# Errata: *A Computational Introduction to Number Theory and Algebra (Version 1)*

Last updated: 9/27/2006.

## Preface

**p. xiii:** Line 1. Insert "a" after "also". [VS, 11/1/05]

## Preliminaries

**p. xv:** Line 5. Replace "(We shall reserve ...)" by "(We shall reserve the notation $S^n$ for other purposes, so as to avoid ambiguity.)" (Not really a typo, but maybe confusing.) [VS, 11/1/05]

**p. xv:** 2 lines above *Functions*. Replace "the the" by "the". [VS, 1/30/06]

## Chapter 1

**p. 7:** Lines 13 and 14. Replace "$a_{k-1}$" by "$a_k$" (once on each line). [VS, 2/1/06]

**p. 7:** 4 lines below (1.3). Delete "is" before "obviously". [Matthew Dempsky, 4/1/06]

**p. 7:** Line $-9$. Replace "$p_i$" by "$p_1$" (two times). [VS, 2/1/06]

**p. 9:** Line $-9$. Insert "and $k > 1$" before first comma.

## Chapter 2

**p. 28:** Exercise 2.18. Both instances of "$[\pm 1]_n$" in the hint should be replaced by "$[\pm 1]_p$". [VS, 10/12/05]

**p. 29:** Line 2 of proof of Theorem 2.17. Second "$\ell$" should be subscripted. [VS, 2/14/06]

## Chapter 3

**p. 33:** Line 4 of §3.1. Replace "taking non-negative" by "ranging over all sufficiently large". This makes the definition more precise, while at the same time more general as well (it allows for functions that are only defined beyond some point). In the same spirit, in Exercise 3.5, replace "takes non-negative" by "ranges over all sufficiently large". [VS, 11/29/05]

**p. 42:** Line $-8$. Replace "$(carry, q_i)$" by "$(q_i, carry)$". [PERRISSIN-FABERT Marie Agnes; DUCHENE Coralie; LAMARQUE Remi, 7/13/06]

**p. 49:** Exercise 3.26. Replace both occurences of "$\ell + O(1)$" by "$\leq \ell + O(1)$". Replace "an additional $2^t + \ell/t + O(1)$ multiplications" by "$\leq 2^t + \ell/t$ additional multiplications". Replace "an additional $2^{t-1} + \ell/t + O(1)$ multiplications" by "$\leq 2^{t-1} + \ell/t + O(1)$ additional multiplications". (Not really a typo, but maybe confusing.) [VS, 1/27/06]

**p. 50:** Exercise 3.27. Replace "$\ell + O(1)$" by "$\leq \ell + O(1)$". Replace "an additional $\ell + 2^k + O(1)$ multiplications" by "$\leq \ell + 2^k + O(1)$ additional multiplications". (Not really a typo, but maybe confusing.) [VS, 1/27/06]

**p. 50:** Exercise 3.28. Replace "$\ell + O(1)$" by "$\leq \ell + O(1)$". Replace "$2^k + O(1)$" by "$\leq 2^k + O(1)$". Replace both instances of "$\ell/k + O(1)$" by "$\leq \ell/k + O(1)$". (Not really a typo, but maybe confusing.) [VS, 1/27/06]

**p. 50:** Lines 2 and 5 of Exercise 3.28. Replace "$\ell$-bit" by "$\ell$-bit (or shorter)".

Unfortunately, the phrase "$\ell$-bit integer" is used a bit inconsistently throughout the text (and is not actually formally defined). Sometimes, it means "an integer $a$ with $\text{len}(a) = \ell$", while at other times (such as the usage here), it means "an integer $a$ with $\text{len}(a) \leq \ell$". To correct for this, the *first* meaning ($\text{len}(a) = \ell$) should be the correct interpretation of this phrase, and all instances where the second meaning was intended should be re-worded (as done here, and in several other instances, as indicated below). [VS, 11/2/05]

**p. 50:** Exercise 3.29. Replace "$\ell + O(1)$" by "$\leq \ell + O(1)$". (Not really a typo, but maybe confusing.) [VS, 1/27/06]

**p. 51:** Line 5, 13. Replace "$\ell$-bit" by "$\ell$-bit (or shorter)". [VS, 11/1/05]

**p. 52:** Line 4 of Exercise 3.36. Replace "that" by "than". [VS, 3/19/2006]

**p. 53:** Line 5.

Replace the sentence beginning "A typical 32-bit ..." with

> A typical 32-bit machine, with 32-bit words, often comes with instructions to compute the double-word product of two single-word integers, and similarly, to divide a double-word integer by a single-word integer (obtaining both the quotient and remainder).

This avoids the dreaded phrase "$\ell$-bit integer". [VS, 11/1/05]

**p. 53:** Lines $-12$, $-11$. Replace "$\ell$-bit" by "$\ell$-bit (or shorter)". [VS, 11/1/05]

## Chapter 4

**p. 56:** Line 4 above Example 4.1. "the fact the" shoup be "the fact that". [George Stephanides, 9/4/06]

**p. 57:** Line 12. Replace "$k$-bit numbers" by "$k$-bit (or shorter) integers". [VS, 11/1/05]

**p. 57:** Line 13. Replace "$k$-bits" with "$k$ bits". [VS, 11/1/05]

**p. 59:** Line 4. "$q_i$" should be "$q_{i-1}$". [Kristiyan Haralambiev, 5/22/06]

**p. 65:** Last line of step 2 in the algorithm. Replace "$n/2 \leq c_{rt} < n/2$" with "$-n/2 \leq c_{rt} < n/2$". [Cameron McInally, 4/27/06]

**p. 73:** Last paragraph. Replace the second sentence by:

> Using the theory of continued fractions, Theorem 4.6 can be improved as follows: if $n > 2r^*t^*$ (rather than $n \geq 4r^*t^*$), then statement (ii) of the theorem holds when $r'$ is chosen as the first remainder $r_i \leq r^*$, and $s' := s_i, t' := t_i$. This fact was observed by Wang, Guy, and Davenport [97].

In fact, this stronger result can be obtained by much more direct proof, such as the one given in the Supplementary Material (see `http://www.shoup.net/ntb/supp-v1.pdf`). [VS, 12/21/05]

## Chapter 5

**p. 89:** Line 15. "$(p_1^{e_1} \cdots p_r^{e_r})^s$" should be "$(p_1^{e_1} \cdots p_r^{e_r})^{-s}$". [VS, 5/17/05]

## Chapter 6

**p. 98:** Line 4. ", Let" should be ". Let". [VS, 8/29/06]

**p. 98:** Exercise 6.1(a). Clarification: $n$ is chosen at random from the set $\{2^{k-1}, \ldots, 2^k - 1\}$. [VS, 9/15/05]

**p. 99:** Exercises 6.3 and 6.5. It may be better to add the hint: use induction on $n$. [VS, 10/11/05]

**p. 107:** Theorem 6.4. Replace the phrase "are mutually independent ..." with the following:

> are mutually independent random variables on the product distribution of $\mathbf{D}_1, \ldots, \mathbf{D}_n$, where the distribution of each $\pi_i$ is $\mathbf{D}_i$.

[VS, 11/1/05]

**p. 111:** Line 3. "let use" should be "let us". [George Stephanides, 9/9/06]

**p. 114:** Proof of Theorem 6.10. The first "$E$" after "=" should be "$\mathsf{E}$" (just a font change). [George Stephanides, 9/27/06]

**p. 122:** Line −9. "modulo $n$" should be "over $\mathbb{Z}_n$". [VS, 8/24/05]

**p. 123:** Line 10. "since than" should be "since then". [George Stephanides, 8/16/06]

**p. 125:** Line 12. "map" should be "maps". [VS, 11/20/05]

**p. 125:** Line 20. "For any $\ell = 1, \ldots, k$" should be "For any $\ell = 2, \ldots, k$". Also, a clarification: the definition only allows $\mathcal{H}$ to be pairwise independent if $k \geq 2$. [VS, 11/30/05]

**p. 130:** Line −5. "measure" should be "measure of". [VS, 5/18/05]

**p. 143:** Second line in proof of Theorem 6.23. "$\sum_{i=1}^{k_0} a_i$" should be "$\sum_{i=1}^{k_0} \Pr[a_i]$". [VS, 10/5/05]

**p. 146:** Last paragraph of §6.10.4. Rewrite as:

> The definition of conditional expectation carries over verbatim. Equations (6.15) and (6.16) hold (assuming the relevant expectations exist). Also, the analog of (6.16) holds for infinite partitions $\mathcal{B}_1, \mathcal{B}_2, \ldots$, provided $\mathsf{E}[X]$ exists.

[VS, 7/28/05]

## Chapter 7

**p. 156:** Last three lines. Too many instances of "we have". [George Stephanides, 9/27/06]

**p. 161:** Line 13. "distribution on $N_i$" should be "distribution of $N_i$". [George Stephanides, 9/27/06]

**p. 164:** Line −2. Replace "the the" by "the". [Sherman Chow, 7/27/06]

**p. 171:** Line −13. Insert "using" before "algorithm". [VS, 6/13/05]

**p. 179:** Line 13. "Lesbegue" should be "Lebesgue". [George Stephanides, 6/26/06]

## Chapter 8

**p. 185:** Proof of Theorem 8.6. One should also remark that $mG$ is non-empty (e.g., $0_G = m0_G \in mG$). A similar remark applies to the proofs of Theorems 8.7, 8.12, and 8.13. [VS, 2/16/06]

**p. 189:** Line 3 of proof of Theorem 8.13. "$-h \in H_2$ and $-h \in H_2$" should be "$-h \in H_1$ and $-h \in H_2$". [Sherman Chow, 4/30/06]

**p. 192:** Lines 7 and 9. Replace both instances of "$[H' : G]$" by "$[H' : H]$". [Rafal Zwierz, 12/02/05]

**p. 194:** Line 6 of Example 8.36. Replace both instances of "$a$" by "$z$". (Not really a typo, but maybe confusing.) [VS, 5/20/05]

**p. 195:** Line 6. Replace "non-zero" by "positive". [VS, 4/28/06]

**p. 195:** Line −3. Replace "part (v) of Theorem 8.3" by "part (ii)". [VS, 4/19/06]

**p. 196:** First line after proof of Theorem 8.20. Replace "particular" by "particularly". [Rafal Zwierz, 1/05/06]

**p. 198:** Line −3. Replace "$\rho_2'$" by "$h_2'$". [VS, 5/4/2006]

**p. 204:** Line −9. Replace "establish" by "establishes". [Rafal Zwierz, 1/05/06]

**p. 207:** Line 7. Replace "is" by "if". [VS, 3/21/06]

**p. 210:** Lemma 8.46. "such that $m_i \mid m_{i+1}$" should read "such that $m_i \mid m_{i+1}$ and $n_i \mid n_{i+1}$". [VS, 3/30/05]

## Chapter 9

**p. 212:** Last sentence of proof of Theorem 9.2. Replace with "Part (iv) follows from part (iii), along with part (iv) of Theorem 8.3." [VS, 4/19/06]

**p. 218:** Line −9. "If fact" should be "In fact". [Sherman Chow, 4/30/06]

**p. 219:** Line 7 of Example 9.23. "element" should be "elements". [VS, 5/22/06]

**p. 221:** Line −7. "let such let such" should be "let such". [Dae Hyun Yum, 9/21/06]

**p. 223:** Line −7. Replace "as" by "an". [Rafal Zwierz, 1/05/06]

**p. 224:** Line 3 of proof of Theorem 9.12. The formula defining $r'$ is broken across two lines, and may be hard to read correctly. It should be typeset on one line. [VS, 4/30/06]

**p. 229:** Equation (9.3). "$\mathtt{Y}_j$" should be "$\mathtt{Y}^j$". [VS, 4/23/05]

**p. 229:** Lines 15 and 16. Font of $X$ and $Y$ is inconsistent. [VS, 5/20/06]

**p. 230:** Line 4. Add parenthetical remark just before semi-colon: "(with distinct exponent sequences among the monomials)". [VS, 4/23/05]

**p. 230:** Line 7. "degree" should be "total degree". [VS, 4/23/05]

**p. 231:** Line 3 of Example 9.32. "polynomial" should be "polynomials". [VS, 5/27/05]

**p. 237:** Line 17. "as a subring of" should be "is a subring of". [VS, 6/15/06]

**p. 240:** Example 9.45, line 7. "In fact, $\bar{\rho}$ it is" should be "In fact, $\bar{\rho}$ is". [Dae Hyun Yum, 9/21/06]

## Chapter 10

**p. 253:** In Algorithm MR. Replace "$\alpha \leftarrow_R \{1, \ldots, n-1\}$" by "choose $\alpha \in \mathbb{Z}_n^+$ at random". [VS, 3/9/2006]

**p. 256:** In Algorithm MRS. Replace "$\alpha \leftarrow_R \{1, \ldots, n-1\}$" by "choose $\alpha \in \mathbb{Z}_n^+$ at random". [VS, 3/9/2006]

**p. 257:** Line 11. Replace "Prime" by "prime". [VS, 4/10/06]

**p. 261:** Section 10.5, line 1. "We are given a integer $n$" should be "We are given an integer $n$". [Dae Hyun Yum, 9/21/06]

**p. 262:** Line 5. "than $n = w^e$ is an a" should be "that $n = w^e$ is a". [George Stephanides, 6/26/06]

**p. 263:** Line 12. "$p^2 + \cdots + n$" should be "$p^2 + \cdots + n = 0$". [George Stephanides, 9/27/06]

**p. 265:** Line 11. Insert "a" before "probabilistic". [Kevin Lawler, 3/31/06]

## Chapter 11

**p. 271:** Line −6. Before the semi-colon, insert: "with which we can perform both table insertions and lookups in time $O(\text{len}(p))$". [VS, 9/22/05]

**p. 272:** Line 16. Insert "of" after "table". [VS, 9/22/05]

## Chapter 12

**p. 283:** Line 10. Insert "of" before "any finite cyclic group". [Cameron McInally, 4/17/06]

**p. 286:** Statement of Theorem 2.6. "$(-1)^{(p^2-1)}/8$" should be "$(-1)^{(p^2-1)/8}$". [Sherman Chow, 4/30/06]

## Chapter 13

**p. 294:** Exercise 13.7. Replace both instances of $\mathbb{Z}_n$ by $\mathbb{Z}_n^*$. [VS, 5/17/2006]

## Chapter 14

**p. 300:** Line 4 of Example 14.1: Replace "$\beta = (b_1, \ldots, a_n)$" by "$\beta = (b_1, \ldots, b_n)$". [Rafal Zwierz, 1/05/06]

## Chapter 15

**p. 329:** Line −7. Insert "of" before "its first $r$ positions". [Cameron McInally, 4/27/06]

**p. 330:** Line −2. Replace "if" by "of". [Sherman Chow, 7/27/06]

**p. 331:** Line −2. Replace "$0_V$" by "$0_W$". [VS, 9/11/05]

**p. 332:** Lines 4 and 7. Replace "$0_V$" by "$0_W$". [VS, 9/11/05]

**p. 332:** Line 7. Replace "equivalent to saying" to "implied by the condition".

For the other direction, all one can say is that if $W$ contains a non-zero self-orthogonal vector, then there exists a subspace $U$ of $W$ such that $U \cap \bar{U} \neq \{0_W\}$.

[Ronald Cramer, 9/11/05]

## Chapter 16

**p. 339:** Line 13. "$\cdots$" should be "$\cdots+$". [George Stephanides, 8/16/06]

**p. 346:** Line 3. "$\cdots$" should be "$\cdots+$". [George Stephanides, 8/16/06]

**p. 357:** Last line. The current factoring record is the challenge number RSA-200, which is a 663-bit integer (F. Bahr, M. Boehm, J. Franke, T. Kleinjung, May 2005). [VS, 11/11/05]

## Chapter 17

**p. 359:** Line 2 of Example 17.4. Replace "ideal of $R$" by "ideal of $R[\mathtt{X}]$". [Rafal Zwierz, 1/05/06]

**p. 360:** Line −8. Replace "$R = R'$" by "$E = E'$". [Rafal Zwierz, 1/05/06]

**p. 361:** Line 2 of subsection *Polynomial evaluation.* Replace "$\sum_i g_i \mathtt{X}_i$" by "$\sum_i g_i \mathtt{X}^i$". [Rafal Zwierz, 1/05/06]

**p. 380:** Line 2 of proof of Theorem 17.21. The summation should be over "$c_i \mathtt{X}^i$", rather than "$c_i$". [George Stephanides, 7/11/06]

**p. 385:** Last two displayed equations. Replace both instances of "$p$" by "$p_i$". [VS, 2/05/06]

**p. 396:** Line 7 of Theorem 17.44. "$\mathtt{X}_i$" should be "$\mathtt{X}^i$". [George Stephanides, 7/7/06]

**p. 397:** Last line. Replace "$\ell$-bit" by "$\ell$-bit (or shorter)". [VS, 11/1/05]

## Chapter 18

**p. 416:** Line 1 of Exercise 18.22. Replace "$\ell$-bit" by "$\ell$-bit (or shorter)". [VS, 11/1/05]

**p. 417:** Lines 3 and 4 of Exercise 18.25. Repplace "$\mathtt{X}_i$" by "$\mathtt{X}^i$" (twice). [George Stephanides, 7/18/06]

**p. 419:** Lines 11, −4. Replace "$\ell$-bit" by "$\ell$-bit (or shorter)". [VS, 11/1/05]

**p. 420:** Line 10. Replace "$t$-bit numbers" by "$t$-bit (or shorter) integers". [VS, 11/1/05]

**p. 420:** Line 14. Replace "of length $\ell$" by "of length at most $\ell$". [VS, 11/1/05]

**p. 441:** 2nd to last para. Delete "It is easy to see that". [VS, 4/19/05]

## Chapter 20

**p. 448:** Statement of Theorem 20.1. After "Then", add the phrase "in the ring $F[\mathtt{X}]$,". The same applies to Theorem 20.3. [Rafal Zwierz, 3/18/06]

**p. 450:** Line −14. Replace "$F$ is isomorphic" by "$E$ is isomorphic". [Rafal Zwierz, 3/18/06]

**p. 461:** 2nd line of Exercise 20.10. Replace "$f := \mathtt{X}^q - \mathtt{X} - a$" by "$f := \mathtt{X}^p - \mathtt{X} - a$". [VS, 1/27/06]

**p. 461:** 2nd line of Exercise 20.12. Replace "a the Frobenius" by "the Frobenius". [Augusto Jun Devegili, 3/14/2006]

## Chapter 21

**p. 477:** Last paragraph. The claim that the running-time bound in Theorem 21.8 is tight is incorrect (as is Exercise 21.10).

In fact, assuming the gcd operation is implemented using Euclid's algorithm, Algorithm SFD uses $O(\ell^2 + \ell(w-1)\operatorname{len}(p)/p)$ operations in $F$. This follows from the fact that on inputs $a, b \in F[\mathtt{X}]$ $\deg(a) \geq \deg(b) \geq 0$, Euclid's algorithm uses only $O(\operatorname{len}(b)\operatorname{len}(a/d))$ operations in $F$, where $d := \gcd(a, b)$ (this could be made an exercise for both the integer and polynomial cases). Combining this fact with Exercise 21.24 will yield (with a careful counting argument) the better $\ell^2$ bound for SFD, instead of the more naive $\ell^3$ bound. The algorithms in §21.6 are still useful, as the output of these algorithms are in a nicer form.

To fix this problem, a number of changes are necessary, here and elsewhere. First, the last paragraph of p. 477 should be replaced by the following:

> While the running-time bound in Theorem 21.8 suffices for our purposes, it is not tight, and in fact it is possible to show with a more careful argument that it uses just $O(\ell^2 + \ell(w-1)\operatorname{len}(p)/p)$ operations in $F$. In §21.6 we examine a variant of Algorithm SFD that has a nicer output format, and that also achieves this running-time bound.

Second, Exercise 21.10 should be replaced by the following.

> Show that on inputs of degree $\ell$, the recursion depth of Algorithm SFD is $\Omega(\ell)$ in the worst case.

Third, the first paragraph of §21.6 should be replaced by the following:

> In §21.4.1 we presented a simple algorithm for square-free decomposition, along with a somewhat sloppy running-time analysis. The following exercises develop a variant whose output is in a somewhat nicer form, and with a tighter running-time analysis.

[VS, 11/1/05]

**p. 482:** Exercise 21.11. Add the following: "Assume that computing $M_1(\beta)$ for $\beta \in F[\mathtt{X}]/(h)$ takes $\Omega(\deg(h)^2 \operatorname{len}(q))$ operations in $F$". [VS, 9/26/05]

## Appendix

**p. 503:** Missing period before "One". [George Stephanides, 7/30/06]

## Bibliography

**p. 504:** Reference [7]. "infintely" should be "infinitely". [George Stephanides, 7/26/06]

**p. 505:** Line −2. "Asymptotocally" should be "Asymptotically". [George Stephanides, 7/12/06]