

Mathematical Ciphers: From Caesar to RSA
Errata
April 11, 2011

page viii

My apologies to Erica Flapan and Gordon Prichett misspelling their names.

page 23, lines 3 and 6:

$$73 - 26 \cdot 2 = 73 - 52 = 21, \quad 73 \equiv 21 \pmod{26}$$

$$-45 + 26 \cdot 2 = -45 + 52 = 7, \quad -45 \equiv 7 \pmod{26}$$

page 24, last line:

$$r \cdot w \equiv s \cdot \text{~~w~~} \pmod{n}$$

page 50:

8. The ordinary Cancellation Law does not always hold in modular arithmetic. Find an example for which $a \cdot b \equiv a \cdot c \pmod{n}$, but $b \not\equiv c \pmod{\text{~~n~~}}$.

page 56:

1. The ciphertext

PXXTSOVCN AT DPEC PJ JTTC PJ P XRUARSF EPJ SFPXEFO P XFSAPVC
UFIFU XSHKATNSPKEH PKKFPSJ JKTCAPCFTRJUH

was enciphered ... [Find the plaintext.](#)

page 97:

The number of positive integers less than or equal to n that are relatively prime to n is denoted by $\phi(n)$.

page 97:

How do we determine $\phi(n)$? One way is to do what we did in Examples 15.3, 15.4, and 15.5. Namely, we could list those positive integers less than or equal to n that are relatively prime to n and then count the number of integers in the list.

page 99, solution of 15.8:

$$\dots \text{ found that } \phi(231) \text{~~! = 120.
$$120 \cdot 231 \text{~~! = 27,720~~$$~~$$

page 123:

$$a^{k \cdot j} = a^{\phi(n) \cdot t + 1} \tag{3}$$

(i.e., $\phi(\text{~~n~~}) \cdot t + 1$)

page 125:

Exponential Cipher Theorem for the product of two distinct primes:

page 139, line above (6):

... we calculate $H^7 H^5$

page 141:

1. This exercise uses the RSA public key list in Example 22.1. On behalf of Sharon, encipher the following message and signature to Alice:

page 141:

5. In designing an RSA Cipher, Emilie has selected primes $p = 1423$ and $q = 3719$. Hence, her modulus is

$n = 1423 \cdot 3719 = 5292137$. Since $k = 5$ is relatively prime to 1422 and 3718~~423 and 3719~~, Emilie has decided to use 5 as her public exponent. Find her private exponent.

page 146:

The converse of the Composite Test is not true. That is, there are composite numbers n for which $a^{n-1} \equiv 1 \pmod{n}$ for all a .

page 154:

Chapter 5

~~7.~~ W

~~8.~~ P

Chapter 8

2. ~~15~~ 25; impossible; ~~9~~ 11; impossible

Chapter 15

2. 2; 6; 4; 6; 4; ~~4~~6; 8; 6; 20; 18; 12; 12; 48

5. ~~almost 24 hours~~ 69.75 hours

Chapter 16

5. ~~1084~~ 513

page 155:

Chapter 22

1. ... 455346 ~~16097~~ 45055

5. ~~5286996~~ 4229597

Note: I want to thank David A. Brannan (Emeritus Professor, Mathematics and Statistics Department, The Open University, UK) and Eve Torrence (Professor of Mathematics, Randolph-Macon College, Ashland, VA) for their contributions to this Errata Sheet.