

**ERRATA AND CORRECTIONS TO
AN INTRODUCTION TO MATHEMATICAL CRYPTOGRAPHY
FIRST EDITION**

JEFFREY HOFFSTEIN, JILL PIPHER, JOSEPH H. SILVERMAN

Acknowledgements

We would like to thank to the following people who have sent us comments and corrections: Robert Bond, Rebecca Constantine, Stephen Constantine, Yamamoto Kato

Page xiv

In the last line of the summary of Chapter 6, “covereed” has an extra “e”.

Page 4, lines 2 and 11

The last part of the ciphertext should be SCVKC B, instead of SCVKV B, and the plaintext is *caesar*, not *caeser*. (But note that it has been corrected on line 14!).

Page 21, Line 17

The text says here that the Euclidean algorithm takes $2 \log_2(b) + 3$ steps, but Theorem 1.7 on page 13 states (and proves) that the Euclidean algorithm takes at most $2 \log_2(b) + 1$ steps.

Page 27, Line -6

In the reference to [126, Chapter 7], the word Chapter is misspelled.

Page 28, Line -11

“described in Exercise 1.28” should be “described in Exercise 1.29”

Page 33, Line 6

$$1 \equiv a^n \equiv a^{kq+r} \equiv (a^k)^r \cdot a^r \equiv 1^r \cdot a^r \equiv a^r \pmod{p}.$$

should be

$$1 \equiv a^n \equiv a^{kq+r} \equiv (a^k)^q \cdot a^r \equiv 1^r \cdot a^r \equiv a^r \pmod{p}.$$

(In the middle formula, $(a^k)^r$ is changed to $(a^k)^q$.)

Page 36, Line 19

“Germany introduced a new Enigama machine”. The name of the machine has an extra “a”, it should be “Enigma”.

Page 47, Problem 1.1(b)

There is an extra “L” in the ciphertext. The block in the middle that currently reads “ZLJYL ALZAO” should read “ZLJYL AZAO”.

Page 73, Example (f)

Although the group G is noncommutative, the matrices used as an example actually commute. The example should read

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Page 74, Proof of Proposition 2.13

There is some confusion with i and j in the first paragraph of the proof. It should read as follows:

Proof. Since G is finite, the sequence

$$a, a^2, a^3, a^4, \dots$$

must eventually contain a repetition. That is, there exist positive integers i and j with $j < i$ such that $a^i = a^j$. Multiplying both sides by a^{-j} and applying the group laws leads to $a^{i-j} = e$. Since $i - j > 0$, this proves that some power of a is equal to e . We let d be the smallest positive exponent satisfying $a^d = e$.

Page 94, Part (c)

We should say that R is always a ring, and it is a field precisely when n is prime.

Page 109, Exercise 2.20

$x = a + cn$ should be $x = a + cm$ in line 3, and $x = a + cn + ymn$ should be $x = a + cm + ymn$ in line 5.

Page 288, Line -9 and -7

There’s an arithmetic error in these calculations, although it does not affect the final answer. (λ should be 12, not 1, although note that 12 is the same as -1 , since we’re working in \mathbb{F}_{13} .) These lines should read as follows:

$$\lambda = \frac{3x_1^2 + A}{2y_1} = \frac{3 \cdot 9^2 + 3}{2 \cdot 7} = \frac{246}{14} = 12 \quad \text{and} \quad \nu = y_1 - \lambda x_1 = 7 - 12 \cdot 9 = 3.$$

Then

$$x_3 = \lambda^2 - x_1 - x_2 = (12)^2 - 9 - 9 = 9 \quad \text{and} \quad y_3 = -(\lambda x_3 + \nu) = -(12 \cdot 9 + 3) = 6,$$

Page 295, Line above equation (5.6)

Replace “for some $t \geq 1$ ” by “for some $t \geq 2$ ”, since we want at least two consecutive ones.

Page 344, Exercise 5.22(b)

The displayed equation should read

$$t_k = t_1 t_{k-1} - 2t_{k-2} \quad \text{for all } k \geq 3.$$

There are two corrections: the pt_{k-2} is changed to $2t_{k-2}$, and the condition $t \geq 3$ has been changed to $k \geq 3$.

Page 344, Exercise 5.23

The upper bound on ℓ should be $\ell \leq 2\lceil \log n \rceil + 1$. We say in the proof of Proposition 5.30 that it is possible to get $\ell \approx \log n$ and we give a reference. However, the algorithm given in Exercise 5.23 seems to only return an expansion with $\ell \leq 2\lceil \log n \rceil + 1$.