# Errata for
# *From Mathematics to Generic Programming*

Alexander A. Stepanov and Daniel E. Rose
Addison-Wesley Professional, 2015
www.fm2gp.com

[This document was last edited December 23, 2015.]

Note: Page numbers refer to print edition. Locations in the Kindle edition are also shown, as a number in brackets with a "k" prefix.

## Third Printing, August 2015

p. 48, 3rd line after Lemma 4.1 [k1051]: "If the result is less than 10" should be "If the result is less than or equal to 10"

p. 92, line 9 [k1820]: "because of our invertibility axiom:" should be "because:"

p. 105, 2nd line after multiplication tables [k2099]: "In theory, there are $4! = 12$ possible mappings…" should be "In theory, there are $4! = 24$ possible mappings…" (Reported by Dave Shapiro.)

P. 116, 4th line after code [k2289]: "slight-of-hand" should be "sleight-of-hand" (Reported by David Sanders.)

p. 134, Exercise 8.2 [k2661]: The exercise originally contained errors and used ambiguous notation. It should be replaced by the following:

> Prove that for any polynomial $p$ and any value $a$, there is a polynomial $q$ such that:
>
> 1. $p = q \cdot (x - a) + p(a)$
> 2. $p(a) = 0 \implies p = q \cdot (x - a)$

(Reported by Daniel Harvey.)

p. 146, equations for Matrix-Vector product and Matrix-Matrix product [k2902]: The upper bound of the summation in the second form of both equations should be $m$, not $n$. That is, the equations should read:

$$w_i = \sum_{j=1}^{m} x_{ij} v_j$$

and

$$z_{ij} = \sum_{k=1}^{m} x_{ik} y_{kj}$$

respectively. (Reported by Jim Shapiro.)

p. 203, line 2 [k4075]: "While the compiler cannot check this condition today, we can indicate it with a comment in the code" should be "While concepts are not yet in the language, we express the required equality of value types with a comment in the code." (Reported by Peter Sommerlad.)

p. 223, Eqn. 12.7 [k4531]: The last variable in the equation should be a $p$, not a $q$. That is, Eqn. 12.7 should read

$$\deg(p) < \deg(q) \implies \gcd(xp + c, xq + d) = \gcd\left(xp + c, q - \frac{d}{c}p\right)$$

(Reported by Peter Sommerlad.)

p. 244, line 10 [k4957]: The value of $k$ in the factorization of 2792 should be 3, not 2. That is, the sentence should read "We factor $n-1 = 2792$ into $2^3 \cdot 349$, so $q = 349$ and $k = 3$." (Reported by Ryan McLean.)

p. 244, line 16 [k4966]: "…and $i = k$…" should read "…and $i = k$ next time the loop starts…"

p. 246, line 22 [k5021]: The "$(n)$" should be part of the superscript exponent in both equations:

$$\ldots a^{\phi}(n) - 1 \text{ is divisible by } n\text{; that is, } a^{\phi}(n) = 1 + vn$$

should be

$$\ldots a^{\phi(n)} - 1 \text{ is divisible by } n\text{; that is, } a^{\phi(n)} = 1 + vn$$

p. 247, line 1 [k5028]: The text starting "Since $p_1$ and $p_2$ are enormous primes…" and concluding at the end of the paragraph should read:

Since $p_1$ and $p_2$ are enormous primes, that probability is practically indistinguishable from 1. If we wanted absolute certainty, we could append an extra byte to the message to ensure that it is coprime. However, it turns out that our initial statement can be shown with other proof techniques, beyond the scope of this book, that do not have the coprime requirement, so this step is not necessary.

(Reported by Yongwei Wu.)

## First and Second Printing, November/December 2014

p. 14, paragraph following `multiply3` code listing [k468]: "…we're making `mult_acc4` do one unnecessary test for $n = 1$…" should be "…we're making `mult_acc4` do one unnecessary test for `odd(n)`…" (Reported by Nitin Kumar.)

p. 19, line 11 [k536]: "…the first $n$ integers…" should be "…the first $n$ positive integers…" (Reported by Alexander Slinkin.)

p. 19, last line of text [k541]: "…the first $n$ integers…" should be "…the first $n$ positive integers…" (Reported by Alexander Slinkin.)

p. 20, line 1 [k541]: "…sum of the first $n$ integers…" should be "…sum of the first $n$ positive integers…" (Reported by Alexander Slinkin.)

p. 20, first line after figure showing squares [k547]: "…the first $n$ odd numbers…" should be "…the first $n$ positive odd numbers…" (Reported by Alexander Slinkin.)

p. 22, line 14 [k580]: "…Eratosthenes already knew that even numbers were not prime…" should be "…Eratosthenes already knew that even numbers greater than 2 were not prime…" (Reported by Abutalib Aghayev.)

p. 25, line 1 [k639]: "step between multiple $k$ and multiple $k + 1$ …" should be "step between multiple $k$ and multiple $k+2$ …" (Reported by Anil Pal, Greg Ives, and Miguel Pinkas.)

p. 25, line 3 [k639]: The second equation, which currently reads

$$= \text{index}(2ki + 3n + 4i + 6) - \text{index}(2ki + 3n)$$

should read

$$= \text{index}(2ki + 3k + 4i + 6) - \text{index}(2ki + 3k)$$

(Reported by Daniel Roldán.)

p. 29, last paragraph of text before Thm. 3.3 [k734]: "…when the the second term is prime" should be "…when the second term is prime." (Reported by Jeremy Murphy.)

p. 31, lines 12 and 13 [k754]: The list of factors on both lines is missing the term, $2^3 3^0$. (Reported by Andy Lawman.)

p. 41, second to last line [k918]: "…the only three-dimensional shapes" should be "…the only convex three-dimensional shapes…" (Reported by Alexander Slinkin.)

p. 44, line 27 [k966]: "…proves that they are the only regular polyhedra" should be "…proves that they are the only regular convex polyhedra…" (Reported by Alexander Slinkin.)

p. 126, line 1 [k2516]: "Even in this small example, the computation does 17 additions, and just the quantity $F_1 + F_0$ is recomputed 5 times" should be "Even in this small example, the computation does 7 additions, and just the quantity $F_1 + F_0$ is recomputed 3 times." (Reported by Boris Vassilev.)

p. 131, line 23 [k2602]: The sentence beginning "Stevin's idea was..." should be "Stevin's idea was to find the interval between two consecutive integers where the function goes from negative to positive, then divide that interval into tenths, and repeat the process with the tenths, hundredths, and so on." (Reported by Alexander Slinkin.)

p. 133, line 9 [k2648]: "To multiply, we multiply every combination of elements" should be "To multiply, we compute the product of every pair consisting of one coefficient from each polynomial." (Reported by Alexander Slinkin.)

p. 164, line 11 [k3178]: "…based on the the assumption that the fifth postulate …" should be "…based on the assumption that the fifth postulate …" (Reported by Jeremy Murphy.)

p. 168, line 7 [k3266]: "at the the University of Königsberg…" should be "at the University of Königsberg…" (Reported by Jeremy Murphy.)

p. 185, last line of "Bidirectional iterators" paragraph [k3643]: "then $y$ has a predecessor" should be "then $y$ has a predecessor $x$."

p. 201, line 6 [k4022]: "We'll look at reverse in greater detail in the next chapter" should be "We'll look at reverse in greater detail in Section 11.5."

p. 221, footnote 2 [k4505]: "…we don't need to run the the test the first time…" should be "…we don't need to run the test the first time…" (Reported by Jeremy Murphy.)

p. 223, line 25 [k4540]: In the second equation in the derivation of $gcd(xp + c, xq + d)$, the second "$+c$" should be "$-c$"; that is, the line should read:

$$= \gcd\left(xp + c - \frac{c}{d}xq - c, xq + d\right)$$

(Reported by Saul Tamari.)

p. 263, example in B.3 [k5323]: The example contains a few minor errors. It should be replaced with the following text:

> Prove that any set of 10 positive integers smaller than 100 will always contain two different subsets with the same sum.
>
> First, let's consider how many possible sums we can get. Since one of the subsets can be the empty set, the smallest possible sum is zero. The largest possible sum would come from the set containing the 10 largest numbers, i.e. $90+91+92+...+99 = 945$. So no matter which numbers we pick, the subset sums must be somewhere in the range $[0, 945]$. That range contains 946 values, so that's the maximum number of possible sums. Next, let's see how many possible subsets of those 10 integers there are. We can represent each subset as a binary number where the $i$th bit is 1 if the $i$th integer in the set is in that subset, and 0 otherwise. There are 10 elements in the set, and we use one bit for each element, so there are $2^{10} = 1024$ possible subsets. Since there are only 946 possible sums, and there are 1024 possible subsets, by the pigeonhole principle, at least two of the subsets must have the same sum.

The footnote is no longer necessary. (Reported by John Lakos.)