

『基礎から学ぶ整数論 RSA暗号入門』 第1刷(正誤表)

このたびは本書をお買い上げいただき、誠にありがとうございます。  
 本書には下記のような誤りがありました。ここに訂正し、謹んでお詫び申し上げます。

頁	箇所	誤	正
8	【解答】(1) 4行目	$-20 \leq a \leq 20$	$-20 \leq b \leq 20$
14	2.2節 1行目	great common	greatest common
38	手順1 1行目	最大公約数を求める。	最大公約数 $g$ を求める。
	手順2 1行目	最大公約数 = 定数項	最大公約数   定数項 $\Rightarrow g   c$
70	式(5.65)	$x = x_1 + nk \dots$	$x = x_1 + n'k \dots$ ( $n$ にダッシュ「'」を付ける)
93	式(6.17)の下 3行目と7行目	とは、定理6.6と同様な背理法… … なお、定理6.6は、ディリクレ…	とは、定理6.5と同様な背理法… … なお、定理6.5は、ディリクレ…
107	定理6.14 2行目	integer without sequence factors	integer without square factors, squarefree integer
111	最下行	$\dots (a, q) = 1$ のとき	$\dots (a, n) = 1$ のとき, $p$ を $n$ で置き換えると
116	章のイントロ文 2~3行目	秘密鍵(secret key : SK)から 公開鍵(public key : PK)を作成し	公開鍵(public key : PK)から 秘密鍵(secret key : SK)を作成し
118	式(7.12)の上 1行目	$\dots$ 偶素数の2の1個分を引いた…	$\dots$ 単数1の1個分(式(6.22)で $i=1$ )を引いた…
142	【3】(2) 1行目	$\dots 24 = 2^4 \times 3, 132 = 2^3 \times 3 \times 11$	$\dots 24 = 2^3 \times 3, 132 = 2^2 \times 3 \times 11$
	【3】(2) 3行目	$\dots = \frac{12 \times 24 \times 132}{g} = \frac{12 \times 24 \times 132}{12} = 264$	$\dots = 2^3 \times 3 \times 11 = 264$