☆ THE ART OF COMPUTER PROGRAMMING ☆

☆☆☆☆ ERRATA TO VOLUME 2 (3rd edition) ☆☆☆☆

This document is a transcript of the notes that I have been making in my personal copy of *The Art of Computer Programming*, Volume 2 (third edition) since it was first printed in 1997.

Three levels of updates — "errors," "amendments," and "plans" — appear, indicated by three 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.

My personal file of updates also includes a fourth category of items, not shown in this list. They are miscellaneous minor corrections or improvements that most readers don't want to know about, because they are so trivial. If you really want to see all of the gory details, you can download the full list from Internet webpage

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

by selecting the "long form" of the errata.

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, future editions of Volumes 1–3 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 4B, Stanford University, Stanford CA 94305-9045, 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, September 1997

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 31 October 2008

Most of these corrections have already been made in recent printings.

Page vii line 17 ——— 28 Oct 2008

cheerfully pay \$2.56 ⇝ cheerfully award \$2.56

▸**Page xii** line 11 ("General Test Procedures") ——— 22 Dec 1997

41 ⇝ 42

Page 2 a new paragraph near the top ——— 27 Feb 2004

f) *Cryptography.* A source of unbiased bits is crucial for many types of secure communications, when data needs to be concealed.

[Now relabel the paragraphs about "aesthetics" and "recreation."]

Page 3 lines 11–13 ——— 05 Sep 2004

[See the articles by Kendall ... 61. See also S. H. Lavington's ⇝ [F. N. David describes the early history in *Games, Gods, and Gambling* (1962). See also Kendall ... 61; S. H. Lavington's

Page 9 exercise 19 ——— 08 May 2005

[*M48*] Solve the problems of exercises 11 through 15 ⇝ [*HM47*] Solve the problems of exercises 11 through 15 asymptotically

Page 9 the rating of exercise 21 ——— 05 Apr 2007

[*42*] ⇝ [*40*]

▸**Page 12** line −4 ——— 26 Oct 1998

(See exercise 3.) ⇝

▸**Page 16** line 5 ——— 29 Dec 1997

do not to provide ⇝ do not provide

▸**Page 17** line 21 ——— 03 Jan 2002

383–389 ⇝ 163–167

▸**Page 18** line 11 ——— 26 Jan 2001

length λ of ⇝ length λ of the period of

Page 26 new copy for exercise 8 ——— 27 Feb 2004

Let $Y_n = \lfloor 10X_n/2^{35} \rfloor$ ... much more often ⇝
Let $Y_n = \lfloor 20X_n/2^{35} \rfloor$; then Y_n should be a random integer between 0 and 19, and the triples $(Y_{3n}, Y_{3n+1}, Y_{3n+2})$ should take on each of the 8000 possible values from $(0,0,0)$ to $(19,19,19)$ with nearly equal frequency. But with 1,000,000 values of n tested, many triples never occurred, and others occurred much more often

▸**Page 29** line −15 ——— 04 Jan 1998

came as shock $\leadsto$ came as a shock

Page 31 line 8 ——— 18 Oct 2006

Section 7.1 $\leadsto$ Section 7.1.3

▸**Page 33** line −2 ——— 29 Dec 1997

from (12) $\leadsto$ from (13)

▸**Page 48** line 4 after Fig. 3 ——— 20 Nov 1997

random fracton $\leadsto$ random fraction

▸**Page 54** bottom line ——— 07 Feb 2000

every few microseconds $\leadsto$ every few milliseconds

▸**Page 69** line −2 ——— 30 Apr 2008

$-6C^{-1}$ $\leadsto$ $-6C_1^{-1}$

▸**Page 72** line 5 ——— 22 Apr 2002

8 (1990) $\leadsto$ **9** (1990)

▸**Page 74** line 21 ——— 03 Oct 2008

(*Proc. Royal* $\leadsto$ [*Proc. Royal*

▸**Page 78** exercise 24 ——— 03 Feb 2005

line 1: [*HM35*] $\leadsto$ [*HM37*]
line 7: $N(\alpha)$ $\leadsto$ $N(\alpha)^2$ (twice)

▸**Page 81** replacement for line −6 ——— 08 Nov 1997

$$\delta(x) = \lfloor x \rfloor + 1 - \lceil x \rceil = [x \text{ is an integer}]; \qquad (6)$$

Page 82 the line following (10) ——— 13 Jun 2001

exercise 2 $\leadsto$ exercises 1.2.4–38 and 1.2.4–39(a,b,g)

▸**Page 89** line −13 ——— 25 Jul 2005

(1978) $\leadsto$ (1977)

▸**Page 90** line 4 ——— 25 Feb 1999

$\sum_{j=1}^{t} a_t$ $\leadsto$ $\sum_{j=1}^{t} a_j$

Page 90 new exercise ——— 13 Jun 2001

[Renumber exercise 3 as exercise 2, delete the former exercise 2, and insert the following new material:]

3. [*M23*] (N. J. Fine.) Prove that $\bigl|\sum_{k=0}^{n-1}((2^k x + \frac{1}{2}))\bigr| < 1$ for all real numbers x.

▸**Page 92** rating of exercise 23 ——— 28 Apr 1999

[*28*] $\leadsto$ [*M28*]

Page 103 lines 6–8 of step S7 ________ 25 Aug 1999

In hundreds ... dimensions. $\rightsquigarrow$ Usually $|z_j| \le 1$, but L. C. Killingbeck noticed in 1999 that larger values occur for about 0.00001 of all multipliers when $m = 2^{64}$.

Page 106 improvement to Table 1 ________ 02 May 2004

L. C. Killingbeck has carried out an exhaustive search of all multipliers $a \equiv 1 \bmod 4$ when $m = 2^{32}$. He found that the multiplier $a = 2650845021$ has $\nu_2^2 = 4938969760$, $\nu_3^2 = 2646962$, $\nu_4^2 = 68342$, $\nu_5^2 = 8778$, and $\nu_6^2 = 1506$, so it outperforms the other multipliers listed for this modulus. Indeed, its spectacular μ scores $(3.61, 4.20, 5.37, 8.85, 4.11)$ exceed all values of μ_2, μ_3, μ_4, and μ_5 for any modulus in the entire table.

▸**Page 107** line number 25 of the table ________ 20 Nov 1998

15.6 $\rightsquigarrow$ 14.6

▸**Page 115** line 1 of exercise 8 ________ 16 Feb 1999

[*M16*] Line 18 $\rightsquigarrow$ [*M18*] Line 10

Page 117 last line of exercise 23 ________ 05 Jan 2001

Alekseev $\rightsquigarrow$ Alexeev

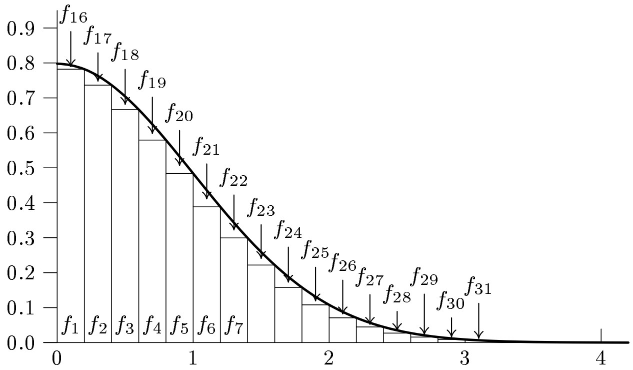
▸**Page 122** line −4 ________ 30 Sep 2003

0.587 $\rightsquigarrow$ 0.590

▸**Page 122** replacement for line −3 ________ 07 Feb 2000

P4. [Compute X_1, X_2.] If $S = 0$, set $X_1 \leftarrow X_2 \leftarrow 0$; otherwise set

▸**Page 124** replacement for Figure 9 ________ 07 Feb 2000



▸**Page 127** line −6 ________ 02 Dec 1999

$15 \le j \le 31 \rightsquigarrow 16 \le j \le 31$

▸**Page 128** in Table 1 ________ 28 Jul 2000

the value of Y_4: $-33.13 \rightsquigarrow -33.16$
the value of Y_5: $-39.55 \rightsquigarrow -39.51$
the value of Y_9: $0.00 \rightsquigarrow$

the value of Z_4: 34.93 $\rightsquigarrow$ 34.96
the value of Z_5: 41.35 $\rightsquigarrow$ 41.31
the value of Z_9: 0.00 $\rightsquigarrow$

▸**Page 129** replacement for lines −3 and −2 ——— 30 Sep 2003

Otherwise set V to a new uniform deviate; and repeat step F4 if the new V is $\le U$. Otherwise (that is, if K is even, in the discussion above), replace U by a new uniform deviate $(.b_0 b_1 \ldots b_t)_2$ and go back to F3.

Page 132 new paragraph following line 15 ——— 21 Mar 2005

With an improved approximation to the acceptance region [see J. L. Leva, *ACM Trans. Math. Software* **18** (1992), 449–455] we can, in fact, reduce the expected number of logarithm computations to only 0.012.

▸**Page 135** line −16 ——— 23 Mar 1999

$(1-2\nu) \rightsquigarrow (1-2/\nu)$

▸**Page 139** exercise 12 ——— 19 Oct 1999

$f(x) < f(y) \rightsquigarrow f(x) > f(y)$

Page 140 bottom line ——— 19 May 2005

$X_1 \lor (X_2 \land (X_3 \lor (X_4 \land X_5))) \rightsquigarrow X_1 \mid (X_2 \mathbin{\&} (X_3 \mid (X_4 \mathbin{\&} X_5)))$

Page 141 line 2 of exercise 27 ——— 18 Oct 2006

Section 7.1 $\rightsquigarrow$ Section 7.1.3

▸**Page 141** line 1 of exercise 29 ——— 10 Nov 1997

a simple $\rightsquigarrow$ Find a simple

▸**Page 146** line 14 ——— 17 Mar 2001

Algorithm S $\rightsquigarrow$ Algorithm P

▸**Page 147** line 1 of exercise 14 ——— 09 Mar 2001

to sequence $\rightsquigarrow$ to a sequence

Page 148 new exercise ——— 22 Nov 2003

▸**18.** [*M32*] People sometimes try to shuffle n items $(X_1, X_2, \ldots, X_n)$ by successively interchanging

$$X_1 \leftrightarrow X_{k_1},\ X_2 \leftrightarrow X_{k_2},\ \ldots,\ X_n \leftrightarrow X_{k_n},$$

where the indices k_j are independent and uniformly random between 1 and n.

Consider the directed graph with vertices $\{1, 2, \ldots, n\}$ and with arcs from j to k_j for $1 \le j \le n$. Describe the digraphs of this type for which, if we start with the elements $(X_1, X_2, \ldots, X_n) = (1, 2, \ldots, n)$, the stated interchanges produce the respective permutations (a) $(n, 1, \ldots, 2)$; (b) $(1, 2, \ldots, n)$; (c) $(2, \ldots, n, 1)$. Conclude that these three permutations are obtained with wildly different probabilities.

Page 148 quotation to follow the exercises ——— 24 Mar 2006

By means of the thread one understands the ball of yarn,
so we'll be satisfied and assured by having this sample.
— MIGUEL DE CERVANTES, *El Ingenioso*
Hidalgo Don Quixote de la Mancha (1605)

▸**Page 173** line 16 ——— 30 Nov 1997

0000, 0001, 1101, or 1110; ⇝ 0000, 0011, 1101, or 1110;

Page 173 line −7 ——— 23 Jun 2001

Walsh transform ⇝ Hadamard transform

▸**Page 176** line −19 ——— 25 Jan 2003

$3R \approx 600000$ ⇝ $\approx 3R = 600000$

▸**Page 176** line −16 ——— 20 Sep 2005

53.5 teraMIP-years ⇝ 535 teraMIP-years

Page 177 lines 11–13 ——— 11 Jan 2000

normal ... 216. ⇝ *entirely normal* to base b, and he stated Theorem C informally without apparently realizing that it required proof [*Rendiconti Circ. Mat. Palermo* **27** (1909), 247–271, §12.]

Page 179 lines 21–23 ——— 08 Aug 2005

Finally Levin ... analyzing Algorithm L. ⇝ Finally Charles Rackoff refined the methods of that paper by introducing and analyzing Algorithm L [see L. Levin, *J. Symbolic Logic* **58** (1993), 1102–1103].

Page 179 lines 25–26 ——— 20 Mar 2000

[*STOC* **21** (1989), 12–24; **22** (1990), 395–404] ⇝ [*SICOMP* **28** (1999), 1364–1396]

Page 179 lines 27–28 ——— 27 Feb 2004

not surveyed here ... practical random number generation. ⇝ beyond the scope of this book.

▸**Page 182** line 2 of exercise 31 ——— 26 Dec 2002

$U_n < \frac{1}{2}$ ⇝ $U_j < \frac{1}{2}$

▸**Page 183** line 7 of exercise 42 ——— 26 Jan 2001

k-bit vectors, ⇝ k-bit vectors, with $c \neq c'$,

Page 187 replacement for lines 12–35 ——— 01 Jan 2002

```
register long ss=(seed+2)&(MM-2);
for (j=0;j<KK;j++) {
  x[j]=ss;                        /* bootstrap the buffer */
  ss<<=1; if (ss>=MM) ss-=MM-2;   /* cyclic shift 29 bits */
```

```
  }
  x[1]++;                  /* make x[1] (and only x[1]) odd */
  for (ss=seed&(MM-1),t=TT-1; t; ) {
    for (j=KK-1;j>0;j--)
      x[j+j]=x[j], x[j+j-1]=0;                    /* "square" */
    for (j=KK+KK-2;j>=KK;j--)
      x[j-(KK-LL)]=mod_diff(x[j-(KK-LL)],x[j]),
      x[j-KK]=mod_diff(x[j-KK],x[j]);
    if (is_odd(ss)) {                         /* "multiply by z" */
      for (j=KK;j>0;j--)  x[j]=x[j-1];
      x[0]=x[KK];           /* shift the buffer cyclically */
      x[LL]=mod_diff(x[LL],x[KK]);
    }
    if (ss) ss>>=1; else t--;
  }
  for (j=0;j<LL;j++) ran_x[j+KK-LL]=x[j];
  for (;j<KK;j++) ran_x[j-LL]=x[j];
  for (j=0;j<10;j++) ran_array(x,KK+KK-1);    /* warm it up */
}
```

(This program incorporates improvements to the author's original *ran_start* routine, recommended by Richard Brent and Pedro Gimeno in November 2001.)

▸**Page 188** line 17 ——— 21 Feb 2001

`void main()` ⇝ `int main()`

Page 188 line 25 ——— 01 Jan 2002

461390032 ⇝ 995235265

▸**Page 189** line −15 ——— 12 Nov 2007

125–136 ⇝ 125–137

Page 196 line 2 (not an error) ——— 05 Jun 2008

[The spelling 'archæologists' here is intentionally archaic.]

▸**Page 196** line −11 ——— 02 Feb 1998

1942), 37–62; ⇝ 1941), 37–67;

Page 196 lines −11 and −10 ——— 20 Feb 2003

"Ancient Mesoamerican computing practices," ... to appear. ⇝ "Pratiche del calcolo nell'antica mesoamerica," *Storia della Scienza* **2** (Rome: Istituto della Enciclopedia Italiana, 2001), 976–990.

Page 198 top line ——— 17 Oct 2007

A.D. 501 ⇝ A.D. 500 or 501

Page 198 line 22 ——— 06 Apr 2006

1596–1610 ⇝ 1586–1610

Page 198 replacement for lines 23–33 ______ 01 Nov 2001

Decimal fractions began to appear sporadically in Europe; for example, a so-called "Turkish method" was used to compute $153.5 \times 16.25 = 2494.375$. Giovanni Bianchini developed them further, with applications to surveying, prior to 1450; but like al-Uqlīdisī, his work seems to have had little influence. Christof Rudolff and François Viète suggested the idea again in 1525 and 1579. Finally, an arithmetic text by Simon Stevin, who independently hit on the idea of decimal fractions in 1585, became popular. Stevin's work, and the discovery of logarithms soon afterwards, made decimal fractions commonplace in Europe during the 17th century. [For further remarks and references, see D. E. Smith, *History of Mathematics* **2** (1925), 228–247; V. J. Katz, *A History of Mathematics* (1993), 225–228, 345–348; and G. Rosińska, *Quart. J. Hist. Sci. Tech.* **40** (1995), 17–32.]

▸**Page 199** line 6 ______ 03 Dec 1998

de Seuil ⇝ du Seuil

▸**Page 199** line 9 ______ 02 Nov 2002

people would ⇝ people

Page 199 bottom line ______ 27 Aug 2004

de Caramuel Lobkowitz ⇝ Caramuel de Lobkowitz

▸**Page 201** line 16 ______ 25 Oct 1999

Colenne ⇝ Collenne

Page 202 line −16 ______ 22 Mar 2002

CACM **2** ⇝ *CACM* **2**, 12

▸**Page 205** line 8 ______ 06 Nov 1997

Marcziński ⇝ Marczyński

▸**Page 205** line 10 ______ 26 Sep 2005

274–276 ⇝ 274–277

Page 205 line 18 ______ 26 Sep 2005

245–247. ⇝ 245–247; **4** (1961), 355.

Page 208 line 24 ______ 07 Dec 2004

mechanical devices for arithmetic. ⇝
mechanical devices for arithmetic. Thomas Fowler independently invented and constructed a balanced ternary calculator at about the same time [see *Report British Assoc. Adv. Sci.* **10** (1840), 55; **11** (1841), 39–40].

Page 209 line 5 ______ 23 Mar 2006

this system, ⇝ this system, which was known in 13th-century India,

Page 209 line 8 ______ 07 Feb 2006

Algorithm 3.3.2P ⇝ Algorithms 3.3.2P and 3.4.2P

▸**Page 210** line 1 ________ 26 Jan 2001

number 1). $\rightsquigarrow$ number 1.)

▸**Page 210** line 2 of exercise 12 ________ 02 Dec 1999

$(b_{n+1} \ldots b_0)_{-2} \rightsquigarrow (b_{n+2} \ldots b_0)_{-2}$

Page 214 lines 19, 20, −8, −7 ________ 28 Jan 1999

2252 $\rightsquigarrow$ 2214 (twice)
6256 $\rightsquigarrow$ 6261 (twice)

Page 214 and following . . . . 16 Apr 1999

In the fourth edition I will change the definitions so that we have $|f| < b$; *equation* (2) *will become* "$-b^p < b^{p-1} f < b^p$" *and* (5) *will become* "$1 \le |f| < b$"; *Avogadro's number with an excess-50 decimal representation will be* $(73, +6.0221400)$, *etc. The net effect will be to change the notion of excess, so that what was excess* q *in the third edition will be called excess* $q+1$ *in the fourth edition. This change in terminology will work much better with respect to IEEE standard floating point conventions (and it will properly match the term "ulp," defined at the bottom of page 232), although equations* (21)–(24) *will become slightly more messy.*

▸**Page 219** replacement for program lines 26–28 ________ 10 Nov 2002

```
26       LD1  FV(0:1)  Check for opposite signs.
27       JAP  1F
28       J1N  N2       If not, normalize.
29       JMP  2F
30   1H  J1P  N2
31   2H  SRC  5        |rX| ↔ |rA|.
```

[Now lines 29–67 must be renumbered 32–70. Also change '4' to '5' on (new) line 38, '`N3A`' to '`N2`' on (new) line 39, and delete '`N3A`' from (new) line 47.]

▸**Page 219** near the bottom ________ 10 Nov 2002

line −6: 25 to 37 $\rightsquigarrow$ 26 to 40
line −1: 55 uses $\rightsquigarrow$ 58 uses

▸**Page 221** line −8 ________ 10 Nov 2002

30–34 $\rightsquigarrow$ 33–37

Page 232 line 15 ________ 01 Mar 2007

$b^{e-1} \le x < b^e \rightsquigarrow b^{e-1} \le |x| < b^e$

Page 238 near the bottom ________ 28 Jan 1999

lines −9 and −1: 60225 $\rightsquigarrow$ 60221
lines −9 and −8: 66256 $\rightsquigarrow$ 66261
line −8: 2252 $\rightsquigarrow$ 2214

▸**Page 239** bottom line ________ 20 Mar 1999

$\delta_{(u \oplus v) \oplus w)} \rightsquigarrow \delta_{(u \oplus v) \oplus w}$

▸**Page 240** line −4 ——— 25 Mar 2001

$[u_0 \bigtriangledown v_0, u_1 \bigtriangleup v_1]$ ⇝ $[u_0 \bigtriangledown v_0 \mathinner{.\,.} u_1 \bigtriangleup v_1]$

Page 240 replacement for bottom two lines ——— 28 Jan 1999

$$N = \bigl[(24, +.60221331) \mathinner{.\,.} (24, +.60221403)\bigr],$$
$$h = \bigl[(-26, +.66260715) \mathinner{.\,.} (-26, +.66260795)\bigr];$$

Page 241 replacement for lines 2 and 3 ——— 28 Jan 1999

$$N \oplus h = \bigl[(24, +.60221331) \mathinner{.\,.} (24, +.60221404)\bigr],$$
$$N \otimes h = \bigl[(-2, +.39903084) \mathinner{.\,.} (-2, +.39903181)\bigr].$$

Page 243 replacement for lines 15–17 ——— 28 Jan 1999

c) $u = (24, +.60221400)$, $v = (27, +.00060221)$;
d) $u = (24, +.60221400)$, $v = (31, +.00000006)$;
e) $u = (24, +.60221400)$, $v = (28, +.00000000)$.

▸**Page 244** line 8 of exercise 19 ——— 10 Mar 2007

$s_n =$ ⇝ $s_n - c_n =$

Page 245 line 3 ——— 21 Jul 2007

$-0 < +0$ ⇝ $-0 < 0 < +0$

Page 246 line 21 ——— 16 Jul 2006

denormal numbers ⇝ *subnormal numbers*

▸**Page 246** lines 21 and 22 ——— 02 Nov 2004

and the so-called NaNs that represent infinite, undefined, or otherwise unusual quantities ⇝ *infinities, and the so-called NaNs that represent undefined or otherwise unusual quantities*

Page 262 line −7 ——— 18 Sep 2005

347. ⇝ 347. See also A. Berger, L. A. Bunimovich, and T. P. Hill, *Trans. Amer. Math. Soc.* **357** (2004), 197–219.

▸**Page 267** line 4 ——— 26 Dec 2000

To A3 if $j = n$. ⇝ Exit the loop if $j = n$.

▸**Page 268** line 6 ——— 10 Aug 2000

`STA  W,1` ⇝ `STA  W+N,1`

▸**Page 268** line 24 ——— 08 Oct 2006

$(u_{m-1} \ldots u_1 u_0) \times v_j$ ⇝ $(u_{m-1} \ldots u_1 u_0)_b \times v_j$

Page 268 line 26 ——— 22 Oct 2006

it is best ⇝ it is simpler

▸**Page 272** lines 10 and 23 ——— 23 Jan 1998

$\lfloor (b-1)/v_{n-1} \rfloor$ ⇝ $\lfloor b/(v_{n-1}+1) \rfloor$

▸**Page 272** line 2 of step D3 ——— 03 Feb 2005

test if $\hat{q} = b$ ↝ test if $\hat{q} \ge b$

▸**Page 273** program line *041* ——— 20 Oct 1998

q ↝ $\hat{q}$

▸**Page 273** program line *044* ——— 03 Feb 2005

quotient $= b$ ↝ quotient $\ge b$

▸**Page 273** program line *046* ——— 22 Jan 1998

u_{j+n-11} ↝ u_{j+n-1}

▸**Page 274** line 2 ——— 19 Mar 1998

`U+B-1,2` ↝ `U+N-1,2`

▸**Page 275** line 19 ——— 23 Jan 1998

106 cycles ↝ 111 cycles

Page 279 line −14 ——— 28 Oct 2000

273–283. ↝ 273–283, **24** (1998), 359–367.

▸**Page 280** line 26 ——— 23 Apr 1998

millenium ↝ millennium

▸**Page 282** line 1 of exercise 16 ——— 17 Dec 1998

a algorithm ↝ an algorithm

▸**Page 282** line 2 of exercise 20 ——— 03 Feb 2005

u_{n-2}, then ↝ u_{n-2} and $\hat{q} < b$, then

▸**Page 282** replacement for line 2 of exercise 23 ——— 23 Jan 1998

have $\lfloor b/2 \rfloor \le v\lfloor b/(v+1) \rfloor < (v+1)\lfloor b/(v+1) \rfloor \le b$.

▸**Page 285** line −7 ——— 15 Nov 2001

of the Section 4.3.1 ↝ of Section 4.3.1

▸**Page 287** line 8 ——— 27 Oct 2004

Civilization ↝ *Civilisation*

Page 293 new sentence at end of exercise 5 ——— 05 Dec 2000

What is the largest possible $m_1 m_2 \ldots m_r$ when each residue u_j must fit in eight bits of memory?

▸**Page 301** line 23 ——— 30 Apr 2008

multiplications of p-bit numbers ↝ multiplications of q-bit numbers

▸**Page 303** in (25) ——— 07 Feb 1999

$O(n^{1.63})$ ↝ $O(n^{1.631})$

▸**Page 304** line 20 ——— 07 Feb 2000

positive integers e and f $\leadsto$ relatively prime positive integers e and f

▸**Page 309** line 1 ——— 14 Aug 2005

$\omega_r = x_r + iy_r \leadsto \omega_r = x_r + iy_r$ and $r \geq 2$

▸**Page 310** replacement for line 15 ——— 08 Nov 1997

$$\bigl|(\hat{\hat{w}}_r)' - \hat{\hat{w}}_r\bigr| < 2^k(4k2^k - 2k)\delta + (2^k - 1)2k\delta; \quad |w'_r - w_r| < 4k2^k\delta. \tag{50}$$

▸**Page 310** renumbering the equations ——— 08 Nov 1997

line 18: (50) $\leadsto$ (51)
lines 20 and 21: (51) $\leadsto$ (52)

▸**Page 310** line −12 ——— 27 Apr 1999

$m = 44 \leadsto m = 144$

▸**Page 311** line 8 ——— 08 Nov 1997

(52) $\leadsto$ (53)

▸**Page 311** line 9 ——— 29 Jan 1998

$\lg \ldots \lg n \leq 1 \leadsto \lg \ldots \lg n \leq 2$

▸**Page 311** line −9 ——— 29 Dec 1997

could than be done $\leadsto$ could then be done

▸**Page 313** line 13 ——— 15 May 1998

constant factor $\leadsto$ constant factor.

▸**Page 316** line 2 of exercise 5 ——— 14 Sep 2000

(21) can be $\leadsto$ (20) can be

Page 322 line −14 ——— 18 Oct 2006

Section 7.1 $\leadsto$ Section 7.1.3

▸**Page 324** line −7 ——— 10 Nov 2002

CE-11 $\leadsto$ **EC-11**

▸**Page 325** line 23 ——— 25 Oct 1999

.9 5 2 4 6 $\leadsto$ .9 5 2 6 4

▸**Page 328** replacement for exercise 9 ——— 14 May 2006

▸**9.** [*M29*] The purpose of this exercise is to compute $\lfloor u/10 \rfloor$ with binary shifting and addition operations only, when u is a nonnegative integer. Let $v_0(u) = 3\lfloor u/2 \rfloor + 3$ and

$$v_{k+1}(u) \;=\; v_k(u) + \lfloor v_k(u)/2^{2^{k+2}} \rfloor \qquad \text{for } k \geq 0.$$

Given k, what is the smallest nonnegative integer u such that $\lfloor v_k[u]/16 \rfloor \neq \lfloor u/10 \rfloor$?

Page 329 in exercise 19 ——— 19 May 2005

line 3: $U \leftarrow U - c_i(U \wedge m_i) \leadsto U \leftarrow U - c_i(U \mathbin{\&} m_i)$
line 4: where "$\wedge$" denotes $\leadsto$ where "&" denotes

Page 330 quotation to follow line 8 —— 11 Jun 2005

Irrationality is the square root of all evil.
— DOUGLAS HOFSTADTER, *Metamagical Themas* (1983)

▸**Page 345** line 11 —— 14 Sep 1999

integer variables only $\rightsquigarrow$ integer values only

Page 352 line 2 after (61) —— 23 Nov 1998

conjecture. $\rightsquigarrow$ conjecture. Vallée has successfully analyzed Algorithm B using rigorous "dynamical" methods of great interest [see *Algorithmica* **22** (1998), 660–685].

Page 355 the rating of exercise 32 —— 23 May 2008

HM47 $\rightsquigarrow$ *HM42*

▸**Page 360** line −16 —— 17 Jun 1998

a interesting $\rightsquigarrow$ an interesting

▸**Page 362** in equation (25) —— 30 Mar 2000

$\zeta(5)x^5 \rightsquigarrow \zeta(5)x^4$

Page 366 lines −3 and −2 —— 23 Nov 1998

Lecture Notes ... to appear. $\rightsquigarrow$ *Combinatorics, Probability and Computing* **6** (1997), 397–433; Flajolet and Vallée, *Theoretical Comp. Sci.* **194** (1998), 1–34.

▸**Page 368** replacement for lines 1–3 —— 18 Feb 2004

Theorem E. *Let $p_k(a,n)$ be the probability that the $(k+1)$st quotient A_{k+1} in Euclid's algorithm is equal to a, when $u = n$ and when v is equally likely to be any of the numbers $\{0,1,\ldots,n-1\}$. Then*

▸**Page 370** line 3 —— 05 Feb 1998

$55.6 \rightsquigarrow 5.6$

Page 372 replacement for line 3 —— 13 Jan 2000

$$\frac{1}{N^2}\sum_{m=1}^{N}\sum_{n=1}^{N} T(m,n) \;=\; \frac{2}{N^2}\sum_{n=1}^{N} nT_n - \frac{1}{2} - \frac{1}{2N}. \qquad (57)$$

Page 372 line 14 —— 13 Jan 2000

John D. Dixon and Hans A. Heilbronn. Dixon $\rightsquigarrow$ Gustav Lochs, John D. Dixon, and Hans A. Heilbronn. Lochs [*Monatshefte für Math.* **65** (1961), 27–52] derived a formula equivalent to the fact that (57) equals $(12\pi^{-2}\ln 2)\ln N + a + O(N^{-1/2})$, where $a \approx 0.065$. Unfortunately his paper remained essentially unknown for many years, perhaps because it computed only an average value from which we cannot derive definite information about T_n for any particular n. Dixon

Page 373 line 1 —— 13 Jan 2000

to prove $\rightsquigarrow$ to confirm Lochs's work, proving

Page 373 new copy to follow (62) —— 21 May 2005

D. Hensley proved in *J. Number Theory* **49** (1994), 142–182, that the variance of τ_n is proportional to $\log n$.

▸**Page 377** line 8 of exercise 34 —— 27 Feb 2004

$\sum_{y=1}^{n}$ ⇝ $\sum$

Page 384 lines −10 through −8 —— 28 Dec 2000

[See D. E. Knuth ... 57–61.] ⇝ [See D. E. Knuth, *Selected Papers on Analysis of Algorithms* (2000), 329–330, 336–337, for references to the relevant literature.]

Page 385 line −13 —— 14 May 1998

mod p. ⇝ mod p; see Arney and Bender, *Pacific J. Math.* **103** (1982), 269–294.

Page 386 replacement for lines 19–24 —— 28 Dec 2000

Experiments by Tomás Oliveira e Silva indicate that $m(p)$ has an average value of about $2\sqrt{p}$, and it never exceeds $16\sqrt{p}$ when $p < 1000000000$. The maximum $m(p)$ for $p < 10^9$ is $m(850112303) = 416784$; and the maximum of $m(p)/\sqrt{p}$ occurs when $p = 695361131$, $m(p) = 406244$. According to these experimental results, almost all 18-digit numbers can be factored in fewer than 64,000 iterations of Algorithm B (compared to roughly 50,000,000 divisions in Algorithm A).

Page 387 line 3 —— 31 Dec 2005

357.] ⇝ 357. An equivalent idea had in fact been used already by Nārāyaṇa Paṇḍita in his remarkable book *Gaṇita Kaumudī* (1356); see Parmanand Singh, *Gaṇita Bhāratī* **22** (2000), 72–74.]

▸**Page 387** step C5 —— 29 Dec 1997

Return to step C3 ⇝ Return to step C4

Page 388 bottom line —— 19 Sep 2005

solution x. ⇝ solution x. Individual primes p and q are, however, preferable to moduli like p^2 unless p is quite small, because we tend to get even more information $\bmod pq$.

Page 390 line 12 —— 19 May 2005

rA ← rA ∧ $S'[2, \mathrm{rI1}]$ ⇝ rA ← rA & $S'[2, \mathrm{rI1}]$

▸**Page 395** near the bottom —— 18 Dec 1998

line −10: about n ⇝ about its input
line −9: certified a billion different primes ⇝ tested a billion different numbers

Page 396 upper middle —— 19 Mar 2005

line 11: first proposed ⇝ proposed
line 16: 35–36]. ⇝ 35–36], and independently discovered by J. L. Selfridge.

Page 396 middle ——————————————— 28 Apr 2005

A completely different . . . purely of theoretical interest. $\rightsquigarrow$

A completely rigorous and deterministic way to test for primality in polynomial time was finally discovered in 2002 by Manindra Agrawal, Neeraj Kayal, and Nitin Saxena, who proved the following result:

Theorem A. *Let r be an integer such that $n \perp r$ and the order of n modulo r exceeds $(\lg n)^2$. Then n is prime if and only if the polynomial congruence*

$$(z+a)^n \equiv z^n + a \qquad (\text{modulo } z^r - 1 \text{ and } n)$$

holds for $0 \le z \le \sqrt{r}\,\lg n$. (See exercise 3.2.2–11(a).) ▮

An excellent exposition of this theorem has been prepared by Andrew Granville [*Bull. Amer. Math. Soc.* **42** (2005), 3–38], who presents an elementary proof that it yields a primality test with running time $\Omega(\log n)^6$ and $O(\log n)^{11}$. He also explains a subsequent improvement due to H. Lenstra and C. Pomerance, who showed that the running time can be reduced to $O(\log n)^{6+\epsilon}$ if the polynomial $z^r - 1$ is replaced by a more general family of polynomials. And he discusses refinements by P. Berrizbeitia, Q. Cheng, P. Mihăilescu, R. Avanzi, and D. Bernstein, leading to a probabilistic algorithm by which a proof of primality can almost surely be found in $O(\log n)^{4+\epsilon}$ steps whenever n is prime.

Page 402 bottom line ——————————————— 14 May 1998

factors. $\rightsquigarrow$ factors. An excellent exposition of this method has been given by Joseph H. Silverman and John Tate in *Rational Points on Elliptic Curves* (New York: Springer, 1992), Chapter 4.

Page 403 line −19 ——————————————— 07 Jul 1999

67 (1998), to appear $\rightsquigarrow$ **68** (1999), 429–451

Page 403 line −9 ——————————————— 20 Jun 2000

to appear $\rightsquigarrow$ *Math. Comp.* **69** (2000), 1297–1304

Page 406 line 5 ——————————————— 07 Jul 1999

considered $\rightsquigarrow$ published

Page 407 after line 10 ——————————————— 07 Jul 1999

Historical note: It was revealed in 1998 that Clifford Cocks had considered encoding messages by the transformation $x^{pq} \bmod pq$ already in 1973, but his work was kept secret.

Page 409 update on Mersenne primes . . . . 02 May 2004

Tens of thousands of people have joined the GIMPS project, and Scott Kurowski has provided Internet software called PrimeNet to make the exponent assignments more systematic. Already in February 1998, more than one year's worth of computing was being done each day looking for Mersenne primes, and the amount of activity was growing steadily. Thus we can expect gradual progress on the hunt for these historic numbers.

I will list all Mersenne primes found after 1997 here, but on page 409 of the printed books I'll abbreviate the following information because space is tight. I won't update page 409 with every new printing, but I did make major amendments when preparing the 15th printing. So far the new primes $2^p - 1$ *found are:*

p	*Discoverer*	*Date found*
3021377	*Roland Clarkson*	*27 January 1998*
6972593	*Nayan Hajratwala*	*1 June 1999*
13466917	*Michael Cameron*	*14 November 2001*
20996011	*Michael Shafer*	*17 November 2003*
24036583	*Josh Findley*	*May 2004*
25964951	*Martin Nowak*	*Feb 2005*
30402457	*Curtis Cooper,Steven Boone*	*Dec 2005*
32582657	*Curtis Cooper,Steven Boone*	*4 Sep 2006*

Page 412 near the top ——— 08 Jan 2005

lines 2 and 3: are prime [see . . . 136]. $\leadsto$ are prime.

line 6: other forms. $\leadsto$ other forms. [See E. Picutti, *Historia Math.* **16** (1989), 123–136; Hugh C. Williams, *Édouard Lucas and Primality Testing* (1998), Chapter 2.]

▸**Page 416** line 11 of exercise 41 ——— 21 Jan 1998

$f(1000, 10) \leadsto f_2(1000, 10)$

▸**Page 416** line 3 of exercise 43 ——— 27 Apr 2001

$y \in S_m \leadsto y \in Q_m$

▸**Page 424** line 18 ——— 28 Oct 2000

Pablo Nuñez $\leadsto$ Pedro Nuñez

▸**Page 432** line 2 after (22) ——— 23 Jun 1998

$b_6^3 \cdot b_6^3 \cdot b_6^3 \leadsto b_6^3 \cdot b_6^3$

▸**Page 436** line 7 of exercise 17 ——— 03 Mar 2000

$\deg(u) \leadsto \deg(U)$

▸**Page 442** line 14 ——— 06 Mar 1998

Pěstováni $\leadsto$ *Pěstování*

▸**Page 442** line −4 ——— 06 Jun 1999

3, ,. . . $\leadsto$ 3, . . .

Page 449 near the top ——— 20 Jul 2000

lines 5–8: A faster . . . arithmetic $\leadsto$ Faster algorithms for distinct-degree factorization when p is very large have been found by J. von zur Gathen, V. Shoup, and E. Kaltofen; the running time is $O(n^{2+\epsilon} + n^{1+\epsilon} \log p)$ arithmetic

lines 10–11: [See . . . to appear.] $\leadsto$ [See *Computational Complexity* **2** (1992), 187–224; *J. Symbolic Comp.* **20** (1995), 363–397; *Math. Comp.* **67** (1998), 1179–1197.]

Page 449 bottom line, and top of page 450 — 17 Jun 2002 — Wattel Jensen Thurber

extended by an astronomer ... von Schubert's method independently ⤳ extended by N. Bernoulli in 1708 and, more explicitly, by an astronomer named Friedrich von Schubert in 1793, who showed how to find all factors of degree n in a finite number of steps; see M. Mignotte and D. Ştefănescu, *Revue d'Hist. Math.* **7** (2001), 67–89. L. Kronecker rediscovered their approach independently,

▸**Page 451** line −13 — 28 Oct 2000

the range $(-\frac{169}{2}, \frac{169}{2})$ ⤳ the range $(-\frac{169}{2} \mathinner{..} \frac{169}{2})$

▸**Page 455** lines 27 and 28 — 30 Sep 1998

Efficient Polynomial Computations ⤳ *Effective Polynomial Computation*

▸**Page 457** line 3 of exercise 20 — 05 Feb 1998

$u(x) = (x-\alpha)u(x)$ and $v(x) = (\bar\alpha x - 1)u(x)$ ⤳ $u(x) = (x-\alpha)w(x)$ and $v(x) = (\bar\alpha x - 1)w(x)$

▸**Page 458** line 11 — 14 Apr 1998

whenever $v_{\mathtt{j}} \neq 0$. ⤳ whenever $u_{\mathtt{j}} \neq 0$.

▸**Page 458** line 20 — 06 Jun 1999

1^1 ⤳ 1^2

▸**Page 459** line 3 of exercise 29 — 01 May 2001

$1/2 - 1/(2p^d)$ ⤳ $1/2 - 1/(2p^{2d})$

▸**Page 461** line −18 — 21 Sep 2004

before 200 B.C. in Piṅgala's Hindu classic *Chandaḥsūtra* ⤳ before A.D. 400 in Piṅgala's Hindu classic *Chandaḥśāstra*
[also change "next 1000 years" to "next several centuries", a few lines down]

Page 466 line 3 — 02 Dec 2005

179 ⤳ 179, 199

Page 466 lines 19–21 — 25 May 2008

Furthermore, as E. G. Thurber ... steps earlier. ⤳ Furthermore, we can omit all the even numbers (except 2) in the first row, if we bring values of the form $d_j/2^e$ into the computation e steps earlier. [See E. Wattel and G. A. Jensen, *Math. Centrum Report* ZW1968-001 (1968), 18 pp.; E. G. Thurber, *Duke Math. J.* **40** (1973), 907–913.]

▸**Page 470** line 28 — 20 Sep 1998

$2^m + 2^{m+1} + 2^{d+1} + 2^d$ ⤳ $2^m + 2^{m-1} + 2^{d+1} + 2^d$

Page 477 line 23 — 15 Sep 2005

948 cases ⤳ 102 cases

Page 477 lines 26–28 or 26–29 ——— 12 Jun 2008

for all $k \geq 5$. ... Kevin R. Hebb $\rightsquigarrow$ for all $k \geq 5$. Neill Clift found in 2007 that $l(n) = l(2n) = l(4n) = 31$ when $n = 30958077$; and in 2008, astonishingly, he discovered that $l(n) > l(2n) = 34$ when $n = 375494703$. Kevin R. Hebb

Page 477 line 28 ——— 08 May 2007

Kevin $\rightsquigarrow$ Neill Clift found in 2007 that $l(n) = l(2n) = l(4n) = 31$ when $n = 30958077$. Kevin

Page 477 replacement for the bottom ten lines ——— 27 May 2008

r	$c(r)$	r	$c(r)$	r	$c(r)$
1	2	12	379	23	196591
2	3	13	607	24	357887
3	5	14	1087	25	685951
4	7	15	1903	26	1176431
5	11	16	3583	27	2211837
6	19	17	6271	28	4169527
7	29	18	11231	29	7624319
8	47	19	18287	30	14143037
9	71	20	34303	31	25450463
10	127	21	65131	32	46444543
11	191	22	110591	33	89209343

▸**Page 478** line 4 ——— 01 Feb 1999

[The $\rightsquigarrow$ The

Page 478 line 5 ——— 27 May 2008

Bleichenbacher. $\rightsquigarrow$ Bleichenbacher, and $c(29)$ through $c(33)$ by Neill Clift.

Page 478 replacement for lines 19–25 ——— 24 May 2008

table lists the first few values of $d(r)$, according to Flammenkamp and Clift:

r	$d(r)$	r	$d(r)$	r	$d(r)$	r	$d(r)$	r	$d(r)$	r	$d(r)$
1	1	6	15	11	246	16	4490	21	90371	26	1896704
2	2	7	26	12	432	17	8170	22	165432	27	3501029
3	3	8	44	13	772	18	14866	23	303475	28	6465774
4	5	9	78	14	1382	19	27128	24	558275	29	11947258
5	9	10	136	15	2481	20	49544	25	1028508	30	22087489

Page 478 the three lines following (49) ——— 27 May 2008

Computer calculations ... for $n = 32$. $\rightsquigarrow$ Computer calculations by Neill Clift show that $l(2^n - 1)$ is exactly equal to $n - 1 + l(n)$ for $1 \leq n \leq 46$; and 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.

Page 479 lines −23 thru −20 ——— 17 Sep 2005

The chain ... theorem due to Hansen: $\rightsquigarrow$ Hansen pointed out that the chain constructed in Theorem F is an l^0-chain (see exercise 22); and he also established the following improvement of Eq. (50):

Page 479 new lines to be inserted at the bottom ________ 17 Sep 2005

Computations by Neill Clift have shown that $l(n) < l^0(n)$ when $n = 5784689$ (see exercise 42). This is the smallest case where Eq. (49) remains in doubt.

▸**Page 483** line 9 of exercise 19 ________ 18 Dec 2000

$\prod_{p\in N} = n \rightsquigarrow \prod_{p\in N} p = n$

Page 483 exercise 27 ________ 15 Oct 2008

line 1: *M21* $\rightsquigarrow$ *M23*
line 2: six $\rightsquigarrow$ eight

Page 485 replacement for exercise 42 ________ 17 Sep 2005

42. [*22*] (Neill Clift, 2005.) Show that neither 1, 2, 4, 8, 16, 32, 64, 65, 97, 128, 256, 353, 706, 1412, 2824, 5648, 11296, 22592, 45184, 90368, 180736, 361472, 361537, 723074, 1446148, 2892296, 5784592, 5784689 nor its dual is an l^0-chain.

43. [*M50*] Is $l(2^n - 1) \le n - 1 + l(n)$ for all integers $n > 0$? Does equality always hold?

▸**Page 493** line 5 ________ 07 Jun 1999

$\lceil n/2 \rceil \rightsquigarrow \lceil n/2 \rceil - 1$

Page 502 lines 8–18 ________ 23 Jun 2001

line 8: the *Walsh transform* $\rightsquigarrow$ the *Hadamard transform* or the *Walsh transform*
line 9: by J. L. Walsh $\rightsquigarrow$ by J. Hadamard [*Bull. Sci. Math.* (2) **17** (1893), 240–246] and by J. L. Walsh
lines 16–18: (See H. F. Harmuth, ... Walsh coefficients.) $\rightsquigarrow$ (See Section 7.2.1.1 for further discussion of the Hadamard–Walsh coefficients.)

▸**Page 504** replacement for bottom line ________ 28 Jun 1999

$$u_{[n]}(x) = \left(\frac{y_0 w_0}{x - x_0} + \cdots + \frac{y_n w_n}{x - x_n}\right) \Big/ \left(\frac{w_0}{x - x_0} + \cdots + \frac{w_n}{x - x_n}\right), \qquad (45)$$

▸**Page 507** replacement for bottom line, in 4th printing only ________ 10 Oct 1999

$$A = \begin{pmatrix} 1&0&\bar1&0&0&1&\bar1 \\ 0&1&0&0&0&1&0 \\ 0&0&1&0&1&\bar1&1 \\ 0&0&0&1&1&\bar1&1 \end{pmatrix}, \quad B = \begin{pmatrix} 1&0&0&\bar1&\bar1&0&1 \\ 0&1&0&1&0&0&0 \\ 0&0&1&1&1&0&\bar1 \\ 0&0&\bar1&\bar1&0&1&1 \end{pmatrix}, \quad C = \begin{pmatrix} 1&1&0&0&0&0&0 \\ 1&0&1&1&0&0&1 \\ 1&0&0&0&1&1&1 \\ 1&0&1&0&1&0&1 \end{pmatrix}. \qquad (53)$$

▸**Page 521** line 2 of exercise 56 ________ 26 Apr 2000

$\tau_{ijk} x_i x_k \rightsquigarrow \tau_{ijk} x_i x_j$

▸**Page 521** line 3 of exercise 60 ________ 26 Jan 2001

and only $\rightsquigarrow$ and only if

▸**Page 522** line 14 ________ 21 Apr 2002

problems of size $m \times n \times s \rightsquigarrow$ problems of the respective sizes $m \times n \times s$ and $s \times m \times n$

▸**Page 523** line 15 of exercise 67 ________ 28 Jun 1999

))) $\rightsquigarrow$))

▸**Page 529** a spurious line just before Algorithm N ——— 07 Feb 2005

N $\rightsquigarrow$ (this error appeared in the 15th, 16th, and 17th printings only)

▸**Page 531** line 7 ——— 09 Aug 1999

$U = \rightsquigarrow U(z) =$

Page 539 replacement for the top three lines ——— 18 Jun 2008

It is almost legitimate to take ten readings $(m_0, \ldots, m_9)$ and then to output j if m_j is strictly less than m_i for all $i \neq j$; try again if the minimum value appears more than once. (See (h).) However, the parameter m isn't really constant in the real world.

Page 539 line 10 of answer 6 ——— 08 Jun 2005

$f(x) = ax$.] $\rightsquigarrow$ $f(x) = ax$. See G. Frobenius, *Sitzungsberichte preußische Akademie der Wissenschaften* (1895), 82–83.]

Page 539 simplification for line −10 ——— 11 Jun 1998

$\lambda\delta_{\mu 0} + \mu + \lambda - 1 - ((\mu + \lambda - 1) \bmod \lambda) \rightsquigarrow \lambda(\lceil \mu/\lambda \rceil + \delta_{\mu 0})$

Page 540 line 12 ——— 25 Dec 2002

$e(n) = \rightsquigarrow e(n) = \rho(n+1) =$

Page 542 new answer ——— 08 May 2005

19. Clearly Pr(no final cycle has length 1) $= (m-1)^m/m^m$. R. Pemantle [*J. Algorithms* **54** (2005), 72–84] has shown that $\Pr(\lambda = 1) = \Theta(m^{k/2})$, and that $\Pr((\mu+\lambda)^2 > 2m^k x$ and $\lambda/(\mu+\lambda) \le y)$ rapidly approaches ye^{-x}, when $x > 0$, $0 < y < 1$, and $m \to \infty$. The k-dimensional analogs of exercises 13 and 14 remain unsolved.

Page 542 update on answer 21 ——— 08 Mar 1998

Scott Fluhrer has discovered *another* fixed point of Algorithm K, namely the value 5008502835(!). He also found the 3-cycle

$$0225923640 \to 2811514413 \to 0590051662 \to 0225923640,$$

making a total of seven cycles in all. Exactly 128 starting numbers lead to the repeating value 5008502835; the smallest of these is 0008502835, the largest is 9944390948.

▸**Page 546** line 20 ——— 28 Sep 2002

word size w $\rightsquigarrow$ word size

▸**Page 546** line 24 ——— 24 Nov 2007

$+\,b_n \rightsquigarrow -\,b_n$

▸**Page 546** replacement for line −4 ——— 24 Nov 2007

$$x_n = (x_{n-3} - x_{n-10} - b_n) \bmod 10 = x_{n-3} - x_{n-10} - b_n + 10b_{n+1}$$

▸**Page 546** line −2 ——— 19 Feb 1999

$\bar{x}_{n-1}\bar{x}_n \rightsquigarrow \bar{x}_{n+1}\bar{x}_n$

▸**Page 547** line 8 of answer 14 ——— 01 Dec 2007

$a_j(x_{n-1} \ldots x_{n-k})_b \rightsquigarrow a_j(x_{n-1} \ldots x_{n-j})_b$

▸**Page 549** lines 3–6 ——— 08 Nov 2005

Now since ... so $\lambda = \lambda_1\lambda_2$. $\rightsquigarrow$ Now let λ' be the order of a_1a_2. Since $(a_1a_2)^{\lambda'} \equiv 1$, we have $1 \equiv (a_1a_2)^{\lambda'\lambda_1} \equiv a_2^{\lambda'\lambda_1}$; hence $\lambda'\lambda_1$ is a multiple of λ_2. This implies that λ' is a multiple of λ_2, since λ_1 is relatively prime to λ_2. Similarly, λ' is a multiple of λ_1; hence λ' is a multiple of $\lambda_1\lambda_2$. But obviously $(a_1a_2)^{\lambda_1\lambda_2} \equiv 1$, so $\lambda' = \lambda_1\lambda_2$.

Page 549 line 6 of answer 16 ——— 28 Mar 2005

distinct roots. $\rightsquigarrow$ distinct roots. [J. L. Lagrange, *Mém. Acad. Roy. Sci. Berlin* **24** (1768), 181–250, §10.]

▸**Page 550** line 19 ——— 13 Jan 1998

succeed in find $\rightsquigarrow$ succeed in finding

Page 551 replacement for line 2 ——— 27 Feb 2004

$$Y_{n+2} \approx (10 + 6(Y_{n+1} + \epsilon_1) - 9(Y_n + \epsilon_2)) \bmod 20,$$

▸**Page 553** line −2 ——— 18 Feb 2004

$X_{n+p^{f+1}}$ $\rightsquigarrow$ $X_{n+p^{f+1}d}$

▸**Page 555** line 10 ——— 01 Jun 2001

$a_1X_{(n-1)1} + a_2X_{(n-2)2} + X_{(n-2)3}$ $\rightsquigarrow$ $a_1X_{(n-1)1} + a_2X_{(n-2)1} + X_{(n-2)3}$

▸**Page 555** line 1 of answer 18 ——— 03 Jun 2001

The third-most-significant $\rightsquigarrow$ By exercise 16, the most significant

Page 556 line 14 ——— 08 Jul 2001

$\langle sX_n + Y_n\rangle$ $\rightsquigarrow$ $\langle (X_n + Y_n) \bmod rs\rangle$

▸**Page 557** lines 3 and 4 ——— 25 Jan 2003

$i \rightsquigarrow j$ (three changes)

Page 557 last lines of answer 29 ——— 29 Jul 2006

S. Xie, ... 157–177 $\rightsquigarrow$ H. Fredricksen and J. Maiorana, *Discrete Math.* **23** (1978), 207–210, who essentially discovered Algorithm 7.2.1.1F.

▸**Page 557** line 1 of answer 30 ——— 28 Sep 2002

By exercise $\rightsquigarrow$ (a) By exercise

▸**Page 558** bottom line ——— 03 Feb 2005

$x - u_2 \rightsquigarrow x + u_2$ and $x - u_d \rightsquigarrow x + u_d$

▸**Page 565** line 5 of answer 24 ——— 05 Feb 2005

strings α, $\rightsquigarrow$ strings α, and we also have $\sum_{|\alpha|=t} N(\alpha) = n$;

▸**Page 566** last two lines of answer 24 ——— 03 Feb 2005

$K\bigl(i : (j : \alpha), (\beta : l) : i\bigr) - K\bigl(i-1 : (j : \alpha), (\beta : l+1) : i-1\bigr)$, where $i = \min(t+k,\, t-l)$ and $j = \max(0,\, k+l)$. $\rightsquigarrow$ $K\bigl(i : (\alpha : i-k),\, i : (\beta : i+l)\bigr) - K\bigl(i-1 : (\alpha : i-k),\, i-1 : (\beta : i+l)\bigr)$, where $i = \min(t+k,\, t-l)$.

▸**Page 566** lines −9, −8, and −7 ——— 18 Sep 2002

Whitworth, who stated the question as problem 667 in *Choice and Chance* (Cambridge, 1867) and gave the solution in $\rightsquigarrow$ Whitworth, in problem 667 of

▸**Page 569** line 10 ——— 12 Apr 1999

$-ic^3t^3 \leadsto -ic_3t^3$

▸**Page 569** line 12 ——— 07 Jan 2004

for $j \geq 8 \leadsto$ for $j \geq 3$

▸**Page 570** line 1 ——— 12 Apr 1999

(1093) $\leadsto$ (1953)

Page 571 improvement to answer 32 ——— 29 Mar 2005

Not if they ... equal strength $\leadsto$ Not if, say, X and Y each take the values $(-n, m)$ with the respective probabilities $(m/(m+n), n/(m+n))$, where $m < n < (1+\sqrt{2})m$. [Suppose two competitors differ by X after playing one round of golf. Then they are of equal strength

Page 572 new answer ——— 13 Jun 2001

[Renumber answer 3 as answer 2, delete the former answer 2, and insert the following new material:]

3. The sum is $((2^n x)) - ((x))$. [See *Trans. Amer. Math. Soc.* **65** (1949), 401.]

▸**Page 577** replacement for last three lines of answer 3 ——— 04 Jul 2003

$$m = 9,\quad a = 4 \text{ or } 7,\quad \nu_2^2 = \nu_3^2 = 5;$$
$$m = 9q,\quad a = 3q+1 \text{ or } 6q+1,\quad \nu_4^2 = 2.$$

▸**Page 578** line 4 of answer 8 ——— 16 Feb 1999

the bound (39) $\leadsto$ the bound (40)

▸**Page 581** in answer 20 ——— 25 Jul 2005

lines 2 and 3: plus $(X_0 \bmod 4)/2^e$, where $\sigma(y) = \bigl(ay + \lfloor a/4\rfloor\bigr) \bmod 2^{e-2}$. $\leadsto$
plus $2^{-e}(t, \ldots, t)$, where $\sigma(y) = \bigl(ay + \lfloor a/4\rfloor t\bigr) \bmod 2^{e-2}$ and $t = X_0 \bmod 4$.
line 9: $\bigl(-ay - \lceil a/4\rceil\bigr) \bmod 2^{e-2} \leadsto \bigl(-ay - \lceil a/4\rceil t\bigr) \bmod 2^{e-2}$

Page 582 new sentence to append to answer 26 ——— 06 Feb 2005

Since $m/d > 1$, we can also replace N by $N \bmod (m/d)$. [And *delete* the first sentence, 'When $m = 1$, ... zero.']

▸**Page 584** line 4 of answer 3 ——— 20 Aug 2001

$U > k\lfloor m/k\rfloor \leadsto U \geq k\lfloor m/k\rfloor$

▸**Page 585** line −3 ——— 04 Oct 1999

absolute minimum $\leadsto$ absolute maximum

▸**Page 587** bottom line ——— 03 Feb 2005

$\frac{2}{5}(a - bu) - \frac{2}{3} \leadsto \frac{2}{5}(a - bu) - \frac{2}{3}a$

▸**Page 588** line 1 ——— 03 Feb 2005

$I = \int_0^{a/b} u\sqrt{a - bu}\,du = \frac{4}{15}a^{5/2}/b^2 \leadsto I = 2\int_0^{a/b} u\sqrt{a - bu}\,du = \frac{8}{15}a^{5/2}/b^2$

▸**Page 588** line −2 of answer 21 ——— 03 Feb 2005

$E = \int_0^{r(x)} \leadsto E = 2\int_0^{r(x)}$

Page 588 beginning of answer 25 — 19 May 2005

line 1: $\vee \rightsquigarrow |$
line 2: $\wedge \rightsquigarrow \&$

▶**Page 589** line 3 of answer 29 — 25 Mar 2006

David Seneschol $\rightsquigarrow$ David Seneschal

Page 590 end of answer 31 — 08 Jul 1999

Preprint ... 1997) $\rightsquigarrow$ *Lecture Notes in Comp. Sci.* **1470** (1998), 1–20

▶**Page 591** in printings 5–14 only — 07 Feb 2004

[the top line of page 591 was a duplicate of the bottom line of page 590]

▶**Page 591** lines -3 and -2 of answer 8 — 29 Jun 1999

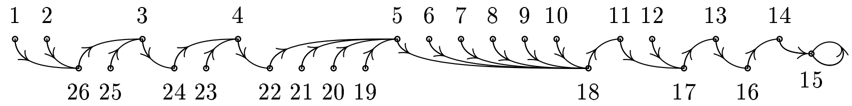
decrease n and N by 1 $\rightsquigarrow$ set $n \leftarrow n-1$, $N \leftarrow N - X - 1$,

▶**Page 592** line 2 of answer 13 — 01 Jan 2008

$(x+1) \rightsquigarrow (x-1)$

Page 592 new answer — 22 Nov 2003

18. (a) Oriented trees that essentially merge $(1, 2, \ldots)$ with $(n, n-1, \ldots)$, such as



(b) Collections of 1-cycles and 2-cycles. (c) Binary search trees on the keys $(1, 2, \ldots, n)$, with k_j the parent of j (or j, at the root); see Section 6.2.2. The number of $(k_1, \ldots, k_n)$ in each case is (a) 2^{n-1}; (b) $t_n \geq \sqrt{n!}$, see 5.1.4–(40); (c) $\binom{2n}{n}\frac{1}{n+1}$. [Case (a) represents the least common permutation; case (b) represents the most common, when $n \geq 18$. See D. P. Robbins and E. D. Bolker, *Æquationes Mathematicæ* **22** (1981), 268–292; D. Goldstein and D. Moews, *Æquationes Mathematicæ* **65** (2003), 3–30.]

▶**Page 593** line 1 of answer 6 — 19 Mar 2005

By exercise 5 $\rightsquigarrow$ By exercise 4

▶**Page 599** line 1 of answer 9 — 26 Jan 2001

The values $\rightsquigarrow$ (a) The values

Page 601 replacement for lines 15–41 — 01 Jan 2002

```
 1    CONTINUE
      X(2)=X(2)+1
      SS=SSEED
      T=TT-1
 10   DO 12 J=KK,2,-1
         X(J+J-1)=X(J)
 12      X(J+J-2)=0
      DO 14 J=KKK,KK+1,-1
         X(J-(KK-LL))=X(J-(KK-LL))-X(J)
         IF (X(J-(KK-LL)) .LT. 0) X(J-(KK-LL))=X(J-(KK-LL))+MM
         X(J-KK)=X(J-KK)-X(J)
```

```
            IF (X(J-KK) .LT. 0) X(J-KK)=X(J-KK)+MM
   14   CONTINUE
        IF (MOD(SS,2) .EQ. 1) THEN
            DO 16 J=KK,1,-1
   16          X(J+1)=X(J)
            X(1)=X(KK+1)
            X(LL+1)=X(LL+1)-X(KK+1)
            IF (X(LL+1) .LT. 0) X(LL+1)=X(LL+1)+MM
         END IF
```

Page 602 (now page 601) two new lines before 'END' ———— 01 Jan 2002

```
         DO 22 J=1,10
   22       CALL RNARRY(X,KKK)
```

Page 602 line 8 of answer 11 ———— 01 Jan 2002

copy in ul $\leadsto$ copy in x

Page 602 from line 28 of answer 11 to that answer's end ———— 01 Jan 2002

```
  double ss=2.0*ulp*((seed&0x3ffffff)+2);
  for (j=0;j<KK;j++) {
    x[j]=0; u[j]=ss;                         /* bootstrap the buffer */
    ss+=ss; if (ss>=1.0) ss-=1.0-2*ulp;  /* cyclic shift of 51 bits */
  }
  x[1]=1; u[1]+=ulp;              /* make u[1] (and only u[1]) "odd" */
  for (s=seed&0x3fffffff,t=TT-1; t; ) {
    for (j=KK-1;j>0;j--)
      x[j+j]=x[j],u[j+j]=u[j],x[j+j-1]=0,u[j+j-1]=0.0;  /* "square" */
    for (j=KK+KK-2;j>=KK;j--) {
      x[j-(KK-LL)]=x[j]^x[j-(KK-LL)],
        u[j-(KK-LL)]=mod_sum(u[j-(KK-LL)],u[j]);
      x[j-KK]=x[j]^x[j-KK],u[j-KK]=mod_sum(u[j-KK],u[j]);
    }
    if (is_odd(s)) {                               /* "multiply by z" */
      for (j=KK;j>0;j--)  x[j]=x[j-1],u[j]=u[j-1];
      x[0]=x[KK],u[0]=u[KK];          /* shift the buffer cyclically */
      x[LL]=x[KK]^x[LL],u[LL]=mod_sum(u[LL],u[KK]);
    }
    if (s) s>>=1; else t--;
  }
  for (j=0;j<LL;j++) ran_u[j+KK-LL]=u[j];
  for (;j<KK;j++) ran_u[j-LL]=u[j];
  for (j=0;j<10;j++) ranf_array(u,KK+KK-1);   /* warm everything up */
}

int main() {
  register int m; double a[2009];             /* a rudimentary test */
  ranf_start(310952);
  for (m=0;m<2009;m++) ranf_array(a,1009);
  printf("%.20f\n", ran_u[0]);           /* 0.36410514377569680455 */
  ranf_start(310952);
```

```
    for (m=0;m<1009;m++) ranf_array(a,2009);
    printf("%.20f\n", ran_u[0]);          /* 0.36410514377569680455 */
    return 0;
  }
```

Page 603 last line of answer 12 ——— 26 Dec 2002

9387 $\leadsto$ 24130

Page 604 insert new line at end of answer 15 ——— 01 Jan 2002

Reset *ran_arr_ptr* = &*ran_arr_sentinel* if *ran_start* is used again.

▶**Page 605** last line of answer 10 ——— 15 Feb 2006

any infinite sequence of integers with $k_{j+1} > k_j$ $\leadsto$
any doubly infinite sequence of integers with $k_{j+1} > k_j$ and $k_0 = 0$.

Page 605 line 2 of answer 12 ——— 26 May 2008

exercise 7.1–18 $\leadsto$ 7.1.3–7

▶**Page 606** line 13 of answer 18 ——— 09 Jun 2003

$|x|$ and $|y|$ are fixed $\leadsto$ $|x|$ and $|y|$ are sufficiently small

▶**Page 607** line 2 of answer 21 ——— 26 Aug 1999

the test $\leadsto$ the text

▶**Page 607** line 3 of answer 21 ——— 26 Jan 2007

the systems $\leadsto$ the system

▶**Page 608** last line of answer 24 ——— 26 Jan 2001

digits.] $\leadsto$ digits.

Page 608 bottom line ——— 03 Jun 2005

induction. $\leadsto$ induction. [A. D. Booth, in *Quarterly J. Mechanics and Applied Math.* **4** (1951), 236–240, applied this principle to two's complement multiplication.]

▶**Page 610** last two lines of answer 31(c) ——— 26 Jan 2007

$2^{-\mu}u$ is an integer. $\leadsto$ $2^r u$ is an integer, for sufficiently large r.

Page 611 replacement for answer 1 ——— 28 Jan 1999

1. $N = (62, +.60\ 22\ 14\ 00)$; $h = (37, +.66\ 26\ 10\ 00)$. Note that the quantity $10h$ would be $(38, +.06\ 62\ 61\ 00)$.

▶**Page 611** line 3 of answer 5 ——— 02 May 2000

$x \sim y \leadsto bx \sim by$

▶**Page 612** line 2 of answer 12 ——— 28 Mar 2006

we have $1/b <$ $\leadsto$ we have $1/b \le$

▶**Page 613** line 4 of answer 16 ——— 22 Mar 2002

(1963) $\leadsto$ (1962)

▸**Page 613** replacement for answer 19 ——— 10 Nov 2002

19. $\bigl(73-\bigl(5-[\text{rounding digits are } \frac{b}{2}0\ldots0]\bigr)(6-[\text{magnitude is rounded up}])+[e_v<e_u]+$ $[\text{first rounding digit is } \frac{b}{2}]-[\text{fraction overflow}]-10[\text{result zero}]+7[\text{rounding overflow}]+$ $7N+\bigl(3+(16+[\text{result negative}])[\text{opposite signs}]\bigr)X\bigr)u$, where N is the number of left shifts during normalization, and X is the condition that rX receives nonzero digits and there is no fraction overflow. The maximum time of $84u$ occurs for example when

$$u=-50\ 01\ 00\ 00\ 00,\quad v=+45\ 49\ 99\ 99\ 99,\quad b=100.$$

[The average time, considering the data in Section 4.2.4, will be less than $47u$.]

▸**Page 614** line 3 of answer 14 ——— 01 Mar 2007

$b^{2-p} \rightsquigarrow (1+b^2)b^{-p}$

▸**Page 615** line 1 of answer 16 ——— 01 Mar 2007

101.11111 $\rightsquigarrow$ 101.11110

Page 615 line -1 ——— 27 Jun 2003

For another $\rightsquigarrow$ Kahan observed that $s_n \ominus c_n = \sum_{k=1}^{n}(1+\phi_k)x_k$ where $|\phi_k| \le 2\epsilon + O((n+1-k)\epsilon^2)$. For another

Page 616 line 1 ——— 27 Jan 2000

can combine them $\rightsquigarrow$ may be able to match them up

▸**Page 616** line 5 of answer 21 ——— 09 Sep 1999

$e_u = e_u = p \rightsquigarrow e_u = e_v = p$

▸**Page 617** line 1 of answer 27 ——— 31 Jul 1998

$1 \oslash u) \oslash u \rightsquigarrow 1 \oslash (1 \oslash u)$

▸**Page 622** answer 19 ——— 27 Sep 1999

line 1: $\log 10F_n \rightsquigarrow \log_{10} F_n$
line 2: $\log 10\phi \rightsquigarrow \log_{10}\phi$

Page 625 last line of answer 22 ——— 07 Apr 2003

$b=10.)\rightsquigarrow b=10$. Similarly, when $b=2^{16}$ we can let $u=(\texttt{7fff800100000000})_{16}$, $v=(\texttt{800080020005})_{16}$.)

▸**Page 625** replacement for answer 23 ——— 23 Jan 1998

23. Obviously $v\lfloor b/(v+1)\rfloor < (v+1)\lfloor b/(v+1)\rfloor \le b$; and the lower bound certainly holds if $v \ge b/2$. Otherwise $v\lfloor b/(v+1)\rfloor \ge v(b-v)/(v+1) \ge (b-1)/2 > \lfloor b/2\rfloor - 1$.

▸**Page 626** replacement for lines 1–5 of answer 25 ——— 23 Jan 1998

25.

```
002      ENTA 1           1
003      ADD  V+N-1       1
004      STA  TEMP        1
005      ENTA 1           1
006      JOV  1F          1  Jump if v_{n-1} = b - 1.
007      ENTX 0           1
008      DIV  V+N-1       1  Otherwise compute ⌊b/(v+1)⌋.
009      JOV  DIVBYZERO   1  Jump if v_{n-1} = 0.
010  1H  STA  D           1
```

[All subsequent line numbers for Program D should now be increased by 4.]

▸**Page 627** line 1 ——— 25 Feb 1998

convex function ⇝ concave function

Page 629 last lines of answer 40 ——— 28 Dec 2000

[See T. Jebelean, ... 459.] ⇝ [See A. Schönhage and E. Vetter, *Lecture Notes in Comp. Sci.* **855** (1994), 448–459; W. Krandick and T. Jebelean, *J. Symbolic Computation* **21** (1996), 441–455.]

Page 629 line 5 of answer 41 ——— 02 May 2006

trial divisor.) ⇝ trial divisor. To compute w' when b is a power of 2, notice that if $w_0w' \equiv 1$ (modulo 2^e) then $w_0w'' \equiv 1$ (modulo 2^{2e}) when $w'' = (2 - w_0w')w'$, by the 2-adic analog of "Newton's method.")

▸**Page 630** answer 43 ——— 08 Nov 2005

$xy/255$ ⇝ $uv/255$ (twice)

▸**Page 631** displayed formula in answer 5 ——— 31 May 1999

p prime ⇝ p prime

Page 631 new sentence at end of answer 5 ——— 05 Dec 2000

Replacing 100 by 256 and allowing even moduli gives $2^8 3^5 5^3 \ldots 251^1 \approx 1.67 \cdot 10^{109}$.

Page 632 last line of answer 14 ——— 07 Apr 2003

324.] ⇝ 324. For improved error bounds, and extensions to moduli of the form $k \cdot 2^n \pm 1$, see Colin Percival, *Math. Comp.* **72** (2002), 387–395.]

▸**Page 632** line 4 of answer 1 ——— 11 Nov 1999

[shift '+03' one column to the left]

▸**Page 636** replacement for answer 9 ——— 14 May 2006

9. Let $p_k = 2^{2^{k+2}}$. By induction on k we have $v_k(u) \le \frac{16}{5}(1 - 1/p_k)(\lfloor u/2 \rfloor + 1)$; hence $\lfloor v_k(u)/16 \rfloor \le \lfloor \lfloor u/2 \rfloor /5 \rfloor = \lfloor u/10 \rfloor$ for all integers $u \ge 0$. Furthermore, since $v_k(u+1) \ge v_k(u)$, the smallest counterexample to $\lfloor v_k(u)/16 \rfloor = \lfloor u/10 \rfloor$ must occur when u is a multiple of 10.

Now let $u = 10m$ be fixed, and suppose $v_k(u) \bmod p_k = r_k$ so that $v_{k+1}(u) = v_k(u) + (v_k(u) - r_k)/p_k$. The fact that $p_k^2 = p_{k+1}$ implies that there exist integers m_0, m_1, m_2, ... such that $m_0 = m$, $v_k(u) = (p_k - 1)m_k + x_k$, and $m_k = m_{k+1}p_k + x_k - r_k$, where $x_{k+1} = (p_k + 1)x_k - p_k r_k$. Unwinding this recurrence yields

$$v_k(u) = (p_k - 1)m_k + c_k - \sum_{j=0}^{k-1} p_j r_j \prod_{i=j+1}^{k-1} (p_i + 1), \qquad c_k = 3\,\frac{p_k - 1}{p_0 - 1}.$$

Furthermore $v_k(u) + m_k = v_{k+1}(u) + m_{k+1}$ is independent of k, and it follows that $v_k(u)/16 = m + (3 - m_k)/16$. So the minimal counterexample $u = 10y_k$ is obtained for $0 \le k \le 4$ by setting $m_k = 4$ and $r_j = p_j - 1$ in the formula $y_k = \frac{1}{16}(v_k + m_k - c_0)$. In hexadecimal notation, y_k turns out to be the final 2^k digits of `434243414342434`.

Since $v_4(10y_4)$ is less than 2^{64}, the same counterexample is also minimal for all $k > 4$. One way to work with larger operands is to modify the method by starting with $v_0(u) = 6\lfloor u/2 \rfloor + 6$ and letting $c_k = 6(p_k - 1)/(p_0 - 1)$, $m_0 = 2m$. (In effect, we are truncating one bit further to the right than before.) Then $\lfloor v_k(u)/32 \rfloor = \lfloor u/10 \rfloor$ when

u is less than $10z_k$, for $1 \le k \le 7$, where $z_k = \frac{1}{32}(v_k + m_k - 6)$ when $m_k = 7$, $r_0 = 14$, and $r_j = p_j - 1$ for $j > 0$. For example, $z_4 =$ `1c342c3424342c34`. [This exercise is based on ideas of R. A. Vowels, *Australian Comp. J.* **24** (1992), 81–85.]

Page 638 last two lines of answer 18 ________ 15 Apr 1999

(Is this ... 10^4?) $\rightsquigarrow$ (The *smallest* example is actually round($(.1111111001)_2 \cdot 2^{784}$) $= .1011 \cdot 10^{236}$, round($.1011 \cdot 10^{235}$) $= (.11111110010)_2 \cdot 2^{784}$, found by Fred J. Tydeman.)

Page 638 answer 4.5.1–1 ________ 15 Jan 2002

positive. $\rightsquigarrow$ positive. (See also the answer to exercise 4.5.3–39.)

▶**Page 641** last line of answer 10 ________ 18 Feb 2004

for arbitrary f and g, when $m \le n$. $\rightsquigarrow$ when $m \le n$, $f(m) = O(m)$, and $g(n) = O(n)$.

▶**Page 641** first line of answer 14 ________ 18 Feb 2004

$(2^p - 1) \rightsquigarrow (p^2 - 1)$

▶**Page 642** line 2 of answer 17 ________ 29 Sep 2001

$u' = 1 \rightsquigarrow u' = u$

Page 645 new answer ________ 23 May 2008

32. Yes: See G. Maze, *J. Discrete Algorithms* **5** (2007), 176–186.

Page 645 new answer ________ 30 Jan 1998

34. Brigitte Vallée [*Algorithmica* **22** (1998), 660–685] has found an elegant and rigorous analysis of Algorithm B, using an approach quite different from that of Brent. Indeed, her methods are sufficiently different that they are not yet known to predict the same behavior as Brent's heuristic model. Thus the problem of analyzing the binary gcd algorithm, now solved rigorously for the first time, continues to lead to ever more tantalizing questions of higher mathematics.

Page 645 lines 4 and 5 of answer 36 ________ 03 Aug 2005

$u = \max(a_{n+2}, 2a_{n+1})$ and $v = a_{n+3} - u \rightsquigarrow u = a_{n+2}$ and $v = u + (-1)^n$

▶**Page 646** in answer 39 ________ 29 Jun 1998

line 1 of step Y6: if $t_1 < 0 \rightsquigarrow$ if $t_1 \le 0$
line 2 after step Y6: $-u$ after $\rightsquigarrow$ $-u$, $0 < u_3 \le u$, $0 < v_3 \le v$ after

Page 646 in lines -8 and -4 of answer 39 ________ 01 May 2006

after step Y2 $\rightsquigarrow$ after step Y1 (twice)

▶**Page 647** line 1 of answer 7 ________ 06 Jan 2000

$F_k F_{n-k} \rightsquigarrow F_k F_{n+1-k}$

Page 649 line 8 ________ 17 Sep 1998

59–62. $\rightsquigarrow$ 59–62. Hurwitz also explained how to multiply by an arbitrary positive integer, in *Vierteljahrsschrift der Naturforschenden Gesellschaft in Zürich* **41** (1896), Jubelband II, 34–64, §2.]

▶**Page 650** line 20 ________ 12 Jan 2006

$n!\, z^n\, {}_2F_0(n+1, -n;\,; -1/z) \rightsquigarrow z^n\, {}_2F_0(n+1, -n;\,; -1/z)$

▸**Page 650** line −3 ———— 12 Jan 2006

$$\sum_{m\ge0} z^m \rightsquigarrow \sum_{m\ge0} \frac{z^m}{m!}$$

Page 652 replacement for answer 29 ———— 13 Jan 2000

29. We have $\sum_{n=1}^N n\ln n = \frac12 N^2\ln N + O(N^2)$ by Euler's summation formula (see exercise 1.2.11.2–7). Also $\sum_{n=1}^N n\sum_{d\backslash n}\Lambda(d)/d = \sum_{d=1}^N \Lambda(d)\sum_{1\le k\le N/d} k$, and this is $O(\sum_{d=1}^N \Lambda(d)N^2/d^2) = O(N^2)$. Indeed, $\sum_{d\ge1}\Lambda(d)/d^2 = -\zeta'(2)/\zeta(2)$.

Page 653 addition to end of answer 32 ———— 19 Mar 2007

paper.) $\rightsquigarrow$ paper. Incidentally, "Morse code" was really invented by F. C. Gerke in 1848; Morse's prototypes were quite different.)

▸**Page 653** corrections to answer 34 ———— 18 Feb 2004

line 5: $s(y) = \sum_{d\backslash y} k(y/d) \rightsquigarrow s(y) = \sum_{d\backslash y} \mu(d)k(y/d)$
line 6: $\sum_{y=1}^n [d\backslash y] \rightsquigarrow \sum_{y=1}^n \sum_{d\backslash y}$

▸**Page 654** line 1 of answer 39 ———— 08 Jan 2000

and no fraction with denominator < 287 lies in $/\!/\,2,1,95/\!/ \rightsquigarrow /\!/2,1,95/\!/$

▸**Page 655** line 8 ———— 25 Jul 2000

6 (1860) $\rightsquigarrow$ **3** (1861)

▸**Page 656** last line of answer 45 ———— 18 May 2002

Theorem L $\rightsquigarrow$ Corollary L

▸**Page 657** line 15 ———— 31 May 1999

$(-1)^{(}j-1) \rightsquigarrow (-1)^{(j-1)}$

▸**Page 658** near the top ———— 14 May 1998

line 13: Henri Cohen has noticed $\rightsquigarrow$ Brent noticed
line 18: *A Course* $\rightsquigarrow$ See the analysis by Henri Cohen in *A Course*

▸**Page 658** answer 8 ———— 21 Aug 2001

line 2: $X[M] \rightsquigarrow X[M-1]$
lines 3 and 6: $k \le M \rightsquigarrow k < M$
line 7: $j \le M \rightsquigarrow j < M$

▸**Page 658** line 3 of answer 8 ———— 23 Apr 2001

$j \leftarrow 1, \rightsquigarrow j \leftarrow 1,\ k \leftarrow 1,$

Page 659 line 9 ———— 18 Oct 2006

Section 7.1 $\rightsquigarrow$ Section 7.1.3

▸**Page 659** answer 9 ———— 18 May 2002

line 8: less than N [see $\rightsquigarrow$ less than N; see
line 9: 722]. $\rightsquigarrow$ 722.]

▸**Page 662** last line of answer 22 ———— 06 Jun 1999

remarks.] $\rightsquigarrow$ remarks.

Page 663 line 9 of answer 27 ——— 07 Apr 2003

a single-precision number. ⇝ small. (See also exercise 4.3.2–14.)

Page 664 line 6 ——— 23 Nov 1998

Comp., to appear. ⇝ *Comp.* **67** (1998), 1735–1738.

▸**Page 664** line 1 of answer 29 ——— 26 Jan 2001

solutions to the equation ⇝ solutions to the inequality

▸**Page 664** line 4 of answer 32 ——— 18 Feb 2004

$M^2 - M \le y \le M^2$ ⇝ $M^2 - M \le y < M^2$

▸**Page 664** line −2 ——— 18 Feb 2004

$(\frac{\bar{x}}{N}) = 1$ ⇝ $(\frac{\bar{x}}{N}) \ge 0$

▸**Page 665** lines 2–4 ——— 18 Feb 2004

$\left(\frac{y}{N}\right) = 1$ and ... negative Jacobi symbols. ⇝ $\left(\frac{y}{N}\right) \ge 0$ and y is even. Then $y = \bar{x}$, since the other square roots of $\bar{x}^2$ are $N - \bar{x}$ and $(\pm f\bar{x}) \bmod N$; the first of these is odd, and the other two either have negative Jacobi symbols or are simply $\bar{x}$ and $N - \bar{x}$.

▸**Page 666** line −5 of answer 40 ——— 18 May 2002

$s \leftarrow r$ ⇝ $s' \leftarrow r$

▸**Page 667** line 4 ——— 21 Jan 1998

$f\left(\frac{N^3}{kp_j}\right)$ ⇝ $f\left(\frac{N^3}{kp_j}, p_{j-1}\right)$

▸**Page 667** last three lines of answer 41 ——— 26 Aug 1999

algebraic number theory ... counts, obtained ⇝ analytic number theory; see *J. Algorithms* **8** (1987), 173–191. But a refinement of the $O(N^{2/3+\epsilon})$ method in this exercise was used for the world-record prime counts obtained

▸**Page 668** answer 43 ——— 14 Feb 2000

line 4: $X_1 \cdots + X_n$ ⇝ $X_1 + \cdots + X_n$
line 23: $2r\epsilon^2$ ⇝ $2r\epsilon^{-2}$

Page 669 lines −13 and −12 ——— 02 Jul 2001

Lecture Notes ... 267–279 ⇝ *J. Cryptology* **13** (2000), 221–244.

▸**Page 670** line 14 of answer 45 ——— 06 Feb 1998

$x^2 - ay_2 \equiv 1$ ⇝ $x^2 - ay^2 \equiv 1$

▸**Page 671** line 5 of answer 46 ——— 09 Feb 1998

(modulo p) ⇝ (modulo $p - 1$)

▸**Page 676** line 4 of answer 18 ——— 03 Mar 2000

$u_1v_1 = u_1v_2$ ⇝ $u_1v_1 = u_2v_2$

▸**Page 677** line 8 ——— 26 Jan 2001

$UV = 1$ ⇝ $UV = I$.

▸**Page 677** line 12 ——— 28 Sep 2002

$T_{(j+1)j} \rightsquigarrow T_{(i+1)j}$

▸**Page 680** line 3 ——— 30 Jun 2002

)); see $\rightsquigarrow$))); see

▸**Page 681** lines 4–9 of answer 15 ——— 07 Aug 2001

in (20), or better ... for large p. $\rightsquigarrow$ suggests that $\gcd\bigl(x^2-u,(sx+t)^{(p-1)/2}-1\bigr)$ will often be a nontrivial factor; and indeed one can show that $(p-1)/2+(0,1,\text{ or }2)$ values of s will succeed. In practice, sequential choices seem to work just as well as random choices, so we obtain the following algorithm: "Evaluate $\gcd(x^2-u,x^{(p-1)/2}-1)$, $\gcd(x^2-u,(x+1)^{(p-1)/2}-1)$, $\gcd(x^2-u,(x+2)^{(p-1)/2}-1)$, ..., until finding the first case where the gcd has the form $x+v$. Then $\sqrt{u}=\pm v$." The expected running time (with random s) will be $O(\log p)^3$ for large p.

Page 681 line −8 ——— 07 Jul 1999

Pub. International Press, to appear) $\rightsquigarrow$ International Press, 1998), 1–11

▸**Page 682** lines 4 and 5 of answer 20 ——— 18 Feb 2004

$u_j = u_m \sum \alpha_{i_1} \ldots \alpha_{i_{m-j}}$ $\ldots |u_m| \sum \beta_{i_1} \ldots \beta_{i_{m-j}}$ $\rightsquigarrow$ $u_j = \pm u_n \sum \alpha_{i_1} \ldots \alpha_{i_{n-j}}$, an elementary symmetric function, hence $|u_j| \le |u_n| \sum \beta_{i_1} \ldots \beta_{i_{n-j}}$

▸**Page 684** line 2 of answer 21(e) ——— 03 Feb 2005

$[v]=[w]=2^n \rightsquigarrow [v]^2=[w]^2=2^n$

Page 686 line 2 of answer 26 ——— 19 May 2005

$D \leftarrow D \vee (D \lll d_j)$, where $\vee$ denotes bitwise "or" and $D \lll d$ denotes D shifted $\rightsquigarrow$
$D \leftarrow D \mid (D \ll d_j)$, where $\mid$ denotes bitwise "or" and $D \ll d$ denotes D shifted

▸**Page 688** line 6 ——— 06 Jun 1999

$(a+t_2) \rightsquigarrow (\alpha+t_2)$

▸**Page 688** lines 10 and 11 of answer 32 ——— 13 Jan 1998

However, ζ^p is ... divisor of $f(x)^p$ $\rightsquigarrow$
However, ζ is a root of $g(x^p)$, so $\gcd\bigl(f(x),g(x^p)\bigr)\ne 1$ over the integers, hence $f(x)$ is a divisor of $g(x^p)$. By (5), $f(x)$ is a divisor of $g(x)^p$

▸**Page 691** line 10 of answer 2 ——— 29 Mar 2000

09 $\rightsquigarrow$ *08*

▸**Page 693** line 4 of answer 15 ——— 31 Mar 1998

precisely by the $\rightsquigarrow$ precisely by not matching any of the

▸**Page 693** bottom line ——— 02 Apr 2000

$(j_i \mathinner{..} i_1] \rightsquigarrow (j_1 \mathinner{..} i_1]$

▸**Page 695** replacement for lines 2–3 of answer 27 ——— 25 May 2008

$c(r+1)$ we have $l(n)-\lambda(n) \le r-\lambda(c(r)) = l(c(r))-\lambda(c(r))$. The answers for $1 \le s \le 7$ are therefore 3, 7, 29, 127, 1903, 65131, 4169527; probably $c(36)$ will require 8.

Page 695 answer 28 — 19 May 2005

line 1: $x \vee y \vee (x+y)$, where "$\vee$" is $\rightsquigarrow$ $x \mid y \mid (x+y)$, where "$|$" is
line 2: $\nu(x \vee y) + \nu(x \wedge y)$ $\rightsquigarrow$ $\nu(x \mid y) + \nu(x \,\&\, y)$

Page 697 replacement for lines 1–5 of answer 37 — 01 Jan 2002

(Solution by D. J. Bernstein.) Let $n = n_m$. First compute 2^e for $1 \le e \le \lambda(n)$, then compute each n_j in $\lambda(n)/\lambda\lambda(n) + O\bigl(\lambda(n)\lambda\lambda\lambda(n)/\lambda\lambda(n)^2\bigr)$ further steps by the following variant of the 2^k-ary method, where $k = \lfloor \lg\lg n - 2\lg\lg\lg n \rfloor$: For all odd $q < 2^k$, compute $y_q = \sum\{2^{kt+e} \mid d_t = 2^e q\}$ where $n_j = (\ldots d_1 d_0)_{2^k}$, in at most $\lfloor \frac{1}{k}\lg n \rfloor$ steps; then use the method in the final stages of answer 9 to compute $n_j = \sum q y_q$ with at most $2^k - 1$ further additions.

Page 698 new answer — 17 Sep 2005

42. The condition fails at 128 (and in the dual 1, 2, ..., 16384, 16385, 16401, 32768, ... at 32768). Only two reduced digraphs of cost 27 exist; hence $l^0(5784689) = 28$. Furthermore, Clift's programs proved that $l^0(n) = l(n)$ for all smaller values of n.

▶**Page 699** line 2 (the displayed equation) — 28 Jun 1999

$\beta_n)$ $\rightsquigarrow$ β_n

▶**Page 699** line 7 of answer 10 — 01 Feb 2005

J. Algebra **5** (1967), 342–357 $\rightsquigarrow$ *J. Algebra* **3** (1966), 1–27.

Page 700 lines 9–12 — 10 Aug 2000

J.-C. Lafon ... If all $\rightsquigarrow$ Markus Bläser, who showed that $2n^2 + n - 3$ nonscalar multiplications are necessary for $n \ge 2$, and $mn + ns + m - n + s - 3$ in the $m \times n \times s$ case for $n \ge 2$ and $s \ge 2$ [*Computational Complexity* **8** (1999), 203–226]. If all

Page 700 append new sentence to line 4 of answer 14 — 07 Jun 2001

Replace $f_k(s_{n-k+1}, \ldots, s_n, t_1, \ldots, t_{n-k})$ by $f_k(t_1, \ldots, t_{n-k}, s_{n-k+1}, \ldots, s_n)$ in (40) if you prefer to work *in situ*.

▶**Page 701** line 3 of answer 16 — 25 Mar 2001

step C8 $\rightsquigarrow$ step T8

▶**Page 703** line 9 of answer 34 — 20 Apr 2000

that uses λ_j $\rightsquigarrow$ that uses λ_i

▶**Page 707** last line of answer 42 — 28 Jun 1999

180.] $\rightsquigarrow$ 180.

▶**Page 713** line −4 — 10 Oct 1999

bit-reversal in s'.) $\rightsquigarrow$ bit-reversal in s'.

▶**Page 714** lines 10 and 11 of answer 60 — 21 Apr 2002

indices of the other. $\rightsquigarrow$ indices $[k,i,j]$ of the other, and work with an $(mn{+}sm) \times (ns{+}mn) \times (sm{+}ns)$ tensor.

▶**Page 715** line 3 of answer 64 — 28 Jun 1999

$zk3$ $\rightsquigarrow$ z_{k3}

▸**Page 715** line 3 of answer 66 ________ 30 Oct 2005

sufficiently large N $\rightsquigarrow$ sufficiently large n

▸**Page 722** line 2 of answer 16 ________ 22 Apr 1999

$\frac{d}{dt}(R_{k+1}(t)/V(t)^n)$ $\rightsquigarrow$ $\frac{d}{dt}(R_k(t)/V(t)^{n+1})$

Page 722 line 4 of answer 19 ________ 08 Jan 2003

These coefficients arise $\rightsquigarrow$ These coefficients, called partial Bell polynomials [see *Annals of Math.* **35** (1934), 258–277], arise

Page 724 last line of answer 26 ________ 11 Jul 1999

to appear $\rightsquigarrow$ *J. Symbolic Computation* **26** (1998), 339–341

Page 727 Table 2 . . . . 06 May 1999

In the next edition I plan to give these constants to 36 hexadecimal places, instead of 45 octal places.

▸**Page 730** entry for Kronecker delta ________ 14 Aug 1998

1.2.6 $\rightsquigarrow$ 1.2.3

▸**Page 731** entry for $\Im z$ ________ 26 Jan 2001

imaginary part z $\rightsquigarrow$ imaginary part of z

▸**Page 733** entry for $\exp x$ ________ 09 Aug 1999

1.2.2 $\rightsquigarrow$ 1.2.9

Page 735 and following ________ 22 Aug 1997

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.