Mathematical Proceedings of the Cambridge Philosophical Society

VOL. 112 SEPTEMBER 1992 PART 2

Math. Proc. Camb. Phil. Soc. (1992), **112**, 225
Printed in Great Britain

On a problem in elementary number theory

BY A. SCHINZEL AND J. WÓJCIK
Mathematical Institute P.A.N., P.O. Box 137, 00-950 *Warsaw, Poland*

(*Received* 4 *November* 1991; *revised* 5 *December* 1991)

Let $\operatorname{ord}_q(a)$ be the exponent with which a prime q occurs in the factorization of a rational number $a \neq 0$ and, if $\operatorname{ord}_q(a) = 0$, let $M_q(a)$ be the multiplicative group generated by a modulo q. In the course of a group-theoretical investigation J. S. Wilson found he needed some results about integers a, b such that $M_q(a) = M_q(b)$, indeed also for algebraic integers, and he proved some of what he needed. J. W. S. Cassels observed that Wilson's argument naturally proved the existence of infinitely many primes q with $M_q(a) = M_q(b)$ for rational integers a, b with $ab > 0, |a| > 1, |b| > 1$. J. G. Thompson found a proof for the case of integers a, b with $ab < 0, |a| > 1, |b| > 1$. He also posed the problem for rational a, b (all this is unpublished). The aim of this paper is to prove that the answer to Thompson's question is affirmative. We also include the case $ab > 0$ settled by Thompson himself. We use the same technique devised by Wilson which has been elaborated by Cassels and Thompson. We thank Professor Cassels for the simplification of our original exposition and the referee for his suggestions.

THEOREM. *For all* $a, b \in \mathbb{Q} \setminus \{0, 1, -1\}$ *there exist infinitely many primes* q *such that* $M_q(a) = M_q(b)$.

Without loss of generality $a \neq b$. The strategy is first to find one prime q with

$$\operatorname{ord}_q a = \operatorname{ord}_q b = \operatorname{ord}_q (a-b) = 0 \quad \text{and} \quad M_q(a) = M_q(b).$$

This requires a fairly elaborate subdivision into cases. At the end, a uniform argument deduces the existence of infinitely many such q.

It is convenient to enunciate one key idea in the following trivial

PROPOSITION. *Let* q *be a prime. Suppose that* $\operatorname{ord}_q a = \operatorname{ord}_q b = 0$ *and that*

$$a^n \equiv b \bmod q$$

where n *is prime to* $q-1$. *Then* $M_q(a) = M_q(b)$.

In the argument, we shall most often take n to be prime. Given a, b we consider

https://doi.org/10.1017/S0305004100070912 Published online by Cambridge University Press

primes l in an appropriate arithmetic progression. A study of the factorization of a^l-b then shows that it must be divisible by some prime $q \not\equiv 1 \bmod l$.

Notation. For all primes p put

$$\alpha_p = \operatorname{ord}_p a, \quad \beta_p = \operatorname{ord}_p b, \quad \gamma_p = \operatorname{ord}_p (a-b)$$

and further put

$$P = \prod_{\alpha_p - \beta_p = 0} p^{\gamma_p}, \quad P_1 = \prod_{p \mid P} (p-1).$$

LEMMA 1. *If either* $ab > 0$, $|a| \neq 1$, $|b| \neq 1$ *or for some prime* p_0 *we have* $\alpha_{p_0}\beta_{p_0} > 0$ *and* $\alpha_{p_0}, \beta_{p_0}, \gamma_{p_0}$ *not all equal, then there exists a prime* q *such that* $\alpha_q = \beta_q = \gamma_q = 0$ *and* $M_q(a) = M_q(b)$.

Proof. Replacing if necessary a by a^{-1} and b by b^{-1}, we may assume without loss of generality

$$1 < |a| < |b| \quad \text{if } ab > 0, \tag{1}$$

$$0 < \alpha_{p_0} \leqslant \beta_{p_0} \quad \text{if } ab < 0. \tag{2}$$

Let l be a sufficiently large prime such that

$$l \equiv 1 \bmod p^{\gamma_p}(p-1) \quad \text{for all } p \mid P.$$

Then

$$a^l \equiv a \bmod p^{\gamma_p+1},$$

so that

$$\operatorname{ord}_p (a^l-b) = \gamma_p \quad \text{for all } p \mid P.$$

On the other hand for all primes p with $\alpha_p\beta_p > 0$ we have since l is large

$$\operatorname{ord}_p (a^l-b) = \begin{cases} l\alpha_p & \text{if } \alpha_p < 0, \\ \beta_p & \text{if } \alpha_p > 0 \end{cases} \tag{3}$$

and for all primes p with $\alpha_p\beta_p \leqslant 0$ the same is true in an obvious way. Finally if $\alpha_p = 0$, $\beta_p \neq 0$ we have

$$\operatorname{ord}_p (a^l-b) = \min\{0, \beta_p\}. \tag{4}$$

Hence

$$a^l-b = \operatorname{sgn} a \,.\, P \prod_{\alpha_p<0} p^{l\alpha_p} \prod_{\substack{\alpha_p=0 \\ \beta_p \neq 0}} p^{\min\{0,\beta_p\}} \prod_{\alpha_p>0} p^{\beta_p} s,$$

where s is an integer prime to the numerator and the denominator of $a, b, a-b$ and positive by (1). We have

$$a^l-b \equiv a-b \bmod l, \quad \prod_{\alpha_p<0} p^{l\alpha_p} \equiv \prod_{\alpha_p<0} p^{\alpha_p} \bmod l \tag{5}$$

and if $s \equiv 1 \bmod l$

$$\operatorname{sgn} a \,.\, P \prod_{\alpha_p<0} p^{\alpha_p} \prod_{\substack{\alpha_p=0 \\ \beta_p \neq 0}} p^{\min\{0,\beta_p\}} \prod_{\alpha_p>0} p^{\beta_p} \equiv a-b \bmod l.$$

For l large enough it follows that

$$\operatorname{sgn} a \,.\, P \prod_{\alpha_p<0} p^{\alpha_p} \prod_{\substack{\alpha_p=0 \\ \beta_p \neq 0}} p^{\min\{0,\beta_p\}} \prod_{\alpha_p>0} p^{\beta_p} = a-b,$$

and hence

$$\operatorname{sgn} a = \operatorname{sgn}(a-b), \alpha_p > 0 \quad \text{implies} \quad \gamma_p = \beta_p, \quad \alpha_p \geqslant \beta_p. \tag{6}$$

https://doi.org/10.1017/S0305004100070912 Published online by Cambridge University Press

By (1) and (6), $ab < 0$, so by (2), $\alpha_{p_0} = \beta_{p_0} = \gamma_{p_0}$ contrary to the assumption. Hence $s \not\equiv 1 \bmod l$ and s has a prime factor $q \not\equiv 1 \bmod l$, $\alpha_q = \beta_q = \gamma_q = 0$. By the Proposition with $n = l$ we have $M_q(a) = M_q(b)$.

LEMMA 2. *Let $ab < 0$. If for a prime $p_0 | P$ there exists an integer $r > 0$ prime to the exponent $\lambda(a)$ or $\lambda(b)$ to which a or b, respectively belongs* $\bmod p_0^{\gamma_{p_0}+1}$ *and such that*

$$\operatorname{ord}_{p_0}(a^r - b) \neq \gamma_{p_0} \quad \text{or} \quad \operatorname{ord}_{p_0}(b^r - a) \neq \gamma_{p_0},$$

respectively, then there exists a prime q such that $\alpha_q = \beta_q = \gamma_q = 0$ and $M_q(a) = M_q(b)$.

Proof. Assume without loss of generality that $(r, \lambda(a)) = 1$ and

$$\operatorname{ord}_{p_0}(a^r - b) \neq \gamma_{p_0}.$$

We choose a positive integer r_0 prime to PP_1 in the arithmetic progression $\lambda(a)x + r$. Let

$$\operatorname{ord}_p(a^{r_0} - b) = e_p \quad \text{for all } p | P.$$

Let l be a sufficiently large prime in the arithmetic progression

$$\prod_{p|P} p^{e_p} P_1 x + r_0.$$

We have $$a^l \equiv a^{r_0} \bmod p^{e_p+1} \quad \text{for all } p | P,$$

and hence $$\operatorname{ord}_p(a^l - b) = e_p \quad \text{for all } p | P.$$

Since l is large we again have (3) and (4). Hence

$$a^l - b = \operatorname{sgn} a \prod_{p|P} p^{e_p} \prod_{\alpha_p < 0} p^{l\alpha_p} \prod_{\substack{\alpha_p = 0 \\ \beta_p \neq 0}} p^{\min\{0, \beta_p\}} \prod_{\alpha_p > 0} p^{\beta_p} s,$$

where s is an integer prime to the numerator and the denominator of $a, b, a-b$ and is positive since $ab < 0$. We again have (5) and if $s \equiv 1 \bmod l$ we would have

$$\operatorname{sgn} a \prod_{p|P} p^{e_p} \prod_{\alpha_p < 0} p^{\alpha_p} \prod_{\substack{\alpha_p = 0 \\ \beta_p \neq 0}} p^{\min\{0, \beta_p\}} \prod_{\alpha_p > 0} p^{\beta_p} \equiv a - b \bmod l.$$

For l large enough both sides of the congruence are equal, so

$$\gamma_{p_0} = e_{p_0} = \operatorname{ord}_{p_0}(a^{r_0} - b).$$

However $r_0 \equiv r \bmod \lambda(a)$, $a^{r_0} \equiv a^r \bmod p_0^{\gamma_{p_0}+1}$ and so

$$\gamma_{p_0} = \operatorname{ord}_{p_0}(a^r - b),$$

contrary to the assumption. Hence $s \not\equiv 1 \bmod l$ and s has a prime factor $q \not\equiv 1 \bmod l$, $\alpha_q = \beta_q = \gamma_q = 0$. By the Proposition with $n = l$ we have $M_q(a) = M_q(b)$.

LEMMA 3. *If for a prime $p_0 | P$ we have*

$$\gamma_{p_0} > \min\{\operatorname{ord}_{p_0}(a^2 - 1), \operatorname{ord}_{p_0}(b^2 - 1)\},$$

then p_0 satisfies the assumptions of Lemma 2.

Proof. Without loss of generality we may assume that

$$\gamma_{p_0} > \operatorname{ord}_{p_0}(a^2 - 1).$$

https://doi.org/10.1017/S0305004100070912 Published online by Cambridge University Press

Let λ_0 be the exponent to which a belongs mod $p_0^{\gamma_{p_0}}$. Clearly $\lambda_0 > 2$, hence there exists an $r_0 \not\equiv 1 \bmod \lambda_0$ such that $(r_0, \lambda_0) = 1$. The arithmetic progression $\lambda_0 x + r_0$ contains a positive integer r prime to $\lambda(a)$ and we have

$$\operatorname{ord}_{p_0}(a^r - a^{r_0}) = \operatorname{ord}_{p_0}(a^{r-r_0} - 1) \geqslant \gamma_{p_0},$$

$$\operatorname{ord}_{p_0}(a^{r_0} - a) = \operatorname{ord}_{p_0}(a^{r_0-1} - 1) < \gamma_{p_0},$$

$$\operatorname{ord}_{p_0}(a^r - b) = \operatorname{ord}_{p_0}(a^r - a^{r_0} + a^{r_0} - a + a - b) < \gamma_{p_0}.$$

LEMMA 4. *If for a prime $p_0 | P$ we have*

$$\gamma_{p_0} = \operatorname{ord}_{p_0}(a^2 - 1) = \operatorname{ord}_{p_0}(b^2 - 1) \tag{7}$$

then p_0 satisfies the assumptions of Lemma 2.

Proof. The condition (7) implies

$$a = \epsilon + p_0^{\mu} a_1, \quad b = \epsilon + p_0^{\mu} b_1, \quad \text{where } \epsilon = \pm 1,\ a_1, b_1 \in \mathbb{Q}, \tag{8}$$

$$\operatorname{ord}_{p_0} a_1 = \operatorname{ord}_{p_0} b_1 = 0, \tag{9}$$

$$\mu = \begin{cases} \gamma_{p_0} - 1 & \text{if } p_0 = 2, \\ \gamma_{p_0} & \text{if } p > 2. \end{cases} \tag{10}$$

We choose a positive integer r such that

$$\left.\begin{array}{ll} a_1 r \equiv b_1 \bmod 4 & \text{if } p_0 = 2, \\ a_1 r \equiv b_1 \bmod p_0 & \text{if } p_0 > 2 \end{array}\right\} \tag{11}$$

and

$$(r, p_0(p_0 - 1)) = 1. \tag{12}$$

This is possible in view of (9). Now (8), (10) and (11) imply

$$\operatorname{ord}_{p_0}(a^r - b) \geqslant \gamma_{p_0} + 1,$$

while (12) implies $(r, \lambda(a)) = 1$.

LEMMA 5. *For all $a, b \in \mathbb{Q} \setminus \{0, 1, -1\}$, there exists a prime q such that $\alpha_q = \beta_q = \gamma_q = 0$ and $M_q(a) = M_q(b)$.*

Proof. In view of Lemmas 1–4 it suffices to consider the case where $ab < 0$ and for all primes p

$$\text{either} \quad \alpha_p \beta_p \leqslant 0 \quad \text{or} \quad \alpha_p = \beta_p = \gamma_p, \tag{13}$$

for all $p | P$,

$$\gamma_p \leqslant \min\{\operatorname{ord}_p(a^2 - 1), \operatorname{ord}_p(b^2 - 1)\} \tag{14}$$

and

$$\gamma_p < \max\{\operatorname{ord}_p(a^2 - 1), \operatorname{ord}_p(b^2 - 1)\}. \tag{15}$$

The last two conditions can be reformulated. If $p = 2$,

$$\gamma_2 < \operatorname{ord}_2(a^2 - b^2) = \operatorname{ord}_2((a^2 - 1) - (b^2 - 1)),$$

and so (15) implies

$$\gamma_2 < \min\{\operatorname{ord}_2(a^2 - 1), \operatorname{ord}_2(b^2 - 1)\}, \tag{16}$$

https://doi.org/10.1017/S0305004100070912 Published online by Cambridge University Press

which is stronger than (14). If $p > 2$,

$$\gamma_p = \operatorname{ord}_p(a^2-b^2) \geqslant \min\{\operatorname{ord}_p(a^2-1), \operatorname{ord}_p(b^2-1)\},$$

hence (14) and (15) are equivalent to (16) and

$$\min\{\operatorname{ord}_p(a^2-1), \operatorname{ord}_p(b^2-1)\} = \gamma_p < \max\{\operatorname{ord}_p(a^2-1), \operatorname{ord}_p(b^2-1)\} \quad (p \neq 2). \tag{17}$$

Note that (16) and (17) are invariant under the replacement of $\langle a, b\rangle$ by $\langle a^{-1}, b^{-1}\rangle$.

Assume first that for a prime $l \nmid P$

$$\alpha_l = \beta_l = \gamma_l \neq 0.$$

Replacing if necessary $\langle a, b\rangle$ by $\langle a^{-1}, b^{-1}\rangle$ we may suppose that

$$\alpha_l = \beta_l = \gamma_l > 0.$$

Hence $l > 2$. For every p with $|\alpha_p| + |\beta_p| > 0$, $\alpha_p \beta_p \leqslant 0$ we have

$$\operatorname{ord}_p(a^l-b) = \begin{cases} l\alpha_p & \text{if } \alpha_p < 0, \\ \min\{0, \beta_p\} & \text{if } \alpha_p = 0, \\ \beta_p = \gamma_p & \text{if } \alpha_p > 0. \end{cases}$$

The same is true by virtue of (13) if $\alpha_p \beta_p > 0$.

For $p \mid P$, if $p = 2$ or $p > 2$, $\operatorname{ord}_p(a^2-1) > \gamma_p$ we have

$$\operatorname{ord}_p(a^l-a) > \gamma_p, \quad \operatorname{ord}_p(a^l-b) = \operatorname{ord}_p(a^l-a+a-b) = \gamma_p;$$

if $p > 2$, $\operatorname{ord}_p(a^2-1) = \gamma_p < \operatorname{ord}_p(b^2-1)$ we have

$$\operatorname{ord}_p(a^{2l}-1) = \gamma_p,$$

$$\operatorname{ord}_p(a^l-b) = \operatorname{ord}_p(a^{2l}-b^2) = \operatorname{ord}_p(a^{2l}-1-(b^2-1)) = \gamma_p.$$

Therefore

$$a^l-b = \prod_{\alpha_p<0} p^{(l-1)\alpha_p}(a-b)\, s,$$

where s is a positive integer prime to the numerator and the denominator of $a, b, a-b$. Here $p^{l-1} \equiv 1 \bmod l$. If also $s \equiv 1 \bmod l$ we would have

$$a-b \equiv (a-b)\, s \prod_{\alpha_p<0} p^{(l-1)\alpha_p} = a^l-b \equiv -b \bmod l^{\alpha_l+1}, \quad a \equiv 0 \bmod l^{\alpha_l+1},$$

a contradiction.

Hence $s \not\equiv 1 \bmod l$ and s has a prime factor $q \not\equiv 1 \bmod l$, $\alpha_q = \beta_q = \gamma_q = 0$. By the Proposition with $n = l$ we have $M_q(a) = M_q(b)$.

Therefore we may assume that

$$\alpha_p \beta_p \leqslant 0 \quad \text{for all primes } p. \tag{18}$$

Let

$$a = \frac{A_1}{A_2}, \quad b = \frac{B_1}{B_2},$$

where

$$A_i, B_i \in \mathbb{Z}, \quad A_1 B_1 < 0, \quad A_2 > 0, \quad B_2 > 0,$$

$$(A_1, A_2) = (B_1, B_2) = 1.$$

https://doi.org/10.1017/S0305004100070912 Published online by Cambridge University Press

By (18), $(A_i, B_i) = 1$ $(i = 1, 2)$ and we have

$$P = |A_1 B_2 - A_2 B_1| \geqslant 2.$$

If P is odd, it has an odd prime factor l. If P is even we have by (16)

$$a \equiv b \equiv \epsilon \bmod 2^{\gamma_2}, \quad \epsilon = \pm 1,$$

hence
$$A_1 = \epsilon A_2 + 2^{\gamma_2} A_3, \quad B_1 = \epsilon B_2 + 2^{\gamma_2} B_3, \quad A_3, B_3 \in \mathbb{Z} \setminus \{0\} \tag{19}$$

and
$$P = 2^{\gamma_2} |A_3 B_2 - A_2 B_3| = 2^{\gamma_2} |A_3 B_1 - A_1 B_3|.$$

Since $A_1 B_1 < 0 < A_2 B_2$ it follows that $P > 2^{\gamma_2}$, so P has an odd prime factor l. By (17) and since $|a| \neq 1$, $|b| \neq 1$ we may assume without loss of generality that

$$a = \epsilon + l^{\mu} a_1, \quad b = \epsilon + l^{\nu} b_1,$$

where
$$\epsilon = \pm 1, \quad a_1, b_1 \in \mathbb{Q}, \quad \operatorname{ord}_l a_1 = \operatorname{ord}_l b_1 = 0, \quad \mu = \gamma_l < \nu.$$

Clearly
$$a - b \equiv l^{\gamma_l} a_1 \bmod l^{\gamma_l + 1}. \tag{20}$$

Consider now the number $a^{l^{n-\mu}} - b$ (where $n \geqslant \mu$).

For every prime p with $|\alpha_p| + |\beta_p| > 0$ we have by (18)

$$\operatorname{ord}_p (a^{l^{n-\mu}} - b) = \begin{cases} l^{n-\mu} \alpha_p & \text{if } \alpha_p < 0, \\ \min\{0, \beta_p\} & \text{if } \alpha_p = 0, \\ \beta_p & \text{if } \alpha_p > 0. \end{cases}$$

For every $p \mid P$ with $p \neq l$, if $p = 2$ or $p > 2$, $\operatorname{ord}_p (a^2 - 1) > \gamma_p$, we have

$$\operatorname{ord}_p (a^{l^{n-\mu}} - a) > \gamma_p, \quad \operatorname{ord}_p (a^{l^{n-\mu}} - b) = \operatorname{ord}_p (a^{l^{n-\mu}} - a + a - b) = \gamma_p;$$

if $p > 2$, $\operatorname{ord}_p (a^2 - 1) = \gamma_p < \operatorname{ord}_p (b^2 - 1)$ we have

$$\operatorname{ord}_p (a^{2l^{n-\mu}} - 1) = \gamma_p,$$

$$\operatorname{ord}_p (a^{l^{n-\mu}} - b) = \operatorname{ord}_p (a^{2l^{n-\mu}} - b^2) = \operatorname{ord}_p (a^{2l^{n-\mu}} - 1 - (b^2 - 1)) = \gamma_p.$$

Finally we obtain by induction on $n \geqslant \mu$

$$a^{l^{n-\mu}} \equiv \epsilon + l^n a_1 \bmod l^{n+1},$$

hence
$$a^{l^{\nu-\mu}} - b \equiv l^{\nu} (a_1 - b_1) \bmod l^{\nu+1}, \tag{21}$$

$$a^{l^{\nu-\mu+1}} - b \equiv -l^{\nu} b_1 \bmod l^{\nu+1}. \tag{22}$$

If $a_1 \not\equiv b_1 \bmod l$ we obtain

$$a^{l^{\nu-\mu}} - b = \prod_{\alpha_p < 0} p^{(l^{\nu-\mu}-1)\alpha_p} l^{\nu-\mu} (a - b)\, s,$$

where s is a positive integer prime to the numerators and the denominators of a, b, $a - b$. If $s \equiv 1 \bmod l$ we obtain from (20) and (21)

$$a_1 l^{\nu} \equiv (a - b)\, l^{\nu-\mu} s = (a^{l^{\nu-\mu}} - b) \prod_{\alpha_p < 0} p^{-(l^{\nu-\mu}-1)\alpha_p}$$

$$\equiv l^{\nu} (a_1 - b_1) \bmod l^{\nu+1}, \quad b_1 \equiv 0 \bmod l,$$

https://doi.org/10.1017/S0305004100070912 Published online by Cambridge University Press

a contradiction. Hence $s \not\equiv 1 \bmod l$ and s has a prime factor $q \not\equiv 1 \bmod l$ with $\alpha_q = \beta_q = \gamma_q = 0$. By the Proposition with $n = l^{\nu-\mu}$ we have $M_q(a) = M_q(b)$.

If $a_1 \equiv b_1 \bmod l$ we obtain

$$a^{l^{\nu-\mu+1}} - b = \prod_{\alpha_p < 0} p^{(l^{\nu-\mu+1}-1)\alpha_p} l^{\nu-\mu}(a-b)\, s,$$

with s as above. If $s \equiv 1 \bmod l$ we obtain from (20) and (22)

$$a_1 l^{\nu} \equiv (a-b)\, l^{\nu-\mu} s = (a^{l^{\nu-\mu+1}} - b) \prod_{\alpha_p < 0} p^{-(l^{\nu-\mu+1}-1)\alpha_p} \equiv -l^{\nu} b_1 \bmod l^{\nu+1},$$

and hence $a_1 \equiv -b_1 \bmod l$, $2a_1 \equiv 0 \bmod l$, a contradiction. Thus $s \not\equiv 1 \bmod l$ and by the Proposition with $n = l^{\nu-\mu+1}$, s has a prime factor q with the desired property.

Proof of the Theorem. Replacing a by a^{-1}, or b by b^{-1}, if necessary we may assume that

$$|a| > \max\{1, |b|\}. \tag{23}$$

We shall construct inductively an infinite sequence of distinct primes $q_1, q_2, \ldots$ such that

$$M_{q_k}(a) = M_{q_k}(b), \quad \alpha_{q_k} = \beta_{q_k} = \gamma_{q_k} = 0 \quad (k = 1, 2, \ldots)$$

and three infinite sequences of positive integers a_k, b_k and c_k such that $(a_k, b_k) = 1$ and for every integer $t \geqslant 0$

$$a^{a_k t + b_k} - b = \operatorname{sgn} a \prod_{\alpha_p < 0} p^{(a_k t + b_k)\alpha_p} \prod_{\substack{\alpha_p = 0 \\ \beta_p \neq 0}} p^{\min\{0, \beta_p\}} \prod_{\alpha_p > 0} p^{\beta_p} \prod_{p \mid P} p^{e_p} \prod_{i=1}^{k} q_i^{c_i} s, \tag{24}$$

where s is a positive integer prime to $q_1 q_2 \ldots q_k$ and to the numerators and the denominators of $a, b, a-b$. Here e_p are non-negative integers independent of k and t. For $k = 1$ we take $q_1 = q$, where q is a prime, the existence of which is asserted in Lemma 5. By that Lemma, $M_q(a) = M_q(b)$, hence $b \equiv a^r (\bmod q)$, $(r, \lambda) = 1$, where λ is the exponent to which a belongs mod q. We choose a positive integer b_1 such that

$$b_1 > \max_{\alpha_p \neq 0} \beta_p / \alpha_p, \quad b_1 \equiv r \bmod \lambda, \quad (b_1, 2qPP_1) = 1 \tag{25}$$

and put

$$\operatorname{ord}_p (a^{b_1} - b) = e_p \quad (p \mid P),$$

$$\operatorname{ord}_q (a^{b_1} - b) = c_1$$

$$a_1 = 2\lambda q^{c_1} \prod_{p \mid P} p^{e_p}(p-1).$$

Clearly $(a_1, b_1) = 1$ and by virtue of (25) we have for $t \geqslant 0$

$$\operatorname{ord}_p (a^{a_1 t + b_1} - b) = \begin{cases} (a_1 t + b_1)\alpha_p & \text{if } \alpha_p < 0, \\ \min\{0, \beta_p\} & \text{if } \alpha_p = 0, \beta_p \neq 0, \\ \beta_p & \text{if } \alpha_p > 0; \end{cases}$$

$$a^{a_1 t + b_1} - b \equiv a^{b_1} - b \bmod \prod_{p \mid P} p^{e_p + 1} . q^{c_1 + 1},$$

https://doi.org/10.1017/S0305004100070912 Published online by Cambridge University Press

hence
$$\operatorname{ord}_p(a^{a_1 t+b_1}-b) = e_p \quad \text{for all } p \mid P,$$
$$\operatorname{ord}_q(a^{a_1 t+b_1}-b) = c_1.$$

Finally, since $a_1 t+b_1$ is odd we have by (23)
$$\operatorname{sgn}(a^{a_1 t+b_1}-b) = \operatorname{sgn} a.$$

Hence (24) holds for $k = 1$.

Assume now that we have constructed $q_1, a_1, b_1, c_1, \ldots, q_{k-1}, a_{k-1}, b_{k-1}, c_{k-1}$. Let l be a sufficiently large prime in the arithmetic progression $a_{k-1}t+b_{k-1}$ $(t \geqslant 0)$.

By the inductive assumption
$$a^l-b = \operatorname{sgn} a \prod_{\alpha_p<0} p^{l\alpha_p} \prod_{\substack{\alpha_p=0\\ \beta_p\neq 0}} p^{\min\{0,\beta_p\}} \prod_{\alpha_p>0} p^{\beta_p} \prod_{p\mid P} p^{e_p} \prod_{i=1}^{k-1} q_i^{c_i} s,$$

where s is a positive integer, prime to $q_1 q_2 \ldots q_{k-1}$ and to the numerators and the denominators of $a, b, a-b$. Since
$$a^l-b \equiv a-b \bmod l, \quad \prod_{\alpha_p<0} p^{l\alpha_p} \equiv \prod_{\alpha_p<0} p^{\alpha_p} \bmod l$$

we have $s \not\equiv 1 \bmod l$. Hence s has a prime factor q_k different from $q_1, q_2, \ldots, q_{k-1}$ and such that $q_k \not\equiv 1 \bmod l$. By the Proposition with $n = l$ we have
$$M_{q_k}(a) = M_{q_k}(b) \quad \text{and} \quad \alpha_{q_k} = \beta_{q_k} = \gamma_{q_k} = 0.$$

We take
$$b_k \geqslant b_{k-1}, \quad b_k \equiv l \bmod a_{k-1}(q_k-1), \quad (b_k, q_k) = 1,$$
$$c_k = \operatorname{ord}_{q_k}(a^{b_k}-b), \quad a_k = a_{k-1}(q_k-1)q_k^{c_k}$$

and easily verify that $(a_k, b_k) = 1$ and (24) holds.

Remark. We do not know whether for all $a, b, c \in \mathbb{Q}$, with $abc \neq 0$, $|a| \neq 1$, $|b| \neq 1$, $|c| \neq 1$ there exist infinitely many primes q with $M_q(a) = M_q(b) = M_q(c)$.

https://doi.org/10.1017/S0305004100070912 Published online by Cambridge University Press