Hugh C. Williams, Édouard Lucas and Primality Testing

page 71, 17 ↓: the line is too long

page 77, 2 ↑: upper bound of sum is $\lfloor (m-1)/2 \rfloor$ and not $\lfloor m/2 \rfloor$.

$$(4.2.28) \quad 2^{m-1}U_{mn} = \sum_{i=0}^{\lfloor \frac{m-1}{2} \rfloor} \binom{m}{2i+1} D^i U_n^{2i+1} V_n^{m-(2i+1)}$$

page 79, 8 ↑: $\binom{n-k-1}{k-1}$ instead of $\binom{n-k-1}{k}$

page 81, 4 ↓: $\cdots + 14Q^{2n}V_n^3 - \cdots$ instead of $\cdots + 14Q^{2n}V_n^5 - \cdots$

page 81, 7 ↑: $\dfrac{\alpha^{mj+k} - \beta^{mj+k}}{\delta}$ instead of $\dfrac{\alpha^{mj+r} - \beta^{mj+r}}{\delta}$

page 84, 3 ↑:

$\equiv 2Q^{(1-\varepsilon)/2}(1 + (Q/p)) \pmod p$ instead of $\equiv 2Q^{(1-\varepsilon)/2}(1 + (Q/p))$

page 85, 11 ↓: $\cdots \equiv p\, U_n V_n^{p-1}$ instead of $\cdots \equiv U_n V_n^{p-1}$

page 87, 3 ↑: $p^{\lambda+\mu+1} \mid U_{mp^{\mu+1}}$ instead of $p^{\lambda+\mu+1} \nmid U_{mp^{\mu+1}}$

page 197, 6 ↓: $\overline{V}_{p-\sigma\varepsilon}$ instead of $V_{p-\sigma\varepsilon}$

page 197, 15 ↓: $\overline{U}_k \mid \overline{U}_n$ instead of $\overline{U}_k \mid \overline{U}_m$

page 215, 11 ↓: $\mathcal{F}$ instead of F

page 215, 15 ↓: $4x^2 + 1$ instead of $4n^2 + 1$

page 215, 6 ↑: The numbers in numbered formulas are mostly in an upright fond, but here (and also in line 6 ↑ on page 219) in italics

page 217, 18 ↑: *vector space* instead of *vector a space*

page 226, 9 ↑: $= \gamma_j^{-k}\Phi_p(\gamma_j) =$ instead of $= \Phi_p(\gamma_j) =$

page 227, 7 seqq. ↑: q is not a prime because $q \equiv 2 \cdot 1^n + 1 \equiv 0 \pmod 3$

page 227, 2 ↑: $s \equiv 2^{14 \cdot 13^{j-1}} \pmod q$ instead of $s \equiv 2^{14 \cdot 13^{j-1}}$

page 228, 17 $\uparrow$ and 6 $\uparrow$: $(\mathrm{mod}\ q)$ instead of $(\mathrm{mod}\ p)$

page 228, 15 $\uparrow$: $\log^8 q$ instead of $\log^8 p$

page 229, 3 and 5 and 6 $\downarrow$ and 1 $\uparrow$: $(\mathrm{mod}\ q)$ instead of $(\mathrm{mod}\ p)$

page 232, 9 $\downarrow$: the last element in the second row of the upper matrix should be ρ_k instead of ρ_n

page 235, 4 $\downarrow$:

$$\prod_{\substack{j=1\\ j\neq i}}^{k} h_j(\alpha_i) \quad \text{instead of} \quad \prod_{\substack{j\neq i\\ i,j=1}}^{k} h_j(\alpha_i)$$

page 237, 10 $\downarrow$: the second formula instead of the first formula

page 238, 9 $\downarrow$: $\sum_{j=0}$ and $Y_{j,n}$ instead of $\sum_{i=0}$ and $Y_{i,n}$

page 239, 14 $\downarrow$: $P_3 W_{1,n} W_{2,n+1}$ instead of $P_3 W_{0,n} W_{2,n+1}$

page 239, 15 $\downarrow$: $P_3 W_{1,n+1} W_{2,n}$ instead of $P_3 W_{0,n+1} W_{2,n}$

page 239, 16 $\downarrow$: $W_{2,n}$ instead of W_{2n}

page 239, 18 $\downarrow$:

$$\cdots + W_{0,n+1} W_{2,n} + W_{0,n} W_{2,n+1}$$

instead of

$$\cdots - W_{0,n+1} W_{2,n} - W_{0,n} W_{2,n+1}$$

page 239, 19 $\downarrow$:

$$+ P_1 W_{2,n} W_{1,n+1} + P_1 W_{1,n} W_{2,n+1}$$

instead of

$$+P_1 W_{0,n} W_{1,n+1} + P_1 W_{1,n} W_{0,n+1}$$

page 242, 4 $\downarrow$: divisibility instead of divisiblity

page 244, 1 $\uparrow$: $\sum_{h=1}^{n}$ instead of $\sum_{h=1}^{h}$

page 251, 1 $\uparrow$: $\alpha^{*^{\psi_1 p^2}} = \alpha^{*^{\psi_1}}$ instead of $\alpha^{*^{\psi_1 p^2}} = \alpha^{*^{\psi_1 p^2}}$

page 253, 12 $\uparrow$: 2^{1-n} instead of 2^{n-1}

page 253, 8 ↑: If $n = 1$, I get

$$J/N^k \le (1 + p^{-k})/p^{(\alpha_1 - 1)(k-1)} \le (1 + p^{-k})/p$$

and therefore $J/N^k \le 4/9$, if $k \ge 2$.
(Perhaps p should better be p_1.)

page 260, 1 ↑: ζ_q^t instead of ζ^t

page 264, 12 ↑: $\prod_{j=1}$ instead of $\prod_{i=1}$

page 269, 6 ↓: A_θ instead of A_ω

page 269, 16 ↑: $|V_{1,n}|$ instead of $|V_1, n|$

page 271, 7/8 ↓: primitive root of p^m instead of primitive root of p

page 272, 4 ↑: Theorem 11.2.7 instead of Theorem 11.2.6

page 273, 16 ↓: $\equiv W_{A/2}^2 - 1 \pmod N$ instead of $\equiv W_{A/2}^2 - 1$

page 275: The notation $C(0, q, 5)$ and $C(1, q, 5)$ in the header of Table 11.3.1 is not consistent with the notation $C(i, p, q)$ on page 274.

page 294, 5 and 8 and 11 ↓ and page 295, 8 ↑: S_{1i} instead S_i
Similarly: S_1, S_2, S_3 on page 296 should be S_{11}, S_{12}, S_{13}.

page 295, 12 ↑: R_1 instead of R

page 300, 3 ↓: $s_1 s_2$ instead of $s_2 s_2$

page 319, 4 ↑: compiled instead of complied

page 327, 11 ↓: $1 \le k < n$ instead of $1 \le k \le n$

page 336, 4 ↑: currently instead of curently

page 363, 14 ↑: $\overline{P} = \left(\overline{X}_0 : \overline{Y}_0 : \overline{Z}_0\right)$ instead of $\overline{P} = \left(\overline{X}_0, \overline{Y}_0, \overline{Z}_0\right)$

page 379, 11 ↓: $\sum_{i=1}^{m} \alpha_i k_i$ instead of $\sum_{i=1}^{m} \alpha_k k_i$

page 381, 7 ↓: $|\, E(N)\,|$ instead of $E(N)$

page 382, 11 ↑: $|\,S(N)\,|$ instead of $S(N)$

page 398, 3 ↑: $P_2(x)$ instead of $P_b(x)$

page 410, 16 ↑: provides (?) instead of processes

page 412, 15 ↑: nonresidue of N instead of nonresidue N

page 415, 12 ↓: $(q_1 - 1)/2$ instead of $(p_1 - 1)/2$

page 419, 16 ↓: pseudosquares instead of psuedosquares

page 423, 8 ↓: $S_1 \equiv W_A(P,Q) \pmod{N}$ instead of $S_1 \equiv W_A(P,Q)$ *(mod N)*

page 423, 12 ↓: $Q^{-(N+1)/4}$ instead of $Q^{(N+1)/4}$

page 424, 9 ↑: $q \equiv 1 \pmod{p}$ instead of $q \equiv 1 \pmod{r}$

page 426, 1 ↓: $(N_n/q_i)_p$ instead of $(N_n/q)_p$

page 426, 14 ↓: $< 1.2 \times 10^{-9}$ instead of $< 1 \cdot 1 \times 10^{-9}$

page 432, 6 ↑: $(-q_0/r) = -1$ instead of $(-q/r) = -1$

page 435, 6 ↑: $(\alpha + \beta)^n \equiv \alpha^n + \beta^n$ instead of $(\alpha + \beta)^n = \alpha^n + \beta^n$

page 435, 3 ↑: residues as t does instead of residues at t does

page 437, 10 ↑: delete the □

page 438, 2 ↑: $r^{p-1} - 1$ instead of $r^{n-1} - 1$

page 440, 6 ↓: $\omega(\chi)$ instead of $\chi(\omega)$

page 440, 1 ↑: condition (iv) instead of condition (ii)

page 441, 5 ↑: $\equiv$ instead of $=$

page 442, 12 ↓: prime p compute instead of prime, p compute

page 445, 5 ↑: $(\overline{X} : \overline{Y} : \overline{Z})$ instead of $(\overline{X}, \overline{Y}, \overline{Z})$

page 445, 3 ↑: s divides $|\,E(\mathbb{F}_r)\,|$ instead of $s \mid E(\mathbb{F}_r)$

page 446, 1 ↓: Theorem 14.4.4 instead of Theorem 14.4.6

page 455, Table 17.4.1, column 2, row 4: $-5 \cdot 11$ instead of -5.11

page 455, Table 17.4.1, column 3, row 3: $-3 \cdot 43$ instead of -989

page 455, Table 17.4.1, column 3, row 8: $53 \cdot 107$ instead of 5671

page 455, Table 17.4.1, column 3, row 9: $-2^9 \cdot 83$ instead of $-29 \cdot 83$

page 455, Table 17.4.1: some entries have a "-"-sign instead of a "−"-sign

page 471, 5 ↓: *Comptes* instead of *Compte*

page 471, 2 ↑: *Grand-Ducal* instead of *Grad-Ducal*

page 473, 17 ↑:
Computers in Mathematical instead of *Computers and Mathematical*

page 473, 2 ↑: *Schriftenreihe* instead of *schriftenreihe*

page 474, 1 ↓: Untersuchungen instead of Untersuchen

page 479, 3 ↓: *Multiplikatorenringe* instead of *Multiplicationenringe*

page 479, 4 ↓: *Funktionenkörper* instead of *Functionenkörper*

page 482, 7 ↓: Studien instead of studien

page 485, 3 ↓: *Math. Comp.* instead of *math. comp.*

page 487, 17 ↑: *Werke*, Vol. 1 instead of *Werke*, volume Vol. 1

page 487, 11 ↑: pseudoprimes instead of pseudorprimes

page 489, 10 ↓: *Scripta Math.* instead of *Scripta. Math.*

page 494, 1 ↑: *Mathematik* instead of *mathematik*

page 507, 13 ↓: insbesondere instead of Insbesondere

page 507, 14 ↓: zweifelhaften instead of sweifelhaften

page 507, 15 ↑: Form instead of form

page 509, 11 ↓: Multiplikation instead of multiplikation

page 510, 4 ↑: Auflösung instead of auflösung