Errata and clarifications for *Prime numbers: a computational perspective*, **2nd edition**

Updated May 28, 2008

R. Crandall and C. Pomerance

==========

p. 14, the stated largest twin prime pair (of D. Papp, 2004) has been doubted; rather than deny/verify that, we simply state here the current largest twin:

$$2003663613 \cdot 2^{195000} \pm 1,$$

per Caldwell's site `http://primes.utm.edu`

p. 20, Conjecture 1.2.3. Change "If $x \geq y \geq 2$, then" to "For integers $x \geq y \geq 2$, we have".
Also, on the last line of the page, insert "integers" at the start of the line.
Also, on p. 81, line 3, insert "integer" before "y".

p. 23, error in Mersenne table:

$$2^{9869} - 1 \text{ should be } 2^{9689} - 1.$$

p. 23, last line, "Chapter 8.8" should be "Chapter 9".

p. 40, paragraph near bottom starting "It is a touch...":
Change "a touch" to "just slightly". Replace "3" with "5" (four times) and replace "$2^{a-1} + 1$" with "$2^{a-1} - 1$" (three times).

p. 42, line -5. Change "$(a, d$" to "(a, d)".

p. 47, 5 lines after (1.40). Change "and are" to "are".

p. 47, line -7. Change "machinations" to "and complicated work".

p. 57, Ex. 1.31. Change [Vaughan] to [Vaughan 1997].

p. 59, Ex. 1.36, second Skewes number should be $10^{10^{10^{964}}}$. (The given expression with e's is correct, but this new version is typographically simpler and easier to compare with the first Skewes number.) Then, remove the sentence "An amusing . . . " appearing lower in the problem.

p. 63, Exercise 1.45. Change "Conjecture, 1.2.1" to "Conjecture 1.2.1".

p. 75, Exercise 1.77, line -7. Change "the more general question" to "this more general question".

p. 78, Exercise 1.86. Change "pi" to "π" (two times).

p. 147, line -9, change $V(c, 1)$ to $V_m(c, 1)$.

p. 156, line -8, change $x^{1/6}$ to $x^{1/3}$.

p. 160, both equations (3.28) and (3.29), change differentials "$\frac{ds}{s}$" to "ds".

p. 162, equation (3.31), change "$F(s)$" to "$F(s,x)$".

p. 186, step [Initialize]. Change expression given for (c_0, c_1) to $(0, r^*(n - rr')/s \bmod s)$.

p. 226, 4th line of last paragraph, change "$\gcd(kn, n)$" to "$\gcd(a - b, n)$".

p. 229, last paragraph, before the word "Clearly" insert the following:
"We are not looking to find two equal iterates of F, but rather two equal iterates of $f(x) = x^2 (\bmod\ p)$. How can we do this knowing only F?"

p. 251, Ex. 5.4.

Change "It is easy to see" to "Prove".

Change "Show the converse. That is if f is any function" to "Show the converse does not hold. That is, there are positive integers n and non-polynomial functions f"

Change the parenthetical to "(Thanks are due to K. Hare who pointed out to us that such functions exist.)"

p. 253, Ex. 5.8. Change the display in part (1) to

$$n = 67030894509517639 = 179424673 \cdot 373587943.$$

In part (2), change the number given to 373587942.
In part (4), change the ending of the sentence to:

$B' = 3000$ (or just use $B = 3000$ with no second stage).

Introduce new part (5):

(5) Amend Algorithm 5.4.1 so that for each prime $p_i \leq B$ we take the exponent a_i as the largest integer with $p_i^{a_i} < n$. Use this version of the algorithm with $B = 100$ and $B' = 1000$ to factor the integer $n = 670308837440379259$.

p. 262, line 15, change ",," to ",".

p. 273, line -14, change $(\frac{p}{n})$ to $(\frac{n}{p})$.

p. 276, line 6, change mod a to mod p.

p. 283, line -11, change $(3+i)(2+i)(1+i)$ to $(3-i)(2-i)(1-i)$.

p. 283, line -9, change $(3+i)(2-i)(1+i) = 8+6i$ to $(3-i)(2+i)(1-i) = 8-6i$.

p. 284, line -13, change $N(\alpha - r)$ to $N(r - \alpha)$.

p. 293, line -13, change $V \times \#S'$ to $\#S' \times V$.

p. 294, line 2, remove }.

p. 297, line -2, change α to $c\alpha$ and change $\beta \in \mathbf{Z}[\beta]$ to $\delta \in \mathbf{Z}[C\beta]$.

p. 298, line 3, change $u - c^k F_x(cm, c)v$ to $v - c^k F_x(cm, c)w$.

p. 300, line 9, change n^d to m^d.

p. 303, line −8, change $+\log_g p_k$ to $+\tau_k \log_g p_k$.

p. 306, line 12, change O_k to O_K.

p. 327, in step [Elliptic double function], change

$$Y' = M(S - X_2) - 8Y^4 \text{ to } Y' = M(S - X') - 8Y^4$$

p. 345, line −6, change "667" to "677" (twice).

p. 388, in the lead-in to Alg. 8.1.1, change "encryption key:" to "encryption key. Though we describe the Diffie–Hellman key exchange in the context of $\mathbf{F}_p^*$, one can (and often does) use other cyclic groups."

p. 390, Algorithm 8.1.4 line 4. Change "}))" to "}])".

p. 392, line -4. Change "may" to "many".

p.393, line −9. Remove comment "//Note that $R \neq 0$." and add new instruction as a new line just below: "if($R == 0$) goto [Alice signs];".

p. 397, line 2. Change "$n = pq$" to "modulo $n = pq$".

p. 403, Algorithm 8.2.7, line 8. Change $[1, 2^{18}]$ to $[1, 2^{18} - 1]$.

p. 405, Definition 8.3.1, line 1. Remove "at least".

p. 412, line 19: Change $n = 1$ to $n = N$; line 20: Change $n = 99$ to $n = 99N$.

p. 412, line -6, change π_5 to $\pi_{5 \cdot 10^6}$.

p. 417, line -9. Change "the solutions" to "whether or not there exist solutions".

p. 422, line 11. Change $\sum_{a=0}$ to $\sum_{c=0}$.

p. 465, in Algorithm 9.4.4 change "not necessarily prime" to "necessarily prime".

Following the discussion on p. 466, l. 3, put in the following: "It may be an interesting problem to investigate this algorithm when p is not necessarily prime. In particular, does it usually work to find the inverse when p does not have any small prime factors?"

p. 481, Algorithm 9.5.6, step 2, change "$d \geq i > 0$" to "$d \geq k > 0$". In addition add new comment on this line: "// Variable k, as with j below, is a dummy counter."

p. 548, [Bach 1990]. The volume number is 55.

p. 549, [Bailey et al. 2003]. Change "2003" to "2004" and in text where this is referred to (p. 80). (This citation is missing from the index; it should be indexed.) Change "Bordeau" to "Bordeaux". Change "(to appear), 2003." to "16 : 487–518, 2004."

p. 549, [Bernstein 1997]. Delete "em Advances ... appear."

p. 551, [Bruin 2003]. Change "2003" to "2005" (and in text, where this is referred to: p. 417 and p. 441). Delete url. Change "to appear." to "111: 179–189, 2005."

p. 556, [Engelsma 2004 1999]. Delete “1999”.

p. 566, [Ohi 2003]. Change “Ohi” to “Oki”.

p. 574, in [Williams 1998], change “Edouard” to “Édouard” and change “Mathematics” to “Mathematical”.