บทที่ 3

การแปลงจำนวนให้อยู่ในรูปน้ำหนักต่ำสุดแบบเชื่อมตรง

ในบทนี้จะกล่าวถึงขั้นตอนที่ใช้ในการลดน้ำหนักของค่า k เพื่อเพิ่มประสิทธิภาพให้การคำนวณในขั้นตอนของชามีร์ โดยได้เสนอสองกระบวนการแปลงค่า ประกอบด้วยอัลกอริทึมการแปลงค่าจากระบบจำนวนฐานสองแบบไม่มีเครื่องหมาย ซึ่งมีเซตตัวเลข (digit set) เป็น $\{0,1\}$ ไปเป็นระบบจำนวนฐานสองแบบมีเครื่องหมายซ้ำซ้อนไอเอสบี ซึ่งมีเซตตัวเลขเป็น $\{\bar{1},0,1\}$ ด้วยความหน่วงเป็นหนึ่ง ดังแสดงในอัลกอริทึมที่ 3.1 และสุดท้ายคือการแปลงให้อยู่ในรูปแบบจำนวนฐานสองน้ำหนักต่ำสุด จากไอเอสบีสู่เซตตัวเลขใหม่ $\{\bar{3},\bar{1},0,1\}$ ด้วยความหน่วงเป็นสอง ดังแสดงในอัลกอริทึมที่ 3.2 ทั้งสองอัลกอริทึมดังกล่าวดำเนินการแบบเชื่อมตรง ทำให้สามารถส่งค่านำออกไปสู่ขั้นตอนของชามีร์เพื่อทำการคูณสเกลาร์ ในอัลกอริทึมที่ 3.3 ได้ทันทีโดยไม่ต้องรอให้การแปลงค่าจบสิ้นสมบูรณ์

3.1 การแปลงจำนวนให้อยู่ในรูปไอเอสบีภายใต้เซตตัวเลข $\{\bar{1},0,1\}$

ในขั้นตอนนี้คือการแปลงจากระบบจำนวนฐานสองแบบไม่มีเครื่องหมายภายใต้เซตตัวเลข $\{0,1\}$ ให้เป็นระบบจำนวนฐานสองแบบมีเครื่องหมายภายใต้เซตตัวเลข $\{\bar{1},0,1\}$ เพื่อเป็นการสร้างความซ้ำซ้อนให้กับระบบจำนวน

ทฤษฎีบทที่ 3.1 *การแปลงจำนวนฐานสองแบบไม่มีเครื่องหมายในเซตตัวเลข* $\{0,1\}$ *ให้อยู่ในรูปของไอเอสบีในเซตตัวเลข* $\{\bar{1},0,1\}$ *สามารถทำได้แบบเชื่อมตรงด้วยความหน่วงเป็นหนึ่ง*

บทพิสูจน์ จะพิสูจน์โดยการเสนออัลกอริทึมการแปลงจำนวนแบบเชื่อมตรง อัลกอริทึมที่ 3.1

อัลกอริทึมที่ 3.1 อัลกอริทึมการแปลงจำนวนเป็นไอเอสบี

นำเข้า: ระบบจำนวนฐานสองแบบไม่มีเครื่องหมายของ k ในรูป $\eta_{J-1},\ldots,\eta_0$ เมื่อ $\eta \in \{0,1\}$

นำออก: ไอเอสบี $\mu_J,\ldots,\mu_0$ เมื่อ $\mu \in \{\bar{1},0,1\}$

$\eta_J \leftarrow 0$

$\eta_{-1} \leftarrow 0$

while $J \geq 0$ do

  $\mu_J \leftarrow \eta_{J-1} - \eta_J$

  $J \leftarrow J-1$

end while

พิสูจน์อัลกอริทึม อัลกอริทึมที่ 3.1 ให้ค่าผลลัพธ์เป็นไอเอสบีที่ถูกต้องเสมอ โดยกำหนดให้ k คือ จำนวนเฉพาะที่ถูกแทนในรูปจำนวนฐานสองแบบไม่มีเครื่องหมายขนาด J-บิต $(\eta_{J-1},\ldots,\eta_0)$ ซึ่งสามารถจัดรูปใหม่ได้เป็น

$$\eta = \eta_{J-1}2^{J-1} + \eta_{J-2}2^{J-2} + \cdots + \eta_1 2 + \eta_0$$

เนื่องจาก $2^J = 2^{J+1} - 2^J$ จึงสามารถเขียนแสดง k ได้ในรูปดังนี้

$$\eta = (\eta_{J-1} - 0)2^J + (\eta_{J-2} - \eta_{J-1})2^{J-1} + \cdots$$
$$+ (\eta_1 - \eta_2)2^2 + (\eta_0 - \eta_1)2 + (0 - \eta_0).$$

ดังนั้น k จึงสามารถเขียนแสดงในรูปของไอเอสบีขนาด (J+1)-บิตได้คือ

$$\eta = ((\eta_{J-1} - 0), (\eta_{J-2} - \eta_{J-1}), \ldots, (\eta_0 - \eta_1), (0 - \eta_0)).$$

โดยผลลัพธ์ที่ได้จะมีคุณสมบัติตามเงื่อนไขของไอเอสบี ดังได้อธิบายไว้ในหัวข้อ 2.8 ■

ตัวอย่างที่ 3.1 *การแปลงจำนวนเป็นไอเอสบีในเซต* $\{\bar{1},0,1\}$ *ด้วยอัลกอรึทึมที่ 3.1*

กำหนด $k = 61$ หรือ 111101 ในระบบฐานสองแบบไม่มีเครื่องหมายจากอัลกอรึทึมที่ 3.1 จะได้ $\eta_{J-1},\ldots,\eta_0 = 111101$ ซึ่งในที่นี้ค่า $J = 6$ โดยมี $\eta_6 \leftarrow 0$ และ $\eta_{-1} \leftarrow 0$ จะมีรอบการแปลงดังนี้

รอบที่1 ค่า $J = 6$	คำนวณหา	$\mu_6 \leftarrow \eta_5 - \eta_6$		
นั่นคือ	$\mu_6 \leftarrow 1 - 0$	จะได้	$\mu_6 \leftarrow 1$	เป็นค่านำออกที่ 1
รอบที่2 ค่า $J = 5$	คำนวณหา	$\mu_5 \leftarrow \eta_4 - \eta_5$		
นั่นคือ	$\mu_5 \leftarrow 1 - 1$	จะได้	$\mu_5 \leftarrow 0$	เป็นค่านำออกที่ 2
รอบที่3 ค่า $J = 4$	คำนวณหา	$\mu_4 \leftarrow \eta_3 - \eta_4$		
นั่นคือ	$\mu_4 \leftarrow 1 - 1$	จะได้	$\mu_4 \leftarrow 0$	เป็นค่านำออกที่ 3
รอบที่4 ค่า $J = 3$	คำนวณหา	$\mu_3 \leftarrow \eta_2 - \eta_3$		
นั่นคือ	$\mu_3 \leftarrow 1 - 1$	จะได้	$\mu_3 \leftarrow 0$	เป็นค่านำออกที่ 4
รอบที่5 ค่า $J = 2$	คำนวณหา	$\mu_2 \leftarrow \eta_1 - \eta_2$		
นั่นคือ	$\mu_2 \leftarrow 0 - 1$	จะได้	$\mu_2 \leftarrow \bar{1}$	เป็นค่านำออกที่ 5
รอบที่6 ค่า $J = 1$	คำนวณหา	$\mu_1 \leftarrow \eta_0 - \eta_1$		
นั่นคือ	$\mu_1 \leftarrow 1 - 0$	จะได้	$\mu_1 \leftarrow 1$	เป็นค่านำออกที่ 6
รอบที่7 ค่า $J = 0$	คำนวณหา	$\mu_0 \leftarrow \eta_{-1} - \eta_0$		
นั่นคือ	$\mu_0 \leftarrow 0 - 1$	จะได้	$\mu_0 \leftarrow \bar{1}$	เป็นค่านำออกที่ 7

ดังนั้นจะได้ไอเอสบีในรูป $\mu_J,\ldots,\mu_0$ เมื่อ $\mu \in \{\bar{1},0,1\}$ คือ $1000\bar{1}1\bar{1}$ □

ตัวอย่างที่ 3.1 ข้างต้นได้แสดงถึงกระบวนการแปลงระบบจำนวนฐานสองแบบไม่มีเครื่องหมายขนาด J-บิต ไปเป็นไอเอสบีที่มีขนาด (J+1)-บิต ซึ่งผลลัพธ์ที่ได้หลังการแปลงมีโอกาสที่จะมีน้ำหนักต่ำลงกว่ารูปแบบตั้งต้น โดยในที่นี้ได้ค่าน้ำหนักคือสี่ซึ่งลดลงหนึ่งจากของเดิมคือห้า และเมื่อนำไปทำการคูณสเกลาร์ด้วยวิธีการของชามีร์จะต้องเพิ่มตัวดำเนินการใหม่ (operator) คือ $-P$ เพื่อสำหรับเรียกใช้เมื่อมีค่านำเข้าเป็น $\bar{1}$ ดังแสดงในตารางที่ 3.1 มีการเรียกใช้ตัวดำเนินการ *double* ทั้งหมดหกครั้ง ตัวดำเนินการ $+P$ ทั้งหมดสองครั้ง และตัวดำเนินการ $-P$ ทั้งหมดสองครั้ง รวมทั้งสิ้นสิบครั้ง

ตารางที่ 3.1 การคำนวณ $61P$ ด้วยวิธีการของชามีร์ใช้เซตตัวเลข $\{\bar{1},0,1\}$

$k=61$	1	0	0	0	$\bar{1}$	1	$\bar{1}$
double	0	$2P$	$4P$	$8P$	$16P$	$30P$	$62P$
$+P$	P	-	-	-	-	$31P$	-
$-P$	-	-	-	-	$15P$	-	$61P$

3.2 การแปลงจำนวนให้อยู่ในรูปน้ำหนักต่ำสุดภายใต้เซตตัวเลข $\{\bar{3},\bar{1},0,1\}$

เมื่อได้ผลลัพธ์เป็นไอเอสบีที่ได้จากอัลกอริทึมที่ 3.1 จะต้องให้อยู่ในรูปที่มีน้ำหนักต่ำสุดด้วยอัลกอริทึมที่ 3.2 ซึ่งสามารถกระทำได้ทันทีเมื่อได้ผลลัพธ์สองบิตแรกและบิตถัดไปทีละบิตโดยไม่ต้องรอให้การแปลงเป็นไอเอสบีเสร็จสิ้น เนื่องจากกระบวนการทำงานเป็นแบบเชื่อมตรงเหมือนกันจึงสามารถรวมการทำงานให้เป็นแบบสายท่อเข้าด้วยกันได้ การทำงานของอัลกอริทึมที่ 3.2 เป็นการแปลงจากระบบจำนวนฐานสองแบบมีเครื่องหมายภายใต้เซตตัวเลข $\{\bar{1},0,1\}$ ให้เป็นระบบจำนวนฐานสองภายใต้เซตตัวเลข $\{\bar{3},\bar{1},0,1\}$ ซึ่งอาจให้ค่าน้ำหนักที่ต่ำกว่าได้ โดยที่ค่าน้ำหนักใหม่นั้นจะมีค่าไม่มากกว่าค่าน้ำหนักเดิม

จุดมุ่งหมายหลักของการแปลงนั้นคือลดค่าน้ำหนักของระบบจำนวนฐานสอง กล่าวคือลดจำนวนบิตที่ไม่ใช่ศูนย์โดยการแปลงให้อยู่ในรูปอื่นที่มีค่าน้ำหนักน้อยกว่า แต่ต้องมีค่าคงเหลือเชิงตัวเลขเท่าเดิม โดยมีรูปแบบที่ใช้ในการแปลงค่าดังนี้

กำหนดให้เครื่องหมาย $\rightarrow$ แทนทิศทางการแปลงจากด้านซ้ายไปด้านขวา

$\bar{1}1 \rightarrow 0\bar{1}$	มีค่าคงเหลือเชิงตัวเลขเป็น $\bar{1}$
$1\bar{1} \rightarrow 01$	มีค่าคงเหลือเชิงตัวเลขเป็น 1
$\bar{1}1\bar{1} \rightarrow 00\bar{3}$	มีค่าคงเหลือเชิงตัวเลขเป็น $\bar{3}$
$\bar{1}01 \rightarrow 00\bar{3}$	มีค่าคงเหลือเชิงตัวเลขเป็น $\bar{3}$

การทำงานจะเริ่มต้นจากบิตแรกซ้ายสุด โดยทำการแปลงค่าตัวเลขตามกฎ ถ้าไม่เข้าตามกฎก็จัดเก็บบิตซ้ายสุดตามค่าเดิม แล้วอ่านบิตเพิ่มทางขวามาเปรียบเทียบจนครบ

ทฤษฎีบทที่ 3.2 *การลดค่าน้ำหนักของจำนวนฐานสองให้น้อยกว่าหรือเท่ากับไอเอสบีกระทำได้โดยการแปลงให้อยู่ในเซตตัวเลข* $\{\bar{3},\bar{1},0,1\}$ *ด้วยความหน่วงเป็นสอง*

บทพิสูจน์ จะพิสูจน์โดยการเสนออัลกอริทึมการแปลงจำนวน อัลกอริทึมที่ 3.2

อัลกอริทึมที่ 3.2 อัลกอริทึมการแปลงจำนวนให้อยู่ในระบบจำนวนฐานสองที่มีน้ำหนักต่ำสุด

นำเข้า: ไอเอสบี $\mu_J,...,\mu_0$ เมื่อ $\mu \in \{\bar{1},0,1\}$

นำออก: ระบบจำนวนฐานสอง $\omega_J,...,\omega_0$ เมื่อ $\omega \in \{\bar{3},\bar{1},0,1\}$

$\mu_{-1},\mu_{-2} \leftarrow 0$

$I \leftarrow J-2$

$S \leftarrow (\mu_J \times 2)+\mu_{J-1}$

while $J \geq 0$ do

  $C \leftarrow \mu_I$

  $S \leftarrow (S \times 2)+C$

  if $S \in \{3,4,5\}$ then

    $\omega_J \leftarrow 1$

  else if $S \in \{\bar{4}\}$ then

    $\omega_J \leftarrow \bar{1}$

  else if $S \in \{\overline{14},\overline{13},\overline{12},\overline{11},\overline{10}\}$ then

    $\omega_J \leftarrow \bar{3}$

  else if $S \in \{\bar{5}\}$ then

    if $C=1$ then

      $\omega_J \leftarrow 0$

    else /* $C=\bar{1}$ */

      $\omega_J \leftarrow \bar{1}$

    end if

  else /* $S \in \{\bar{7},\bar{6},\bar{3},\bar{2},\bar{1},0,1,2\}$ */

    $\omega_J \leftarrow 0$

  end if

  $S \leftarrow S-(\omega_J \times 2^2)$

  $J \leftarrow J-1$

  $I \leftarrow I-1$

end while

พิสูจน์อัลกอริทึม

ส่วนที่หนึ่ง อัลกอริทึมที่ 3.2 ให้ค่าผลลัพธ์ที่ถูกต้องเสมอ โดยต้องการพิสูจน์ว่า $\mu_J,...,\mu_0$ เท่ากับ $\omega_J,...,\omega_0$ เมื่อ $\mu \in \{\bar{1},0,1\}$ และ $\omega \in \{\bar{3},\bar{1},0,1\}$ ดังนี้

จาก $S \leftarrow (S \times 2) + C$ โดยที่ $C \leftarrow \mu_I$ ซึ่งเป็นค่านำเข้าปัจจุบันจะได้ว่าค่า S คือค่าเชิงตัวเลขคงเหลือในปัจจุบัน ซึ่งเป็นตัวกำหนดค่านำออก ω ที่มีค่าเชิงตัวเลขโดยรวมเท่ากันกับ μ ตามเงื่อนไขดังต่อไปนี้

ถ้า $S \in \{3,4,5\}$	จะได้ค่านำออก ω เป็น 1
ถ้า $S \in \{\bar{4}\}$	จะได้ค่านำออก ω เป็น $\bar{1}$
ถ้า $S \in \{\bar{1}\bar{4},\bar{1}\bar{3},\bar{1}\bar{2},\bar{1}\bar{1},\bar{1}\bar{0}\}$	จะได้ค่านำออก ω เป็น $\bar{3}$
ถ้า $S \in \{\bar{7},\bar{6},\bar{3},\bar{2},\bar{1},0,1,2\}$	จะได้ค่านำออก ω เป็น 0
ถ้า $S \in \{\bar{5}\}$ และ $C = 1$	จะได้ค่านำออก ω เป็น 0
ถ้า $S \in \{\bar{5}\}$ และ $C = \bar{1}$	จะได้ค่านำออก ω เป็น $\bar{1}$

นั่นคือ ผลลัพธ์ที่ได้หลังการแปลงจะมีค่าเชิงตัวเลขเท่ากันกับค่าตั้งต้น ภายใต้ระบบจำนวนฐานสอง ด้วยเซตตัวเลข $\{\bar{3},\bar{1},0,1\}$

ส่วนที่สอง อัลกอริทึมที่ 3.2 ให้ค่าผลลัพธ์ที่มีค่าน้ำหนักต่ำสุดภายใต้ระบบจำนวนฐานสอง และมีเซตตัวเลขเป็น $\{\bar{3},\bar{1},0,1\}$

จากคุณสมบัติของไอเอสบี ทำให้ค่านำเข้าไม่มีบิตที่มีค่าน้ำหนักเดียวกันอยู่ติดกัน กล่าวคือ จะไม่ปรากฏลำดับ 10...01 และ $\bar{1}0...0\bar{1}$ ขึ้น โดยจำนวนของบิตที่เป็นศูนย์มีมากกว่าหรือเท่ากับศูนย์ นั่นทำให้สามารถแปลงรูปตามกฎได้ด้วยความหน่วงเป็นสองดังนี้

1) $\bar{1}1 \rightarrow 0\bar{1}$ มีค่าคงเหลือเชิงตัวเลขเท่ากันคือ $\bar{1}$
2) $1\bar{1} \rightarrow 01$ มีค่าคงเหลือเชิงตัวเลขเท่ากันคือ 1
3) $\bar{1}1\bar{1} \rightarrow 00\bar{3}$ มีค่าคงเหลือเชิงตัวเลขเท่ากันคือ $\bar{3}$
4) $\bar{1}01 \rightarrow 00\bar{3}$ มีค่าคงเหลือเชิงตัวเลขเท่ากันคือ $\bar{3}$
5) หากไม่สามารถแปลงได้ตามกฎก็ให้นำออกบิตซ้ายสุดตามค่าเดิมแล้วอ่านบิตใหม่ทางขวาเข้ามาเพื่อเปรียบเทียบ

จากกฎที่ใช้ในการแปลงนั้น ได้แสดงให้เห็นว่า ค่านำเข้านั้นได้ถูกแปลงเป็นค่านำออกซึ่งให้ค่าเชิงตัวเลขคงเดิม ภายใต้เซตตัวเลข $\{\bar{3},\bar{1},0,1\}$ ในระบบจำนวนฐานสอง และเป็นรูปแบบที่มีค่าน้ำหนักต่ำสุด ■

อัลกอริทึมที่ 3.2 สามารถเขียนเป็นเครื่องแปลงสัญญาณในรูปของตารางสถานะ เพื่อให้ง่ายต่อการเข้าใจ ได้ดังตารางที่ 3.2 ซึ่งคอลัมน์แรก current state แสดงถึงค่าเชิงตัวเลขคงเหลือที่รับเข้ามา คอลัมน์ที่สอง possible digit pattern แสดงถึงชุดตัวเลขนำเข้าที่เป็นไปได้ซึ่งให้ค่าเชิงตัวเลขคงเหลือเท่ากับค่าในคอลัมน์แรก คอลัมน์ที่สาม current output คือค่านำออกของแต่ละสถานะ และคอลัมน์สุดท้าย next state ซึ่งมี μ คือค่านำเข้าที่กำหนดสถานะถัดไป

ตารางที่ 3.2 ตารางสถานะของกระบวนการในอัลกอริทึมที่ 3.2

current state	possible digit pattern	current output	next state		
			$\mu=0$	$\mu=1$	$\mu=\bar{1}$
0	000	0	0	1	$\bar{1}$
1	$001\mid 01\bar{1}$	0	2	3	1
2	$010\mid 1\bar{1}0$	0	4	5	3
3	$10\bar{1}\mid 1\bar{1}1$	1	$\bar{2}$	$\bar{1}$	$\bar{3}$
4	100	1	0	1	$\bar{1}$
5	101	1	2	-	1
$\bar{1}$	$00\bar{1}\mid 0\bar{1}1$	0	$\bar{2}$	$\bar{1}$	$\bar{3}$
$\bar{2}$	$0\bar{1}0\mid \bar{1}10$	0	$\bar{4}$	$\bar{3}$	$\bar{5}$
$\bar{3}$	$\bar{1}01\mid 0\bar{1}\bar{1}\mid \bar{1}1\bar{1}$	0	$\bar{6}$	$\bar{5}$*	$\bar{7}$
$\bar{4}$	$\bar{1}00$	$\bar{1}$	0	1	$\bar{1}$
$\bar{5}$	$\bar{1}0\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{1}$	-
$\bar{5}$*	$0\bar{3}1\mid \bar{1}\bar{1}1$	0	$\overline{10}$	-	$\overline{11}$
$\bar{6}$	$0\bar{3}0\mid \bar{1}\bar{1}0$	0	$\overline{12}$	$\overline{11}$	$\overline{13}$
$\bar{7}$	$0\bar{3}\bar{1}$	0	$\overline{14}$	$\overline{13}$	-
$\overline{10}$	$\bar{3}10$	$\bar{3}$	4	-	3
$\overline{11}$	$\bar{3}01\mid \bar{3}1\bar{1}$	$\bar{3}$	2	3	1
$\overline{12}$	$\bar{3}00$	$\bar{3}$	0	1	$\bar{1}$
$\overline{13}$	$\bar{3}01$	$\bar{3}$	$\bar{2}$	-	$\bar{3}$
$\overline{14}$	$\bar{3}\bar{1}0$	$\bar{3}$	$\bar{4}$	$\bar{3}$	-

ในการออกแบบเครื่องแปลงสัญญาณจะกำหนดให้สถานะที่ 1 หรือ 001 เป็นสถานะเริ่มต้น เพราะต้องใช้บิตศูนย์สมมุติสองบิตแรกแทนค่าความหน่วง

ตัวอย่างที่ 3.2 *การแปลงจำนวนให้อยู่ในเซตตัวเลข* $\{\bar{3},\bar{1},0,1\}$ *ด้วยอัลกอริทึมที่ 3.2*

กำหนดไอเอสบี $\mu_J,...,\mu_0$ เมื่อ $\{\bar{1},0,1\}$ ของ $k=61$ คือ $1000\bar{1}1\bar{1}$ จากอัลกอริทึมที่ 3.1จะได้ $J=6$ และ $I=4$ โดยกำหนดให้ $\mu_{-1},\mu_{-2} \leftarrow 0$ และจาก $S \leftarrow (\mu_6 \times 2)+\mu_5$ จะได้ $S \leftarrow 2$ เป็นค่าเริ่มต้น ซึ่งแสดงถึงค่าเชิงตัวเลขคงเหลือในปัจจุบัน โดยจะเริ่มรอบการแปลงดังนี้

รอบที่1 ค่า	$J=6, I=4$	คำนวณหา $S \leftarrow (S\times 2)+C$	เมื่อ $C \leftarrow \mu_4$
	นั่นคือ $S \leftarrow 4$	ได้ค่านำออก $\omega_6 \leftarrow 1$	ทำให้เหลือ $S \leftarrow 0$
รอบที่2 ค่า	$J=5, I=3$	คำนวณหา $S \leftarrow (S\times 2)+C$	เมื่อ $C \leftarrow \mu_3$
	นั่นคือ $S \leftarrow 0$	ได้ค่านำออก $\omega_5 \leftarrow 0$	ทำให้เหลือ $S \leftarrow 0$
รอบที่3 ค่า	$J=4, I=2$	คำนวณหา $S \leftarrow (S\times 2)+C$	เมื่อ $C \leftarrow \mu_2$
	นั่นคือ $S \leftarrow \bar{1}$	ได้ค่านำออก $\omega_4 \leftarrow 0$	ทำให้เหลือ $S \leftarrow \bar{1}$
รอบที่4 ค่า	$J=3, I=1$	คำนวณหา $S \leftarrow (S\times 2)+C$	เมื่อ $C \leftarrow \mu_1$
	นั่นคือ $S \leftarrow \bar{1}$	ได้ค่านำออก $\omega_3 \leftarrow 0$	ทำให้เหลือ $S \leftarrow \bar{1}$
รอบที่5 ค่า	$J=2, I=0$	คำนวณหา $S \leftarrow (S\times 2)+C$	เมื่อ $C \leftarrow \mu_0$
	นั่นคือ $S \leftarrow \bar{3}$	ได้ค่านำออก $\omega_2 \leftarrow 0$	ทำให้เหลือ $S \leftarrow \bar{3}$
รอบที่6 ค่า	$J=1, I=\bar{1}$	คำนวณหา $S \leftarrow (S\times 2)+C$	เมื่อ $C \leftarrow \mu_{-1}$
	นั่นคือ $S \leftarrow \bar{6}$	ได้ค่านำออก $\omega_1 \leftarrow 0$	ทำให้เหลือ $S \leftarrow \bar{6}$
รอบที่7 ค่า	$J=0, I=\bar{2}$	คำนวณหา $S \leftarrow (S\times 2)+C$	เมื่อ $C \leftarrow \mu_{-2}$
	นั่นคือ $S \leftarrow \bar{1}\bar{2}$	ได้ค่านำออก $\omega_0 \leftarrow \bar{3}$	ทำให้เหลือ $S \leftarrow 0$

ดังนั้นจะได้จำนวนฐานสอง $\omega_J,...,\omega_0$ เมื่อ $\omega \in \{\bar{3},\bar{1},0,1\}$ คือ $100000\bar{3}$ □

จากไอเอสบี $1000\bar{1}1\bar{1}$ ของ $k=61$ เมื่อผ่านการแปลงในอัลกอริทึมที่ 3.2 จะได้ผลลัพธ์คือ $100000\bar{3}$ โดยมีค่าน้ำหนักเป็นสอง และเมื่อนำไปคำนวณด้วยวิธีการของชามีร์จะได้ผลดังแสดงในตารางที่ 3.3 ซึ่งมีการเรียกใช้ตัวดำเนินการ *double* ทั้งหมดหกครั้ง ตัวดำเนินการ $+P$ หนึ่งครั้ง และตัวดำเนินการ $-3P$ หนึ่งครั้ง รวมทั้งสิ้นแปดครั้ง

ตารางที่ 3.3 การคำนวณ $61P$ ด้วยวิธีการของชามีร์ใช้เซตตัวเลข $\{\bar{3},\bar{1},0,1\}$

$k=61$	1	0	0	0	0	0	$\bar{3}$
double	0	$2P$	$4P$	$8P$	$16P$	$32P$	$64P$
$+P$	P	-	-	-	-	-	-
$-P$	-	-	-	-	-	-	-
$-3P$	-	-	-	-	-	-	$61P$

3.3 การคูณสเกลาร์ด้วยวิธีการของชามีร์ภายใต้เซตตัวเลข $\{\bar{3},\bar{1},0,1\}$

ผลลัพธ์ที่ได้หลังการแปลงให้อยู่ในรูปน้ำหนักต่ำสุดจะถูกส่งไปดำเนินการคูณสเกลาร์ด้วยวิธีการของชามีร์ทันที โดยไม่ต้องรอให้การแปลงเสร็จสิ้นเนื่องจากการทำงานเป็นแบบเชื่อมตรง และมีทิศทางการแปลงจากทางซ้ายไปขวา จึงเชื่อมการทำงานให้เป็นแบบสายท่อกับการคูณสเกลาร์ได้ เนื่องจากวิธีการของชามีร์ดำเนินการแบบอย่างเป็นลำดับต่อเนื่อง (sequential) จากซ้ายไปขวาเช่นกัน โดยในที่นี้จะใช้ตัวดำเนินการในการคูณสเกลาร์ทั้งหมดสี่ตัวคือ $double$, $+P$, $-P$ และ $-3P$ เพื่อการคำนวณสำหรับชุดตัวเลข $\{\bar{3},\bar{1},0,1\}$ ในระบบจำนวนฐานสอง

ทฤษฎีบทที่ 3.3 *การคูณสเกลาร์สามารถทำได้อย่างเป็นลำดับต่อเนื่องจากซ้ายไปขวาด้วยเซตตัวเลข* $\{\bar{3},\bar{1},0,1\}$ *ในระบบจำนวนฐานสอง*

บทพิสูจน์ จะพิสูจน์โดยการเสนออัลกอริทึมการคูณสเกลาร์ อัลกอริทึมที่ 3.3

อัลกอริทึมที่ 3.3 อัลกอริทึมการคูณสเกลาร์ภายใต้เซตตัวเลข $\{\bar{3},\bar{1},0,1\}$ ฐานสอง

นำเข้า: ระบบจำนวนฐานสอง $\omega_J,\dots,\omega_0$ เมื่อ $\omega \in \{\bar{3},\bar{1},0,1\}$

นำออก: ผลการคูณสเกลาร์ $G = kP$

$G \leftarrow 0$

while $J \geq 0$ do

  $G \leftarrow G + G$

  $k \leftarrow \omega_J$

  if $k = 1$ then

    $G \leftarrow G + P$

  else if $k = \bar{1}$ then

    $G \leftarrow G - P$

  else if $k = \bar{3}$ then

    $G \leftarrow G - 3P$

  else /* $k = 0$ */

    $G \leftarrow G$

  end if

  $J \leftarrow J - 1$

end while

พิสูจน์อัลกอริทึม อัลกอริทึมที่ 3.3 ให้ค่าผลลัพธ์ที่ถูกต้องเสมอ พิจารณารอบการทำงานดังนี้ กำหนดให้ G มีค่าตั้งต้นเป็นศูนย์ จะมีการเรียกใช้ตัวดำเนินการในแต่ละรอบ ดังนี้

รอบที่ J อ่าน $k \leftarrow \omega_J$ มีการเรียกใช้ตัวดำเนินการคือ $G \leftarrow G+G$ และ $G \leftarrow G+kP$

รอบที่ $J-1$ อ่าน $k \leftarrow \omega_{J-1}$ มีการเรียกใช้ตัวดำเนินการคือ $G \leftarrow G+G$ และ $G \leftarrow G+kP$

รอบที่ $J-2$ อ่าน $k \leftarrow \omega_{J-2}$ มีการเรียกใช้ตัวดำเนินการคือ $G \leftarrow G+G$ และ $G \leftarrow G+kP$

$\vdots$ $\vdots$ $\vdots$

รอบที่ 0 อ่าน $k \leftarrow \omega_0$ มีการเรียกใช้ตัวดำเนินการคือ $G \leftarrow G+G$ และ $G \leftarrow G+kP$

สามารถเขียนรูปการทำงานทั่วไปคือ $G = \left(\sum_{i=0}^{J} \omega_{J-i} 2^{J-i}\right)P$ ซึ่งก็คือ $G = kP$ นั่นเอง ■

ตัวอย่างที่ 3.3 *การคูณสเกลาร์ด้วยอัลกอริทึมที่ 3.3*

กำหนดข้อมูลนำเข้าตัวอย่างที่มีการใช้งานครบทุกตัวดำเนินการคือ $\omega = 1000\bar{3}00\bar{1}$ ซึ่งมี $J = 7$ และมีค่าเชิงตัวเลขเท่ากับ 103 จะได้รูปแบบการทำงานดังแสดงในตารางที่ 3.4

ตารางที่ 3.4 ตารางการเรียกใช้ตัวนำเนินการเพื่อคำนวณ $103P$ ด้วยวิธีการของชามีร์

J	$k \leftarrow \omega_J$	$G \leftarrow operator$			
		double	$+P$	$-P$	$-3P$
7	1	0	P	-	-
6	0	$2P$	-	-	-
5	0	$4P$	-	-	-
4	0	$8P$	-	-	-
3	$\bar{3}$	$16P$	-	-	$13P$
2	0	$26P$	-	-	-
1	0	$52P$	-	-	-
0	$\bar{1}$	$104P$	-	$103P$	-

จากตารางที่ 3.4 มีการเรียกใช้งานตัวดำเนินการ *double* ทั้งหมดแปดครั้งแต่ไม่นับครั้งแรกเพราะ G ถูกกำหนดค่าตั้งต้นไว้เป็นศูนย์จึงไม่มีการทำงานเกิดขึ้นจึงเหลือการเรียกใช้งานจริงเพียงเจ็ด และมีการเรียกใช้งานตัวดำเนินการอื่นๆ ทุกตัวอีกอย่างละหนึ่งครั้ง รวมการเรียกใช้งานตัวดำเนินการทั้งหมดสิบครั้ง ซึ่งได้ค่าผลลัพธ์ที่ถูกต้อง และตรงตามขั้นตอนการทำงานของอัลกอริทึมที่ 3.4 □

3.4 สรุป

ขั้นตอนการทำงานจะเริ่มต้นจากอัลกอริทึมที่ 3.1 อัลกอริทึม 3.2 และอัลกอริทึม 3.3 ตามลำดับ ซึ่งสามารถรวมการทำงานของทั้งสามอัลกอริทึมเข้าด้วยกันเป็นสายท่อได้ โดยไม่ต้องรอให้อัลกอริทึมก่อนหน้าทำงานเสร็จสิ้น เนื่องจากทั้งสามอัลกอริทึมมีรูปแบบการทำงานแบบเชื่อมตรงจากทางซ้ายไปขวาเหมือนกัน โดยมีความหน่วงในการทำงานรวมเป็นสาม และมีความซับซ้อนเชิงเวลาคือ $\Theta(n)$ เมื่อ n คือขนาดของจำนวนนำเข้า