On $2^r | 3^s - 1$ and $2^r - 1 | 3^s - 1$

Tomás Feder* Carlos Subi†

Abstract

We prove that if 2^r divides $3^s - 1$, and s is least for such an r, then $s = 2^t$ for some t. This implies that if $2^r = 3^s - 1$, then either $r = s = 1$, or $r = 3$ and $s = 2$.

We next prove that if $2^r - 1$ divides $3^s - 1$ for $r \geq 2$, then r is odd and s is even. This implies that $2^r - 1$ does not divide $3^r - 1$ unless $r = 1$.

We finally conclude with some remarks on Ulam's $3x + 1$ problem and generalizations.

1 Results and Proofs

Theorem 1 *If 2^r divides $3^s - 1$, and s is least for such an r, then $s = 2^t$ for some t.*

Proof. We have that 3^s is congruent to 1 modulo 2^r. There are $\phi(2^r) = 2^{r-1}$ numbers modulo 2^r that are relatively prime to 2^r, namely the odd numbers. These 2^{r-1} numbers modulo 2^r form a multiplicative group of order 2^{r-1} in which 3 has order s that divides 2^{r-1}, so $s = 2^t$ for some $t < r$. □

Corollary 1 *If $2^r = 3^s - 1$, then either $r = s = 1$, or $r = 3$ and $s = 2$.*

Proof. We have that $s = 2^t$ for some t by Theorem 1. For each $u \leq t$, we have that $(3^{2^u} - 1)(3^{2^u} + 1) = (3^{2^{u+1}} - 1)$, so $3^{2^u} - 1$ divides $3^{2^t} - 1 = 2^r$. In particular, if $r \geq 4$, then $t \geq 2$, and setting $u = 2$ gives that $3^4 - 1 = 80$ divides 2^r, a contradiction. □

We define Legendre's symbol $(\frac{a}{p})$, where p is an odd prime and a is any number not divisible by p, to be 1 if a is congruent to a square modulo p, and to be -1 is a is not congruent to a square modulo p. Gauss's law of reciprocity states the following (see [1], p. 76).

Lemma 1 *If p and q are odd primes, then $(\frac{p}{q}) = (\frac{q}{p})$, unless both p and q are of the form $4n + 3$, in which case $(\frac{p}{q}) = -(\frac{q}{p})$.*

Theorem 2 *If $2^r - 1$ divides $3^s - 1$ for $r \geq 2$, then r is odd and s is even.*

*268 Waverley Street, Palo Alto, CA 94301. Email: tomas@theory.stanford.edu
†Email: carlos.subi@hotmail.com

Proof. If r is even, then 2 divides r, so

$$2^r - 1 = (2^2 - 1)(1 + 2^2 + \cdots + 2^{r-2}),$$

therefore 3 divides $2^r - 1$, and 3 divides $3^s - 1$, a contradiction. Thus r is odd.

If s is odd, then since 3^s is congruent to 1 modulo $2^r - 1$, we have modulo every prime factor p of $2^r - 1$ that 3^s is congruent to 1. Therefore $\left(3^{(s+1)/2}\right)^2$ is congruent to 3 modulo p, and thus $(\frac{3}{p}) = 1$.

We have that $2^r - 1 = n = 4k - 1 = 3\ell + 1 = 12t - 5$. Note that $12t - 5 = 4k - 1$ must have a prime factor of the form $p = 4k' - 1$, and thus $p = 12t' - 1$ or $p = 12t' - 5$. If $p = 12t' - 5$, then $p = 4k' - 1 = 3\ell' + 1$, so $(\frac{3}{p}) = -(\frac{p}{3}) = -1$ by Lemma 1, a contradiction. If $p = 12t' - 1$, then $(12t - 5)/(12t' - 1) = 12u + 5$. This number in turn must have a prime factor of the form $p' = 3\ell'' - 1$, and thus $p' = 12u' - 1$ or $p' = 12u' + 5$. If $p' = 12u' + 5$, then $p' = 4k' + 1 = 3\ell' - 1$, so $(\frac{3}{p'}) = (\frac{p'}{3}) = -1$ by Lemma 1, a contradiction. If $p = 12u' - 1$, then $(12u + 5)/(12u' - 1) = 12t'' - 5$ and we are back to the first case, which follows by induction, that is, we eventually get a prime factor either $p = 12t' - 5$ or $p' = 12u' + 5$, which gives a contradiction by Lemma 1 as above. Thus s is even. □

Corollary 2 $2^r - 1$ *does not divide* $3^r - 1$ *unless* $r = 1$.

Proof. By Theorem 2, the number r would have to be both odd and even. □

In Ulam's $3x + 1$ problem, we start with an integer $x \geq 1$, replace x by $x/2$ if x is even, and replace x by $(3x + 1)/2$ if x is odd. We may repeat this step for ever until a number repeats or the numbers go to infinity. It has been conjectured that every number $x \geq 1$ eventually leads to the number 1 (although this could take a long time). This is a long standing open problem. Now consider a periodic sequence of steps $s = s_1 s_2 \cdots s_n$, where either $s_i = 0$ and the number considered is even, or $s_i = 1$ and the number considered is odd. Let m be the number of s_i out of n that are equal to one. Could this sequence start at some x and then return to x? Could this sequence start at some x and keep happening for ever to infinity?

Theorem 3 *No sequence s can repeat periodically to infinity, and a sequence s can start at x and return to x for at most one x.*

Proof. The sequence s starts at x and ends at $(3^m x + a)/2^n$ for some integer a. We write $x = y + b$ and $(3^m x + a)/2^n = (3^m/2^n)y + b$. Then

$$(3^m(y + b) + a)/2^n = (3^m/2^n)y + b$$

$$(1 - (3^m/2^n))b = a/2^n$$

$$b = a/(2^n - 3^m).$$

But then repeating this sequence r times will go from $y + b$ to $(3^{mr}/2^{nr})y + b$, which as r goes to infinity divides by a power of two larger than the power of two in the numerator of y, which since the denominator of b has no power of two, gives a fractional number, a contradiction. Thus s cannot repeat periodically to infinity. The only point $x = y + b$ that stays the same is $y = 0$, $x = b$, which may or may not occur. □

More generally, we may replace 3 and 2 by p and q in Ulam's problem, where $p > q \geq 2$ and p, q are relatively prime. So we start with $x \geq 1$, if x is divisible by q we replace x by x/q, and if not we replace x by $(px + c)/q$, where $1 \leq c < q$ is chosen so that the result is integer. This time the sequence $s = s_1 s_2 \cdots s_n$ has the s_i equal to the c value, where we take $c = 0$ in the case where x is divisible by q, and let m be the number of nonzero s_i. This time we go with the sequence s from $x = y + b$ to $(p^m x + a)/q^n = (p^m/q^n)y + b$, where $b = a/(q^n - p^m)$, and the theorem follows for this generalization as well.

Note that for $p = 4, q = 3$, we get the cycle $1, 2, 3, 1$, with $s = 2, 1, 0$, but also the cycle $7, 10, 14, 19, 26, 35, 47, 63, 21, 7$, with $s = 2, 2, 1, 2, 1, 1, 1, 0, 0$.

If we try the $3x + 1$ problem for $-x < 0$, it becomes the $3x - 1$ problem for $x > 0$. We get at least the cycles 1 for $s = 1$, the cycle $5, 7, 10, 5$ for $s = 1, 1, 0$, and $17, 25, 37, 55, 82, 41, 61, 91, 136, 68, 34, 17$ for $s = 1, 1, 1, 0, 1, 1, 1, 0, 0, 0$.

It is easy to show that for any x, the beginning sequence $s = s_1 s_2 \cdots s_k$ is uniquely determined by the value of x modulo q^k. This gives an easy alternative proof of the theorem for p, q.

References

[1] G.H. Hardy and E.M. Wright, An Introduction to the Theory of Numbers, Oxford Science Publications.