**Errata for Elliptic Curves: Number Theory and Cryptography**
**by Lawrence C. Washington**

page 5, line -5: change "integer" to "rational"

page 7, line 5: change 881/6 to 881/60

page 7, line 17: the displayed formulas should be

$$x = 2\frac{b^2+c^2}{a^2}, \quad y = 4\frac{b(b^2+c^2)}{a^3}$$

page 10, line -7: the coefficient of $x$ should be $a_4 + \frac{a_1 a_3}{2}$

page 12, Figure 2.2: The point $P'$ in the diagram should be $P'_3$.

page 14, line 11: change $L$ to $E$

page 21, line -5: change $u - \frac{u_0}{v_0}$ to $u - u_0$

page 21, line -4: change $(v_0 u - u_0)^k$ to $(u - u_0)^k$

page 21, line -3: change $H(u,v) = v^{m-k}h(u/v)$ to $H(u,v) = (v^{m-k}/v_0^m)h(uv_0/v)$

page 21, line -1: this line should read:

$$G(u,v) = \left(\frac{v}{v_0}\right)^m g\left(\frac{uv_0}{v}\right) = \frac{v^{m-k}}{v_0^m}\left(v_0 u - u_0 v\right)^k h\left(\frac{uv_0}{v}\right) = (v_0 u - u_0 v)^k H(u,v),$$

page 23, line -12: change $-(3x^3 + A)$ to $-(3x^2 + A)$

page 23, Definition 2.4: change $\mathbf{P}^1_K$ to $\mathbf{P}^2_K$

page 25, line 18: add comma between 0 and $b_3$

page 25, line 20: change $F_z/_x$ to $F_z/F_x$

page 26, lines 10, 11: change "Since $P_{11}, P_{12}, P_{13}$ lie on $m_j$, we have $\tilde{m}_j(u_i, v_i) = 0$ for $i = 1, 2, 3$" to "Since $P_{1,j}$ lies on $m_j$, we have $\tilde{m}_j(u_j, v_j) = 0$ for $j = 1, 2, 3$"

page 28, line -13: the first "$\geq$" can be replaced by "$=$"

page 32, line 9: add "or $Q + R = R$"

page 32, line 12: Add the sentence "The case $Q + R = R$ is similar."

page 37, line 9: change "$x$ to $x + p$" to "$u$ to $u + p$"

page 39, line 1: change "first" to "second"

page 41, line 15: change $v = \frac{1-2m-2m^2}{1+m^2}$ to $v = \frac{1-2m-m^2}{1+m^2}$

page 41, line -9: change "Weierstrass equation" to "generalized Weierstrass equation"

page 41, line -6: change $y_1^2 = x^3 + 2x^2 - 5x + 8$ to $y_1^2 = x^3 + 2x^2 - 5x - 6$

page 42, line -3: change "$\Delta \neq 0$" to "$4A_i^3 + 27B_i^2 \neq 0$"

page 43, line -3: change "defined over $\overline{K}$." to "defined over $\overline{K}$)."

page 44, line 8: change $y$ to $y_0$

page 48, line -9: change "Section 2.8" to "Proposition 2.27"

page 50, line-6: change $\alpha_1$ to $\alpha$

page 51, line 15: change $z^3 + Aa + B$ to $a^3 + Aa + B$

page 52, line 14: the $a$ should be $A$ (4 occurrences)

page 53, line -5: change 2.23 to 2.25

page 56, line 15: change "Substituting $x_i = 1/t_i^3$ yields" to "Substituting $x_i = 1/t_i^2$ and $y_i = 1/t_i^3$ yields"

page 59, line 1: change $x = \frac{4\alpha t_i}{(t_i-1)^2}$ to $x = \frac{4\alpha^2 t_i}{(t_i-1)^2}$

page 59, line 4: change "$= x =$" to "$=$"

page 59, line 10: change $t_1 t_2 = t_2$ to $t_1 t_2 = t_3$

page 60, line -8: the curve should be $y^2 = x^3 + 3x - 3$

page 60, line -6: the second coordinate of the point should be 16379/6859 (positive, not negative)

page 61, line -4: change "a primitive $m \times n$ matrix" to "an $m \times n$ matrix" (primitivity is assumed later in the sentence)

page 64, line -9: change $(x_3'', y_3'', z_3'') = (20, 12, 0)$ to $(x_3''', y_3''', z_3''') = (20, 12, 0)$

page 65. line 6: change "if" to "is"

page 67, line 9: change $3x^3 + A$ to $3x^2 + A$

page 67, line 13: change "2.1" to "page 18, Section 2.2"

page 68, line 16: change $(1 : 1, 0)$ to $(1 : 1 : 0)$

page 69, line -18: the second equation should be $y^2 = x^3 + a_4' x + a_6'$

page 69, line -16: the change of variables should be $y \mapsto ay$, $x \mapsto bx + c$, with $a, b \in \overline{K}^\times$ and $c \in \overline{K}$.

page 77, line 13: change $m \geq 2$ to $m \geq 3$

page 80, line 7: change $a$ to $A$ and $b$ to $B$

page 90, line 6: the equation should be $0 = x^3 - 4x^2 + x + 1$

page 92, line -1: the first $\phi$ should be $\phi_q$

page 94, lines 1, 3: change $\phi^n - 1$ to $\phi_q^n - 1$

page 94, line 7: change $\phi$ to $\phi_q$

page 96, lines 5, 7, 8, 9 (twice): change $\phi$ to $\phi_q$

page 98, line 7: change $+\left(\frac{-1+\sqrt{-7}}{2}\right)^2$ to $-\left(\frac{-1-\sqrt{-7}}{2}\right)^2$

page 98, line 15: change the second $\sqrt{-7}$ to $-\sqrt{-7}$

page 101, line 16: change "the elliptic curve $x^3 + 7x + 12$" to "the elliptic curve $y^2 = x^3 + 7x + 12$"

page 103, line -12: the line should be "$M$ is the order of the point $P$"

page 103, line -10: change "greatest" to "least"
page 104, line 16: change $(M/p_i)P$ to $(M/p_i)g$
page 107, line -10: change "points at infinity" to "the point at infinity"
page 112, line -3: remove one of the equality signs
page 115, line 9: change $q_\ell = q$ to $q_\ell \equiv q$
page 115, line -10: change $(x, y)$ to $q_\ell(x, y)$
page 115: the last few lines should read as follows:

for integers $j$. We may compute $x_j$ and $y_j$ using division polynomials, as in Section 3.2. Moreover, $x_j = r_{1,j}(x)$ and $y_j = r_{2,j}(x)y$, as on page 47. We have

$$x' = \left(\frac{y^{q^2} - y_{q_\ell}}{x^{q^2} - x_{q_\ell}}\right)^2 - x^{q^2} - x_{q_\ell}.$$

Writing

$$\begin{aligned}\left(y^{q^2} - y_{q_\ell}\right)^2 &= y^2\left(y^{q^2-1} - r_{2,q_\ell}(x)\right)^2 \\ &= (x^3 + Ax + B)\left((x^3 + Ax + B)^{(q^2-1)/2} - r_{2,q_\ell}(x)\right)^2,\end{aligned}$$

page 118, line 4: change $(y' - y_j)$ to $(y' - y_j^q)$
page 118, line -3: change $x^2 + 13x + 14$ to $x^2 + 12x + 14$
page 119, line -5: change $(x_1, y_1)$ to $(x', y')$ and change $(x_2, y_2)$ to $(x'', y'')$
page 120, line 2: change $x_1$ to $x'$ and change $x_2$ to $x''$
page 120, line 7: change $(x_1, y_1)$ to $(x', y')$
page 120, line 12: change $(y_1 + y_2^{19})$ to $(y' + y_2^{19})$
page 120, line 14: change $(x_1, y_1)$ to $(x', y')$
page 121, line 10: change $a_{n-1}$ to $s_{n-1}$
page 121, Corollary 4.30: $E$ is defined over $\mathbf{F}_\mathbf{p}$
page 122, line 7: insert "if" after "only"
page 124, line -10: change the sentence to "By Proposition 4.29, $E$ is supersingular if and only if $A_q = 0$ in $\mathbf{F}_q$.
page 129, line 5: change $\delta_{2 \pmod 3}$ to $\delta_{2(3)}$ and change $\delta_{3 \pmod 4}$ to $\delta_{3(4)}$
page 129, line 8: change $j = 1728$ to $j = 0$
page 130, Exercise 4.2: it should be $2^n + 1 - 2(-2)^{n/2}$ if $n$ is even
page 130, line -13: change $\left(\frac{r-s}{\mathbf{F}_q}\right)$ to $-\left(\frac{r-s}{\mathbf{F}_q}\right)$

page 131, line 15: change "Show that if $n$ is sufficiently large, then" to "Use Hasse's theorem in the form $a^2 \leq 4q$ to show that"

page 131, line 21: change (2) to (b)

page 132, line 8: change $\#E(\mathbf{F}_q)$ to $\#E^{(d)}(\mathbf{F}_q)$

page 132, line 10: change $\mathbf{F}_2$ to $\mathbf{F}_q$

page 132, line -14: change $a^2 = 4b^2$ to $a^2 - 4b^2$

page 135, line -16: change $\pmod{1217}$ to $\pmod{1216}$

page 135, line -3: change *exp* to exp

page 136, line 10: Insert "For simplicity, it is usually assumed that $P$ generates $G$."

page 136, line -11: change $k_0 = k$ to $k_0 \equiv k$

page 137, line 7: change $0 \leq i \leq 7$ to $1 \leq i \leq 7$

page 138, line -7: change $(v_j + b_j)Q$ to $v_j + b_i)Q$

page 149, line 7: change $\tilde{E}_1$ to $\tilde{E}_r$

page 150, lines -16 to -13: Remove the sentences "Usually ... 2.10." and replace with "Since $\tilde{P}_1 \in \tilde{E}_2$, we have $p^2$ in the denominator of $x$, so $\tilde{P}_1$ is already at $\infty$ mod $p^2$. Therefore, we cannot obtain information directly from calculating $\lambda_1(\tilde{P}_1)$ ."

page 151, lines 8-14: The curve should be $\tilde{E}: \quad y^2 = x^3 + 7522715x + 4$. The point $\tilde{Q}$ should be $(563, 66436)$. The point $\tilde{P}_2$ should be $(159511, 58855)$ and the point $\tilde{Q}_2$ should be $(256463, 645819)$. Also,

$$m_1 = 853\frac{58855 - 2}{159511 - 0} = \frac{58853}{187}$$

and

$$m_2 = 853\frac{645819 - 66436}{256463 - 563} = \frac{579383}{300}.$$

(The curve given in the original text works if it is regarded as a curve mod $853^2$.)

page 151, line -4: this actually should say that $a/(b + O(p^k))$ can be changed to $(a/b) + O(p^k)$. (The problem with "=" is that the right side sometimes cannot be changed back to the left side.)

page 152, line 4: the denominator $v - x_1$ should be $u - x_1$

page 154, line 6: change $\tau_n(P_1 + P_1, Q)$ to $\tau_n(P_1 + P_2, Q)$

page 155, lines 11, 12: change $\pmod{p}$ to $\pmod{\ell}$

page 155, line -9: change $\phi^m \equiv I$ to $((\phi_q)_l)^m \equiv I$

page 156, line -4: change "$Q - jP$ for $j = 0, 1, 2, \cdots, m$" to "$Q - jmP$ for $j = 0, 1, 2, \cdots, m - 1$"

page 156, line -2: change "$Q - jP$ to "$Q - jmP$"

page 162, line -9: change "Joux [43]" to "Joux [43] (see also [E. Verheul, Evidence that XTR is more secure than supersingular elliptic curve cryptosystems, in B. Pfitzmann (ed.), Eurocrypt 2001, Springer LNCS 2045 (2001) 195–210.])"

page 165, line 5: change $\mathbf{E}(\mathbf{F_q})$ to $E(\mathbf{F_q})$

page 168, line 5: change $h(m_1) = h(m_2)$ to $H(m_1) = H(m_2)$

page 168, line 17: change $V_1 = f(R)B + sR$ to $V_1 = f(R_H)B + s_H R_H$

page 171, line 13: change "Equation 6.1" to "(6.1)"

page 171, line -16: change $Z_n$ to $\mathbf{Z_n}$

page 173, line -2: change *idbob* to *bobid*

page 174, line -5: change $\tilde{e}$ to $\tilde{e}_\ell$

page 175, line 1: change $\tilde{e}$ to $\tilde{e}_\ell$

page 175, line 4: (4 times) change $\tilde{e}$ to $\tilde{e}_\ell$

page 175, line -4: change ")" to ".)"

page 176, line -11: insert "for some $n \not\equiv 0 \pmod{p}$" after $E(\mathbf{F_p})$

page 180, lines -5, -6: change 4553 to 4453

page 181, line 14: change "prime factors of $B$" to "prime factors of $m$"

page 183, line -6: change $x^2(x-1)$ to $x^2(x+1)$

page 187, line -5: change $t^2 - 2$ to $t_1^2 - 4$

page 188, line 11: change $Pmodp$ to $P \bmod p$

page 190, line 14: $E_r/E_{r+1}$ should be $E_r/E_{5r}$

page 191, line 2: change $Ast^2$ to $Ats^2$

page 191, line -11: insert "(and therefore $E_r$ is a subgroup)" before ". Therefore"

page 192, line -15: change $s = t^3 + Ats^2 = Bs^3$ to $s = t^3 + Ats^2 + Bs^3$

page 192, line -15: change $(t, s) = (x/y, 1/y)$ to $(s, t) = (1/y, x/y)$

page 193, lines 3, 5, 6, 8: change $3s^2$ to $3Bs^2$

page 193, line 6: change $(t, s)$ to $(s, t)$

page 193, line -1: change $(t_1, s_1)$ and $(t_2, s_2)$ to $(s_1, t_1)$ and $(s_2, t_2)$

page 194, line 2: change $s^2 = t^3 + As^t + Bs^3$ to $s = t^3 + Ats^2 + Bs^3$

page 195, line 6: change "$P \in E_{4r}$. Since $4r > r$" to "$P \in E_{5r}$. Since $5r > r$"

page 196, line -18: change $17B^2$ to $27B^2$

page 197, line -10: change "order 12 times a power of 7" to "order dividing 12 times a power of 7"

page 197, line -7: change "group of" to "in"

page 199, lines -16 to -13: change "Note that ... same sign." to "Since $x(x-1)(x+2) = y^2 > 0$, we have $cw^2 = x+2 > 0$, so $c > 0$. Since $abc > 0$, it follows that $a$ and $b$ must have the same sign."

page 200, line 3: change $(-2, 2, -1)$ to $(-2, -2, 1)$

page 200, line -10: change "Write" to "Assuming that $x, y \in \mathbf{Q}$, write"

page 201, line 18: change $v_1$ to $u$

page 202, line -11 to page 203, line 6: Franz Lemmermeyer pointed out that the argument can be simplified as follows: By inspection, $\phi_1(P)\phi_2(P)\phi_3(P) = 1$ for all $P$. Since $\phi_i(P_1)\phi_i(P_2) = \phi_i(P_1 + P_2)$ for $i = 2, 3$, the relation holds for $i = 1$, too. Therefore, $\phi$ is a homomorphism.

page 203, line -12: change the first $e_1$ to $v_1$

page 203, line -11: change the first $e_2$ to $v_2$

page 203, line -10: change the first $e_3$ to $v_3$

page 204, line 15: change $u_2/u_2^3$ to $1/u_2^2$

page 205, line 3: change $(-2, 2, -1)$ to $(-2, -2, 1)$

page 207, line 16: Add $H(x, y) = H(x), \quad H(\infty) = 1$ to the displayed formula.

page 209, line 4: the displayed formula should be $|h(P+Q)+h(P-Q)-2h(P)-2h(Q)| \leq c_1$

page 209, line 4: the displayed formula should be $\frac{1}{4^n}|h(2^nP + 2^nQ) + h(2^nP - 2^nQ) - 2h(2^nP) - 2h(2^nQ)| \leq \frac{c_1}{4^n}$.

page 210, line -5: remove "with $\gcd(c_i, d_i) = 1$ for $i = 1, 2$"

page 211, line 8: change $c_1d_2$ to $c_2d_1$

page 212, line 9: change $b_3b_3$ to $b_3b_4$

page 217, line -6 to page 218, line 13: The argument in the last 6 lines of page 217 is incorrect and not needed. The whole argument can be simplified with the following:

Let $(a, b)$ be any pair. There is a point $P$ with $\phi(P) = (a', b)$ on the list $L$ for some $a'$. If there is a point $Q$ with $\phi(Q) = (a, b)$, then

$$\phi(P - Q) = (a', b)(a, b)^{-1} = (a'', 1)$$

for some $a''$. We showed that $(a'', 1)$ is not in the image of $\phi$ when $a'' \neq 1$. Therefore, $a'' = 1$, so $a = a'$ and $(a, b) = (a', b) = \phi(P)$. Consequently, the only pairs in the image of $\phi$ are those on the list $L$.

page 223, line 10: change "Equation 8.13" to "(8.13)"

page 224, line 7: change "Equation 8.14" to "(8.14)"

page 227, line 4: the equation should be $y'^2 = x'^3 - 2Cx'^2 + (C^2 - 4A)x'$

page 227, line 6: $C$ should be $A$

page 227, line 8: switch $A$ and $C$

page 230: The statement of Theorem 8.28 should read: *If* $p \equiv 9 \pmod{16}$, *then* $C_{1,p,p}$ *has q-adic points for all primes* $q \leq \infty$, *but has no rational points.*

page 231, line 17: change "Equation 8.15" to "(8.15)"

page 231, line -15: change $p = 2$ to $q = 2$

page 237, line -2: add a right parenthesis at the end of the sentence

page 238, line -14: change $T_0$ to $T_g$

page 238, line -5: change $T_{g-1g_2}$ to $T_{g_1g_2}$

page 239, line -15: change $\tau_{phi_i}$ to $\tau_{\phi_i}$

page 240, line 3: change "Equation 8.24" to "(8.24)"

page 242, lines 8, 13, 14: change $g\sqrt{p}$ to $g(\sqrt{p})$

page 242, line 12: add a right parenthesis at the end of the sentence

page 244, line -5: (twice) change $\phi$ to $\psi$

page 244,line -1: change $\phi$ to $\psi$

page 247, line -2: change $C/L$ to $\mathbf{C}/L$

page 250, line -11: change $f =$ to $f(z) =$

page 253, line 12: the double integral should be multiplied by 1/area of $F$

page 254, line -12: remove "adding a"

page 255, line 15: change the second $\wp(z)$ to $f(z)$

page 258, line -6: change "By 9.1" to "By Theorem 9.1"

page 256, line 6: change $\omega_3$ to $\omega$

page 263, line -4: change "$k \geq 1$" to "$k \geq 2$"

page 264, line -9: change $(2\pi i)^k$ to $(2\pi i)^{2k}$

page 268, line -2: change $\alpha + \mathbf{Z}\beta$ to $\mathbf{Z}\alpha + \mathbf{Z}\beta$

page 273, line 16: change $\mu^{-2}$ to $\mu^{-4}$

page 279, line 2: change the second displayed formula to $b_n \geq \sqrt{b_{n-1}b_{n-1}} = b_{n-1}$

page 279, line 6.5: Insert "Therefore, $a_n - b_n \leq (1/2)^n(a-b)$, so $a_n - b_n \to 0$."

page 284, line 3: change $f$ to $f_n$

page 285, line 6: change $\omega_i$ to $\omega_j$

page 285, line -10: the last factor should be squared

page 285, line -9: remove the $-$, so the line should read $= \left(1 - \frac{1}{n^2}\right) z^{-2} + \cdots$,

page 292, lines 5 and 7: the summations should start at $n = 0$ instead of $n = 1$

page 292, line 14: the sum should be for $z \neq i, \rho, i\infty$

page 293, line 7: change $\{y + \frac{1}{2}y, 2y\}$ to $\{y + \frac{1}{2}i, 2y\}$

page 293, line -3: change $\frac{\sqrt{1-x^2}}{\sqrt{1-k^2x^2}}$ to $\frac{\sqrt{1-k^2x^2}}{\sqrt{1-x^2}}$

page 294, line 3: change $4aE(\sqrt{1-(a/b)^2})$ to $4bE(\sqrt{1-(a/b)^2})$

page 294, line -6: change $\int_1^\infty \frac{dx}{x(x^2-1)}$ to $\int_1^\infty \frac{dx}{\sqrt{x(x^2-1)}}$

page 295, line -3: change $i\wp(z)$ to $i\wp'(z)$

page 297, line 9: change $\tilde{\alpha}(z)$ to $\tilde{\alpha}(h)$

page 298, line -12: change $\delta$ to $f\delta$

page 299, line 15: change $\beta = a$ to $\beta = j$

page 299, line -9: change $4x^4$ to $4x^4$

page 303, line 5: change $R$ to $\mathcal{R}$

page 307, line -3: Insert "By multiplying by $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ if necessary, we may also assume that $s > 0$.

page 308, line 5: Insert "$\in S_N$" after the matrix.

page 308, line -9: change $j \circ S$ to $(j \circ S)(\tau)$

page 317, line -4: change $(1, \pm 17, 43), (5, \pm 11, 67), (21, 29, 29)$ to $(17, \pm 1, 43), (11, \pm 5, 67), (29, 21, 29)$

page 318, lines 7, 8, 9(twice), -8, -7: change $a$ to $a_p$

page 319, line3: change $a$ to $a_p$

page 321, line -1: change the second factor to $(a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k})$

page 327, line 7: the denominator of the fraction should be $x - x_3$

page 327, line -13: change $P_1 + P_1$ to $P_1 + P_2$

page 328, line -9: change $E(K)$ to $E(\overline{K})$

page 330, line 4: change $\mathrm{ord}_Q = 0$ to $\mathrm{ord}_Q(f) = 0$

page 330, line 11: the superscript on $h$ should be $\mathrm{ord}_Q(f)$

page 331, line 8: change $P_1^3 + AP_1^2P_2 + BP_2^3$ to $P_1^3 + AP_1P_2^2 + BP_2^3$

page 336, line -10: change $f \circ \tau_{jT}$ to $f \circ \tau_{jT} \circ n$

page 338, line 9: (6) should be be (5)

page 349, line -11: change $\deg(\mathrm{div}(\mathcal{K}))$ to $\deg(\mathcal{K})$

page 358, line 8: the factors in the product should be $\left(1 - \frac{1}{p^s}\right)^{-1}$

page 362, line -4: change the first half of the line to "$f_E(\tau)$ is a modular form (in fact, a cusp form (see page 376)) of weight 2 and level $N$."

page 363, line -1: change $e^t$ to $e^{-t}$

page 365, line -5: change $\sqrt{112}\pi$ to $\sqrt{11}/2\pi$

page 376, formula 13.6: change $\sum_{n=1}^{\infty} b_n q^{rn}$ to $\sum_{n=1}^{\infty} r b_n q^{rn}$

page 379, line 5: change $\rho_{\mathcal{M}}$ to $\rho$

page 388, line -7: change $p$ to $\tilde{p}$

page 396, lines 11, 12, 16: insert $\ell \notin S$ in the product and move "where $S$ is a finite set of bad primes (in our example, $S = \{5, 17, 37\}$)" to line 12

page 403,line -6: change $g^i = g^j$ to $ig = jg$ page 412, Proposition C.7: The assumption that the set is finite can be changed to assuming that the set is countable, with essentially the same proof.

page 412, line -10: Change C.7 to C.5

(last updated 9/27/2007)

Many thanks to Satoshi Tomabechi, Ashvin Rajan, Michael Cheng, Susan Schmoyer, Pinaki Das, Simon Allewaert, David Goldberg, Steven Galbraith, Chris Christopoulos, Robin Chapman, Keith Conrad, Cory Brunson, Gottfried Barthel, Ryuji Tsushima, Ning Shang, Tsz Wo Sze, Anders Nielsen, Jerry Metzger, Ralph May, Susan Margulies, Franz Lemmermeyer, Will Murray, Chang An Zhao, Rainer Urian, Qiao Zhang, Rahul P, and Koichiro Harada for finding the above errors.