PAIRS WHERE $2^a - 2^b$ DIVIDES $n^a - n^b$ FOR ALL $n$

SUN QI AND ZHANG MINGZHI

ABSTRACT. Recently Selfridge asked for what $a$ and $b$ does $2^a - 2^b$ divide $n^a - n^b$ for all $n$? In this paper, the authors prove that there exist only fourteen such pairs $(a, b)$ when $0 \leq b < a$.

Selfridge [1] notices that

$$2^2 - 2^1|n^2 - n, \quad 2^2^2 - 2^2|n^2^2 - n^2, \quad 2^2^2^2 - 2^2^2|n^2^2^2 - n^2$$

for all integers $n$ and he asks for what $a$ and $b$

(1) $2^a - 2^b|n^a - n^b$

is true for all $n$?

In this paper we solve this problem completely, we prove

**THEOREM.** For $0 < b < a$, if and only if

$$(a, b) = (1, 0), (2, 1); \quad (3, 1), (4, 2), (5, 3); \quad (5, 1), (6, 2), (7, 3),$$

$$(8, 4); \quad (8, 2), (9, 3); \quad (14, 2), (15, 3), (16, 4).$$

(1) is true for all $n$.

We call the pair of numbers $(a, b)$ a solution of (1) if for this pair (1) is true for all $n$. Putting $n = 2^a - 1$, it is easy to verify that $(a, 0)$ is not a solution of (1) apart from the trivial solution $(1, 0)$ so we can suppose $1 \leq b < a$ and $a - b = c$.

**LEMMA 1.** Suppose $(a, b)$ is a solution of (1), then $2|c$ except $(a, b) = (2, 1)$.

**PROOF.** If $b > 2$, put $n = 3$, then $2^b|3^c - 1$, and $3^c \equiv 1 \pmod{4}$, so that $2|c$.

If $b = 1$ and $c$ is odd, $c > 1$, we have $2^c - 1 \equiv 7 \pmod{12}$ and $2^c - 1$ has a prime factor $p \not\equiv \pm 1 \pmod{12}$, then 3 is a quadratic nonresidue of $p$ and $p \equiv 3^c - 1$, therefore (1) is not true when $n = 3$. The proof is complete.

In what follows we consider only the case when $2|c$.

**LEMMA 2.** Suppose $2 < b < a$ and $2^a - 2^b = 2^b p_1^{a_1} p_2^{a_2} \ldots p_s^{a_s}$ where $p_i$ are distinct odd primes, then a necessary and sufficient condition for $(a, b)$ to be a solution of (1) is

(i) $2^{a-b}|c$;

(ii) $\varphi(p_i^{a_i})|c (i = 1, 2, \ldots, s)$, where $\varphi(t)$ is Euler’s function;

(iii) $b \geq \max_{1 \leq i \leq s}(\alpha_i)$.

**PROOF.** Suppose $(a, b)$ is a solution of (1), put $n = 5$, then $5^c \equiv 1 \pmod{2^b}$. Since the exponent to which 5 belongs $(\mod 2^b)$ is $2^{b-2}$, so that $2^{b-2}|c$.

---

Received by the editors July 15, 1983.

1980 Mathematics Subject Classification. Primary 10A10; Secondary 10A20.
Let $n$ be a primitive root of $p_i^{\alpha_i}$, since $p_i^{\alpha_i}|n^b(n^c - 1)$, and $n^c \equiv 1 \pmod{p_i^{\alpha_i}}$, so that $\varphi(p_i^{\alpha_i})|c$.

Put $n = p_i$, since $p_i^{\alpha_i}|p_i^b(p_i^c - 1)$, it follows that $b \geq \alpha_i$.

Conversely, suppose that conditions (i), (ii) and (iii) are satisfied and $n$ is an arbitrary integer.

If $2|\text{n}$, then $2^b|n^a - n^b$. If $2|\text{n}$, then, from (i), we have $n^c \equiv 1 \pmod{2^b}$ and $2^b|n^a - n^b$.

If $p_i|\text{n}$, then $p_i^{\alpha_i}|n^a - n^b$ from (iii). If $p_i|\text{n}$, then $n^c \equiv 1 \pmod{p_i^{\alpha_i}}$ and $p_i^{\alpha_i}|n^a - n^b$ from (ii). Hence, we have $2^b|n^a - n^b$ for arbitrary $n$. The proof is complete.

Similarly, we can prove

**Lemma 3.** For $b = 1, 2$, $(a, b)$ is a solution of (1) if and only if the conditions (ii), (iii) above are satisfied.

**Corollary.** Suppose $(a, b)$ is a solution of (1), $s$ is the number of distinct prime factors of $2^c - 1$, then

$$s \leq d(c/2)$$

where $d(k)$ is the number of divisors of $k$.

In fact, by $p_i - 1|\varphi(p_i^{\alpha_i})$ and the condition (ii) above, we obtain $(p_i - 1)/2|c/2$, so that $s$ can not exceed the number of divisors of $c/2$.

**Lemma 4.** If $8|\text{c}$, then $(a, b)$ is not a solution of (1).

**Proof.** Suppose $(a, b)$ is a solution of (1), but $c = 2^tu$, $t \geq 3$, $2|\text{u}$. Since $2^{2^tu} - 1 = (2^{2^t} - 1) \cdot f = f \cdot \prod_{i=1}^{t-1}(2^{2^i} + 1)$, where $f$ is an integer, and every prime factor $q$ of $2^{2^t+1} + 1$ is of the form $k \cdot 2^{t+1} + 1 [2]$, so we have $q|2^c - 1$. From Lemma 2 and Lemma 3 we get $\varphi(q)|c$, $2^{t+1}|2^tu$ which is impossible and this completes the proof.

**Lemma 5.** Suppose $c > 2$, if $c$ satisfies

$$2^{c/d(c/2)} > 3c/2$$

then $(a, b)$ is not a solution of (1).

**Proof.** We continue to use the notation in Lemma 2 and put $M = p_j^{\alpha_j} = \max_{1 \leq i \leq s}(p_i^{\alpha_i})$.

If $s = 1$, then $M = 2^c - 1$. Since $\varphi(M) = M \cdot (1 - 1/p_j) \geq 2M/3 > 2(2^c - 1)/3 > c$ when $c > 2$, and this contradicts (ii), so that $(a, b)$ is not a solution of (1) when $c > 2$ and $s = 1$.

If $s > 1$, then $M^s > 2^c - 1$. Since $M^s$ is odd, so $M^s > 2^c$. By inequality (2) we have $\varphi(M) \geq 2M/3 > 2/3 \cdot 2^{c/s} \geq 2/3 \cdot 2^{c/d(c/2)}$. If (3) is true, then $\varphi(M) > c$ which contradicts (ii). The proof is complete.

**Corollary.** Suppose $p$ is a prime and $p \geq 5$, then $(a, b)$ is not a solution of (1) when $c = 2p$.

In fact, in this case (3) can be reduced to $2^p > 3p$, and this is true for $p \geq 5$.

**Lemma 6.** For all positive integers $n$ we have

$$d(n) \leq \sqrt{3n}.$$
PROOF. Assume \( n = \prod_{i=1}^{r} q_i^{\beta_i} \) to be the standard decomposition of \( n \), then

\[
\frac{d(n)}{\sqrt{n}} = \prod_{i=1}^{r} \frac{\beta_i + 1}{q_i^{\beta_i/2}}.
\]

Put \( f(\beta) = (\beta + 1)/q^{\beta/2} \), by differentiation, it is easy to verify that \( f(\beta) \) is decreasing in the interval \([1, +\infty)\) if \( q > e \), and \( f(\beta) \) is decreasing in the interval \([2, +\infty)\) if \( q > e^{2/3} \), so that we have

\[
\frac{\beta_i + 1}{q_i^{\beta_i/2}} \leq \frac{2}{\sqrt{3}} \quad \text{for } q_i \geq 3,
\]

\[
\frac{\beta_i + 1}{q_i^{\beta_i/2}} \leq 1 \quad \text{for } q_i \geq 5,
\]

and \((\beta_i + 1)/2^{\beta_i/2} \leq 3/2\). Therefore \( d(n)/\sqrt{n} \leq 3/2 \cdot 2/\sqrt{3} = \sqrt{3} \).

The proof is complete.

By the way, the coefficient \( \sqrt{3} \) in (4) can not be reduced further, since the two sides of (4) are equal when \( n = 12 \).

PROOF OF THEOREM. From Lemma 6 we have \( 2^c/d(c/2) \geq 2\sqrt{2c/3} \). By Lemma 5, it follows that \((a, b)\) is not a solution of (1) when \( 2\sqrt{2c/3} > 3c/2 \). Put \( g(c) = 2\sqrt{2c/3} - 3c/2 \), by differentiation, it is easy to verify \( g(c) \geq g(66) > 0 \) for \( c \geq 66 \).

Hence \((a, b)\) is not a solution of (1) for \( c \geq 66 \). Therefore we need only to consider the cases when \( 2 \leq c \leq 64 \).

We can reject \( c = 64, 56, 48, 40, 32, 24, 16, 8 \) from Lemma 4 and \( c = 62, 58, 46, 38, 34, 26, 22, 14, 10 \) from Corollary of Lemma 5. By straightforward calculation, we have that (3) is true for \( c = 60, 54, 52, 50, 44, 42, 36, 30, 28, 20, 18 \) and all of them can be rejected.

Hence, there remain \( c = 12, 6, 4, 2 \). In these cases \( b \) can not exceed \( 4, 3, 4, 3 \) respectively. For \( c = 12 \) and \( b = 1 \), since \( 2^{12} - 1 = 3^2 \cdot 5 \cdot 7 \cdot 13 \), the condition (iii) in Lemma 3 is not satisfied, so that it can be rejected. Similarly, the case \( c = 6, b = 1 \) also can be rejected, since \( 2^6 - 1 = 3^2 \cdot 7 \). It is easy to verify that for the other twelve cases the conditions in Lemma 2 and Lemma 3 are satisfied, and \((a, b)\) are solutions of (1). Adding \((a, b) = (1, 0), (2, 1)\), we obtain all solutions of (1). The proof is complete.

The authors would like to thank Professor Ko Chao for his helpful suggestions.

REFERENCES