☆ THE ART OF COMPUTER PROGRAMMING ☆

☆☆☆☆ ERRATA TO VOLUME 2 (after 2010) ☆☆☆☆

This document is a transcript of the notes that I had been making in my personal copy of *The Art of Computer Programming*, Volume 2 (third edition, 26th printing) from the time it was printed in 2011 until the 45th printing came out in 2022. Previous errata are recorded in another file '`all2-prepre.ps`'.

Four levels of updates — "errors," "amendments," "plans," and "improvements" — appear, indicated by four different typographic conventions:

▸**Page 666** line 1 ________ 04 Jul 1776

Technical or typographical errors (aka bugs) are the most critical items, so they are flagged with a '▸' preceding the page number. The date on which I first was told about the bug is shown; this is the effective date on which I paid the finder's fee. The necessary corrections are indicated in a straightforward way. If, for example, the book says 'n' where it should have said '$n+1$', the change is shown thus:

$n \rightsquigarrow n+1$

Page 666 line 2 ________ 14 Jul 1789

Amendments to the text appear in the same format as bugs, but without the '▸'. These are things I wish I had known about or thought of when I wrote the original text, so I added them later. The date is the date I drafted the new text.

Page 666 line 3 . . . . 20 Nov 1917

Plans for the future represent a third kind of item. In such notes I sketched my intentions about things that I wasn't ready to flesh out further when I wrote them down. You can identify these items because they're written in slanted type, and preceded by a bunch of dots '. . . . .' leading to the date on which I recorded the plan in my files.

Page 666 line 4 ________ 10 Jan 1938

The fourth and final category — indicated by page and line number in smaller, slanted type — consists of minor corrections or improvements that most readers don't want to know about, because they are so trivial. You wouldn't even be seeing these items if you hadn't specifically chosen to print the complete errata list in all its gory details. Are you sure you wanted to do that?

My shelves at home are bursting with preprints and reprints of significant research results that I want to digest and summarize, where appropriate, in the ultimate edition of Volume 2. I didn't do that in the third edition because I would surely have to do it over again later: New results continue to pour forth at a great rate, and I will have time to rewrite that volume only once. Volumes 4 and 5 need to be finished first. So I've put most of my effort so far into writing up those parts of the total picture that seem to have converged to their near-final form. It follows, somewhat paradoxically, that the updates in this document are most current in the areas where there has been least activity.

On the other hand I do believe that the changes listed here bring Volume 2 completely up to date in two respects: (1) All of the research problems in the previous edition — i.e., all exercises that were rated 46 and above — have received new ratings of 45 or less whenever I learned of a solution; and in such cases, the answer now refers to that solution. (2) All of the historical information about pioneering developments has been amended whenever new details have come to my attention.

The ultimate, glorious, 100% perfect editions of Volumes 1–4 are works in progress. Please let me know of any improvements that you think I ought to make. Send your comments either by snail mail to D. E. Knuth, Computer Science, Gates Building 1B, Stanford University, Stanford CA 94305-9015, or by email to `taocp@cs.stanford.edu`*. (Use email for book suggestions only, please — all other correspondence is returned unread to the sender, or discarded, because I have no time to read ordinary email.) Although I'm working full time on Volume 4 these days, I will try to reply to all such messages within a year of receipt. Current news about The Art of Computer Programming is posted on*

`http://www-cs-faculty.stanford.edu/~knuth/taocp.html`

and updated regularly.

— Don Knuth, January 2011

Oh! If only someone would give me time, time,
time to do everything properly,
to read everything at my own *tempo,*
to take it apart and put it together again.
— KARL BARTH (1922)

☆☆☆☆☆☆ SEMINUMERICAL ALGORITHMS ☆☆☆☆☆☆

Last updated 16 August 2022

All of these corrections have been made in subsequent printings.

▸**Page 0** (on the back page of the dustcover, line 23) ——— 10 Sep 2012

Whatever your backgound, ⇝ Whatever your background,

Page vii line 5 before the author's signature ——— 23 Sep 2015

nobody noticed ⇝ nobody else noticed

Page x line 16 ——— 16 Jun 2011

a *45* rating ⇝ a *40* rating

Page x line 20 ——— 30 Jan 2013

creativity. ⇝ creativity. All exercises with ratings of *46* or more are open problems for future research, rated according to the number of different attacks that they've resisted so far.

Page xi new rating of exercise 3 ——— 24 Jan 2014

[*34*] ⇝ [*M34*]

Page 7 lines 14 and 15 ——— 28 Apr 2017

the digit he names ⇝ that digit

Page xiii new page number for Section 4.5.4 ——— 10 Jul 2018

379 ⇝ 380

Page 3 lines −15 and −14 ——— 16 Jul 2020

rap music. . . . noise.") ⇝ rap music.

Page 13 lines 1 and 2 ——— 15 Sep 2011

overflow will be on after program (2) if and only if the result equals w ⇝ the result equals w if and only if program (2) turns overflow on

Page 17 after the statement of Theorem A ——— 13 Mar 2014

The ideas ⇝ *Proof.* The ideas

Page 20 lines 8 and 14 ——— 13 May 2016

smallest integer λ ⇝ smallest positive integer λ

Page 20 new sentence at the beginning of Theorem C ——— 13 May 2016

Let p be a prime number.

Page 24 in the line before (4) ——— 14 May 2016

the least integer s ⇝ the least positive integer s

Page 34 two lines after (14) ——— 16 Sep 2014

of overhead ⇝ of additional overhead

▸**Page 39** line 1 of exercise 19 ———— 18 May 2016

[*M41*] ⇝ [*M40*]
specified in the first column ⇝ specified by the first two columns

Page 40 new exercise ———— 21 Apr 2019

38. [*20*] (H. Nakazawa, 2004.) Show that multiplicative congruential sequences with unbounded moduli can be considered to be "universal" in the following approximate sense: If $\langle x_n\rangle$ is *any* periodic b-ary sequence whatsoever, with $0 \le x_n < b$ and $x_{n+\lambda} = x_n$ for all $n \ge 0$, let $X = (x_0x_1\ldots x_{\lambda-1})_b$. Then the sequence $\langle X_n\rangle$ defined by $X_0 = X/d$, $m = (b^\lambda - 1)/d$, $d = \gcd(X, b^\lambda - 1)$, and $X_{n+1} = bX_n \bmod m$ satisfies $|X_n/m - x_n/b| < 1/b$ for all n.

Page 43 lines 9 and 10 ———— 10 May 2017

at least one that has proved to be most important ⇝ or at least one that has become traditional

Page 46 lines 13 and 14 ———— 14 Feb 2017

reject the value $V = 4.27$ ⇝ reject the value $V = \frac{64}{15} \approx 4.27$
$V \ge 4.27$ ⇝ $V \ge \frac{64}{15}$

Page 50 line 1 ———— 15 Nov 2016

following statistics: ⇝ following "supremum" statistics:

Page 56 lines 2 and 3 after (20) ———— 29 Apr 2014

over the interior of a $(k-1)$-dimensional hypersphere ⇝
over a $(k-1)$-dimensional ball

Page 56 new paragraph before the bottom three lines ———— 10 May 2017

G. Valiant and P. Valiant recently discovered, to everyone's surprise, that

$$\sum_{s=1}^{k} \frac{(Y_s - np_s)^2 - Y_s}{p_s^{2/3}} \tag{23}$$

is superior to the chi-square statistic (6). [See *SICOMP* **46** (2017), 429–455.]

Page 56 bottom line ———— 10 May 2017

[delete the equation number (23)]

Page 68 line 4 after (14) ———— 20 Apr 2019

consists of ⇝ amounts to

Page 117 line −4 ———— 02 Apr 2013

[*HM47*] (I. Borosh.) ⇝ [*HM48*] (I. Borosh and H. Niederreiter.)

Page 135 line 12 ———— 01 May 2017

beta variate ⇝ beta deviate

Page 135 line 13 ———— 23 Apr 2017

The t-distribution ⇝ *Student's t-distribution*

Page 135 line −12 ——— 29 Apr 2014

Random point on an n-dimensional sphere ⇝ *Random point on the surface of an n-dimensional ball*

Page 136 line 1 ——— 29 Apr 2014

n-sphere ⇝ n-ball

Page 136 line −10 ——— 01 May 2017

beta variate ⇝ beta deviate

Page 145 line 25 ——— 23 Feb 2012

Let X_1, X_2, ..., X_t be a set ⇝ Let $(X_1, X_2, \ldots, X_t)$ be a sequence

▸**Page 151** line −11 ——— 17 Sep 2017

exercise 5 ⇝ exercise 4

Page 153 line 1 ——— 21 Apr 2019

these integer sequences ⇝ these 2^j-ary sequences

Page 176 line −10 ——— 29 Jun 2017

no factoring algorithm ⇝ no usable factoring algorithm

Page 183 rating of exercise 39 ——— 08 Sep 2016

[*HM45*] ⇝ [*HM42*]

Page 185 and possibly 186 ——— 27 Sep 2019

just before the C code, say 'with the following C code:'
and just after it, say 'Here `X` is type `long`, ...'.

Page 188 lines 2 and 5 of the displayed program ——— 14 Sep 2019

`ran_start(310952);` ⇝ `ran_start(310952L);` (twice)

Page 189 a new quotation to insert before the exercises ——— 06 Feb 2013

Almost all good computer programs
contain at least one random-number generator.

— DONALD E. KNUTH, *Seminumerical Algorithms* (1969)

▸**Page 196** line −11 ——— 08 Jun 2011

Pratiche del calcolo ⇝ Pratiche di calcolo

▸**Page 196** line −8 ——— 20 Nov 2015

sand and/or pebbles ⇝ sand or pebbles

▸**Page 197** line −4 ——— 10 Apr 2021

never used sexagesimals ⇝ used sexagesimals only rarely

▸**Page 200** line 20 ——— 24 Jan 2013

an appendix to his little book *Rhabdologia* ⇝ part three of his little book *Rabdologiæ*

▸**Page 200** line −15 — 13 Sep 2011

K. Gehrhardt ⇝ C. I. Gerhardt

Page 203 line 15 — 23 Nov 2018

shifting right does not divide ⇝ shifting right, in the latter, does not always divide

Page 209 lines 5 and 6 — 01 Mar 2018

system, which was known in 13th-century India, ⇝ system [C.-A. Laisant, *Bull. Soc. Math. France* **16** (1888), 176–183],

Page 214 lines 20 and 21 — 28 Jun 2020

Avogadro's number …erg sec. ⇝ Avogadro's number $N = 6.02214076 \times 10^{23}\ \mathrm{mol}^{-1}$, or very small numbers like Planck's constant $h = 6.62607015 \times 10^{-34}$ J s.

Page 214 new values in (3) — 28 Jun 2020

$$\begin{aligned} &\text{Avogadro's number} \quad N = (74, +.60221408);\\ &\text{Planck's constant} \qquad h = (17, +.66260702).\end{aligned} \tag{3}$$

Page 231 line 15 — 17 Aug 2021

properly. ⇝ properly. (These laws assume, of course, that there's no overflow or underflow.)

Page 238 lines −12 thru −8 — 28 Jun 2020

For example, …would be nice ⇝ Before 2019, for example, the values of Avogadro's number and Planck's constant were not known to eight significant digits, and it would have been more appropriate to denote them, respectively, by

$$(26, +.000602214) \qquad \text{and} \qquad (-30, +.00066261)$$

instead of by $(24, +.60221408)$ and $(-33, +.66260702)$. It would be nice

Page 238 bottom two lines — 28 Jun 2020

$(1, +.00039903)$ ⇝ $(-6, +.00039903)$
$(27, +.00060221)$ ⇝ $(26, +.00602214)$

Page 240 replacement for the bottom two lines — 28 Jun 2020

$$N = \bigl[(24, +.60221407)\,..\,(24, +.60221408)\bigr],$$
$$h = \bigl[(-33, +.66260701)\,..\,(-33, +.66260702)\bigr];$$

Page 241 replacement for lines 2 and 3 — 28 Jun 2020

$$N \oplus h = \bigl[(24, +.60221407)\,..\,(24, +.60221408)\bigr],$$
$$N \otimes h = \bigl[(-9, +.39903126)\,..\,(-9, +.39903128)\bigr].$$

▸**Page 243** line 2 of exercise 7 — 31 May 2021

$2(u^{②} + v^{②})$ ⇝ $2(u^{②} \oplus v^{②})$

Page 245 new exercise ——— 17 Jan 2014

32. [*M21*] For what pairs (a, b) is round_to_even$(x) = \lfloor ax + b \rfloor + \lceil ax - b \rceil$ for all x?

Page 255 line 6 ——— 09 Apr 2015

Dept of ⇝ Dept. of

▸**Page 275** line 19 ——— 04 Apr 2011

$235M$ ⇝ $23.5M$

Page 279 new paragraph to precede part '3)' ——— 02 May 2021

N. Möller and T. Granlund, *IEEE Trans.* **C-60** (2011), 165–175, have developed highly tuned methods that work well on modern machines.

Page 280 line 26 ——— 14 Mar 2019

Stay tuned for new records as we move into a new millennium. ⇝ By 14 March 2019 the world record had risen to 31,415,926,535,897 digits(!), obtained by A. J. Yee and E. H. Iwao using the Chudnovsky formula together with exercise 39. That computation, which involved 170 terabytes of data, took 121 days on 25 cloud-based virtual machines.

▸**Page 287** lines 2 and 3 ——— 10 Apr 2021

Sun Tsŭ, who gave ... 473. ⇝ Sun Tsŭ, probably some time after A.D. 280 and some time before A.D. 473.

Page 287 lines 7 and 8 ——— 10 Apr 2021

(1247); the latter ... exercise 3. ⇝ (1247). Ch'in called it ta-yen-shu (the "great generalization procedure"), and considered also the case where the moduli might have common factors, as in exercise 3.

▸**Page 290** line −4 ——— 14 Sep 2019

$(u_1, \ldots, u_r)$ is less than $(u'_1, \ldots, u'_r)$ ⇝ $(v_1, \ldots, v_r)$ is less than $(v'_1, \ldots, v'_r)$

Page 293 line 4 of exercise 13 ——— 26 Nov 2012

218 ⇝ **218**, 1

Page 295 line −13 ——— 15 Nov 2016

in *Doklady Akad. Nauk SSSR* **145** (1962), 293–294 [English ⇝
[see *Doklady Akad. Nauk SSSR* **145** (1962), 293–294; English

Page 295 line −11 ——— 12 Nov 2018

before 1962 ⇝ before 1960

Page 308 line −16 ——— 12 Mar 2015

column for $\hat{v}_s$ ⇝ column for $2^7 \hat{v}_s$

Page 311 new paragraph following line 25 ——— 16 Sep 2021

In fact, $O(n \log n)$ bit operations suffice also in the ordinary Turing machine model, as shown in 2019 by D. Harvey and J. van der Hoeven [*Ann. Math.* **191** (2021), 563–617], using asymptotically fast transforms on multivariate polynomials.

Page 311 near the bottom ______________________________ 02 Mar 2011

Supercomputing **2** (1988) $\leadsto$ *Supercomputing* **2** (International Supercomputing Institute, 1988)

Page 323 replacement for the bottom 19 lines ______________________________ 10 Jul 2018

ber, inserting a radix point after the leading digit. Then at the kth step, double the leading digits left of the point, using decimal arithmetic; and subtract this from the leading digits after shifting the point right, again using decimal arithmetic. The process terminates in m steps if the given number has $m+1$ digits. The radix point clarifies which digits are to be doubled.

Example 1. Convert $(\mathit{1234567})_8$ to decimal.

$$
\begin{array}{cccccccc}
 & 1. & \mathit{2} & \mathit{3} & \mathit{4} & \mathit{5} & \mathit{6} & \mathit{7} \\
- & & 2 & & & & & \\
\hline
 & 1 & 0. & \mathit{3} & \mathit{4} & \mathit{5} & \mathit{6} & \mathit{7} \\
- & & 2 & 0 & & & & \\
\hline
 & & 8 & 3. & \mathit{4} & \mathit{5} & \mathit{6} & \mathit{7} \\
- & & 1 & 6 & 6 & & & \\
\hline
 & & 6 & 6 & 8. & \mathit{5} & \mathit{6} & \mathit{7} \\
- & & 1 & 3 & 3 & 6 & & \\
\hline
 & & 5 & 3 & 4 & 9. & \mathit{6} & \mathit{7} \\
- & & 1 & 0 & 6 & 9 & 8 & \\
\hline
 & & 4 & 2 & 7 & 9 & 8. & \mathit{7} \\
- & & & 8 & 5 & 5 & 9 & 6 \\
\hline
 & & 3 & 4 & 2 & 3 & 9 & 1
\end{array}
\qquad \textit{Answer:}\ (342391)_{10}.
$$

Page 324 lines 5 and 6 ______________________________ 10 Jul 2018

$1+4+\cdots\ 36 \leadsto 3+4+2+3+9+1=22$, and $7-6+5-4+3-2+1=4$; the difference is 18

Page 324 replacement for lines 15–34 ______________________________ 10 Jul 2018

Converting decimal integers to octal. A similar procedure can be used for the opposite conversion: Write down the given decimal number, inserting a radix point after the leading digit. Then at the kth step, double the leading digits left of the point, using *octal* arithmetic; and *add* these to the leading digits after shifting the point right, again using *octal* arithmetic. The process terminates in m steps if the given number has $m+1$ digits.

Example 2. Convert $(342391)_{10}$ to octal.

$$\begin{array}{cccccccc}
 & & \mathit{3}. & 4 & 2 & 3 & 9 & 1 \\
+ & & & \mathit{6} & & & & \\ \cline{3-4}
 & & \mathit{4} & \mathit{2}. & 2 & 3 & 9 & 1 \\
+ & & \mathit{1} & \mathit{0} & \mathit{4} & & & \\ \cline{3-5}
 & & \mathit{5} & \mathit{2} & \mathit{6}. & 3 & 9 & 1 \\
+ & & \mathit{1} & \mathit{2} & \mathit{5} & \mathit{4} & & \\ \cline{3-6}
 & & \mathit{6} & \mathit{5} & \mathit{3} & \mathit{7}. & 9 & 1 \\
+ & & \mathit{1} & \mathit{5} & \mathit{2} & \mathit{7} & \mathit{6} & \\ \cline{2-7}
 & \mathit{1} & \mathit{0} & \mathit{2} & \mathit{6} & \mathit{7} & \mathit{7}. & 1 \\
+ & & \mathit{2} & \mathit{0} & \mathit{5} & \mathit{5} & \mathit{7} & \mathit{6} \\ \cline{2-8}
 & \mathit{1} & \mathit{2} & \mathit{3} & \mathit{4} & \mathit{5} & \mathit{6} & \mathit{7}
\end{array}
\qquad \textit{Answer: } (\mathit{1234567})_8.$$

(Notice that the nonoctal digits 8 and 9 might enter into this octal computation.)

Page 327 new paragraph before the exercises ——— 02 May 2021

See T. Granlund and P. L. Montgomery, *SIGPLAN Notices* **29**, 6 (June 1994), 61–72, for state-of-the-art techniques that convert binary integers to decimal strings without division.

Page 328 replacement for exercise 11 ——— 11 Jul 2018

11. [*18*] Convert $(\mathit{21446})_8$ to decimal, and back again to octal.

Page 329 exercise 19 is now "recommended" ——— 06 Sep 2013

19. ⇝ ▸ **19.**

Page 334 line -2 ——— 17 Mar 2015

2250 years ⇝ 2300 years

Page 339 lines 1 and 2 after Fig. 9 ——— 06 Sep 2013

just a little more code than for Algorithm A. ⇝ a bit more code than for Algorithm A, but the steps are elementary.

Page 343 lines 13 and 14 ——— 20 Apr 2021

can be traced to . . . Northern India ⇝ can be traced to the *Āryabhaṭīya* (c. 500) by Āryabhaṭa of northern India

Page 351 in (58) ——— 22 Mar 2021

B_k ⇝ $(-1)^k B_k$

Page 352 replacement for the paragraph that contains (61) ——— 08 Feb 2016

All of these calculations are highly plausible, but they rely on unproved assumptions. By introducing a slightly different model, and applying deep methods from the theory of dynamical systems, Brigitte Vallée was finally able to complete the first rigorous analysis of Algorithm B [see *Algorithmica* **22** (1998), 660–685]. Her results led her to suspect that the constants λ and b might be related by the remarkable formula

$$\frac{\lambda}{b} \;=\; \frac{2\ln 2}{\pi^2}\,; \tag{61}$$

and indeed, she was right! More than a decade later, Ian D. Morris found a proof of (61), as a byproduct of an analytic *tour de force* with which he successfully demonstrated the complete validity of Brent's model [see exercise 34].

Page 355 replacement for exercise 31 ——— 08 Feb 2016

31. [*HM46*] Prove or disprove the "wild conjecture" in the answer to exercise 25.

Page 355 replacement for exercise 34 ——— 08 Feb 2016

34. [*HM44*] Find a rigorous proof that Brent's model describes the asymptotic behavior of Algorithm B, and indeed that $G(z)$ is an analytic function when $\Re z > 0$.

Page 367 replacement for line -8 ——— 18 Sep 2011

Furthermore $r_n \le |\mathcal{I} \cap P_n| \le r_n + t_n$, because $\mathcal{I}_N \subseteq \mathcal{I} \subseteq \mathcal{I}_N \cup \mathcal{K}$. Consequently

Page 367 replacement for line -5 ——— 18 Sep 2011

Given ϵ, this holds for all n; so $\lim_{n\to\infty} r_n/n = \lim_{n\to\infty}(r_n + t_n)/n = \mu(\mathcal{I})$. ▮

▸**Page 378** and 379, in the 2019 printings only ——— 01 Jan 2020

[The first two lines of exercise 4.5.3–43, quoted here, were mistakenly dropped when the new exercise 4.5.3–52 was added.]

43. [*M30*] (D. W. Matula.) Show that the "mediant rounding" rule for fixed slash or floating slash numbers, Eq. 4.5.1–(1), can be implemented simply as follows, when

Page 379 new exercise ——— 10 Jul 2018

▸**52.** [*M21*] (A. Ostrowski, 1922.) Let a_1, a_2, $\ldots$ be a sequence of positive integers, and let $q_n = K_n(a_1, \ldots, a_n)$ as in exercise 42 and other exercises. Prove that every nonnegative integer n has a unique representation of the form

$$n = c_0q_0 + c_1q_1 + c_2q_2 + \cdots, \qquad 0 \le c_k \le a_{k+1},$$

where $c_k = a_{k+1}$ implies that $k > 0$ and $c_{k-1} = 0$. (When $a_k = 1$ for all k, this is the Fibonacci number system of exercise 1.2.8–34.)

Page 382 replacement for (5) ——— 09 Dec 2011

$$\pi(x) \;\approx\; \sum_{k=1}^{\lg x} \frac{\mu(k)}{k} L\bigl(\sqrt[k]{x}\,\bigr) \;=\; L(x) - \frac{1}{2}L\bigl(\sqrt{x}\,\bigr) - \frac{1}{3}L\bigl(\sqrt[3]{x}\,\bigr) + \cdots \tag{5}$$

Page 387 line 10 ——— 20 Apr 2019

consists of searching $\rightsquigarrow$ searches

Page 404 line 18 ——— 06 Nov 2011

is between 0 and N $\rightsquigarrow$ lies in the range $0 \le x_i < N$

Page 404 line 22 ——— 05 Oct 2011

$(x^3)^d \bmod N = x$ $\rightsquigarrow$ each secret component $(x_i^3 \bmod N)^d \bmod N = x_i$

Page 409 another Mersenne prime ——— 16 Feb 2013

[add '57885161' to (26), and use it instead of 43112609 in the remarks below, noting that $2^{57885161} - 1$ has 17,425,170 decimal digits]

Page 409 well, yet another Mersenne prime ——— 15 Apr 2016

[add '74207281' to (26), and use it instead of 43112609 in the remarks below, noting that $2^{74207281} - 1$ has 22,338,618 decimal digits]

Page 409 and the 50th and 51st ——— 24 Apr 2019

[add '77232017' and '82589933' to (26), and use the latter instead of 74207281 in the remarks below, noting that $2^{82589933} - 1$ has more then 24 million decimal digits]

Page 417 replacement for lines 3–9 of exercise 47 ——— 23 Oct 2012

```
(8372e6cadf564a9ee347092daefc242058b8044228597e5f2326bbbff1583ea4200d895d9564d39229c79af8
 72a72e38bb92852a22679080e269c30690fab0ec19f78e9ef8bae74b600f4ebef42a1dd5a6d806dc70b96de2
 bf4a6c7d2ebb51bfd156dd8ac3cb0ae1c1c38d76a3427bcc3f12af7d4d04314c0d8377a0c79db1b1f0cd1702,
 2aabcd0f9f1f9fb382313246de168bae6a28d177963a8ebe6023f1c5bd8632caee9604f63c6a6e33ceb1e1bd
 4732a2973f5021e96e05e0da932b5b1d2bc618351ca584bb6e49255ba22dca55ebd6b93a9c94d8749bb53be2
 90650878b17f4fe30bbb08453929a94a2efe3367e2cd92ea31a5e0d9f466870b162272e9e164e8c3238da519)
```

in hexadecimal notation, where N is

```
c97d1cbcc3b67d1ba197100df7dbd2d2864c4fef4a78e62ddd1423d972bc7a420f66046386462d260d68a8b2
3fbf12354705d874f79c22698f750c1b4435bc99174e58180bd18560a5c69c4eafb573446f79f588f624ec18
4c3e7098e65ac7b88f89e1fadcdc3558c878dde6bc7c32be57c5e7e8d95d697ad3c6c343485132dcbb74f411.
```

Page 424 line 18 ——— 30 Jan 2022

Pedro Nuñez $\leadsto$ the Portuguese mathematician Pedro Nuñez

Page 424 line −15 ——— 30 Jan 2022

Simon Stevin $\leadsto$ the Flemish mathematician Simon Stevin

Page 435 lines 6 and 7 ——— 09 Mar 2013

derived by C. L. Dodgson (aka Lewis Carroll) from a theorem of Jacobi, is also highly relevant to these methods. $\leadsto$ *published in 1853 by Felice Chiò and rediscovered by C. L. Dodgson (aka Lewis Carroll), is also highly relevant.*

Page 435 line 8 ——— 03 Mar 2021

paper #R5, §3 $\leadsto$ *#R5, 1–13, §3*

▸**Page 453** replacement for line 5 ——— 22 Apr 2012

$$\deg(v_{i_1}) + \cdots + \deg(v_{i_d}) \in \bigcap D_j.$$

Page 453 line 24 ——— 22 Jan 2015

in practice. $\leadsto$ in practice. Mark van Hoeij [*J. Number Theory* **95** (2002), 167–189] has found an efficient way to apply LLL when those heuristics fail; its running time depends on r, not n.

▸**Page 478** line 6 ——— 30 Aug 2011

$c(33) \leadsto c(39)$

Page 478 lines −11 through −5 — 30 Aug 2011

Computer calculations ... Arnold Scholz ⇝
Notice that 2^n-1 is the worst case for the binary method, because $\nu(2^n-1)=n$. E. G. Thurber [*Discrete Math.* **16** (1976), 279–289] has shown that several of these values, including the case $n=32$, can actually be calculated by hand. Computer calculations by Neill Clift [*Computing* **91** (2011), 265–284] show that $l(2^n-1)$ is in fact exactly equal to $n-1+l(n)$ for $1\le n\le 64$. Arnold Scholz

▸**Page 478** line −3 — 30 Mar 2011

deutschen ⇝ *Deutschen*

▸**Page 482** line 2 of exercise 11 — 16 Apr 2015

all i in the chain ⇝ all a_i in the chain

Page 490 line 6 after (9) — 29 Apr 2013

savings is worthwhile ⇝ change is worthwhile

Page 496 better wording in lines 17–19 — 13 Sep 2019

complete the proof, ... possible ⇝ complete the proof; but we must be careful because the polynomials that are obtained, as $\beta_1, \ldots, \beta_{q+1}$ range over all real values, may not include all polynomials that are representable by the original chain (see exercise 26). It is possible

Page 501 lines 1–3 — 01 Aug 2017

The best ... $2n^2-1$ ⇝ Exercise 67 discusses how Coppersmith and Winograd [*SICOMP* **11** (1982), 472–492] lowered this further, eventually leading to $O(n^{2.373})$. By contrast, the best current lower bound is $3n^2-O(n^2/\log n)$ (see exercise 12).

Page 523 rating of exercise 68 — 08 Sep 2016

[*M45*] ⇝ [*M46*]

Page 524 last line of exercise 73 — 16 Feb 2011

steps. ⇝ steps. How big can their determinants be?

Page 537 a new quotation to append here — 03 Dec 2012

This business of series, the most disagreeable thing in mathematics,
is no more than a game for the English;
Stirling's book, and the one by de Moivre, are proof.

— PIERRE DE MAUPERTUIS, letter to d'Ortous de Mairan (30 Oct 1730)

Page 537 another new quotation to append here — 23 Oct 2012

He was daunted and bewildered by their almost infinite series.

— G. K. CHESTERTON, *The Man Who Was Thursday* (1907)

Page 538 line 2 of answer 3 — 24 Jan 2014

422481^4. ⇝ 422481^4 and (therefore) $191600^4+435038^4+829120^4=844962^4$.

Page 547 line 11 of answer 14 ______ 13 May 2016

$x_{j \bmod \lambda}$, where $\rightsquigarrow$ $x_{j \bmod \lambda}$, where λ is the least positive integer with

Page 548 line 6 of answer 11 ______ 01 Nov 2018

maximum period $\rightsquigarrow$ maximum order

Page 551 line 2 ______ 14 May 2016

$Y_{n+1} \approx$ $\rightsquigarrow$ $Y_{n+1} =$

▶**Page 554** line −4 of answer 11 ______ 28 Apr 2017

A_{n+p} $\rightsquigarrow$ $A_{n+p\lambda}$

Page 555 new answer ______ 05 Sep 2013

20. For $k = 64$ one can use `CONTENTS(A)` = $(\texttt{243F6A8885A308D3})_{16}$ (the bits of π!).

Page 559 new answer ______ 21 Apr 2019

38. In fact [`www10.plala.or.jp/h-nkzw/04eprsq1.pdf`], $bX_n = mx_n + X_{n+1}$ for all n.

Page 564 line 4 ______ 10 May 2017

following Eq. 3.3.1–(23) $\rightsquigarrow$ preceding Eq. 3.3.1–(24)

Page 569 top half of page ______ 22 Mar 2021

line 6 and line 13: k^l $\rightsquigarrow$ $(-k)^l$
line 8: $1 - e^{-z}$ $\rightsquigarrow$ $e^z - 1$
line 11: $\frac{n(n+1)}{2}B_1$ $\rightsquigarrow$ $-\frac{n(n+1)}{2}B_1$

▶**Page 579** bottom line ______ 10 Jul 2012

5 (1848) $\rightsquigarrow$ **13** (1848)

Page 584 line 5 of answer 31 ______ 02 Apr 2013

172. $\rightsquigarrow$ 172, and an excellent survey of later work has been prepared by A. Kontorovich in *Bull. Amer. Math. Soc.* **50** (2013), 187–228.

▶**Page 584** line −3 of answer 31 ______ 02 Apr 2013

BIT **25** (1980), 193–208 $\rightsquigarrow$ *BIT* **23** (1983), 65–74

Page 591 lines 6 and 7 of answer 8 ______ 17 Sep 2011

$(N-j-k)/(N-j)$ $\rightsquigarrow$ $\bigl((N-j-k)/(N-j)\bigr)$

▶**Page 608** line 15 of answer 24 ______ 22 Aug 2019

(3) **18** (1978), 581–595 $\rightsquigarrow$ (3) **37** (1978), 213–229

Page 611 replacement for answer 1 ______ 28 Jun 2020

1. $N = (62, +.60\ 22\ 14\ 08)$; $h = (34, +.06\ 62\ 60\ 70)$. Note that the quantity $10h$ would be $(34, +.66\ 26\ 07\ 02)$.

Page 614 last line of answer 7 ______ 31 May 2021

$u^{②} + v^{②} = (.10\ldots011)_2$ $\rightsquigarrow$ $u^{②} + v^{②} = (.10\ldots011)_2 = u^{②} \oplus v^{②}$

Page 614 lines 3–4 of answer 15 ______ 14 Sep 2019

there are numbers $v \neq w$ such that $v \oplus v = w \oplus w$ $\rightsquigarrow$ there are numbers v such that $(v \oplus v) \oslash 2 \neq v$

▶**Page 615** line −2 — 05 Mar 2021

$s_n \ominus c_n \leadsto s_n - c_n$

Page 617 in answer 29 — 29 Dec 2019

$\hat{h} \leadsto h$ (twice)

Page 617 new answer — 17 Jan 2014

32. (J. Ziegler Hunts, 2014.) $a = 1/2$ and $b \bmod 1 = 1/4$.

▶**Page 618** first line of answer 5 — 24 Nov 2012

lines 22 $\leadsto$ lines 23

▶**Page 618** line 4 of answer 7 — 24 Nov 2012

.99999999 $\leadsto$ −.99999999

▶**Page 619** line −2 of answer 8 — 24 Nov 2012

better then $\leadsto$ better than

▶**Page 626** line *008* of answer 25 — 04 Apr 2011

`V+N+1` $\leadsto$ `TEMP` and $(v+1) \leadsto (v_{n-1}+1)$

▶**Page 626** lines *110* and *111* of answer 26 — 04 Apr 2011

`DEC2` $\leadsto$ `DEC1` and $j+1 \leadsto j-1$ and `J2NN` $\leadsto$ `J1NN`

▶**Page 632** in answer 14 — 31 Jul 2020

$w = \sum_{k=0}^{n-1} t_k a_k 2^{kq/n}$ where $t_k \approx z_k/a_k \leadsto w = \sum_{k=0}^{n-1} t_k a_k 2^{kq/n-1}$ where $t_k \approx 2z_k/a_k$
from those integers. $\leadsto$ from those integers, although overlapping bit sequences must be added together before reducing mod $2^q - 1$.

▶**Page 633** line 5 of answer 4 — 09 Jul 2012

$\frac{1}{2}(W(j) - W(-j)) \leadsto (W(j) - W(-j))/(2j)$.

Page 634 first lines of answer 15 — 07 Aug 2020

The best upper bound known ... pointer machines. $\leadsto$ M. J. Fischer and L. J. Stockmeyer achieved time $O\bigl(n(\log n)^2 \log\log n\bigr)$ [*J. Comp. and Syst. Sci.* **9** (1974), 317–331]; their construction works on multitape Turing machines, and it is $O(n \log n)$ on pointer machines. That upper bound was improved to $O\bigl(n \log n\, e^{\sqrt{\ln 4}\sqrt{\ln\ln n}} \sqrt{\ln\ln n}\bigr)$ by J. van der Hoeven [*Int. Symp. Symbolic and Algebraic Comp.* **39** (2014), 405–412].

Page 634 last line of answer 16 — 21 Nov 2020

$K(-1) = 1$ and $K(1) = \frac{1}{5}$. $\leadsto$ $K(-2) = 2$, $K(-1) = 1$, and $K(1) = \frac{1}{5}$, if we're cavalier about convergence.

Page 635 line 1 of answer 3 — 19 Feb 2011

Jon L. White $\leadsto$ Jon L White

Page 637 replacement for answer 11 —— 11 Jul 2018

11.

$$
\begin{array}{rr}
 & 2.1446 \\
- & 4 \\ \hline
 & 17.446 \\
- & 34 \\ \hline
 & 140.46 \\
- & 280 \\ \hline
 & 1124.6 \\
- & 2248 \\ \hline
 & 8998
\end{array}
\qquad \textit{Answer: } (8998)_{10}.
\qquad\qquad
\begin{array}{rr}
 & 8.998 \\
+ & 20 \\ \hline
 & 131.98 \\
+ & 262 \\ \hline
 & 1603.8 \\
+ & 3406 \\ \hline
 & 21446
\end{array}
\qquad \textit{Answer: } (21446)_{8}.
$$

Page 643 line 2 of answer 27 —— 22 Mar 2021

$B_l \leadsto (-1)^l B_l$

Page 645 replacement for answer 34 —— 08 Feb 2016

34. Ian D. Morris [*Advances in Mathematics* **290** (2016), 73–145, whose function $\xi(z)$ is $G'(z)$] has successfully resolved this long-standing problem by applying and extending delicate methods of dynamical systems theory. Thus the problem of analyzing the binary gcd algorithm, now solved rigorously by Valleé and Morris in two quite different ways, continues to lead to ever more tantalizing questions of higher mathematics.

Page 645 line 3 of answer 36 —— 23 Dec 2020

representation. Notice $\leadsto$ representation, and it arises in diverse applications. See H. Brocard, *Nouvelle Corresp. Math.* **6** (1880), 146. Notice

▶**Page 645** line −2 —— 13 Dec 2013

simulated odd operand $\leadsto$ simulated even operand

Page 646 line 1 of answer 39 —— 23 Jan 2014

Penk.) $\leadsto$ Penk.) Assume that u and v are positive.

Page 646 line −2 of answer 39 —— 20 May 2015

Computers and Math. **14** (1987), 233 $\leadsto$ *Computers and Mathematics with Applications* **14** (1987), 233–238

Page 654 lines 9–10 of answer 40 —— 16 May 2017

by M. A. Stern ... *Crelle* $\leadsto$ by G. Eisenstein, who described them on 14 January 1850 in a letter to his friend M. A. Stern [see Eisenstein's *Mathematische Werke* **2** (1975), 819]. Stern developed the ideas in *Crelle*

Page 657 new answer —— 10 Jul 2018

52. Induction. [See *Abhandlungen Math. Sem. Hamburg* **1** (1922), 77–98, 249–250.]

Page 658 in the top paragraph —— 22 May 2015

$= 1.98277\sqrt{m} \leadsto \approx 1.98277\sqrt{m}$ and $\sim 1.92600\sqrt{m} \leadsto \approx 1.92600\sqrt{m}$

▶**Page 663** line 2 of answer 25 —— 10 Dec 2011

if $n \leadsto$ if x

▶**Page 667** last line of answer 41 —— 25 May 2015

impracticably large. $\leadsto$ impracticably large.]

Page 671 new answer ——— 23 Oct 2012

47. Earlier printings of this book had a 211-digit N, which was cracked in 2012 using the elliptic curve method and the general number field method by Greg Childers and about 500 volunteers(!).

Page 675 line 4 ——— 17 Jan 2022

$x_j - s_k \mid s_k \in S_j$ ⇝ $x_j - s_{jk} \mid s_{jk} \in S_j$

Page 683 line 10 ——— 30 May 2015

Graeffe, *Auflösung* ⇝ Gräffe, *Die Auflösung*

Page 691 in answer 2 ——— 16 Sep 2014

line 25: $L = \lambda(n)$ ⇝ $L = \lambda n = \lfloor \lg n \rfloor$
line 26: $K = \nu(n)$ ⇝ $K = \nu n$

Page 700 lines 7–16 ——— 05 Feb 2021

is 100 noncommutative ... following (36). ⇝ is 98 noncommutative multiplications, by A. Sedoglavic and A. V. Smirnov [see arXiv:2101.12568 [cs.CC] (2021), 8 pages]. The best lower bound known so far is due to J. M. Landsberg, A. Massarenti, and E. Raviolo, who showed that $m \times n$ by $n \times n$ multiplication requires at least $(2 - 1/p)mn + n^2 - (2\binom{2p-2}{p} - \binom{2p-4}{p-2} + 2)n$ nonscalar multiplications, for any $p \le n$. [See *SICOMP* **43** (2014), 144–149; arXiv:1211.6320 [cs.CC] (2013), 10 pages.] Setting $m = n$ and $p \approx \frac{1}{2}\lg(n/\lg n)$ gives the asymptotic lower bound $3n^2 - O(n^2/\log n)$.

The best upper bounds known for large n are discussed in answer 67.

▸**Page 709** line −3 ——— 15 Jun 2015

one of the F's or S's ⇝ one of the F's or s's

Page 714 line 6 of answer 60 ——— 05 Feb 2021

method of Makarov ⇝ method of Sedoglavic and Smirnov

▸**Page 715** replacement for lines 2, 3, 4 of answer 64 ——— 21 Dec 2011

$(x_{k1} + u^2 x_{k2})(y_{2k} + u^2 y_{1k}) z_{kk} + (x_{k1} + u^2 x_{k3}) y_{3k}((1+u)z_{kk} - u(z_{1k} + z_{2k} + z_{3k})) - x_{k1}(y_{2k} + y_{3k})(z_{k1} + z_{k2} + z_{k3})$ and $g_{jk}(u) = (x_{k1} + u^2 x_{j3})(y_{3k} + u y_{1j})(z_{kj} + u z_{jk}) + (x_{k1} + u^2 x_{j2})(y_{2k} - u y_{1j}) z_{kj}$. [The best upper bound known for $(T(3,3,3))$ is 23;

Page 717 replacement for last paragraph of answer 67 ——— 16 Sep 2021

[Sophisticated refinements yield $\omega < 2.3729$. See *J. Symbolic Comp.* **9** (1990), 251–280; A. Ambainis, Y. Filmus, and F. Le Gall, *STOC* **47** (2015), 585–593; J. Alman and V. Vassilevska Williams, *SODA* **32** (2021), 522–539.]

Page 728 in Table 3 (the value of B_1) ——— 21 Mar 2021

$-1/2$ ⇝ $1/2$

Page 730 through page 734 ——— 07 Apr 2012

[replace the notation $(R \Rightarrow x;\ y)$ by $(R?\ x\colon y)$ in fourteen places]

Page 731 Bernoulli number entry ——— 21 Mar 2021

$(e^z - 1)$ ⇝ $(1 - e^{-z})$

Page 735 and 736 new entries for Appendix C ——— 17 Apr 2011

Program 4.3.1A′, 623.
Program 4.3.1B, 624.
Program 4.5.2A′, 373.

▸**Page 735** in Appendix C ——— 17 Apr 2011

Algorithm 3.3.4S, 101–103.
Program 4.2.3D, 251–252.
Program 4.3.1D, 273–275, 626.
Algorithm 4.5.4F, 659–660.
Theorem 4.6.4C, 496.
Theorem 4.6.4W, 513–514.

Page 737 and following ——— 01 Jan 2011

Miscellaneous changes to the existing index of Volume 2 are collected here, including corrections and amendments to the old entries as well as new entries that are occasioned by the new material. Thus, the lines of the full index that have changed serve also as an index to the present document. However, when a correction or amendment has caused an old index entry to be deleted, the deletion is usually not indicated.