$\omega^{(r)} = \frac{1}{r} \cdot \text{L. C. M. } (\omega, r)$$

except when ω divides r in which case $\omega^{(r)} = p$.

Proof. We seek in the series U the first term whose rank is a multiple of ω and also of r. This is clearly the L. C. M. (ω, r). In forming the derived series this rank becomes $\frac{1}{r}$ L. C. M. (ω, r). If ω divides r, $\Delta^{(r)} = \Delta U_r^2$ is divisible by p. Hence in $U^{(r)}$, $\epsilon = 0$, then by Theorem 1.9 $\omega = p$.

If τ is the quadratic character of Q with respect to p, then the quadratic characters σ, ϵ and τ become on derivation $\left(\frac{V_r^2}{p}\right)$, $\left(\frac{\Delta U_r^2}{p}\right)$ and $\left(\frac{Q^r}{p}\right)$ respectively. Unless $U_{2r} \equiv 0 \pmod{p}$ we have

* Lucas, *loc. cit.*, p. 189.

$$\left.\begin{aligned}\varepsilon^{(r)} &= \varepsilon\\ \sigma^{(r)} &= \sigma\\ \tau^{(r)} &= \tau\end{aligned}\right\} r = 2k+1, \qquad \left.\begin{aligned}\varepsilon^{(r)} &= \sigma\varepsilon\\ \sigma^{(r)} &= 1\\ \tau^{(r)} &= 1\end{aligned}\right\} r = 2k.$$

This table gives the following

THEOREM 4.2. *If $U_{2r} \not\equiv 0 \pmod p$, then $\sigma\varepsilon$ is invariant under derivation of order r.*

2. Derivation of periodic and degenerate series.

THEOREM 4.3. *If a series U is invariant under derivation of order $r>1$, then it is either a periodic or a degenerate series.*

Proof. If $U_n^{(r)} = U_n$, then $a^r = a$, $b^r = b$, $Q^r = Q$. Hence a and b are either reciprocal or negative reciprocal roots of unity. This condition on the roots (a, b) coincides with that imposed by periodicity except when $a = \pm b$ in which case we get degenerate series. It follows that each of the series discussed in section 2 is either left invariant on derivation, or else is transformed into another periodic or degenerate series.

3. Derivation of $G_n(R, Q)$. Let us consider the result of deriving the binary form $G_n(R, Q)$. If we make the substitution $R^{(r)} = V_r^2$, $Q^{(r)} = Q^r$ for R and Q in the binary form $G_n(R, Q)$ we get a new form $G_n^{(r)}(R, Q)$.

THEOREM 4.4. *If r and n are any two integers prime to each other, then $G_n^{(r)} = \prod G_{nd_i}$, where d_i are the divisors of r (including 1 and r).*

This theorem may be proved easily by induction from the proper divisors of n to n itself.

THEOREM 4.5. *If the prime factors of an integer r divide the integer n, then $G_n^{(r)} = G_{nr}$.*

Proof. First let $n = kr^\alpha$, where r is a prime not dividing k, and where $\alpha>0$. Then we show that

$$G_{kr^\alpha}^{(r^\lambda)} = G_{kr^{\alpha+\lambda}}. \tag{4.1}$$

The proof is by induction. We assume the theorem to hold for all proper divisors a_i of k and start with $\alpha = 0$ and $\lambda = 1$. Then

$$G_{kr} = U_{kr} \Big/ \Big(G_r\, G_k \prod G_{a_i} \prod G_{ra_i}\Big).$$

On derivation of order r the left side becomes $G_{kr}^{(r)}$. On the right

U_{kr} becomes U_{kr^2}/G_r,

$\prod G_{a_i}$ and G_k become $\prod G_{a_i} \prod G_{ra_i}$ and G_{kr},

and $\prod G_{ra_i}$ becomes $\prod G_{r^2a_i}$ by hypothesis of the induction.

Finally $G_r = U_r$ becomes G_{r^2}. Hence we have

$$G_{kr}^{(r)} = U_{kr^2} \Big/ \Big(G_r\, G_{r^2}\, G_{kr} \prod G_{a_i} \prod G_{ra_i} \prod G_{r^2a_i}\Big).$$

On the right we have U_{kr^2} divided by the product of the G's corresponding to all the proper divisors of kr^2. That is $G_{kr}^{(r)} = G_{kr^2}$.

Next let k be a prime, then $G_{kr} = U_{kr}/G_k G_r$ and $G_{kr}^{(r)} = U_{kr^2}/U_r G_k G_{kr} G_{r^2}$. Hence for all k, $G_{kr}^{(r)} = G_{kr^2}$. Successive applications of this result give (4.1), applications of which give the theorem. The above discussion may be summed up in the following theorem.

THEOREM 4.6. *Let r and n be any two positive integers and let r/d be the largest divisor of r prime to n, then*

$$G_n = \prod G_{nd\delta_i} \tag{4.2}$$

where δ_i are the divisors of r/d.

4. Anti-derived series. The series $U^{(1/r)}$ which on derivation of order r becomes the given series U, is said to be the anti-derived series, of order r, of U. Anti-derivation is not always possible, that is to say, $U^{(1/r)}$ does not always belong to the class of series with integral R and Q. In order that the series $U^{(1/r)}$ should exist it is necessary and sufficient that the constants (R, Q) of U satisfy

(4.3) Q is a perfect r-th power;

(4.4) R is properly represented by the polynomial V_r^2 in which the given Q is replaced by $Q^{1/r}$. That is, $V_r^2(R^{(1/r)}, Q^{1/r}) = R$.

THEOREM 4.7. *If a series U possess more than one anti-derived series of a fixed order r, then it is either a degenerate series, or one of the periodic series 1_0 or 1_1.*

Proof. If there were two series with constants (a_1, b_1) and (a_2, b_2) yielding the same series on derivation or order r, we should have $a^{(r)} = a_1^r = a_2^r$ and $b^{(r)} = b_1^r = b_2^r$. Hence $a^{(r)}$ and $b^{(r)}$ would be zero or roots of unity and the series $U^{(1/r)}$ would be degenerate or periodic. Examining the periodic series we see that the only possible cases are those mentioned in the theorem.

COROLLARY. *For any fixed value of $Q \neq 0, \pm 1$, the polynomial in R,*

$$V_r^2 = \text{integer},$$

has not more than one integral root.

Since $U^{(rs)} = (U^{(r)})^{(s)}$ it is sufficient to discuss anti-derivation in which the order is a prime number. When $r = 2$ the conditions (4.3) and (4.4) reduce to the condition that R and Q be perfect squares. We have computed a complete list of those series whose constants (R, Q) are each less than one million, that possess anti-derived series of prime order > 3. The results are omitted to save space. There are only 98 such series for $r > 5$ and 328 for $r = 5$.

5. **Anti-derivation of G_n.** If R and Q take on values for which $U(R, Q)$ is anti-derivable, $G_n(R, Q)$ may become reducible. That is to say, for every n, the form $G_n(R, Q)$, although irreducible in the rational field, may become reducible when R and Q are replaced by V_r^2 and Q^r respectively. In fact (4.2) may be written

$$G_n = \prod G_{nd\delta_i}^{(1/r)}. \tag{4.5}$$

If the prime factors of r divide n, then G_n does not become reducible. For in this case (4.5) becomes

$$G_n = G_{nr}^{(1/r)}.$$

When $r = 2$, the reducibility of G_n is also shown by (3.16). The possibility of anti-deriving G_n greatly simplifies its factorization. Not only is it often possible to separate G_n at once into a product of two or more factors, but also the restriction on the prime factors of G_n (or its residual factors) is appreciably increased. This topic will be discussed in detail in a paper on the factorisation of G_n.

6. **Two extensions of the concept of power residuacity.** We close this section with a brief discussion of two possible definitions which generalize the idea of quadratic and higher residues. We can give space to a detailed account of the quadratic cases only. In what follows, the odd prime p shall not divide $RQ\Delta$.

The first definition is an extension of that classical definition of r-th power residuacity, which depends on the existence or non-existence of solutions x of the congruence $x^r \equiv D \pmod{p}$. If a given series U is congruent modulo p, term by term, to a series $U^{(r)}$ which is anti-derivable with the order r, then we say that U is anti-derivable modulo p. In order that U be anti-derivable modulo p it is necessary and sufficient that there exist a solution (α, β) of the pair of congruences

$$\begin{aligned} \alpha^r &\equiv a, \\ \beta^r &\equiv b, \end{aligned} \pmod{p},$$

where a and b are the constants of the given series U. In order to obtain a pair of congruences involving integers we may change conditions (4.3) and (4.4) to congruences modulo p. We define the symbol* $\left(\frac{a, b}{p}\right)_r$ to be 1 if and only if the series U determined by a and b is anti-derivable modulo p with the order r. For example, if $r = 2$ the series U is anti-

* The values, other than 1, of this symbol need to be mentioned here. This remark applies also to the other symbol about to be defined.

derivable modulo p if and only if R and Q are quadratic residues of p. Hence we have the

THEOREM 4.8. *The symbol* $\left(\frac{a, b}{p}\right)_2 = 1$ *if and only if* $\sigma = \tau = 1$.

The second definition we consider, is an extension of Euler's criterion

$$\left(\frac{c}{p}\right)_r = 1 \text{ if and only if } c^{(p-1)/r} - 1 \equiv 0 \pmod{p}. \tag{4.6}$$

We define the symbol $\left[\frac{R, Q}{p}\right]_r$ to be 1 if and only if

$$U_{(p-\sigma\varepsilon)/r}(R, Q) \equiv 0 \pmod{p}, \tag{4.7}$$

which for $R = (c+1)^2$ and $Q = c$ becomes Euler's criterion.

THEOREM 4.9. *The symbol* $\left[\frac{R, Q}{p}\right]_2 = 1$ *if and only if* $\sigma = \tau$.

Proof. Let $p - \sigma\varepsilon = 2k$ so that $U_{p-\sigma\varepsilon} = U_k V_k$, then $\left[\frac{R, Q}{p}\right]_2 = 1$ if and only if V_k is not divisible by p. First let $\sigma = \varepsilon$. Then by Table 1, $V_{p-1} = V_{2k} = V_k^2 - 2Q^k \equiv 2\sigma \pmod{p}$. Hence $V_k \not\equiv 0 \pmod{p}$ if and only if $\sigma = \tau$. Next let $\sigma = -\varepsilon$. Then $V_{p+1} = V_k^2 - 2QQ^k \equiv 2Q\sigma \pmod{p}$. Hence $V_k \not\equiv 0 \pmod{p}$ if and only if $\sigma = \tau$. Hence the theorem.

A glance at Theorems 4.8 and 4.9 shows that if $\left(\frac{a, b}{p}\right)_2 = 1$ then $\left[\frac{R, Q}{p}\right]_2 = 1$ but not conversely. More generally we have the theorem

THEOREM 4.10. *If* $\left(\frac{a, b}{p}\right)_r = 1$, *then* $\left[\frac{R, Q}{p}\right]_r = 1$.

Proof. If $\left(\frac{a, b}{p}\right)_r = 1$, there exists a series U' such that

$$U'_{rn} / U'_r \equiv U_n, \qquad U'_r \not\equiv 0 \pmod{p}$$

holds for every value of n. Let $p - \sigma\varepsilon = kr$. Then, since $\sigma\varepsilon$ is invariant under derivation, we have, for $n = k$

$$U_k \equiv U'_{kr} / U'_r \equiv U'_{p-\sigma\varepsilon} / U'_r \equiv 0 \pmod{p}.$$

Hence the theorem follows at once.

The more inclusive of the two extensions of the power residue notion, expressed by $\left[\frac{R, Q}{p}\right]_r$, gives rise to a generalisation of the theory of the binomial congruence $c^k - 1 \equiv 0 \pmod{p}$. The rank of apparition $\omega(R, Q)$ of p takes the place of the exponent to which c belongs modulo p, while pairs (R, Q) for which $\omega(R, Q) = p - \sigma\varepsilon$ replace primitive roots. How-

ever we cannot give further space to this subject. The discussion given here is necessary to the development of the final section.

Section 5. Tests for Primality.

1. **Introduction.** Perhaps the most remarkable results of Lucas are included in a set of theorems concerning the prime or composite character of integers of certain forms. His conditions for primality are sufficient but not necessary.* One is uncertain whether Lucas' tests will reveal the character of a number which is actually a prime. Carmichael has given a set of conditions, both necessary and sufficient for the primality, which except for two cases depend upon the existence or non-existence of a certain auxiliary number pair used in testing a given integer. From a practical point of view these tests are not applicable since no method is given for determining in advance an appropriate number pair. In this section we give non-tentative, necessary and sufficient conditions for the primality of numbers of the form $2^n A - 1$. For practical methods of testing numbers of unknown form or of the form $2^n A + 1$, the reader is referred to an article on the converse of Fermat's theorem.†

2. **General theorems.** We first give three theorems governing the primality of any integer N prime to $2RQ\Delta$.

Theorem 5.1. *If $N \pm 1$ is the rank of apparition of N, then N is a prime.*

Proof. Suppose N is composite, $N = \prod_{i=1}^{\nu} p_i^{\alpha_i}$, then $T(N)$ in (1.16) is different from $N \pm 1$. By Theorem 1.12, $U_{(T(N))/2} \equiv 0 \pmod{N}$. By hypothesis $U_{N\pm 1} \equiv 0 \pmod{N}$. Therefore $U_{(T(N))/2-(N\pm 1)} \equiv 0 \pmod{N}$. But $\left[p_i - \left(\frac{R, \Delta}{p_i}\right)\right] \leqq p_i + 1$ so that $\frac{1}{2} T(N) < 2N$. Moreover $T(N) > N \pm 1$, since $N \pm 1$ is the rank of apparition of N. Hence

$$0 < \frac{1}{2} T(N) - (N \pm 1) < N \pm 1.$$

We have thus exhibited a term in the series U, divisible by N, whose rank is less than the rank of apparition on N. This contradiction proves that N is not composite.

Theorem 5.2. *If $U_{N\pm 1} \equiv 0 \pmod{N}$ and if $U_{m_i} \not\equiv 0 \pmod{N}$ where $m_i = (N \pm 1)/q_i$, and q_i are the prime factors of $N \pm 1$, then N is a prime.*

Proof. Let ω be the rank of apparition of N. Then ω is a divisor of $N \pm 1$, but not of m_i. Consequently ω contains q_i to the same power as $N \pm 1$. Hence $\omega = N \pm 1$, and N is a prime by the preceding theorem.

* Although Lucas did not attempt to give necessary tests, one of them actually is necessary. See paragraph 3.

† *Bull. Amer. Math. Soc.*, 33 (1927), pp. 327–340, 34 (1928), pp. 54–56.

THEOREM 5.3. *If* $U_{N+1} \equiv 0 \pmod{N}$ *and* $U_{(N+1)/q} \equiv s \not\equiv 0 \pmod{N}$ *and if the G. C. D. of* N *and* s *is* ϱ, *then the prime factors of* N *which do not divide* ϱ *are of the forms** $kq^{\alpha} \pm 1$, *where* α *is the highest power to which the prime* q *occurs as a factor of* $N \pm 1$.

Proof. Let p be a prime factor of N not dividing ϱ and let ω be the rank of apparition of p, then ω divides $N \pm 1$ but not $(N \pm 1)/q$. For otherwise s would be divisible by p, contrary to the hypothesis that p does not divide ϱ. Therefore ω contains the prime factor q to the same power α as $N \pm 1$. Since ω divides $p \pm 1$ we have $p = kq^{\alpha} \pm 1$, which is the theorem.

Ordinarily we find that $\varrho = 1$, but there are examples in which this is not the case. We proceed to apply these theorems to numbers N of special forms and to obtain necessary and sufficient conditions for primality.

3. **A test for Mersenne numbers.** We first consider the Mersenne numbers $2^n - 1$ with n an odd prime. Lucas has given two theorems† for testing these numbers, each theorem consisting of three disjunctive statements. The present extension enables us to replace these six statements by the following

THEOREM 5.4. *The number* $N = 2^n - 1$ *is a prime if and only if it divides the* $(n-1)$*-st term of the series*

$$4, \quad 14, \quad 194, \quad 37634, \quad \cdots, \quad S_k, \quad \cdots$$

where $S_k = S_{k-1}^2 - 2$.

Proof of necessity. Let N be a prime. Consider the series U defined by $R = 2$, $Q = -1$, $\Delta = 6$. Then

$$\varepsilon = \left(\frac{\Delta}{N}\right) = \left(\frac{6}{N}\right) = \left(\frac{3}{N}\right) = \left(\frac{-N}{3}\right) = -1,$$

$$\sigma = \left(\frac{R}{N}\right) = \left(\frac{2}{N}\right) = +1, \qquad \tau = \left(\frac{Q}{N}\right) = \left(\frac{-1}{N}\right) = -1.$$

Since $\sigma = -\tau$, it follows from Theorem 4.9 that N divides $V_{2^{n-1}}$. From (1.10) $V_{2^{k+1}} = V_{2^k}^2 - 2$ for $k > 0$. Since $V_2 = 4$, it follows that $S_k = V_{2^k}$ and hence N divides the $(n-1)$-st term of the series S.

Proof of sufficiency. By hypothesis N divides $V_{2^{n-1}}$ (and hence U_{2^n}) but is prime to $U_{2^{n-1}}$. The rank of apparition of N is thus a divisor of 2^n, but since N does not divide $U_{2^{n-1}}$, the rank of apparition of N is $2^n = N+1$. Consequently, by Theorem 5.1, N is a prime.

---

* The signs in $N \pm 1$ and $kq^{\alpha} \pm 1$ do not necessarily go together. Compare this theorem with *Bull. Amer. Math. Soc.*, 34 (1928), p. 54, Theorem 4 in which "Prime factors of N/ϱ", should be "prime factors of N not dividing ϱ".

† *Loc. cit.*, pp. 305, 316.

For numbers of the form $2^{4n-1}-1$ Lucas advises the use of the series 3, 7, 37, $\cdots$. This series does not give a necessary condition for primality, while the series 4, 14, 194, $\cdots$ gives a necessary and sufficient test for both $2^{4n\pm1}-1$.

4. **Further tests for Mersenne numbers.** We digress to consider other series S which may be used instead of 4, 14, 194, $\cdots$.

In order not to double the labor of applying the tests, we shall consider only those* in which $Q=\pm1$, that is, $S_{k+1}=S_k^2-2$, $k>1$. We are then to choose R and Q so that $\left(\frac{R}{N}\right)=\sigma$ and $\left(\frac{\Delta}{N}\right)=\varepsilon$ are known for N considered to be a prime. Suppose first that $Q=1$ and R_1 be a choice of R. Then R_1 must be a non-residue of N (taken to be a prime) and $\Delta_1=R_1-4$ must be a residue. For we need $\sigma\varepsilon=-1$ and $\sigma\tau=-1$, that is $\sigma=-1$, $\varepsilon=1$. If now $Q=-1$, R_1 and Δ_1 would be interchanged. We have already considered this transformation and have proved that if n is even, V_n is invariant as shown in (3.5). Since $S_k=V_{2^k}$, the series S is the same for $Q=\pm1$. If $N=2^n-1$, n being an arbitrary odd integer, the quadratic characters σ and ε cannot be determined except for certain values of R and Δ. The non-residue R must be chosen only from numbers of the form

$$-y^2, \qquad -2y^2, \qquad 3y^2, \qquad 6y^2,$$

where y is any integer. The residue Δ is chosen only from

$$x^2, \qquad 2x^2, \qquad -3x^2, \qquad -6x^2.$$

Since $S_1=V_2=(R+\Delta)/2$ is independent of the interchange of R and Δ, there remain only ten essentially distinct ways in which we can write the equation $\Delta-R=-4$. These are given below.

$$\begin{array}{llll}(1)\ x^2+y^2=-4, & (2)\ x^2+2y^2=-4, & (3)\ x^2-3y^2=-4, & (4)\ x^2-6y^2=-4,\\ (5)\ 2x^2+2y^2=-4, & (6)\ 2x^2-3y^2=-4, & (7)\ 2x^2-6y^2=-4,\\ & (8)\ -3x^2-3y^2=-4, & (9)\ -3x^2-6y^2=-4,\\ & & (10)\ -6x^2-6y^2=-4.\end{array}$$

But most of these equations are impossible. At first glance we rule out (1), (2), (5), (8), (9), and (10). Equations (3) and (4) are impossible because there are no solutions of $t^2-Du^2=-1$ for $D=3$ or 6. We are left with equations (6) and (7). In (6) x and y are both even. Setting $y=2u$,

* For tests in which $Q\neq\pm1$, see Pepin, *Comptes Rendus*, 86 (1877), pp. 307-310 (Carmichael, *loc. cit.*, p. 70) and Pomey, *Comptes Rendus*, 170 (1920), p. 100.

we get $x^2 - 6u^2 = -2$. This equation has infinitely many solutions as we find by expanding $6^{1/2}$ in a continued fraction. Solutions (x, y) are obtained from the convergents to $6^{1/2}$. Calculating the corresponding values of R and remembering that $V_2 = R - 2$, we get as many first terms S_1 as we wish. These are

$$S_1 = 10,\ 970,\ 95050,\ \cdots,\ u_n, \cdots, \quad \text{where } u_n = 98\,u_{n-1} - u_{n-2}.$$

Finally consider (7). Dividing by 2 we have $x^2 - 3y^2 = -2$. This equation has infinitely many solutions. By expanding $3^{1/2}$ we obtain the following values of $V_2 = S_1$

$$S_1 = 4,\ 52,\ 724,\ 10084,\ \cdots,\ u_n, \cdots, \quad \text{where } u_n = 14\,u_{n-1} - u_{n-2}.$$

Summing up the problem, we have two infinite sets of possible series S which may be used with every $2^n - 1$, (n odd). These series may be classified according to their first terms. There are 11 series whose first terms are $< 10^8$. These are

$S_1 =$ 4, 10, 52, 724, 970, 10084, 95050, 140452, 1956244, 9313930, 27246964.

COROLLARY. The number $2^n - 1$ is a prime if and only if the $(n-2)$-nd *term of any of the above series is* $\equiv \pm 2^{(n+1)/2} \pmod{n}$.

For n fixed, other residues and non-residues may be chosen which are characteristic of $N = 2^n - 1$, and hence other tests than those given above may be devised for this N. For example for $2^{257} - 1$ one may use the series 11, 119, 14159, $\cdots$. The total number of distinct series modulo N which may be used to test the number $N = 2^n - 1$ is 2^{n-2}. In fact the first terms of the series are obtainable from the expression

$$+\sqrt{2+\sqrt{2+\sqrt{2+\cdots+\sqrt{2}}}} \pmod{n} \qquad [(n-2) \text{ radicals}]$$

by varying the $+$ signs to $-$ signs in the 2^{n-2} possible ways.

5. **Tests for $3 \cdot 2^n - 1$.** We proceed to discuss tests for numbers of the form $A \cdot 2^n - 1$, A odd. The case $A = 3$ requires special treatment. The number $N = 3 \cdot 2^n - 1$ is a multiple of 5 if $n \equiv 1 \pmod 4$. We therefore exclude this case. The case $n \equiv 2 \pmod 4$ is an exceptional one, which we shall take up later. For the remaining 2 cases, we have the following

THEOREM 5.5. *If $n \equiv 0$ or $3 \pmod 4$, then a necessary and sufficient condition for the primality of $N = 3 \cdot 2^n - 1$ is that N divides the $(n-1)$st term of the series*

$$5778,\ 33385282,\ \cdots,\ S_k,\ \cdots, \quad \text{where } S_k = S_{k-1}^2 - 2.$$

Proof of necessity. Suppose N is a prime, and consider the series U defined by $R = 20$, $Q = 1$, and $\Delta = 16$. We have

$$\varepsilon = \left(\frac{16}{N}\right) = +1, \quad \sigma = \left(\frac{20}{N}\right) = \left(\frac{N}{5}\right) = -1, \quad \tau = \left(\frac{1}{N}\right) = +1.$$

Since $\sigma = -\tau$, we know by Theorem 4.9 that $V_{3\cdot 2^{n-1}} \equiv 0 \pmod N$. Moreover $V_6 = 5778 = S_1$, $V_{3\cdot 2^k} = S_k$ and hence $S_{n-1} \equiv 0 \pmod N$.

Proof of sufficiency. Let $S_{n-1} \equiv 0 \pmod N$. Then N divides $U_{3\cdot 2^n} = U_{N+1} = U_{3\cdot 2^{n-1}} \cdot V_{3\cdot 2^{n-1}}$, but is prime to $U_{3\cdot 2^{n-1}} = U_{(N+1)/2}$. Thus the hypotheses of Theorem 5.3 are satisfied and the factors of N are of the form $k2^n \pm 1$, the smallest of which, $2^n - 1$, exceeds $N^{1/2}$, hence N is a prime.

6. **Tests for $A \cdot 2^n - 1$.** For $N = A \cdot 2^n - 1$, $A > 3$ and odd, we give the following test.

THEOREM 5.6. *If $N = A \cdot 2^n - 1 \neq 3N'$, where $n > 2$, and A is prime to 6 and $< 2^n$, then a necessary and sufficient condition for N to be a prime is that N divides the $(n-1)$st term of the series*

$$S_1, S_2, S_3, \cdots, S_k, \cdots \text{ where } S_k = S_{k-1}^2 - 2, \quad S_1 = V_{2A}(12,1).$$

Proof of necessity. If N is a prime, then

$$\varepsilon = \left(\frac{8}{N}\right) = +1, \qquad \sigma = \left(\frac{12}{N}\right) = -1, \qquad \tau = \left(\frac{1}{N}\right) = +1.$$

Since $\sigma = -\tau$, we have $V_{(N-\sigma\varepsilon)/2} = V_{A\cdot 2^{n-1}} \equiv 0 \pmod N$ so that $S_{n-1} \equiv 0 \pmod N$.

Proof of sufficiency. If N divides $V_{A\cdot 2^{n-1}}$ (and hence U_{N+1}), but is prime to $U_{(N+1)/2}$, it follows again by Theorem 5.3 that the smallest possible factor of N is $2^n - 1$ which exceeds $N^{1/2}$. Thus N is a prime.

As special cases of this theorem we have the following tests.

1) *The number $N = 5 \cdot 2^n - 1$, $n > 2$ and even, is a prime if and only if N divides the $(n-1)$st term of the series*

$$95050, \quad 9034502498, \quad \cdots.$$

2) *The number $N = 7 \cdot 2^n - 1$, $n > 2$ and odd, is a prime if and only if N divides the $(n-1)$st term of the series*

$$9313930, \quad 86749292044898, \quad \cdots.$$

Any number of the above forms not covered by the above tests is a multiple of 3. The numbers $A \cdot 2^n - 1$ which we have failed to consider are $3 \cdot 2^{4n+2} - 1$, $3A2^n - 1$ for $A < 2^n$, and $A2^n - 1$ where $A > 2^n$ and may be a multiple of 3. A necessary and sufficient condition for the

primality of any number belonging to the first two cases may be readily found. To this effect we search for values of R, Q and Δ such that $\sigma\varepsilon = \sigma\tau = -1$. For convenience in computing we let $Q = 1$. Hence Δ must be a residue and R a non-residue of N (considered to be a prime). To find R and Δ we select a prime p, of the form $4k+1$, of which N is a non-residue. Setting $\Delta = x^2$, and $R = py^2$ we have $x^2 - py^2 = -4$. This equation always has solutions (x, y) which can be found as usual by expanding $p^{1/2}$ in a regular continued fraction. If $p = 8m+1$, (x, y) are taken as $(2t, 2u)$ in $t^2 - pu^2 = -1$. The value of $R = py^2$ follows at once and $V_{2A} = S_1$ can be calculated. The following table gives the values of R corresponding to different values of p.

TABLE 3.

p	R	p	R
5	20	53	53
13	13	61	1525
17	68	73	4562500
29	29	89	1000004
37	148	97	130073508
41	4100	101	404

The use of this table will be illustrated later.

Finally consider the numbers $A2^n - 1$, $A > 2^n$. Here we no longer have a proof of the sufficiency but we can assert that any factor of N is of one of the forms $k2^n \pm 1$. When n is large this gives a good restriction on the factors of N, and a better restriction on the squares which differ by N. This matter will be discussed elsewhere.

7. Tests for $A2^n+1$. For numbers of the forms $A2^n+1$, a similar discussion may be made. In particular we could give new tests for the primality of $2^{2^n}+1$, but those Fermat numbers which have not already been tested are too large for the application of any known test. As for the numbers $A2^n+1$, tests by the converse of Fermat's theorem are equally applicable and often more practical. Even if one does not insist that practical applicability is the only virtue of a test for primality, a discussion of the tests for $A2^n+1$ involves so many separate cases that it is easiest to invent an individual test for each number following the general methods described above.

8. The series S_k modulo N. In applying any of the above theorems the series S_k is taken modulo N. If and only if N is a prime, $S_k \equiv 2 \pmod{N}$ for all $k > n$. If N is composite, the series S_k becomes periodic modulo N, hence there is a pair of indices μ and ν such that $S_\mu \equiv S_\nu$

and $S_{\mu-1} \not\equiv S_{\nu-1}$. But this implies $S_{\mu-1}^2 \equiv S_{\nu-1}^2$ so that N divides the product $(S_{\mu-1}+S_{\nu-1})(S_{\mu-1}-S_{\nu-1})$. Provided $S_{\mu-1} \not\equiv -S_{\nu-1}$ we can decompose N into a pair of factors by the G. C. D. process. For example if we apply Theorem 5.6 to $N = 5 \cdot 2^6 - 1 = 319$ we find $S \equiv 307, 142, 65, 76, 32, 65, \cdots$. Consequently $142^2 - 32^2 = 174 \cdot 110 \equiv 0 \pmod{N}$. Hence $N = 11 \cdot 29$. In general this periodicity manifests itself before the term of rank $(N+1)/2$ is reached. Many examples indicate that the period is much shorter, but there seems to be very little regularity in the results.

9. **Examples.** In conclusion we give a few examples showing the application of the above discussion.

1) $N = 7 \cdot 2^{29} - 1 = 3758096383$. In accordance with the second special case of Theorem 5.6 we form the sequence

$$9313930, \quad 86749292044898, \quad \cdots, \qquad (\text{mod } N).$$

The 28th remainder is found to be zero, hence N is a prime.

2) $N = 9 \cdot 2^{21} - 1 = 18874367$. We have not developed a test for this number. However we see that $\left(\frac{N}{5}\right) = -1$. From Table 3 we take $R = 20$, $Q = 1$ and find that $V_{18} = S_1 = 4122878$. Calculating the series S modulo N we find that $S_{20} \equiv 0$. Consequently N is a prime.

3) $N = 3 \cdot 2^{38} - 1 = 824633720831$. Since $38 = 4m + 2$, Theorem 5.5 does not apply. We find however that $\left(\frac{N}{13}\right) = -1$. From Table 3, we take $R = 13$, $Q = 1$, $V_6(13, 1) = S_1 = 1298$. The 37th term of the series S modulo N is zero, hence N is a prime.