ON A CONJECTURE OF CARMICHAEL

V. L. KLEE, JR.[1]

Carmichael [1][2] conjectured that for no integer n can the equation $\phi(x)=n$ (ϕ being Euler's totient) have exactly one solution. To support the conjecture, he showed that each n for which there is a unique solution must satisfy a restriction which implies $n>10^{37}$. In this note we prove the validity of restrictions considerably stronger than those of Carmichael, and raise the lower bound on n to 10^{400}.

We shall denote by X the set of all integers x for which $\phi(y)=\phi(x)$ implies $y=x$. (If the conjecture is correct, X is empty, and the theorems stated are vacuously satisfied.)

(1) THEOREM. *Suppose that $\bar{x}=\prod_A p_i^{a_i}$ is in X, where the p_i's are distinct primes and A is the range of the index i. Let $m=\prod_B p_i^{a_i-1}(p_i-1)\cdot\prod_C p_i^{c_i}$ where B and C are disjoint subsets of A (one of them may be empty) and $c_i\leqq a_i-1$ for i in C. Then if p is prime and $p-1=m$, we have $p\mid\bar{x}$.*

For if $p\nmid\bar{x}$, we have $\phi(p\cdot\prod_{A-B-C}p_i^{a_i}\cdot\prod_C p_i^{a_i-c_i})=\phi(\bar{x})$, contrary to the definition of X.

(1.1) COROLLARY. *Suppose, under the hypotheses of* (1), *that B has the following property: if q is prime and $q\mid(p_j-1)$ for some j in B, then $q\mid\bar{x}$. We must then have $p^2\mid\bar{x}$.*

For under this condition we have $p-1=\prod_D p_i^{d_i}$, D being a subset of A. So if $p\mid\bar{x}$ but $p^2\nmid\bar{x}$, then $\phi(\prod_{A-D}p_i^{a_i}\cdot\prod_D p_i^{a_i+d_i}/p)=\phi(\bar{x})$, contrary to the definition of X.

(1.2) COROLLARY. *If, in the hypotheses of* (1), *B is empty, we have $p^2\mid\bar{x}$.*

(1.3) COROLLARY. *$4\mid\bar{x}$. If f is a Fermat prime such that $f\mid\bar{x}$, then $f^2\mid\bar{x}$.*

(1.2) and (1.3) are Carmichael's original conditions. From (1.1) and (1.3) it follows that $\bar{x}$ is divisible by 3^2, 7^2, 43^2, 3^3 or 13^2, $\cdots$. (By extending this list Carmichael showed both $\bar{x}$ and $\phi(\bar{x})$ to be greater than 10^{37}.)

Presented to the Society, October 25, 1947; received by the editors December 12, 1946, and, in revised form, April 5, 1947.

[1] I should like to thank Professor C. G. Jaeger of Pomona College for arousing my interest in Euler's ϕ-function.

[2] Numbers in brackets refer to the references at the end of the paper.

(2) THEOREM. *Suppose* $u=2^a s\prod_A f_i^{a_i}$ *is in* X, *where the* f_i*'s are distinct Fermat primes other than* 3, *and* s *is odd and divisible by no Fermat prime other than* 3. *Suppose that* $C\subset A$, $2\leqq c\leqq a$, $v=2^c s\prod_C f_i^{a_i}$. *Then* v *is in* X *if and only if either* $C=A$, *or for each index* i *in* $A-C$, $2^c\mid(f_i-1)$.

Clearly if v is in X, one of the stated conditions is valid. Now suppose that y is an even integer such that $\phi(y)=\phi(v)$, and let D denote the subset of $A-C$ consisting of all indices i in $A-C$ for which $f_i\mid y$. Let $d_i=a_i-1$ for i in D, $d_i=a_i$ for i in $(A-C)-D$, and $e=a-c+\sum_D k_i$ (where $f_i=2^{k_i}+1$). Let $w=2^e y\prod_{A-C} f_i^{d_i}$. Then $\phi(w)=\phi(u)$. If one of the stated conditions holds, $y\neq v$ implies that either y is divisible by some prime q such that $q\nmid u$, or u is divisible by a non-Fermat prime p such that $p\nmid y$. In either case $w\neq u$, contradicting the hypothesis that u is in X. Hence we have $y=v$ and v is in X.

(2.1) COROLLARY. *If* u *is in* X, *there is an element* v *of* X *such that* (i) $v\mid u$; (ii) $8\nmid v$, *and* v *is divisible by no Fermat prime other than* 3.

An element of X which satisfies condition (ii) of (2.1) will be called a reduced element of X, and the collection of all reduced elements will be denoted by $R(X)$. Clearly the structure of X is fairly well determined by that of $R(X)$, so henceforth we shall confine our attention to $R(X)$. If an element of X has no divisor in X, we shall call it irreducible, and shall denote the collection of all such elements by $I(X)$.

(3) THEOREM. *Let* $\bar{x}=\prod_B p_i^{b_i}$ *be in* $R(X)$, *where the* p_i*'s are distinct primes. For an integer* m, *let* $B(m)$ *denote the subset of* B *consisting of all indices* i *for which* $m\mid(p_i-1)$. *Let* $w=\prod_{B-B(m)} p_i^{b_i}$. *Then either* w *is in* $R(X)$ *or* $m\mid\phi(w)$.

Suppose $w\notin R(X)$. Then $w\notin X$, and there is an integer $y\neq w$ such that $\phi(y)=\phi(w)$. And if $(y,\ \bar{x}/w)=1$, $\phi(y\bar{x}/w)=\phi(\bar{x})$, contradicting the fact that $\bar{x}\in X$. So for some i in $B(m)$, we have $p_i\mid y$, whence $(p_i-1)\mid\phi(w)$. But $m\mid(p_i-1)$, so $m\mid\phi(w)$.

(3.1) COROLLARY. *If, in* (3), $\bar{x}\in I(X)$, m *is prime, and* $B(m)$ *is not empty, then* $m^2\mid\bar{x}$.

Since $B(m)$ is not empty, $w<\bar{x}$. But then, since $\bar{x}\in I(X)$, $w\notin X$. Hence $m\mid\phi(w)$, whence from the definition of w it is clear that $m^2\mid\bar{x}$.

(3.2) COROLLARY. If $\bar{x}\in I(X)$, p *is prime and* $p\mid\bar{x}$, *then* $p^2\mid\bar{x}$.

This follows from (1.1).

(3.3) COROLLARY. *If* $\bar{x}\in I(X)$, $\phi(\bar{x})$ *is divisible by no Fermat prime other than* 3.

This is an immediate consequence of (3.1). (3.1), (3.2), and (3.3) together eliminate 11, 23, 31, 41, 47, $\cdots$ as possible divisors of $\bar{x}$ or $\phi(\bar{x})$ if $\bar{x}\in I(X)$.

It would be of interest to know the relationship of $R(X)$ to $I(X)$, and of $I(X)$ to its smallest member.

We now apply (1.1) to show the following theorem.

(4) THEOREM. *If* $\bar{x}$ *is in* X, *then both* $\bar{x}$ *and* $\phi(\bar{x})$ *are greater than* 10^{400}.

We know $3^2|\bar{x}$, and shall consider three possibilities: (I) $3^3\nmid\bar{x}$; (II) $3^3|\bar{x}$ but $3^4\nmid\bar{x}$; (III) $3^4|\bar{x}$. Suppose that $\bar{x}=\prod p_i^{\alpha_i}$, the p_i's being distinct primes, and let $m=\prod p_i^{\alpha_i-1}$. In each case 3, 7, and 43 are divisors of m.

In case (I) any prime of the form $6k+1$ or $12k+1$, where $k|m$ and $(6, k)=1$, must be a divisor of m. Applying (1.1), we find the following prime divisors: 13, 79, 157, 547, 1093, 3319, 3613, 6163, 6637, 6709, 36979, 39829, 40507, 42667, 45949, 46957, 74419, 81013, 85333, 91813, 170509, 258847, 282253, 303493, 518083, 529933, 596779, 1041853, 1053157, 1573207, 1834639, 1854763, 1954869, 3623803, 3641917, 3669277, 3856147, 3944389, 6318943, 6772039, 6806893, 7161379, 7207243, 7372093.

In cases (II) and (III), m is divisible by each prime of the form $6k+1$ or $18k+1$, where k and m are as above. So in these cases m is divisible by 19, 127, 2287, 4903, 5419, 13723, 82339, 98299, 101347, 304039, 617761, 688087, 1676827, 3736087, 4130323, 4324363, 4693267.

In case (II) we also have as divisors primes of the form $36k+1$, and in case (III) of the form $54k+1$. This fact gives rise to additional divisors as follows:

Case (II): 37, 223, 1549, 4219, 4663, 4789, 9547, 10837, 25309, 27883, 29527, 176509, 196597, 197359, 200467, 399643, 494029, 544123, 545947, 1059517, 1063159, 1088467, 1184149, 1198927, 1203019, 1235419, 1564309, 2397853, 2407141, 3265399, 3702367, 7082029, 7221439, 7274053, 7619263, 8262367, 8387839, 8647927, 9139519.

Case (III): 379, 6823, 15919, 40939, 43207, 123499, 130483, 143263, 202627, 264763, 302443, 368443, 741043, 859699, 1857859, 2018383, 2053423, 2333467, 4446759, 5030479, 5480287.

The stated divisors were found with the aid of [2]. It is easy to find still more divisors by this method. Those obtained imply the following lower bounds for $\bar{x}$ and $\phi(\bar{x})$: (I)10^{458}; (II) 10^{586}; (III) 10^{400}.

REFERENCES

1. R. D. Carmichael, *Note on Euler's ϕ-function*, Bull. Amer. Math. Soc. vol. 28 (1922) pp. 109–110.
2. D. N. Lehmer, *List of prime numbers*, Carnegie Institution Publication, no. 165.

UNIVERSITY OF VIRGINIA

ON THE DARBOUX TANGENTS

V. G. GROVE

1. **Introduction.** In a recent paper [1][1] Abramescu gave a metrical characterization of the cubic curve obtained by equating to zero the terms of the expansion of a surface S at an ordinary point O_1, up to and including the terms of the third order. This cubic curve is rational and its inflexions lie on the three tangents of Darboux through O_1. In this paper we give a projective characterization of such a curve, and hence a new derivation of the tangents of Darboux. By using the method employed in this characterization to the curve of intersection of the tangent plane of the surface at O_1 with S, a simple characterization of the second edge of Green is found. Another application exhibits the correspondence of Moutard. Finally a new interpretation of the reciprocal of the projective normal is given in terms of the conditions of apolarity of a cubic form to a quartic form. The canonical tangent appears in a similar fashion.

Let S be referred to its asymptotic curves, and let the coordinates (x^1, x^2, x^3, x^4) of the generic point O_1 of S be normalized so that they satisfy the system [2] of differential equations

$$\begin{aligned} x_{uu} &= \theta_u x_u + \beta x_v + p x, \\ x_{vv} &= \gamma x_u + \theta_v x_v + q x, \qquad \theta = \log R. \end{aligned} \tag{1.1}$$

The line l_1 joining O_1 to O_4 ,whose coordinates are x^i_{uv}, is the R-conjugate line, and the line l_2 determined by O_2, O_3, whose respective coordinates are x^i_u, x^i_v, is the R-harmonic line.

If we define the local coordinates (x_1, x_2, x_3, x_4) with respect to

Presented to the Society, April 26, 1947; received by the editors April 11, 1947.

[1] Numbers in brackets refer to the references cited at the end of the paper.