Errata for
Elliptic Curves: Number Theory and Cryptography, 2nd ed.

by Lawrence C. Washington

page vi, line 17: Insert a period at the end of the sentence.

page xviii, line -2: the references start on page 499 (not 501).

page 17, Example 4: The sentence “The real points \( E(\mathbb{R}) \) are obtained by intersecting the torus with a plane.” is not accurate. If the torus is in \( \mathbb{C}^2 \), regarded as \( \mathbb{R}^4 \), then the plane \( \text{Im}(x) = \text{Im}(y) = 0 \) intersects the torus in the real points. However, this is not the case with the torus in \( \mathbb{R}^3 \). The real points in this case could correspond to one or two non-contractible circles on the torus. In the first case, this is not the intersection of a plane in \( \mathbb{R}^3 \) with the torus. The last sentence of the example (“If it does not pass through the hole . . .”) is not correct.

Exercise 2.18 (d): \( y^2 = x^3 + a'_4x^2 + a'_6 \) should be \( y^2 = x^3 + a'_4x + a'_6 \)

page 92, Exercise 3.1(b): the gcd equals \( x(x - 1) \)

page 109, lines 17-22: change \( n \) to \( m \) (13 times) and change \( m \) to \( n \) (once)

page 125, line 6: change page 47 to page 51.

page 150, line -2, to page 151, line 4: this paragraph and the preceding description of the lambda method do not match Pollard’s explanation of kangaroos, which are assumed to have bounded jump length. See Pollard’s paper [87] and his more recent paper in J. of Cryptology 13 (2000), 437-447.

page 155, line -1: This will give \( k \) (mod \( d_1 \)) for some divisor \( d_1 \) of \( d \).

page 156, line 2: change \( d \) to \( d_1 \) (in the notation of the preceding correction)

page 163, line 17: \( m_2 \) should equal 579383/300

page 174, line 17: \( 0 \leq m < p/100 \) should be \( 0 \leq m \leq (p/100) - 1 \)

page 209, line -16: change \( x(x - 1)(x + 2) \) to \( x(x - 2)(x + 2) \)

page 340, line 18: change \( u(P) = 0 \) to \( u_P(P) = 0 \)

page 371, line 10: \( c(nV, vW) \) should be \( c(nV, nW) \)

page 393, line 3: The \( q_g^y \) at the end of the formula for \( Y \) should be \( g_q^y \)
page 413, line 14: change $k = -P(a)/2$ to $k = -P(a)/(2b)$

page 479, line -8: the first $G_2$ should be $G_3$

Many thanks to Andreas Peter, Ten H Lai, John M. Pollard, Loren Olson, John McColgan, Yu Tsumura, Dan Shumow, John Jones, Daniel Lännström, Leif Nilsen, Gianira Alfarano, and Rene Schoof for pointing out some of the above errors.