A 2-ADIC RIGIDITY THEOREM FOR COMPLEMENTARY DIVISORS OF MERSENNE NUMBERS

YUTO NIWA

Abstract. Let p be an odd prime and let $M_p = 2^p - 1$. We prove that if $M_p = DE$, where $D, E > 1$, and

$$D \equiv 1 \pmod{2^t}, \qquad E \equiv -1 \pmod{2^t}$$

for an integer $t > p/4$, then necessarily $(p, D, E) = (11, 89, 23)$. Thus, apart from the factorization $2^{11} - 1 = 89 \cdot 23$, a complementary divisor pair of a prime-index Mersenne number cannot lie simultaneously this deep in the residue classes 1 and -1 at the prime 2. The proof is elementary. After normalization, the factorization splits into two Diophantine branches. One branch is impossible by infinite descent; the other descends to a second-order Lucas-type recurrence, whose relevant power-of-two terms are classified by congruences and a doubling identity.

hexagon:2611.01272v1

1. Introduction

Write $M_n = 2^n - 1$ for the nth Mersenne number. The prime divisors and divisor statistics of Mersenne numbers have been investigated in, among other works, [1, 3, 5, 4, 2]. The present note concerns a local property of an arbitrary *complementary divisor pair*: a factorization $M_p = DE$ in which one factor is close to 1 and the other is close to -1 in the 2-adic metric.

Our main result is the following rigidity statement.

Theorem 1.1 (2-adic rigidity)**.** *Let p be an odd prime, and suppose that*

$$2^p - 1 = DE, \qquad D, E > 1.$$

If, for some integer $t > p/4$,

$$D \equiv 1 \pmod{2^t}, \qquad E \equiv -1 \pmod{2^t},$$

then

$$p = 11, \qquad D = 89, \qquad E = 23.$$

The condition is equivalently $t \geq \lfloor p/4 \rfloor + 1$. A useful valuation form follows immediately.

Corollary 1.2. *Let $p > 11$ be prime and let $2^p - 1 = DE$, where $D, E > 1$, $D \equiv 1 \pmod 8$, and $E \equiv -1 \pmod 8$. Then*

$$\nu_2(D - 1) = \nu_2(E + 1) \leq \left\lfloor \frac{p}{4} \right\rfloor.$$

Primality of the exponent is essential. Indeed, for every integer $\tau \geq 2$, putting $x = 2^\tau$ gives

$$2^{3\tau} - 1 = (x^2 + x + 1)(x - 1),$$

and the two factors are congruent to 1 and -1 modulo 2^τ, respectively. Here $\tau > (3\tau)/4$. This family also explains why the boundary case $p = 3\tau$ must be treated explicitly below.

The proof has three stages. First, the exact 2-adic depths of the two factors are shown to agree, and elementary size estimates force that depth into a narrow interval. Next, the normalized

Date: August 26, 2026.

2020 *Mathematics Subject Classification.* Primary 11A51; Secondary 11B39, 11D61.

Key words and phrases. Mersenne number, complementary divisors, 2-adic valuation, infinite descent, Lucas sequence.

factorization is reduced to two Diophantine systems, denoted N and P. Finally, the P-system is eliminated by infinite descent, while the N-system descends to a Lucas-type recurrence. Every step is included for completeness.

2. Normalization

We use $\nu_2(m)$ for the exponent of 2 in a nonzero integer m.

Lemma 2.1. *Under the hypotheses of Theorem 1.1,*

$$\nu_2(D-1) = \nu_2(E+1) =: \tau.$$

Moreover,

$$3\tau < p < 4\tau.$$

Proof. Write

$$D = 1 + 2^\alpha A_0, \qquad E = -1 + 2^\beta C_0,$$

where A_0 and C_0 are positive and odd. Expanding $DE + 1 = 2^p$ gives

$$2^p = -2^\alpha A_0 + 2^\beta C_0 + 2^{\alpha+\beta} A_0 C_0. \tag{1}$$

If $\alpha < \beta$, the right-hand side has 2-adic valuation exactly α, so $p = \alpha$. But then $D > 2^p$, whereas $D < DE = 2^p - 1$. This is impossible. The case $\beta < \alpha$ is symmetric. Hence $\alpha = \beta = \tau$.

Set $x = 2^\tau$ and write

$$D = xA + 1, \qquad E = xC - 1,$$

with A, C positive and odd. Since

$$2^p - 1 = DE \geq (x+1)(x-1) = x^2 - 1,$$

we have $p \geq 2\tau$. As p is odd, in fact $p > 2\tau$. Expanding the factorization now yields

$$x^2 AC + x(C - A) = 2^p.$$

Consequently $x \mid C - A$; write

$$C - A = jx.$$

After division by x^2 we obtain

$$AC + j = 2^{p-2\tau}. \tag{2}$$

Suppose first that $p < 3\tau$. Then the right-hand side of (2) is smaller than x. If $j > 0$, then $C = A + jx$ and $AC + j > x$. If $j = 0$, then $A = C$ and an odd square would equal a power of 2 greater than 1. If $j = -k < 0$, then $A = C + kx$ and

$$AC + j = C^2 + k(xC - 1) \geq x.$$

Each case is a contradiction.

It remains to exclude $p = 3\tau$. The same three cases show that equality in (2) can occur only when $j = -1$ and $C = 1$. Then $A = x + 1$ and

$$DE = (x^2 + x + 1)(x - 1) = x^3 - 1.$$

Since $p = 3\tau$ is prime, necessarily $(p, \tau) = (3, 1)$; but then $E = x - 1 = 1$, contrary to the hypotheses. Thus $p > 3\tau$. Finally, $\tau \geq t > p/4$ gives $p < 4\tau$. □

Define

$$H = 2^{p-3\tau}, \qquad y = 2^{4\tau-p}. \tag{3}$$

Lemma 2.1 implies

$$x = Hy, \qquad H \geq 2, \qquad y \geq 2, \qquad H < x, \tag{4}$$

and (2) becomes

$$AC + j = xH. \tag{5}$$

Both H and y are powers of 2.

3. Reduction to two Diophantine branches

Lemma 3.1. *There exist positive integers H, a, q, r such that q and r are odd and $\gcd(a, q) = 1$, and exactly one of the following systems holds:*

$$H = qr + a, \qquad r^2 = aHy + q; \tag{N}$$

$$H = qr + a, \qquad r^2 = aHy - q. \tag{P}$$

Proof. First we show that $A, C < x^2$. Since H is a proper power-of-two divisor of x, we have $H \le x/2$. If $A \ge x^2$, then

$$DE \ge (x^3 + 1)(x - 1) > \frac{x^4}{2} - 1 \ge x^3 H - 1 = 2^p - 1,$$

a contradiction. If $C \ge x^2$, the analogous estimate

$$DE \ge (x + 1)(x^3 - 1) > \frac{x^4}{2} - 1$$

gives the same contradiction.

Because $A \equiv C \pmod{x}$, there are integers r, s, u such that

$$A = r + sx, \qquad C = r + ux,$$

where $1 \le r < x$, r is odd, and $0 \le s, u < x$. Since $j = (C - A)/x = u - s$, substitution in (5) gives

$$r^2 + r(s + u)x + sux^2 + u - s = xH.$$

It follows that

$$a := \frac{r^2 + u - s}{x}$$

is an integer. The numerator is a multiple of x strictly between $-x$ and x^2, so $0 \le a < x$. Dividing the preceding identity by x yields

$$H = a + r(s + u) + sux. \tag{6}$$

Because $H < x$ and all terms on the right are nonnegative, $su = 0$. The case $s = u = 0$ would give $x \mid r^2$, impossible because x is even and r is odd.

If $u = 0$ and $s = q > 0$, then (6) and the definition of a give the N-system. If $s = 0$ and $u = q > 0$, they give the P-system. In either case q is odd, because x divides $r^2 - q$ or $r^2 + q$. Also $a > 0$: if $a = 0$, then $H = qr$ would be odd, contrary to $H \ge 2$ being a power of 2. Finally, every common divisor of a and q divides $H = a + qr$. Such a divisor is odd, while H is a power of 2; hence $\gcd(a, q) = 1$. □

4. Infinite descent

We first dispose of the P-branch. The following lemma is deliberately stated without a coprimality assumption; this makes the descent closed under iteration.

Lemma 4.1. *Let $y \ge 2$ be even and let q, r be positive odd integers. There are no positive integers H, a satisfying*

$$H = qr + a, \qquad r^2 = aHy - q.$$

Proof. Assume that a solution exists. Since $H = qr + a > r$, eliminating q gives

$$H(ayr - 1) = r^3 - a. \tag{7}$$

Comparison with $H > r$ gives

$$r^2(r - ay) + (r - a) > 0.$$

Because r is odd and ay is even, equality $r = ay$ is impossible. If $r < ay$, the left-hand side is at most $-r^2 + r - a < 0$. Therefore

$$r > ay. \tag{8}$$

In particular $r \geq 3$. From (7) we then obtain

$$H = \frac{r^3 - a}{ayr - 1} < \frac{r^3}{2r - 1} < r^2,$$

and hence

$$q = \frac{H - a}{r} < r. \tag{9}$$

Set

$$c = r - aqy.$$

A direct calculation using the P-system gives

$$cr = a^2y - q. \tag{10}$$

The integer c is odd. If $c \leq 0$, then $-c \geq 1$, and (10) together with (9) gives

$$r \leq (-c)r = q - a^2y < q < r,$$

a contradiction. Thus $c > 0$. If $c \geq a$, then (10) gives $r < ay$, contradicting (8). Consequently

$$0 < c < a. \tag{11}$$

Put $b = a - qc$. Substituting $r = aqy + c$ in (10) gives

$$c^2 = aby - q, \qquad a = qc + b. \tag{12}$$

The first identity shows that $b > 0$. If $b \geq c$, then

$$c^2 + q = aby \geq 2(q + 1)c^2 > c^2 + q,$$

which is impossible. Hence $0 < b < c$.

Equations (12) say that (a, c, b) is another P-solution: its variables (H, r, a) are replaced by (a, c, b), while q and y are unchanged. All required positivity and parity conditions are preserved, and the first component decreases because $a < H = qr + a$. Iteration would therefore produce an infinite strictly decreasing sequence of positive integers, a contradiction. □

We turn to the N-branch.

Lemma 4.2. *Let $y \geq 2$ be even and let q, r be positive odd integers. Suppose that positive integers H, a satisfy*

$$H = qr + a, \qquad r^2 = aHy + q, \qquad \gcd(a, q) = 1.$$

Then $q = 1$. Repeated descent terminates at

$$H = y + 2, \qquad r = y + 1, \qquad a = 1.$$

Proof. Set

$$c = r - aqy.$$

The N-system gives

$$cr = a^2y + q, \tag{13}$$

so $c > 0$. We claim that $c \le a$. If $c > a$, then

$$r = aqy + c > aqy + a,$$

whereas (13) gives

$$r = \frac{a^2y + q}{c} < ay + \frac{q}{a}.$$

Combining the two inequalities yields

$$a^2y(q-1) + a^2 < q. \tag{14}$$

For $q = 1$ this says $a^2 < 1$. For the remaining odd values $q \ge 3$, the left-hand side is at least $y(q-1) + 1 \ge 2q - 1 > q$. Thus (14) is always impossible.

If $c = a$, then (13) gives $q = a(r - ay)$. Coprimality forces $a = 1$. Now $c = r - qy = 1$ and $q = r - y$, so

$$(q-1)(y-1) = 0.$$

Since $y \ge 2$, we obtain $q = 1$, $r = y + 1$, and $H = y + 2$.

It remains to consider $0 < c < a$. Put $b = a - qc$. Substitution in (13) gives

$$c^2 = aby + q, \qquad a = qc + b. \tag{15}$$

We show that $b > 0$. If $b < 0$, set $e = -b = qc - a > 0$. Then

$$q - c^2 = aye > 0.$$

As $1 \le e \le qc - 1$, the elementary bound $e(qc - e) \ge qc - 1$ gives

$$q - c^2 = aye \ge 2(qc - 1).$$

But

$$2(qc - 1) - (q - c^2) = q(2c - 1) + c^2 - 2 > 0 :$$

for $c = 1$ this is $q - 1 > 0$ because $q > c^2$, and for $c \ge 3$ it is immediate. This is a contradiction. If $b = 0$, then $q = c^2$ and $a = qc$. Coprimality would force $q = c = a = 1$, contrary to $c < a$. Hence $b > 0$.

Since $c < a$ and $y \ge 2$, we have $ay > c$. The first identity in (15) therefore implies $b < c$. Moreover,

$$\gcd(b, q) = \gcd(a - qc, q) = 1.$$

Thus (a, c, b) is another N-solution with the same q and y, and its first component a is smaller than H. Repeated descent must eventually reach the case $c = a$, which, as shown above, forces $q = 1$ and gives the stated terminal solution. □

5. The terminal recurrence

It remains to determine which N-solutions with $q = 1$ can have H a power of 2.

Lemma 5.1. *Fix an even integer $y \ge 2$. Define*

$$\begin{pmatrix} H_0 \\ r_0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \qquad \begin{pmatrix} H_{m+1} \\ r_{m+1} \end{pmatrix} = \begin{pmatrix} y+1 & 1 \\ y & 1 \end{pmatrix} \begin{pmatrix} H_m \\ r_m \end{pmatrix}.$$

Every positive N-solution with $q = 1$ occurs uniquely among the pairs (H_m, r_m) with $m \ge 1$. In particular,

$$H_0 = 1, \qquad H_1 = y + 2, \qquad H_{m+2} = (y+2)H_{m+1} - H_m. \tag{16}$$

If y and some $H_m > 1$ are both powers of 2, then $y = 2$ and $m = 1$.

Proof. For $q = 1$, the inverse of the descent in Lemma 4.2 sends a smaller pair (H', r') to

$$r = yH' + r', \qquad H = (y+1)H' + r'.$$

The terminal solution $(y+2, y+1)$ is the image of $(1,1)$, so repeated inversion gives the displayed matrix recurrence. Conversely, the relation

$$r^2 - yH(H-r) = 1$$

is preserved by this transformation; hence every pair with $m \geq 1$ is an N-solution with $a = H_m - r_m > 0$. Lemma 4.2 proves that every positive N-solution descends uniquely to the terminal one, so the list is exhaustive and has no repetitions.

The matrix has trace $y+2$ and determinant 1, which gives the scalar recurrence (16). Modulo 2 it gives $H_{m+2} \equiv H_m$, so precisely the odd-indexed H_m are even. Thus, if $H_m > 1$ is a power of 2, then m is odd. Modulo $y+2$, the same recurrence gives $H_{m+2} \equiv -H_m$. Since $H_1 = y+2$, every odd-indexed term is divisible by $y+2$. Therefore $y+2$ is itself a power of 2. As y is a positive power of 2, this forces

$$y = 2. \tag{17}$$

For $y = 2$, let

$$U_0 = 0, \quad U_1 = 1, \quad U_{k+2} = 4U_{k+1} - U_k.$$

Then $H_m = U_{m+1}$. Define the companion sequence

$$V_0 = 2, \quad V_1 = 4, \quad V_{k+2} = 4V_{k+1} - V_k.$$

If λ and λ^{-1} are the roots of $X^2 - 4X + 1$, then

$$U_k = \frac{\lambda^k - \lambda^{-k}}{\lambda - \lambda^{-1}}, \qquad V_k = \lambda^k + \lambda^{-k}.$$

Consequently

$$U_{2k} = U_k V_k. \tag{18}$$

An induction in the recurrence modulo 8 gives

$$V_k \equiv \begin{cases} 2 & (k \equiv 0 \pmod 4), \\ 4 & (k \equiv 1 \pmod 4), \\ 6 & (k \equiv 2 \pmod 4), \\ 4 & (k \equiv 3 \pmod 4). \end{cases} \pmod 8.$$

Also $V_2 = 14$, and the positive sequence is strictly increasing from that point onward. Hence every V_k with $k \geq 2$ has an odd divisor greater than 1. By (18), U_{2k} cannot be a power of 2 for $k \geq 2$.

Finally, m is odd, so write $m + 1 = 2k$. The preceding paragraph forces $k = 1$, and therefore $m = 1$. □

6. Proofs of the main results

Proof of Theorem 1.1. Lemmas 2.1 and 3.1 reduce the factorization to the N-system or the P-system. Lemma 4.1 excludes the P-system. In the N-system, Lemma 4.2 gives $q = 1$, while Lemma 5.1, applied to the powers of two y and H, gives

$$y = 2, \qquad H = 4.$$

Since $x = Hy$, it follows that $x = 8$ and $\tau = 3$. The definition $H = 2^{p-3\tau}$ then gives $p = 11$.

The relevant N-solution is the terminal one:

$$r = y + 1 = 3, \qquad a = q = 1.$$

In the notation of Lemma 3.1, the N-branch arose from $u = 0$ and $s = q$, so

$$A = r + qx = 11, \qquad C = r = 3.$$

Therefore

$$D = xA + 1 = 89, \qquad E = xC - 1 = 23.$$

Conversely, $2^{11} - 1 = 89 \cdot 23$, with $89 \equiv 1 \pmod 8$ and $23 \equiv -1 \pmod 8$, so the exceptional case does satisfy the hypotheses. □

Proof of Corollary 1.2. The first part of Lemma 2.1 gives equality of the two valuations. If their common value were greater than $p/4$, then Theorem 1.1 would force $p = 11$. Since the common value is an integer, the stated bound follows. □

7. Concluding remarks

Theorem 1.1 applies to arbitrary complementary factors; neither factor is assumed prime, and no hypothesis is made on the number of prime factors of M_p. The exceptional factorization $2^{11} - 1 = 23 \cdot 89$ has a structural explanation in the proof: it corresponds to the first nontrivial term $H_1 = 4$ of the terminal Lucas-type recurrence, whereas every later relevant term has an odd divisor.

The theorem does not imply that there are infinitely many Mersenne primes. It only rules out one particularly deep form of simultaneous 2-adic cancellation in a composite prime-index Mersenne number.

Formal verification

The main theorem has been formalized in Lean 4.25.2 with mathlib v4.25.2. The proof of `MersenneRigidity.mersenne_rigidity` is available in the companion Lean formalization. The Lean proof was generated using ChatGPT.

Declarations

Competing interests. The author reports no competing interests.

Generative AI use. ChatGPT generated nearly all of the manuscript text, including the written proof. It was also used for proof exploration, bounded counterexample searches, and literature searches. The main theorem was separately checked by the Lean kernel. The human author is responsible for the manuscript, including the statement of the theorem, the exposition, and the references.

References

[1] J. Brillhart, On the factors of certain Mersenne numbers. II, *Math. Comp.* **18** (1964), 87–92. doi:10.1090/S0025-5718-1964-0159776-X

[2] A. Cambraia Jr., M. P. Knapp, A. Lemos, B. K. Moriya, and P. H. A. Rodrigues, On prime factors of Mersenne numbers, *Palestine J. Math.* **11** (2022), no. 2, 449–456. journal page

[3] J. R. Ehrman, The number of prime divisors of certain Mersenne numbers, *Math. Comp.* **21** (1967), 700–704. doi:10.1090/S0025-5718-1967-0223320-1

[4] P. Erdős, P. Kiss, and C. Pomerance, On prime divisors of Mersenne numbers, *Acta Arith.* **57** (1991), 267–281. doi:10.4064/aa-57-3-267-281

[5] S. S. Wagstaff, Jr., Divisors of Mersenne numbers, *Math. Comp.* **40** (1983), 385–397. doi:10.1090/S0025-5718-1983-0679454-X

Independent Researcher, Japan
Email address: yutoniwa0118@gmail.com