MATHEMATICS OF COMPUTATION
VOLUME 64, NUMBER 211
JULY 1995, PAGES 1333–1336

ON A CONJECTURE OF CRANDALL CONCERNING THE $qx + 1$ PROBLEM

ZACHARY FRANCO AND CARL POMERANCE

ABSTRACT. R. E. Crandall has conjectured that for any odd integer $q > 3$, there is a positive integer m whose orbit in the "$qx + 1$ problem" does not contain 1. We show that this is true for almost all odd numbers q, in the sense of asymptotic density.

For positive odd numbers q and m, let $C_q(m)$ denote the largest odd factor of $qm + 1$. For $q = 3$, the sequence of iterates m, $C_3(m)$, $C_3(C_3(m))$, ... consists of the odd numbers in the orbit of m under the $3x + 1$ function. The (unproved) $3x + 1$ conjecture asserts that such an orbit always contains the number 1, cf. [3]. When $q > 3$, one might still consider the sequence of iterates m, $C_q(m)$, $C_q(C_q(m))$, ... Let $C_q^j(m)$ denote the j th iterate of C_q applied to m.

Definition 1. We say a positive odd integer q is a *Crandall number* if there is some positive odd integer m such that $C_q^j(m) \neq 1$ for every positive integer j.

Let $\mathscr{C}$ denote the set of Crandall numbers. In [1], Crandall conjectured that every odd number $q > 3$ is in $\mathscr{C}$ and showed that $\mathscr{C}$ contains 5, 181 and 1093. The proofs for 5 and 181 involve cycles: for $q = 5$, we have the cycle 13, 33, 83, 13, and for $q = 181$, we have the cycle 27, 611, 27. The proof for 1093 depends on the fact that it is a "Wieferich prime," that is, a prime p with $2^{p-1} - 1$ divisible by p^2. For an odd number q, let $\ell(q)$ denote the order of 2 mod q in the group $(\mathbb{Z}/(q\mathbb{Z}))^*$.

Definition 2. We say a positive odd integer q is a *Wieferich number* if q and $(2^{\ell(q)} - 1)/q$ are not relatively prime.

Note that Wieferich primes are Wieferich numbers and that prime Wieferich numbers are Wieferich primes, so there should be no confusion with the two definitions.

Wieferich primes are historically connected with Fermat's last theorem: if a prime p is *not* a Wieferich prime, all integer solutions to $x^p + y^p = z^p$ have $p|xyz$. It is conjectured that very few primes are Wieferich primes, but

Received by the editor February 1, 1994.
1991 *Mathematics Subject Classification.* Primary 11A99.
Key words and phrases. $3x + 1$ problem, $qx + 1$ problem, Wieferich prime.
This paper is based in part on the first author's Ph.D. dissertation at the University of California, Berkeley, 1990. The second author is supported in part by an NSF grant.

©1995 American Mathematical Society

that there are infinitely many. The only other Wieferich prime known is 3511, though they have been searched for up to $6 \cdot 10^9$ (see [5]).

As it turns out, there are quite a few Wieferich numbers. In this paper we shall first show, following Crandall's argument, that every Wieferich number is a Crandall number. We shall next show that asymptotically all odd numbers are Wieferich numbers, so that the set of numbers for which Crandall's conjecture is true has relative density 1 in the odd numbers.

In fact, for Wieferich numbers, a stronger version of Crandall's conjecture is true. Call an odd number q a "strong Crandall number" if the set of integers m for which $C_q^j(m) = 1$ for some j has asymptotic density zero. Our proof shows that every Wieferich number is a strong Crandall number, so that almost all odd numbers q are strong Crandall numbers.

Proposition 3. *Every Wieferich number is a Crandall number.*

Proof. If $C_q(m) = 1$, then clearly $m = (2^{k \cdot \ell(q)} - 1)/q$ for some positive integer k. Thus, if $C_q^2(m) = 1$, then

$$qm + 1 = 2^t(2^{k \cdot \ell(q)} - 1)/q$$

for some positive integers t and k. If q is a Wieferich number, then the right side above, being divisible by $(2^{\ell(q)} - 1)/q$, is not coprime to q. But the left side obviously is coprime to q, so that if q is a Wieferich number, then $C_q^2(m) = 1$ has no solutions m. It follows that if q is a Wieferich number, then $C_q^j(m) = 1$ forces $j = 1$ and $m = (2^{k \cdot \ell(q)} - 1)/q$ for some positive integer k. In particular, the set of such integers m has asymptotic density 0, so that q is a (strong) Crandall number.

Theorem 4. *The Wieferich numbers have relative density* 1 *in the odd numbers.*

Proof. For each number $B > 0$ let

$$\mathscr{W}(B) = \{q \text{ odd} : \text{there is some prime } p_0 \le B \text{ with } p_0 \| q\}.$$

By $p \| q$ we mean that p divides q, but p^2 does not divide q. It is easy to see that the asymptotic density of $\mathscr{W}(B)$ in the odd numbers is

$$d_B := 1 - \prod_{2 < p \le B} \left(1 - \frac{p-1}{p^2}\right),$$

where the product is over primes. Since the sum of the reciprocals of the primes diverges, d_B tends to 1 as B tends to infinity.

For p_0 a prime, let $\mathscr{P}(p_0)$ denote the set of primes $p \equiv 1 \bmod p_0$ with $2 \bmod p$ not a p_0 th power in $(\mathbb{Z}/(p\mathbb{Z}))^*$. The splitting field K of $x^{p_0} - 2$ has degree $p_0(p_0 - 1)$ over $\mathbb{Q}$. Thus, by the prime ideal theorem of Landau [4] (also see Marcus [6, Theorem 43]), the proportion of rational primes p which split completely in the ring of integers of K is $1/(p_0(p_0 - 1))$. These are the rational primes p for which $p \equiv 1 \bmod p_0$ and $2 \bmod p$ *is* a p_0 th power in $(\mathbb{Z}/(p\mathbb{Z}))^*$. By the same theorem applied to the splitting field of $x^{p_0} - 1$ (or by the prime number theorem for arithmetic progressions), the proportion of rational primes p for which $p \equiv 1 \bmod p_0$ is $1/(p_0 - 1)$. Thus, the relative density of $\mathscr{P}(p_0)$ in the rational primes is

$$1/(p_0 - 1) - 1/(p_0(p_0 - 1)) = 1/p_0.$$

This result on the relative density of $\mathscr{P}(p_0)$ is true in the strong sense of asymptotic density; that is, we take the proportion among all primes up to x of the members of $\mathscr{P}(p_0)$, and let $x \to \infty$. But we shall only need it in the weaker sense of polar or Dirichlet density, which essentially considers the ratio of the sum of the reciprocals of the members of $\mathscr{P}(p_0)$ up to x and the sum of the reciprocals of all of the primes up to x, and then lets $x \to \infty$. In particular, the sum of the reciprocals of the primes in $\mathscr{P}(p_0)$ diverges. Thus, the set of integers not divisible by any member of $\mathscr{P}(p_0)$ has asymptotic density zero. Indeed, the asymptotic density of the set of such numbers is at most $\prod_{p\in\mathscr{P}(p_0),\, p\le T}(1-1/p)$ for any T. But as T tends to infinity, this product tends to zero by the result on the sum of reciprocals of the members of $\mathscr{P}(p_0)$. Thus, the asymptotic density in the odd numbers of

$$\mathscr{W}^*(B) := \{q \in \mathscr{W}(B) : \text{ there are primes } p_0 \le B,\ p \in \mathscr{P}(p_0) \text{ with } p_0 \| q,\ p \mid q\}$$

is also d_B.

Note that $\mathscr{W}^*(B)$ is contained in the set of Wieferich numbers. Indeed, if $q \in \mathscr{W}^*(B)$, then there is some prime $p_0 \le B$ with $p_0 \| q$ and some prime $p \in \mathscr{P}(p_0)$ with $p \mid q$. We have $\ell(p_0) \mid \ell(q)$ and $\ell(p) \mid \ell(q)$. But since $p \in \mathscr{P}(p_0)$, we have $p_0 \mid \ell(p)$. Thus, $p_0\ell(p_0) \mid \ell(q)$. Note that $\ell(p_0^2) \mid p_0\ell(p_0)$. Thus, $p_0^2 \mid 2^{\ell(q)} - 1$, and since p_0^2 does not divide q, it follows that q is a Wieferich number as claimed.

It thus follows that the relative density of the Wieferich numbers in the odd numbers is at least d_B for any $B > 0$. But, as noted above, d_B tends to 1 as B tends to infinity, which proves the theorem.

Remarks. Our proof shows that for each fixed prime p_0, the set of odd numbers q with p_0 not dividing $\ell(q)$ has asymptotic density zero. By replacing the number field K in the proof with the splitting field of $(x^{p_0} - 2)(x^{p_0^a} - 1)$, one can show the density of the odd numbers q with p_0^a not dividing $\ell(q)$ is zero. As a corollary we have the following result of independent interest:

Theorem 5. *For each fixed positive integer n, the set of odd numbers q with $\ell(q)$ not a multiple of n has asymptotic density zero.*

If $r = C_q(m)$ for some m, then every positive odd number congruent to r mod q is also in the range of C_q. Thus, the range of C_q has an asymptotic density. In fact, this density (in the odd numbers) is $\ell(q)/q$. To see this, note that the odd number r is in the range of C_q if and only if $2^j r \equiv 1 \bmod q$ for some integer j, so that the residue classes in the range are precisely those in the subgroup of $(\mathbb{Z}/(q\mathbb{Z}))^*$ generated by 2 mod q. From [2, Theorem 2], it follows that there is a set $\mathscr{Q}$ of odd numbers of relative asymptotic density 1 such that $\ell(q)/q$ tends to zero as $q \in \mathscr{Q}$ tends to infinity. That is, for almost all odd numbers q, the density of the range of C_q tends to 0 as q tends to infinity.

The Crandall numbers 5 and 181, found by Crandall himself, are not Wieferich numbers. We do not know if there are infinitely many Crandall numbers that are not Wieferich numbers, or even if there are any more after 5 and 181.

We list below the Wieferich numbers below 1000:
21, 39, 57, 105, 111, 147, 155, 165, 171, 183, 195, 201, 203, 205, 219, 231, 237, 253, 273, 285, 291, 301, 305, 309, 327, 333, 355, 357, 385, 399, 417, 429,

453, 465, 483, 489, 495, 497, 505, 507, 525, 543, 555, 579, 597, 605, 609, 615, 627, 633, 651, 655, 657, 663, 689, 715, 723, 735, 737, 741, 755, 759, 777, 791, 813, 855, 861, 889, 897, 903, 905, 915, 921, 935, 939, 955, 969, 975, 979, 981, 987, 993.

Acknowledgment

We take this opportunity to thank Jeff Lagarias for his helpful comments and encouragement.

Bibliography

1. R. E. Crandall, *On the* $3x + 1$ *problem*, Math. Comp. **32** (1978), 1281–1292.
2. P. Erdős, C. Pomerance, and E. Schmutz, *Carmichael's lambda function*, Acta Arith. **58** (1991), 363–385.
3. J. C. Lagarias, *The* $3x + 1$ *problem and its generalizations*, Amer. Math. Monthly **92** (1985), 3–23.
4. E. Landau, *Einführung in die elementare und analytische Theorie der algebraischen Zahlen und der Ideale*, Chelsea Reprint, 1949.
5. D. H. Lehmer, *On Fermat's quotient, base two*, Math. Comp. **36** (1981), 289–290.
6. D. A. Marcus, *Number fields*, Springer-Verlag, New York, 1977.

Department of Mathematics, Texas A & M University, Kingsville, Texas 78363
E-mail address: zac@taiu.edu

Department of Mathematics, University of Georgia, Athens, Georgia 30602
E-mail address: carl@ada.math.uga.edu