Canad. Math. Bull. Vol. **20** (1), 1977

ON NUMBERS ANALOGOUS TO THE CARMICHAEL NUMBERS

BY
H. C. WILLIAMS

1. **Introduction.** A base a pseudoprime is an integer n such that

$$a^{n-1} \equiv 1 \pmod{n}. \tag{1}$$

A Carmichael number is a composite integer n such that (1) is true for all a such that $(a, n)=1$. It was shown by Carmichael [1] that, if n is a Carmichael number, then n is the product of k (>2) distinct primes p_1, p_2, $p_3, \ldots p_k$ and $p_i-1 \mid n-1$ $(i=1,2,3,\ldots,k)$. The smallest such number is $561=3\cdot 11\cdot 17$.

The Lucas functions $V_n(P, Q)$, $U_n(P, Q)$ are defined as

$$V_n(P, Q)=\alpha^n+\beta^n,$$
$$U_n(P, Q)=(\alpha^n-\beta^n)/(\alpha-\beta),$$

where α, β are the zeros of x^2-Px+Q, and P, Q are coprime integers. We also define Δ to be the discriminant P^2-4Q of the above quadratic function. The following theorem concerning Lucas functions is well known.

THEOREM 1. *If p is an odd prime and $p \nmid Q$, then*

$$U_{\delta(p)}(P, Q) \equiv 0 \pmod{p},$$

where $\delta(p)=p-\epsilon(p)$, $\epsilon(p)=(\Delta \mid p)$, and $(\Delta \mid p)$ is the Legendre symbol.

Rotkiewicz [4] considered a composite integer n such that

$$U_{n-\epsilon(n)}(P, Q) \equiv 0 \pmod{n}$$

to be a type of pseudoprime with respect to the Lucas functions. Here $\epsilon(n)$ is defined to be the value of the Jacobi symbol $(\Delta \mid n)$. We shall concern ourselves here with those odd composite integers n which possess, for a given value of Δ, the property (A) below.

$$\text{(A)} \qquad \begin{cases} \text{For all integers } P, Q \text{ such that} \\ (P, Q)=1,\ P^2-4Q=\Delta, \qquad (n, Q\Delta)=1, \\ \text{we have} \\ U_{n-\epsilon(n)}(P, Q) \equiv 0 \pmod{n}. \end{cases}$$

In view of the preceding remarks, we see that such integers are analogous to

Received by the editors, in revised form, January 13, 1977

Carmichael numbers; in fact, it can be shown that if $\Delta=1$ and n satisfies (A), then n is a Carmichael number. In this paper we shall characterize and develop some properties of those integers which satisfy (A) for any given Δ.

2. **Preliminary results.** In order to establish some properties of the numbers we are seeking, it is necessary to first make some preliminary observations.

We first note that

$$(2)\qquad \begin{aligned} 2^{n-1}V_k(P,Q) &= \sum_{r=0}^{[k/2]} \binom{k}{2r} P^{k-2r}(P^2-4Q)^r \\ 2^{n-1}U_k(P,Q) &= \sum_{r=0}^{[k/2]} \binom{k}{2r+1} P^{k-2r-1}(P^2-4Q)^r. \end{aligned}$$

If, for a fixed Δ, we define the polynomials $T_k(x)$ and $S_k(x)$ by the formulas

$$T_k(x)=\sum_{r=0}^{[k/2]} \binom{k}{2r+1} x^{k-2r-1}\Delta^r,$$

$$S_k(x)=\sum_{r=0}^{[k/2]} \binom{k}{2r} x^{k-2r}\Delta^r,$$

then we have

$$(3)\qquad \begin{aligned} 2^{n-1}U_k(P,Q) &= T_k(P), \\ 2^{n-1}V_k(P,Q) &= S_k(P), \end{aligned}$$

when $P^2-4Q=\Delta$. We also have the result

$$T_{k+m}(x)=2S_m(x)T_k(x)-(x^2-\Delta)^m\, T_{k-m}(x)$$

and from this it follows easily by induction that if $m \mid k$,

$$T_k(x)=T_m(x)Q_{k,m}(x),$$

where $Q_{k,m}(x)$ is a polynomial in x with integer coefficients.

Before proceeding any further we require the following simple lemma.

LEMMA 1. *If P, Q are any two integers such that $P^2-4Q=\Delta$, then for any odd integer m, where $(m,\Delta)=1$, there exist integers P', Q' such that $P'\equiv P$, $Q'\equiv Q$ $(\text{mod } m)$, $P'^2-4Q'=\Delta$, and $(P',Q')=1$.*

Proof. Select some integer d such that $(d,\Delta)=2^i(0\le i\le 2)$, where the value of i is determined by

$$d\equiv P+2Q-2 \pmod 4.$$

Solve

$$(4)\qquad 2mK\equiv d-P \pmod{\Delta}$$

for K. If $2 \mid P$, then $4 \mid \Delta$ and $K\equiv(d-P)/2\equiv(Q+1) \pmod 2$. Put $P^1=P+2Km$,

https://doi.org/10.4153/CMB-1977-025-9 Published online by Cambridge University Press

$Q' = Q + Km(P + mK)$. We see that $P'^2 - 4Q' = \Delta$ and it suffices to show that $(P', Q') = 1$. If q is a prime and $q \mid (P', Q')$, then q must be odd; for, if $q = 2$, then $2 \mid \Delta$, $2 \mid P$, and $Q' \equiv 2Q + 1 \pmod 2$. If q is odd, then $q \mid \Delta$, and by (4) $q \mid d$, which, by selection of d, is impossible.

Finally, it should be noted that if X is any integer, then

$$T_{\delta(p)}(X) \equiv 0 \pmod p$$

where p is any odd prime such that $(p, (X^2 - \Delta)) = 1$. This result follows easily from Theorem 1, (3), and Lemma 1.

3. Some results concerning the Lucas functions. The rank of apparition modulo m of the Lucas sequence $\{U_k(P, Q)\}$ is defined to be the least positive value of k such that $m \mid U_k(P, Q)$. We denote this value of k by $\omega(m; P, Q)$. If $m \mid U_r(P, Q)$, then $\omega(m; P, Q) \mid r$; hence, $\omega(p; P, Q) \mid \delta(p)$ when p is a prime.

For a fixed discriminant Δ and a fixed odd prime p, let the function $\psi(d)$, where $d \mid \delta(p)$, be the number of distinct values of P modulo p such that $\omega(p; P, Q) = d$. In the following theorem we evaluate $\psi(d)$.

THEOREM 2. *If $d > 1$, $\psi(d) = \phi(d)$, where $\phi(x)$ is Euler's totient function.*

Proof. If $\epsilon(p) = 0$, the theorem follows easily. Suppose $\epsilon(p) \neq 0$ and put $\delta = \delta(p)$. If $d < \delta$, let the polynomial congruence

$$T_d(x) \equiv 0 \pmod p \tag{5}$$

have j solutions. Referring to the remarks at the beginning of this section and Lemma 1, we see that

$$\sum_{h \mid d} \psi(h) = j.$$

Since $T_d(x)$ is a polynomial of degree $d - 1$ with leading coefficient d we have $j \leq d - 1$. Also

$$T_\delta(x) \equiv 0 \pmod p \tag{6}$$

has exactly $\delta - 1$ solutions $\pmod p$. For, if $\epsilon(p) = 1$, (6) is satisfied by any x except the two values of x which satisfy $x^2 \equiv \Delta \pmod p$; if $\epsilon(p) = -1$, (6) is satisfied by any value of x since there is no x such that $x^2 \equiv \Delta \pmod p$.

Now

$$T_\delta(x) = T_d(x) Q_{\delta,d}(x);$$

Thus, if (5) has j solutions, then

$$Q_{\delta,d}(x) \equiv 0 \pmod p \tag{7}$$

has $\delta - 1 - j$ solutions. Since the degree of $Q_{\delta,d}(x)$ is $\delta - d$ and its leading coefficient is prime to p, (7) can have no more than $\delta - d$ solutions. If $j < d - 1$, then $\delta - 1 - j > \delta - d$; consequently, $j = d - 1$.

Putting

$$\chi(h)=\psi(h)\ (h\neq 1), \qquad \chi(1)=1,$$

we get

$$\sum_{h\mid d}\chi(h)=d;$$

by Möbius inversion $\chi(d)=\phi(d)$.

COROLLARY. *If Δ is any fixed discriminant, p is any odd prime, and $d(>1)$ is any divisor of $\delta(p)$, there exist integers P, Q such that $(P, Q)=1$, $P^2-4Q=\Delta$, and $\psi(p; P, Q)=d$.*

Define

$$C_k(P, Q)=\frac{\partial}{\partial P}U_k(P, Q)$$

$$D_k(P, Q)=\frac{\partial}{\partial Q}U_k(P, Q).$$

Since $U_k(P, Q)$ is a polynomial in P and Q with integer coefficients, so are $C_k(P, Q)$ and $D_k(P, Q)$.

We will assume here that P, Q are fixed and write U_k for $U_k(P, Q)$, C_k for $C_k(P, Q)$ etc.

Since

$$U_{k+1}=PU_k-QU_{k-1},$$

we get differentiation

$$(8)\qquad \begin{aligned} C_{k+1}&=PC_k+U_k-QC_{k-1}\\ D_{k+1}&=PD_k-QD_{k-1}-U_{k-1}.\end{aligned}$$

By induction we can show that

$$(9)\qquad D_k=-C_{k-1}.$$

Also, by differentiating the second formula of (2) with respect to P and Q and putting $k=p$ (an odd prime, $(p, \Delta Q)=1$), we get

$$\Delta C_p\equiv -P\epsilon(p) \pmod p$$

$$\Delta D_p\equiv 2\epsilon(p) \pmod p.$$

Using (8) and (9) together with the fact that

$$U_p\equiv\epsilon(p) \pmod p,$$

we have

$$\Delta C_{p+1}\equiv -2Q\epsilon(p) \pmod p$$

and if $\epsilon(p)=1$,

$$Q\Delta C_{p-1}\equiv -P \pmod p.$$

It follows that

$$PC_\delta+2QD_\delta\equiv 0 \pmod p$$

and $p\nmid C_\delta$, where $\delta=\delta(p)$.

By using Taylor's Expansion, we see that

$$U_\delta(P+2Kp, Q+Mp)\equiv U_\delta(P,Q)+p[2KC_\delta(D,Q)+MD_\delta(P,Q)] \pmod{p^2}.$$

If $p^2 \mid U_\delta(P,Q)$, select a value for K such that $p\nmid K$ and put $M=KP+pK^2$. Then if $P'=P+2Kp$, $Q'=Q+Mp$, we have $P'^2-4Q'=\Delta$.
Now if

$$4Qu\equiv P \pmod p,$$

then since $p\nmid\Delta$,

$$1-uP\not\equiv 0 \pmod p,$$

$$K(1-uP)\not\equiv 0 \pmod p$$

and

$$K\not\equiv 2uM \pmod p;$$

hence, $p^2\nmid U_\delta(P',Q')$. By using Lemma 1, we can show that for any Δ there exists a pair of integers P'', Q'' such that $(P'',Q'')=1$, $P''^2-4Q''=\Delta$, $(p,Q'')=1$, and $p^2\nmid U_\delta(P'',Q'')$.

Since $\omega(p;P'',Q'')=\omega(p;P,Q)$ when $P''\equiv P$, $Q''\equiv Q \pmod p$ and $\omega(p;P,Q)\mid\delta(p)$, we deduce from Theorem 2 the fact that, for any given Δ, any odd prime $p((p,\Delta)=1)$, and d any divisor of $\delta(p)$ $(d>1)$, there exist integers P'', Q'' such that $p\nmid Q''$, $(P'',Q'')=1$, $P''-4Q''=\Delta$, $\omega(p;P'',Q'')=d$, $\omega(p^2;P'',Q'')>d$.

By using the Law of Repetition of Lucas Functions, we have

THEOREM 3. *For any given Δ, any odd prime $p((p,\Delta)=1)$, and d any divisor of $\delta(p)$ $(d>1)$, there exist integers P'', Q'' such that $p\nmid Q''$, $(P'',Q'')=1$, $P''^2-4Q''=\Delta$, and $\omega(p^k,P'',Q'')=p^{k-1}d$.*

4. **Characterization of integers with property (A).** In this section we will find the forms of those integers which possess the property (A) for a given fixed Δ. In order to do this we first require two lemmas. We give these lemmas here in a form somewhat stronger than we need to obtain the results of this section; however, we will need the stronger results in section 5.

LEMMA 2. *If r, Δ, η are three given integers such that r is odd, $(r,\Delta)=1$, $|\eta|=1$ (we restrict η to be 1 when r is a perfect square and if $\Delta\equiv 1 \pmod 3$, we restrict η*

https://doi.org/10.4153/CMB-1977-025-9 Published online by Cambridge University Press

to be -1 *when* $r=3t^2$), *then there exists a pair of integers* y, γ *such that*

$$y^2 \equiv 4\gamma + \Delta \pmod r$$

and $(\gamma \mid r) = \eta$, *where* $(\gamma \mid r)$ *is the Jacobi symbol.*

Proof. Let

$$r = \prod_{i=0}^{k} q_i^{\beta_i}$$

where $q_i (i = 1, 2, 3, \cdots, k)$ are distinct odd primes and q_1 is the least of these k primes. Select $\eta_1, \eta_2, \eta_3, \cdots, \eta_k$ such that $|\eta_i| = 1$ for $i = 1, 2, 3, \cdots, k$ (restrict η_1 to be -1 if $q_1 = 3$ and $\Delta \equiv 1 \pmod 3$) and

$$\prod_{i=1}^{k} \eta_i^{\beta_i} = \eta.$$

It is well known that if q is a prime and $q \nmid \Delta$, then there are $q-1$ solutions (x, y) of

$$y^2 - x^2 \equiv \Delta \pmod q \tag{10}$$

and at least $q-3$ of these have $x \not\equiv 0 \pmod q$. Thus, if $q > 3$, there exist y and λ such that

$$y^2 \equiv 4\lambda + \Delta \pmod q \tag{11}$$

and $(\lambda \mid q) = +1$. If $q = 3$ and $\Delta \equiv -1 \pmod 3$ we see that $y \equiv 0$, $\lambda \equiv 1 \pmod 3$ is a solution of (11) with $(\lambda \mid q) = +1$.

If for each $y \pmod q$ there were a value of $x \pmod q$ such that (10) held, there would be at least $2q-2$ solutions of (10) with $x \not\equiv 0 \pmod q$. Since $2q-2 > q-1$, there must be values of y and λ such that (11) is satisfied and $(\lambda \mid q) = -1$.

It follows that for each q_i which divides r there must exist a pair of integers (y_i, λ_i) such that

$$y_i^2 \equiv 4\lambda_i + \Delta \pmod{q_i}$$

and $(\lambda_i \mid q_i) = \eta_i$. We can then find integers Y_i and γ_i such that

$$Y_i^2 \equiv 4\gamma_i + \Delta \pmod{q_i^{\beta_i}}$$

and $\gamma_i \equiv \lambda_i \pmod{q_i}$. By the Chinese Remainder Theorem, there exist integers γ and y such that $y \equiv Y_i$; $\gamma \equiv \gamma_i \pmod{q_i^{\beta_i}}$ $(i = 1, 2, 3, \ldots, k)$. Thus we have

$$y^2 \equiv 4\gamma + \Delta \pmod r$$

and $(\gamma \mid r) = \eta$.

https://doi.org/10.4153/CMB-1977-025-9 Published online by Cambridge University Press

LEMMA 3. *Let* r, m, Δ, η *be given integers such that* r *is odd,* $(r, m\Delta)=1$, $|\eta|=1$ ($\eta=1$ *when* r *is a perfect square;* $\eta=-1$ *when* $\Delta\equiv 1 \pmod 3$ *and* $r=3t^2$). *If* $P^2-4Q=\Delta$, *there exists a pair of integers* P', Q' *such that* $P'^2-4Q'=\Delta$, $P'\equiv P$. $Q'\equiv Q \pmod m$ *and* $(Q' \mid r)=\eta$.

Proof. Let γ and y be selected such that $(\gamma \mid r)=\eta$

$$y^2\equiv 4\gamma+\Delta \pmod r$$

Select K such that

$$2mK+P\equiv y \pmod r.$$

If we put

$$P'=P+2mK,$$

$$Q'=Q+Km(P+mK),$$

we have $P'^2-4Q'=\Delta$, $P'\equiv P$, $Q'\equiv Q \pmod m$ and $Q'\equiv\gamma \pmod r$.

COROLLARY. Let r, Δ, m *be three integers such that* r *is odd and* $(r, m\Delta)=1$. *If* $P^2-4Q=\Delta$, *there exists a pair of integers* P', Q' *such that* $P'^2-4Q'=\Delta$, $P'\equiv P$, $Q'\equiv Q \pmod m$ *and* $(Q', r)=1$.

We are now able to prove our main theorem.

THEOREM 4. *If for a fixed* Δ, n *possesses property* (A), *then* n *is the product of* k *distinct primes* $p_1, p_2, p_3, \ldots, p_k$ *and*

$$p_i-\epsilon(p_i) \mid n-\epsilon(n) \qquad (i=1,2,3,\ldots,k).$$

Proof. Let p be any odd prime divisor of n and let $n=p^\alpha r$, where $(r,p)=1$. Find P, Q such that $(P,Q)=1$, $P^2-4Q=\Delta$, $\omega(p^\alpha; P, Q)=p^{\alpha-1}\delta(p)$. By the Corollary of Lemma 3, there exist P', Q', such that $P'^2-4Q'=\Delta$, $P'\equiv P$, $Q'\equiv Q \pmod{p^\alpha}$ and $(Q', r)=1$; also, by Lemma 1, we can find P'', Q'' such that $P''^2-4Q''=\Delta$, $P''\equiv P'$, $Q''\equiv Q' \pmod n$ and $(P'', Q'')=1$. Since $(n, Q''\Delta)=1$ and $P''\equiv P$, $Q''\equiv Q \pmod{p^\alpha}$, we have

$$U_{n-\epsilon(n)}(P'', Q'')\equiv 0 \pmod n$$

and

$$\omega(p^\alpha; P'', Q'')=p^{\alpha-1}\delta(p);$$

hence,

$$p^{\alpha-1}\delta(p) \mid p^\alpha r-\epsilon$$

where $|\epsilon|=1$. We see that $\alpha=1$ and the theorem follows.

If $n=p_1p_2$, we must have $\epsilon(n)=\epsilon(p_1)\,\epsilon(p_2)$ and if $\epsilon_i=\epsilon(p_i)$,

$$p_1-\epsilon_1 \mid p_1p_2-\epsilon_1\epsilon_2, \qquad p_2-\epsilon_2 \mid p_1p_2-\epsilon_1\epsilon_2.$$

That is $p_1-\epsilon_1 \mid p_2-\epsilon_2$ and $p_2-\epsilon_2 \mid p_1-\epsilon_1$; hence, $p_1-\epsilon_1=p_2-\epsilon_2$. If we assume $p_1<p_2$, we have $\epsilon_1-\epsilon_2=-2$, i.e. $\epsilon_1=-1$, $\epsilon_2=1$ and $p_1=p_2-2$.

Thus, n can be the product of two primes and satisfy property (A) for a fixed Δ if and only if

$$n=p_1p_2,$$

where

$$p_1=p_2-2; \qquad (\Delta \mid p_1)=-1 \quad \text{and} \quad (\Delta \mid p_2)=+1.$$

For example, if $\Delta=5$, $p_1=17$, $p_2=19$, then $n=17\cdot 19$ satisfies (A).

Integers with property (A) and $k>2$ can frequently be found by using a modification of the method of Chernick [2]. For example, let $k=3$ and prescribe values for ϵ_1, ϵ_2, ϵ_3. If d satisfies the congruence

$$d(\epsilon_1r_2r_3+\epsilon_2r_1r_3+\epsilon_3r_1r_2)+\epsilon_1\epsilon_2r_3+\epsilon_1\epsilon_3r_2+\epsilon_2\epsilon_3r_1\equiv 0 \pmod{r_1r_2r_3} \tag{10}$$

for values of r_1, r_2, r_3 such that $(\Delta \mid dr_i-\epsilon_i)=\epsilon_i$ $(i=1,2,3)$ and $dr_1+\epsilon_1$, $dr_2+\epsilon_2$, $dr_3+\epsilon_3$ are distinct primes, then

$$n=(dr_1+\epsilon_1)(dr_2+\epsilon_2)(dr_3+\epsilon_3)$$

has property (A).

If we have $\Delta=8$ and put $\epsilon_1=-1$, $\epsilon_2=\epsilon_3=1$, we must have $p_1=dr_1-1$, $p_2=dr_2+1$, $p_3=dr_3+1$ and $(2 \mid p_i)=\epsilon_i$. Let $p_1\equiv 3$, $p_2\equiv p_3\equiv 7 \pmod 8$. We get $d=2d''$ and

$$d''r_1\equiv 2, \qquad d''r_2\equiv d''r_3\equiv 3 \pmod 4;$$

hence, putting $r_1=2$, $r_2=3$, $r_3=7$, we have $d''\equiv 1 \pmod 4$ and by (10), $d''\equiv -4 \pmod{21}$. When $d''=17$, we get $p_1=67$, $p_2=103$, $p_3=239$ and $n=p_1p_2p_3$ has property (A) for $\Delta=8$. In fact, this number has property (A) for $\Delta=8m^2$ for any m such that $(m,n)=1$.

5. **Some further remarks.** Recently Lehmer [3] has considered the problem of the existence of strong Carmichael mumbers. These are integers which satisfy the following congruence

$$a^{(n-1)/2}\equiv (a \mid n) \pmod n$$

for all a such that $(a,n)=1$. In [3] it is shown that there are no strong Carmichael numbers. In this section we will find a result analogous to that of Lehmer.

The result in the theory of Lucas functions which is analogous to

$$a^{(p-1)/2}\equiv (a \mid p) \pmod p,$$

where p is an odd prime and $(a,p)=1$, is given in the following theorem.

https://doi.org/10.4153/CMB-1977-025-9 Published online by Cambridge University Press

THEOREM 5. *If* $\epsilon = (\Delta \mid p)$, *then*

$$U_{(p-\epsilon)/2}(P, Q) \equiv 0 \pmod p \quad \textit{when} \quad (Q \mid p) = 1,$$

and

$$V_{(p-\epsilon)/2}(P, Q) \equiv 0 \pmod p \quad \textit{when} \quad (Q \mid p) = -1.$$

We say that an odd integer n satisfies property (B) for a given Δ if

(B) For all P, Q such that $P^2 - 4Q = \Delta$, $(P, Q) = 1$ and $(n, \Delta Q) = 1$ we have

$$U_{(n-\epsilon(n))/2}(P, Q) \equiv 0 \pmod n$$

whenever $(Q \mid n) = +1$ and

$$V_{(n-\epsilon(n))/2}(P, Q) \equiv 0 \pmod n$$

whenever $(Q \mid n) = -1$.

We will show that there are no odd composite integers satisfying (B) and we will do this by first characterizing all those odd composite integers n which satisfy property (C) below.

(C) for all P, Q such that $P^2 - 4Q = \Delta$, $(P, Q) = 1$, $(n, \Delta Q) = 1$, and $(Q \mid n) = -1$, we have

$$V_{(n-\epsilon(n))/2}(P, Q) \equiv 0 \pmod n.$$

THEOREM 6. *If n (odd, composite) is not a perfect square or if $n \neq 15$ whenever* $\Delta \equiv 4 \pmod{15}$, *then n can not satisfy* (C).

Proof. Suppose that some odd n satisfies (C) and that n is not a perfect square. Let p be any prime divisor of n and let $n = p^\alpha r$ where $(r, p) = 1$.

Put $\theta = \theta(p) = 1$ if $r = 3t^2$ and $\Delta \equiv 1 \pmod 3$; otherwise, put $\theta = 0$. Find P, Q such that $(P, Q) = 1$, $P^2 - 4Q = \Delta$, $\omega(p^\alpha; P, Q) = \kappa\delta(p)p^{\alpha-1}$, where $\kappa = 1 - \theta/2$; then $(Q \mid p) = (-1)^{\theta-1}$. We now find P', Q' such that $P'^2 - 4Q' = \Delta$ and $P' \equiv P, Q' \equiv Q \pmod{p^\alpha}$, $(Q' \mid r) = (-1)^{\alpha(\theta-1)+1}$. From these we can determine P'', Q'' such that $(P'', Q'') = 1$, $(n, Q'') = 1$, $P''^2 - 4Q'' = \Delta$, $\omega(p^\alpha; P'', Q'') = \kappa p^{\alpha-1}\delta(p)$, $(Q'' \mid n) = (Q \mid p)^\alpha (Q' \mid r) = (-1)^{2\alpha(\theta-1)+1} = -1$.

Now since $p^\alpha \mid n$,

$$V_{(n-\epsilon(n))/2}(P'', Q'') \equiv 0 \pmod{p^\alpha};$$

hence

$$U_{n-\epsilon(n)}(P'', Q'') \equiv 0 \pmod{p^\alpha}$$

and $\kappa\delta(p)p^{\alpha-1} \mid n - \epsilon(n)$. We conclude that $\alpha = 1$ and by repeating the above argument on all primes which divide n, we see that n must be a product of distinct primes. It follows that, if $\theta = 1$ for some prime p which divides n, then $n/p = 3$. Also $(\Delta \mid 3) = 1$ and $(p - \epsilon(p))/2 \mid 3p - \epsilon(p)$; hence, we must have $p = 5$ and $\epsilon(5) = +1$. Since $(\Delta \mid 5) = (\Delta \mid 3) = 1$, $(Q \mid 3) = -1$, and $(Q \mid 5) = +1$, we also must have $\Delta \equiv 4 \pmod{15}$. Thus, if $n \neq 15$ whenever $\Delta \equiv 4 \pmod{15}$, we see

https://doi.org/10.4153/CMB-1977-025-9 Published online by Cambridge University Press

that $\theta(p)$ must be zero for each prime p which divides n and consequently $\delta(p) \mid n-\epsilon(n)$.

Let $n = pr$, where p is a prime and $p \neq 3$ and select P, Q such that $(P, Q) = 1$, $P^2 - 4Q = \Delta$, $\omega(p; P, Q) = \delta(p)/2$. We can then find P'', Q'' such that $(P'', Q'') = 1$, $(n, Q'') = 1$, $P''^2 - 4Q = \Delta$, $\omega(p; P'', Q'') = \delta(p)/2$, $(Q'' \mid n) = -1$.

Since

$$V_{(n-\epsilon(n))/2}(P'', Q'') \equiv 0 \pmod p$$

and $p \nmid (V_m(P'', Q''), U_m(P'', Q''))$ for any m, we see that $\omega(p; P'', Q'') \nmid (n-\epsilon(n)/2)$. However, $\omega(p; P'', Q'') = \delta(p)/2$ and $\delta(p) \mid n-\epsilon(n)$; hence, $\delta(p)/2 \mid (n-\epsilon(n))/2$, which is a contradiction.

In the following theorem we obtain our result.

THEOREM 7. *There are no odd composite integers which satisfy* (B) *for any* Δ.

Proof. If n satisfies (B) for some Δ, it must satisfy (A) for that same Δ. Hence n is the product of distinct primes and not a perfect square. Since n must also satisfy (C) we see that n can only be 15 when $\Delta \equiv 4 \pmod{15}$; however, in this case, we do not have $\delta(5) \mid 15-\epsilon(15)$.

Another problem of some interest is that of whether there exists a Carmichael number n which possesses property (A) for some Δ such that $(\Delta \mid n) = -1$. It is not difficult to show that if such numbers Δ and n exist, n must be the product of an odd number of distinct primes $p_1, p_2, p_3, \ldots, p_k$, $\epsilon(p_i) = -1$ $(i = 1, 2, 3, \ldots, k)$, and $p_i + 1 \mid n+1$, $p_i - 1 \mid n-1$ for $i = 1, 2, 3, \ldots, k$. For suppose $p \mid n$ and $\epsilon(p) = +1$, then $p-1 \mid n+1$ and $p-1 \mid n-1$, which means that $p = 3$. If q is any other prime divisor of n, then $\epsilon(q) = -1$, $q+1 \mid n+1$ and $q-1 \mid n-1$. If $3 \mid n$, this is impossible; hence, $\epsilon(p) = -1$ for any $p \mid n$. Since $\epsilon(n) = -1 = \epsilon_n(p_1)\epsilon(p_2) \cdots \epsilon(p_n) = (-1)^k$, k must be odd.

It is not known to the author whether any such numbers exist. It can be shown, however, that if n is such a number, $k \geq 5$. To show this it suffices to show that $k \neq 3$. Suppose $k = 3$ and $n = p_1p_2p_3$ with $p_1 < p_2 < p_3$. We have

$$\begin{aligned} p_1p_2 - 1 &\equiv 0 \pmod{p_3 - 1} \\ -p_1p_2 + 1 &\equiv 0 \pmod{p_3 + 1}; \end{aligned}$$

hence, $(p_3^2 - 1)/2$ is a divisor of $p_1p_2 - 1$. Since $p_3 > p_2, p_1$, we have $p_3^2 + 1 = 2p_1p_2$. It is also true that $p_2p_3 - 1$ is divisible by $(p_1^2 - 1)/2$ and $p_1p_3 - 1$ is divisible by $(p_2^2 - 1)/2$. Thus,

$$\frac{p_2p_3 - 1}{(p_1^2 - 1)/2} > \frac{p_1p_3 - 1}{(p_2^2 - 1)/2} > \frac{p_1p_2 - 1}{(p_3^2 - 1)/2}$$

and each of these three numbers is an integer. Since

$$p_1p_3 \neq p_2^2,\ p_1p_2 - 1 \geq 3(p_2^2 - 1)/2,\ p_2p_3 - 1 \geq 4(p_1^2 - 1)/2$$

https://doi.org/10.4153/CMB-1977-025-9 Published online by Cambridge University Press

and

$$p_1p_2+p_2p_3+p_3p_1-3\geq(p_3^2-1)/2+3(p_2^2-1)/2+4(p_1^2-1)/2.$$

Since

$$p_1p_2+p_2p_3+p_3p_1\leq p_1^2+p_2^2+p_3^2,$$

we have

$$2(p_1^2+p_2^2+p_3^2)\geq p_3^2+3p_1^2+4p_1^2-2;$$

hence,

$$p_3^2+1\geq p_2^2+2p_1^2-1>p_2^2+p_1^2\geq 2p_1p_2,$$

which is impossible.

References

1. R. D. Carmichael. *A new number theory function*, Bull. Amer. Math. Soc., **19** (1910), pp. 232–238.

2. Jack Chernick, *On Fermat's simple theorem*, Bull. Amer. Math. Soc., **45** (1939), pp. 269–274.

3. D. H. Lehmer, *Strong Carmichael numbers, J. Aust. Math. Soc.*, Ser. **A**, **21** (1976) pp. 508–510.

4. A Rotkiewicz, *On the pseudoprimes with respect to the Lucas sequences*, Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys., **21** (1973), pp. 793–797.

University of Manitoba.
Winnipeg, Man. R3T 2N2

https://doi.org/10.4153/CMB-1977-025-9 Published online by Cambridge University Press