Errata for *Factorization and Primality Testing*

I no longer recommend REXX for implementing factorization and primality testing algorithms. It was chosen because it was available and allowed arbitrary precision. I would now recommend using Mathematica or Maple or programming directly in C.

The best of the packages for factorization and primality testing — indeed for general work in computational number theory — is PARI-GP, a C-based high level language that is available free at
http://www.parigp-home.de/
For more information on packages, see appendix A of Henri Cohen's "A Course in Computational Algebraic Number Theory."

If you have access to Mathematica, you may want to refer to the recent book by Stan Wagon and myself, A Course in Computational Number Theory, which gives all of the algorithms in Mathematica code:
http://www.keycollege.com/Pages/ProdBressoudCompThry.html

Note: line 7 refers to the 7th line as counted from the top of the page, line 7b refers to the 7th line as counted from the bottom of the page.

page 10, line 18 should read

$$v_1 \leftarrow 0; v_2 \leftarrow 1; v_3 \leftarrow b$$

page 12, lines 1-5 should read

```
PULL_TWOS:      WHILE a and b are even DO
                        a ← a/2
                        b ← b/2
                        e ← e + 1
                a ← REDUCE(a)
                b ← REDUCE(b)
```

page 12, lines 13-15 should read

```
REDUCE(x):      IF x = 0 THEN RETURN
                WHILE x is even DO
                        x ← x/2
                RETURN
```

page 14, line 11b "than" should read "then"

integer, then the square root ...

page 16, line 6b should read

$r_1/r_2 = m_3 + r_3/r_2$

page 20, lines 15-19 should read

```
SIEVE(j):        i ← 2 × j
                 WHILE i ≤ n DO
                       a_i ← 0
                       i ← i + j
                 RETURN
```

page 20, line 24 should read

And if you want to use it to prove

page 22, line 5 should read

BIG_PRIME: IF $d^2 >$ f AND f $\neq 1$ THEN DO

page 23, line 6 should read

$496 = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248,$

page 27, line 7 should read

S $\leftarrow$ (S $\times$ S $-$ 2) MOD M.

page 39, lines 4 and 5 should read

$2^{p-1} = (2^4)^m \times 4 \equiv 4 \pmod 5$, and
$2^p - 1 = 2^{p-1} \times 2 - 1 \equiv 7 \pmod 5$, and so

page 51, line 16 should read

variables suppressed.

page 68, line 7b should read

or this algorithm does not work with this value of `c`.

page 72, lines 4b and 5b should read

19 931 831
392 583 509

page 74, line 7 should read 78 59947 71339

page 82, lines 3 and 4 should read

$b^r \equiv 1 \pmod{p}$ *and* $b^s \equiv 1 \pmod{p}$, *then*
$b^g \equiv 1 \pmod{p}$.

page 85 lines 3 and 4 should read

6.4 Same problem as Exercise 6.3 but with 2 replaced by 3.

6.5 Same problem as Exercise 6.3 but with 2 replaced by 5.

page 88, line 5b and 6b should read

Corollary 7.2 *The Legendre symbol (-1/p) is +1 if* $p \equiv 1 \pmod{4}$ *and is -1 if* $p \equiv 3 \pmod{4}$.

page 89, line 13 should read

$$r_i \equiv b \times (2i-1) \pmod{p}, \quad 0 < r_i < p.$$

page 89, line 4b should read

$p - r_1, p - r_2, \ldots, p - r_t, r_{t+1}, r_{t+2}, \ldots, r_m$

page 106, line 4b should read

congruent to 3 modulo 8, then multiply it by 3, if congruent to 5 then

page 115, line 1, “4330” should read “4340”

page 116, line 13b should read

36 30-digit vectors, ...

page 120, line 1 Algorithm 8.7 should read Algorithm 8.3

page 122, line 1b should read

35419 05253 35205 94597 94529

page 149, line 5, 11/13 should be 11/3

page 154, line 7,

$$\frac{p_{i-2}+a_ip_{i-1}}{q_{i-2}+a_iq_{i-2}} \quad \text{should read} \quad \frac{p_{i-2}+a_ip_{i-1}}{q_{i-2}+a_iq_{i-1}}$$

page 184, lines 9 and 11, (D/P) should read (D/p)

page 191, exercises 12.4 and 12.5, change "fifty" to "twenty"

page 192, line 14 should read

$$F_i = \frac{(1+\sqrt{5})^i - (1-\sqrt{5})^i}{2^i\sqrt{5}}$$

page 193, exercise 12.18, Replace "compute V_i" with "find the last fifty digits of V_i (*ie* calculate V_i modulo 10^{50})"

page 206, line 9 should read

$$(x_4, y_4) = (4,3)\partial(0,2) \qquad \lambda \equiv (3-2)\times 4 \equiv 4 \pmod 5,$$

page 233, 417 should be 419

I would greatly appreciate communication of any other errors or misprints you might find. E-mail: bressoud@macalester.edu, snailmail: Department of Mathematics & Computer Science, Macalester College, St. Paul, MN 55105, USA. Thank you for your interest in my book.

David M. Bressoud