

On the $1093N + 1$ Algorithm

S.J. Eigen and V.S. Prasad

The height function for the $1093N + 1$ algorithm is known to take only the two values $\{1, \infty\}$. We present a condition which implies this, and use it to find other examples.

1. Introduction. The notorious $3N + 1$ problem [2] is concerned with the orbits of positive integers, \mathbb{Z}^+ , under repeated iteration of the function

$$T(n) = \begin{cases} (3n + 1)/2 & \text{for } n \equiv 1 \pmod{2} \\ n/2 & \text{for } n \equiv 0 \pmod{2} \end{cases}$$

Since it is clear that every even integer eventually maps to an odd integer one often just examines the function on the positive odds \mathbb{D}^+ . This is a specific case of the $qN + r$ problem, for $q > 1$ and $r \geq 1$ positive odd integers. In particular, define

$$C_{q,r}(n) = \frac{qn + r}{2^{e_{q,r}(n)}}$$

where $e_{q,r}(n)$ is chosen so that the result is again an odd integer. Hence T corresponds to $C_{3,1}$ when restricted to the odds.

Define the **height** $h(n) = h_{q,r}(n) > 0$ of a positive odd integer n as the first iterate which reaches 1, i.e. $C_{q,r}^{h(n)}(n) = 1$. The height is infinite if the orbit never reaches 1. This means either the orbit goes off to infinity, or enters a cycle which does not contain 1. **Crandall's Conjecture (8.1)** says that except in the case $(q, r) = (3, 1)$ there is always an n with infinite height.

A small amount of information is known for this conjecture (see [1] section 8). One immediately obtains infinite heights for all cases with $r > 1$, since the integers in the orbit of $n = r$ are all multiples of r and so never reach 1. The cases $C_q = C_{q,1}$ are known to have integers with infinite height for $q = 5, 181, \text{ and } 1093$. On the other hand, very little else is known. For example, the orbit of 3 for $C_{7,1}$ has been calculated beyond 10^{2000} iterations without repetition [1].

The height function for $C_{1093} = C_{1093,1}$ on \mathbb{D}^+ is known to take only two values $\{1, \infty\}$ [1]. Crandall showed that C_3 has numbers of height n for all $n > 0$. (It is of course open whether the height function for C_3 takes the value ∞ .) This leads to the still open question: given any positive integer n does there exist an odd integer q so that the height function $h_{q,1}$ takes only the $n + 1$ values $\{1, 2, \dots, n, \infty\}$?

2. The Height Function

In this section, we will assume $r = 1$ and denote $C_q = C_{q,1}$ where $q > 1$ is odd. We begin with an elementary result.

(2.1) Proposition. For any q , there are always numbers of height 1 for C_q .

The proof follows from the following two observations:

(2.2) x is of height 1 if and only if for some n

$$x = \frac{2^n - 1}{q}$$

is an integer (which is then obviously odd).

(2.3) The numbers $\{2^1, 2^2, 2^3, \dots\} \text{ MOD } q$ form a cyclic subgroup of the multiplicative group $U(q) = \{0 < k < q : \text{GCD}(q, k) = 1\}$.

Hence there always exist infinitely many n so that the corresponding x 's are integers. Since at most one of them could again be 1, the proposition follows. \square

Denote by $a = a(q) > 0$, the first exponent so that $(2^a - 1)/q$ is an integer.

(2.4) Corollary. $x = (2^n - 1)/q$ is an integer, if and only if $n = ka, k > 0$ for $a = a(q)$, in which case

$$\frac{2^{ka} - 1}{q} = \frac{2^a - 1}{q} \left(2^{(k-1)a} + 2^{(k-2)a} + \dots + 1 \right) \quad (1)$$

i.e., $(2^a - 1)/q$ divides $(2^{ka} - 1)/q$ for all $k > 0$.

This approach gives a simple proof that C_{1093} has no positive odd integers of height 2 or higher. First we make the following observation.

(2.5) A number y is of height 2 if and only if

$$y = \frac{2^m \frac{2^n - 1}{q} - 1}{q} \quad (2)$$

is an integer. Notice, that if y is an integer then $(2^n - 1)/q$ must be an integer, and so $n = ka$ with $a = a(q)$ as before.

For $q = 1093$, we get $a = 364$. A straightforward calculation shows that $x = (2^{364} - 1)/1093$ is again divisible by 1093. But then $2^m x/1093 - 1/1093$ can never be an integer. Further, since $2^{364} - 1$ divides $2^{364k} - 1$ by (1), it follows that y of the form (2), is never an integer.

We extend this argument to obtain

(2.6) Theorem. Let $a = a(q)$ as above. Then there are no integers of height 2 if and only if $GCD(\frac{2^a - 1}{q}, q) > 1$.

Proof. Suppose $ps = (2^a - 1)/q$, where $q = pt$ for some $p > 1$. Then

$$\begin{aligned} \frac{2^b \frac{2^{ak} - 1}{q} - 1}{q} &= \frac{2^b(2^{a(k-1)} + 2^{a(k-2)} + \dots + 2^0) \frac{2^a - 1}{q} - 1}{q} \\ &= \frac{2^b(2^{a(k-1)} + 2^{a(k-2)} + \dots + 2^0)(ps) - 1}{pt} \\ &= \frac{1}{t} (2^b(2^{a(k-1)} + 2^{a(k-2)} + \dots + 2^0)s - \frac{1}{p}) \end{aligned}$$

which cannot be an integer.

Suppose $GCD(\frac{2^a - 1}{q}, q) = 1$. Now by assumption on the choice of a , $2^a \equiv 1 \pmod{q}$. Hence $2^{ka} \equiv 1 \pmod{q}$ for $k \geq 0$, and $\sum_{j=0}^{v-1} 2^{ja} \equiv v \pmod{q}$. Since $\frac{2^a - 1}{q}$ is relatively prime to q , $2^b \frac{2^a - 1}{q}$ is also relatively prime to q for each $b \geq 1$. Therefore, $2^b \frac{2^a - 1}{q}$ has a multiplicative inverse in $U(q)$. The sums, $\sum_{j=0}^{v-1} 2^{ja}$ as $v = 0, 1, 2, \dots$, run through all the equivalence classes modulo q . So for some v , depending on b

$$2^b \frac{2^{va} - 1}{q} \equiv 1 \pmod{q}$$

i.e.

$$\frac{2^b \frac{2^{va} - 1}{q} - 1}{q}$$

is an integer (which then must be odd). Furthermore, for any $r \geq 0$, $\sum_{j=0}^{v-1+rq} 2^{ja} \equiv \sum_{j=0}^{v-1} 2^{ja} \pmod{q}$, and so

$$\frac{2^b \frac{2^{v(a+rq)} - 1}{q} - 1}{q}$$

are all integers, and we again have infinitely many integers of height 2. \square

Examples This allows an easy method to find new examples of C_q with only the two heights $\{1, \infty\}$. We mention two. For $q = 21$ we have $a = 6$ and $(2^6 - 1)/21 = 3$. For $q = 39$, $a = 12$ and $(2^{12} - 1)/39 = 105$ yielding $GCD(105, 39) = 3$. The number $q = 1093$ is a prime and happens to be the first number such that $q \mid ((2^a - 1)/q)$ (see [3, 4] for related results).

3. Conclusion

There is an obvious way by which (2.6) can be extended. However, we point out that if $GCD(x, q) = 1$ this does not imply that there exists a $b > 0$ so that $y = (2^b x - 1)/q$ is an integer, i.e. $C_q(y) = x$. Consider $q = 7$ and $x = 5$ then $2^b 5 \pmod{7}$ cycles through $\{5, 3, 6\}$ and never hits 1. The problem is due to the fact that $\{2^k \pmod{7}\}$ is not all of $U(7)$. Without this obstacle, we obtain

(3.1) Proposition. If $\{2^k \pmod{q} : k = 1, 2, \dots\} = U(q)$, the group of integers relatively prime to q , then $GCD(x, q) = 1$ for x an odd integer implies there exists an integer $b > 0$ so that $y = (2^{b+a_k} x - 1)/q$ is an odd integer where $a = a(q)$ as in (2.1) and $k \geq 0$.

We conclude with a generalization of a result of Crandall's for the $3N + 1$ problem.

(3.2) Theorem Let q satisfy $GCD((2^a - 1)/q, q) = 1$ for $a = a(q)$ as in (2.1). If $\{2^k \pmod{q^2} : k \geq 1\} = U(q^2)$, then there are numbers of height n for every $n > 0$.

Proof. Put $A = a(q^2)$. So, $2^{Ak} \equiv 1 \pmod{q^2}$ for all $k \geq 0$. By assumption there exists $c > 0$ so that $2^{c+kA} \equiv 1 + q \pmod{q^2}$ for $k \geq 0$. Therefore, the odd integers $(2^{c+kA} - 1)/q$ are relatively prime to q .

We can then repeat this process inductively. Let x odd, be relatively prime to q . Then there is a $b > 0$ so that $2^{b+kA} x \equiv 1 + q \pmod{q^2}$. Hence the numbers $(2^{b+kA} x - 1)/q$ are again odd and relatively prime to q . \square

References

- [1] R.E. Crandall, *On the $3x + 1$ problem*, Math. Comp. 32 (1978), 1281-1292.
- [2] J. C. Lagarias, *The $3x + 1$ problem and its generalizations*, Amer. Math. Monthly 92 (1985) 3-23.
- [3] W. Meissner, *Über die Teilbarkeit von $2^p - 2$ durch das Quadrat der Primzahl $p = 1093$* , Sitzungsber. Akad. d. Wiss., Berlin (1913) 663-667.
- [4] P. Ribenboim, *1093*, Mathematical Intelligencer 5, (1983) 28-34.

Department of Mathematics
Northeastern University
Boston MA 02115
eigen@neu.edu

Department of Mathematics
University of Mass. Lowell
Lowell, MA 01854
prasadv@woods.uml.edu