Primality Testing in Polynomial Time

Errata

Sorted by page
Last update: March 29, 2007
Segments of original text are enclosed in double brackets: $\langle\langle \cdots \rangle\rangle$

1. **p. 7, line 6 from bottom:** Replace $\langle\langle$algorithm$\rangle\rangle$ by $\langle\langle$algorithms$\rangle\rangle$.

2. **p. 11, line 18:** Replace $\langle\langle$is lead$\rangle\rangle$ by $\langle\langle$is led$\rangle\rangle$.

3. **p. 15, line 7:**

   Replace $\langle\langle$"loop body" *ins*$\rangle\rangle$ by $\langle\langle$"loop body" *stm*$\rangle\rangle$.

4. **p. 19, line 16:** Replace $\langle\langle s_0 = a \bmod n\rangle\rangle$ by $\langle\langle s_0 = a \bmod m\rangle\rangle$.

5. **p. 20, line 7, 9, and 11 from bottom:** Replace $\langle\langle$`p`$\rangle\rangle$ by $\langle\langle$`c`$\rangle\rangle$ (3 occurrences).

6. **p. 20, line 9 from bottom:**

   Replace $\langle\langle \prod_{0\le j\le i} a^{2^j} \rangle\rangle$ by $\langle\langle \prod_{0\le j\le i,\, b_j=1} a^{2^j} \rangle\rangle$

   p. 20, line 7 from bottom:

   Replace $\langle\langle \prod_{0\le j\le k} a^{2^j} \rangle\rangle$ by $\langle\langle \prod_{0\le j\le k,\, b_j=1} a^{2^j} \rangle\rangle$

7. **p. 21, line 10 from bottom:** Replace $\langle\langle c - b\rangle\rangle$ by $\langle\langle c - a\rangle\rangle$.

8. **p. 21, line 11:** (Line 0 in Perfect Power Test)

   Replace $\langle\langle$`a`,`b`,`c`,`m`: **integer**$\rangle\rangle$ by $\langle\langle$`a`,`b`,`c`,`m`,`p`: **integer**$\rangle\rangle$.

9. **p. 21, line 26 (5th line after Algorithm 2.3.5):**
   Replace $\langle\langle$break off and report the answer $n + 1$.$\rangle\rangle$ by
   $\langle\langle$break off the exponentiation and assign $n + 1$ to `p` to indicate that m^b is larger than n.$\rangle\rangle$.

10. **p. 25, line 14:** Replace $\langle\langle qd \le a\rangle\rangle$ by $\langle\langle qd \le n\rangle\rangle$.

11. **p. 28, line 7:** (Line 3 of the algorithm.)
    Replace $\langle\langle$**else** $b \leftarrow |m|$; $a \leftarrow |n|\rangle\rangle$ by $\langle\langle$**else** $a \leftarrow |m|$; $b \leftarrow |n|\rangle\rangle$.

12. **p. 34, line 11 from bottom:**

    Replace $\langle\langle a$ must divide $b\rangle\rangle$ by $\langle\langle m$ must divide $b\rangle\rangle$.

13. **p. 36, line 5:** Replace $\langle\langle 11^5 \bmod 24 = 5\rangle\rangle$ by $\langle\langle 11^5 \bmod 24 = 11\rangle\rangle$.

14. **p. 38, line 16:**

    Replace $\langle\langle u \in \mathbb{Z}_n^*\rangle\rangle$ by $\langle\langle u \in \mathbb{Z}_n\rangle\rangle$.

15. **p. 44, line 16:** (Second line in Proposition 3.5.11)

    Replace $\langle\langle$Then a, b are$\rangle\rangle$ by $\langle\langle$Then n, m are$\rangle\rangle$.

16. **p. 46, lines 9 and 10:**

    Replace $\langle\langle 1/\ln(10^{50}-1)\rangle\rangle$ by $\langle\langle 1/(\ln(10^{50})-1)\rangle\rangle$ and $\langle\langle 1/\ln(10^{100}-1)\rangle\rangle$ by $\langle\langle 1/(\ln(10^{100})-1)\rangle\rangle$.

17. **p. 48, line 8:**

    Replace $\langle\langle \nu_2(20)\rangle\rangle$ by $\langle\langle \nu_2(20!)\rangle\rangle$.

18. **p. 50, lines 1–4:**

    In line 1, replace $\langle\langle$the product $N!\rangle\rangle$ by $\langle\langle$the product $\lceil \alpha N \rceil !\rangle\rangle$. In line 2, replace $\langle\langle \alpha N\rangle\rangle$ by $\langle\langle \lceil \alpha N \rceil\rangle\rangle$. In line 4, replace $\langle\langle (\alpha N)!\rangle\rangle$ by $\langle\langle \lceil \alpha N \rceil !\rangle\rangle$ (two occurrences).

19. **p. 57, line 1:** Replace $\langle\langle$Example 4.1.2(d)$\rangle\rangle$ by $\langle\langle$Example 4.1.2(e)$\rangle\rangle$.
    p. 57, line 3: Replace $\langle\langle$Example 4.1.2(e)$\rangle\rangle$ by $\langle\langle$Example 4.1.2(f)$\rangle\rangle$.
    p. 57, line 8: Replace $\langle\langle$Example 4.1.2(a),(b), and (c)$\rangle\rangle$ by $\langle\langle$Example 4.1.2(a),(b), (c), and (d)$\rangle\rangle$.

20. **p. 63, line 3 from bottom:** Replace $\langle\langle (a^m)^{-1}\rangle\rangle$ by $\langle\langle (a^i)^{-1}\rangle\rangle$.

21. **p. 69, line 25:** (Line 3 of Algorithm 4.3.9)

    Replace $\langle\langle \mathtt{s} \leftarrow \mathtt{s} \cdot \mathtt{s} \bmod m;\rangle\rangle$ by $\langle\langle \mathtt{s} \leftarrow \mathtt{s} \circ \mathtt{s};\rangle\rangle$.

22. **p. 80, line 13:** (First line in Definition 5.2.3)

    Replace $\langle\langle n = u \cdot 2^k\rangle\rangle$ by $\langle\langle n - 1 = u \cdot 2^k\rangle\rangle$.

23. **p. 80, line 12 from bottom:**

    To Definition 5.2.3 append the sentence $\langle\langle$*The set of all A-liars for n is denoted by* L_n^{A}.$\rangle\rangle$

24. **p. 81, line 20:** (Line 1 in Miller-Rabin Test)

    Replace $\langle\langle n = u \cdot 2^k \rangle\rangle$ by $\langle\langle n - 1 = u \cdot 2^k \rangle\rangle$.

25. **p. 86, line 14:** Replace $\langle\langle g^{2i}, 0 \le i < p-1 \rangle\rangle$ by $\langle\langle g^{2i}, 0 \le i < \frac{1}{2}(p-1) \rangle\rangle$.

26. **p. 87, line 14 from bottom:** Replace $\langle\langle \gcd(a, n) = 0 \rangle\rangle$ by $\langle\langle \gcd(a, n) = 1 \rangle\rangle$.

27. **p. 90, line 4 from bottom:** Replace

$$\langle\langle \left(\frac{150}{173}\right) \rangle\rangle \text{ by } \langle\langle \left(\frac{150}{773}\right) \rangle\rangle$$

    and

$$\langle\langle \left(\frac{75}{173}\right) \rangle\rangle \text{ by } \langle\langle \left(\frac{75}{773}\right) \rangle\rangle \ .$$

28. **p. 98, line 17:** Replace $\langle\langle i \le \min\{d, d'\} \rangle\rangle$ by $\langle\langle i \le d \rangle\rangle$.

29. **p. 99, line line 17 from bottom:**

    Replace $\langle\langle \deg(f \cdot h) \rangle\rangle$ by $\langle\langle \deg(f \cdot g) \rangle\rangle$.

30. **p. 99, line line 12 from bottom:**

    Replace $\langle\langle$(i) and (ii)$\rangle\rangle$ by $\langle\langle$(a) and (b)$\rangle\rangle$.

31. **p. 100, line 17:** Replace $\langle\langle f(b) \rangle\rangle$ by $\langle\langle f(s) \rangle\rangle$.

32. **p. 103, line 3 from bottom (line 8 of Algorithm 7.2.2):** Replace $\langle\langle \texttt{f[j]} \leftarrow \texttt{f[j]} - \texttt{a} \cdot \texttt{h[j]} \rangle\rangle$ by $\langle\langle \texttt{f[j]} \leftarrow \texttt{f[j]} - \texttt{a} \cdot \texttt{h[j} - \texttt{i} + d\texttt{]} \rangle\rangle$.

33. **p. 104, line 3:** Replace $\langle\langle$In line 5$\rangle\rangle$ by $\langle\langle$In lines 5–6$\rangle\rangle$.

34. **p. 108, line 17 from bottom:** Replace $\langle\langle 3 \cdot (X+4) \cdot (X^2+4) \rangle\rangle$ by $\langle\langle 3 \cdot (X+4) \cdot (X^2+3) \rangle\rangle$.

35. **p. 117, line 4 from bottom:** (Line 10 of Algorithm 4.3.9)

    A comment: We use here the bound $2\lceil\sqrt{r}\rceil \cdot \lceil \log n \rceil$, because this number is easy to calculate in integer arithmetic. Later (page 123, lines 16–17) we only use that numbers a with $1 \le a \le 2\sqrt{r} \cdot \log n$ have definitely been tested.

36. **p. 119, line 11:** Replace $\langle\langle$(Definition 7.1.2)$\rangle\rangle$ by $\langle\langle$(Definition 7.1.3)$\rangle\rangle$.

37. **p. 128, line 11:**

    Replace $\langle\langle$Key Lemma 8.5.8$\rangle\rangle$ by $\langle\langle$Key Lemma 8.5.9$\rangle\rangle$.

38. **p. 137, line 8 from bottom:** Replace $\langle\langle H\rangle\rangle$ by $\langle\langle H_p\rangle\rangle$ (two occurrences).

39. **p. 138, line 11 from bottom:** Replace $\langle\langle p/2-k\rangle\rangle$ by $\langle\langle (p-1)/2-k\rangle\rangle$.

40. **p. 143, lines 8 and 10:** The links have become obsolete. The original version of the AKS paper and a revised version are available at `http://www.cse.iitk.ac.in/users/manindra/primality_original.pdf` and `http://www.cse.iitk.ac.in/users/manindra/primality_v6.pdf`.

41. **p. 143, lines 22 and 24:** Replace $\langle\langle$Bernstein, D.G.$\rangle\rangle$ by $\langle\langle$Bernstein, D.J.$\rangle\rangle$.

42. **p. 143, lines 23 and 26:** The links have become obsolete. Bernstein's exposition [10] of the AKS result can now be found at `http://cr.yp.to/papers/aks.pdf`; his survey [11] is at `http://cr.yp.to/primetests/prime2004-20041223.pdf`.