The proof of Lemma 4.3 in our paper [AKS04] is incorrect (we thank the anonymous referees together with CS05, RS05, R18 for pointing it out). In the proof, it is claimed that if there is an \( s \leq B = \max\{3, [\log^5 n]\} \) such that \( s \not\in \{r_1, \ldots, r_t\} \) (the set of all numbers \( r_i \leq B \) that divide the product \( n \cdot \prod_{i=1}^{[\log^5 n]} (n^i - 1) \)) then for \( r = \frac{s}{(s,n)} \), \( o_r(n) > \log^2 n \). The claim is wrong because it does not handle the case when \( s \) is a multiple of a power of a number dividing \( n \). In those cases \( \frac{s}{(s,n)} \) may not be coprime to \( n \) and so \( o_r(n) \) is undefined.

It is easy to fix the proof. We give a corrected proof below, by changing the definition of \( r \).

**Lemma 4.3** There exists an \( r \leq \max\{3, [\log^5 n]\} \) such that \( o_r(n) > \log^2 n \).

**Proof.** This is trivially true when \( n = 2 \): \( r = 3 \) satisfies all conditions. So assume that \( n > 2 \). Then \( [\log^5 n] > 10 \) and Lemma 3.1 applies. Observe that the largest value of \( k \) for any number of the form \( m^k \leq B = [\log^5 n] \), \( m \geq 2 \), is \( \lfloor \log B \rfloor \). Now consider the smallest number \( s \) that does not divide the product \( n^{\lfloor \log B \rfloor} \cdot \prod_{i=1}^{[\log^5 n]} (n^i - 1) \).

How small is \( s \)? Note that,

\[
n^{\lfloor \log B \rfloor} \cdot \prod_{i=1}^{[\log^5 n]} (n^i - 1) < n^{\lfloor \log B \rfloor + \frac{1}{2} \log^2 n \cdot (\log^2 n - 1)} \leq n^{\log^4 n} \leq 2^{\log^5 n} \leq 2^B.
\]

(The second inequality holds for all \( n \geq 2 \)). By Lemma 3.1, the lcm of first \( B \) numbers is at least \( 2^B \). Therefore, \( s \leq B \). As a result, the part of \( s \) coprime to \( n \) is \( r := \frac{s}{(s,n)} \). Furthermore, by the choice of \( s \) we have that \( r \) does not divide the product \( \prod_{i=1}^{[\log^5 n]} (n^i - 1) \).

Thus, \( r \) (which is coprime to \( n \)) does not divide any of \( n^i - 1 \) for \( 1 \leq i \leq [\log^2 n] \), implying that \( o_r(n) > \log^2 n \). \( \square \)

**References**


