Annals of Mathematics **189** (2019), 317–318
https://doi.org/10.4007/annals.2019.189.1.6

Errata:
PRIMES is in P

By Manindra Agrawal, Neeraj Kayal, and Nitin Saxena

The proof of Lemma 4.3 in our paper [AKS04] is incorrect. (We thank the anonymous referees together with [CS05], [RG05], [Rui18] for pointing this out.) In the proof, it is claimed that if there is an $s \leq B = \max\{3, \lceil \log^5 n \rceil\}$ such that $s \not\in \{r_1, \ldots, r_t\}$ (the set of all numbers $r_i \leq B$ that divide the product $n \cdot \prod_{i=1}^{\lfloor \log^2 n \rfloor}(n^i - 1)$), then for $r = \frac{s}{(s,n)}$, $\mathrm{o}_r(n) > \log^2 n$. 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 $\mathrm{o}_r(n)$ 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 $r \leq \max\{3, \lceil \log^5 n \rceil\}$ 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 $\lceil \log^5 n \rceil > 10$ and Lemma 3.1 applies. Observe that the largest value of k for any number of the form $m^k \leq B = \lceil \log^5 n \rceil$, $m \geq 2$, is $\lfloor \log B \rfloor$. Now consider the smallest number s that does not divide the product

$$n^{\lfloor \log B \rfloor} \cdot \prod_{i=1}^{\lfloor \log^2 n \rfloor} (n^i - 1).$$

How small is s? Note that,

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

(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 $r := \frac{s}{(s, n^{\lfloor \log B \rfloor})}$. Furthermore, by the choice of s we have that r does

Keywords: primality, derandomization, cyclotomic, AKS, identity testing, deterministic, polynomial-time

AMS Classification: Primary: 11A51, 68Q25, 11R18.

not divide the product

$$\prod_{i=1}^{\lfloor \log^2 n \rfloor} (n^i - 1).$$

Thus, r (which is coprime to n) does not divide any of $n^i - 1$ for $1 \le i \le \lfloor \log^2 n \rfloor$, implying that $\mathrm{o}_r(n) > \log^2 n$. □

References

[AKS04] M. Agrawal, N. Kayal, and N. Saxena, PRIMES is in P, *Ann. of Math.* (2) **160** no. 2 (2004), 781–793. MR 2123939. Zbl 1071.11070. https://doi.org/10.4007/annals.2004.160.781.

[CS05] W. Carlip and L. Somer, Private communication, April 2005.

[RG05] L. Rempe-Gillen, Private communication with L. Rempe-Gillen and students of Deutsche Schuelerakademie, July 2005.

[Rui18] S. M. Ruiz, Private communication, July 2018.

(Received: June 24, 2018)
(Revised: August 7, 2018)

Department of Computer Science and Engineering, Indian Institute of Technology, Kanpur, India
E-mail: manindra@cse.iitk.ac.in

Microsoft Research, Bangalore, India
E-mail: neeraka@microsoft.com

Department of Computer Science and Engineering, Indian Institute of Technology, Kanpur, India
E-mail: nitin@cse.iitk.ac.in