

**TYPOS TO BE CORRECTED IN THE SECOND EDITION**

1. On page 10, in Footnote 1.25, change “nomenclatures” to “nomenclators”. Also, make this change in lines 13-14 (above the footnotes) on that page; as well as its singular on page 11, line 18.
2. Thanks also go to students in PMAT 321 at U of C, during the Fall 2002 term, for pointing out that the statement of the Rabbit Problem on page 20 is unclear with respect to the solution of the problem (Exercise 1.11) given on page 304. The following is a corrected statement to replace the paragraph on page 20.

Suppose that a male rabbit and a female rabbit have just been born. Assume that any given rabbit reaches sexual maturity after one month and that the gestation period for a rabbit is one month. Furthermore, once a female rabbit reaches sexual maturity, it will give birth every month to exactly one male and one female. Assuming that no rabbits die, how many male/female pairs are there after  $n$  months?

3. On page 21, delete the last sentence of the proof of Theorem 1.6 and replace it with the following.  
Given that

$$(2^{st} - 1) = (2^s - 1) \sum_{j=0}^{(t-1)} 2^{js},$$

then for  $s > 1$ ,  $(2^s - 1) \geq 3$ , so  $(2^{st} - 1)$  is composite if  $t > 1$ . In other words,  $n$  is prime whenever  $2^n - 1$  is prime.

4. On page 29, the statement of part (b) of Exercise 1.19 should read:  
(b) If  $p \mid (a^n - 1)$ , then  $p = nb + 1$  for some  $b \in \mathbb{N}$ , or  $p \mid (a^k - 1)$ , where  $k \mid n$ .  
This is consistent with the solution of the exercise on pages 304–305. Thanks go to James Robert Buchanan of Millersville University of Pennsylvania, who is also responsible for pointing out typos in part 7 below.
5. There is a small typo in Definition 2.39 on page 81. In line 4 of the definition  $m = (m_1 m_2 \dots m_r)$  should be  $m = (m_1, m_2, \dots, m_r)$ .

6. On page 82 in Definition 2.40, replace the second and third sentences by:

For  $e = (e_1, e_2, \dots, e_r) \in \mathcal{K}$ , and  $m = (m_1, m_2, \dots, m_s) \in \mathcal{M}$ , let

$$E_{e_j}(m_j) = m_j + e_{j \pmod{r}} \pmod{n} \text{ for all } j = 1, 2, \dots, s,$$

and for  $c = (c_1, c_2, \dots, c_s) \in \mathcal{C}$ , let

$$D_{d_j}(c_j) = c_j - e_{j \pmod{r}} \pmod{n} \text{ for all } j = 1, 2, \dots, s.$$

This cryptosystem is called the *Vigenère cipher* with period  $r$ , which is why the subscript on the key is taken modulo  $r$  (where we choose  $r$  rather than 0 in order to keep all subscripts positive).

7. On page 85, line 5, add that  $e \in \mathcal{K}$ .
8. On page 90, in  $\mathbf{S}_3$ , the sixth entry in the first row should be a 3 instead of a 13.  
On page 101, in Exercise 43, the ciphertext should read *MGFSDYGPPHLH* instead of *MGSDYGPPHLH*.

9. The next two typos were pointed out by Professor Nikos Tzanakis of The University of Crete, Greece.  
On page 94, line -5 ( $b_1 \dots b_{48}$ ) should be ( $b_1 \dots b_{56}$ ).

On page 118, in Example 2.64, replace sentences 6–7 by:

Then we encipher via:  $E_{k_j}(m_j) = m_j + k_j \pmod{n} = c_j$  for  $j = 1, 2, \dots, r$ , and

$$E_{k_j}(m_j) = m_j + m_{j-r} \pmod{n} = c_j \text{ for } j > r,$$

and decipher via:  $D_{k_j}(c_j) = c_j - k_j \pmod{n} = m_j$  for  $j = 1, 2, \dots, r$ , and

$$D_{k_j}(c_j) = c_j - m_{j-r} \pmod{n} = m_j \text{ for } j > r.$$

10. On page 139, line 10, “ $c$  knowing only” should be  $m$  knowing only<sup>1</sup>.
11. On page 145, in Exercise 3.15, line 3, replace “ciphertext  $c$ ” by “plaintext  $m$ ”.
12. Thanks go to Robert Buchanan of Millersville University, PA for finding the following two typos.  
On page 154, line 17, the displayed equation should be

13. Thanks go to Nichole Robinson (a student of Robert Buchanan (see item ??), whose class is clearly diligent). Nichole observed that although the conclusion of Example 4.22 on page 169 is correct, it cannot be deduced from Theorem 4.17 which does not apply since  $g$  does not divide  $b = 4$ . The conclusion can be deduced from, for instance, trying to solve the congruence via index calculus employing 2 as a primitive root modulo 27.

Also, on page 191, on line 19,

$$\text{In the latter case, } (p-1) \mid 2^j m \text{ and } 2^j m \mid (n-1),$$

should be:

$$\text{In the latter case, } (p-1) \mid 2^{j+1} m \text{ and } 2^{j+1} m \mid (n-1),$$

Moreover, on page 191, line -3: "If  $x \equiv 1 \pmod{n}$  for any such  $j$ ," should be:

$$\text{"If } x \not\equiv -1 \pmod{n} \text{ for any such } j\text{"}$$

14. On page 180, line -6 above the footnote,  $j = 1, 2, \dots, n-1$  should be  $j = 2, 3, \dots, n-1$ .
15. On page 228, line 10, delete the subscript 1 on  $m$  in the expression for  $B$ . Also, on that page, line -5,  $P + Q + R = 0$  should be  $P + Q + R = \mathfrak{o}$ . These are thanks to Robert Buchanan and his class, especially Sean Laverty.
16. On page 256, in Example 6.4,  $r = 98 = m \cdot t_A^c$  should be replaced by  $r = 98 = m \cdot s_A^c$ .
17. On page 315, in the solution of Exercise 3.5, the two displayed equations with  $(\text{mod } p)$  should be replaced with  $(\text{mod } p-1)$ .