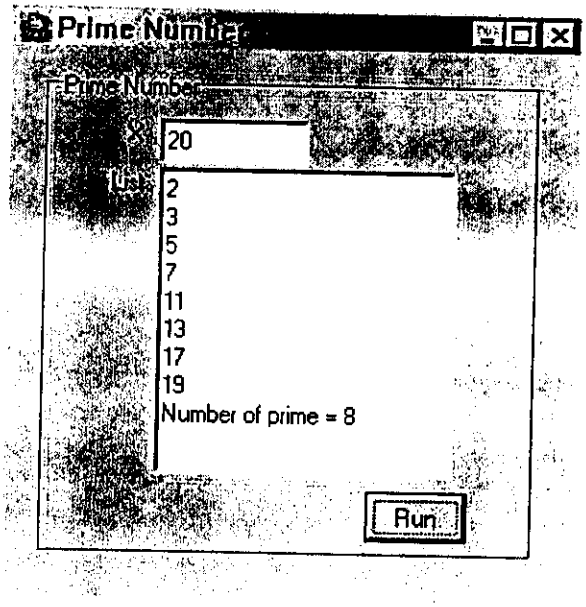
ภาคผนวก ก
คู่มือการใช้งานชุดโปรแกรมทฤษฎีจำนวน

1. Prime number คือโปรแกรมย่อยที่ใช้หาจำนวนเฉพาะตั้งแต่ 2 ไปจนถึงจำนวนที่ผู้ใช้ได้กำหนดไว้ ดังเช่นตัวอย่างภาพประกอบที่ ก.1 ซึ่งตัวอย่างคือการหาจำนวนเฉพาะตั้งแต่ 2 จนถึง 20

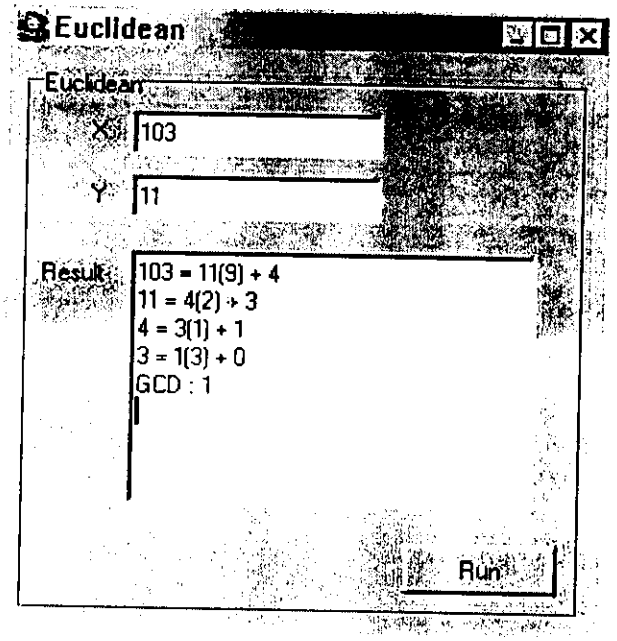


ภาพประกอบที่ ก.1 การหาจำนวนเฉพาะ

1.1 ป้อนค่าที่ต้องการ ในที่นี้คือค่า 20 ในช่อง X

1.2 คลิกที่ปุ่ม Run เพื่อดูคำตอบ ซึ่งคำตอบจะปรากฏในช่อง List เมื่อแสดงจำนวนเฉพาะจนครบแล้วโปรแกรมย่อยจะแสดงจำนวนของจำนวนเฉพาะที่แสดงออกมา

2. Euclidean Algorithm คือโปรแกรมย่อยที่ใช้หาตัวหารร่วมมากระหว่างจำนวน 2 จำนวนโดยใช้ขั้นตอนวิธีของยูคลิด ดังตัวอย่างภาพประกอบที่ ก.2 ซึ่งหาตัวหารร่วมมากระหว่าง 113 และ 11

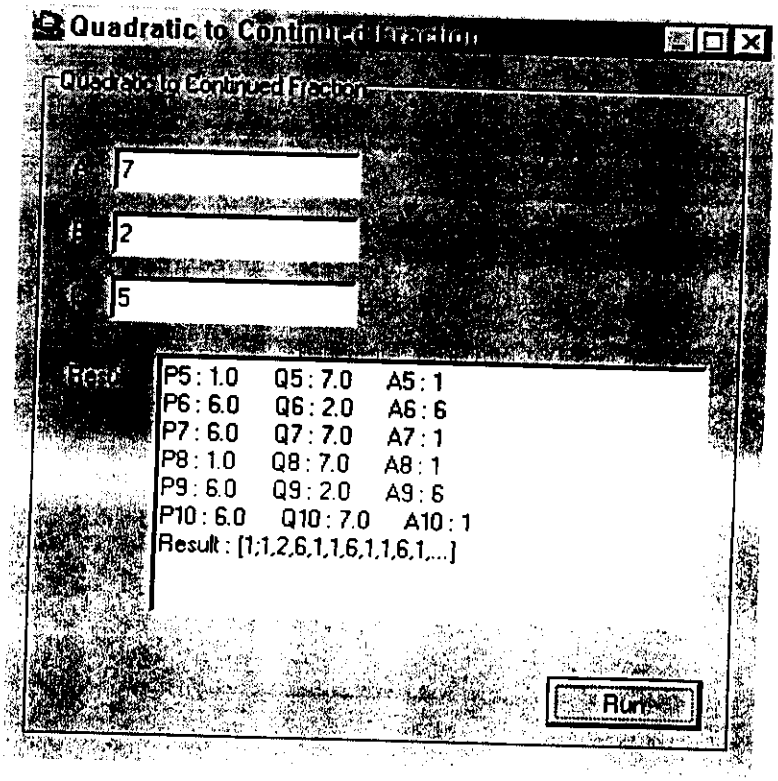


2.1 ใส่ค่าตัวเลขที่ต้องการหาตัวหารร่วมมากจำนวน 2 จำนวนลงในช่อง X และ Y

2.2 คลิกที่ปุ่ม Run เพื่อหาคำตอบที่ต้องการ โดยคำตอบที่ต้องการพร้อมขั้นตอนการคำนวณโดยวิธีของยูคลิดจะแสดงในช่อง Result

ภาพประกอบที่ ก.2 การหาตัวหารร่วมมากโดยใช้ขั้นตอนวิธีของยูคลิด

3. การเปลี่ยนจำนวนอตรรกยะเป็นเศษส่วนต่อเนื่อง ดังภาพประกอบที่ ก.3



ภาพประกอบที่ ก.3 การเปลี่ยนจำนวนอตรรกยะเป็นเศษส่วนต่อเนื่อง

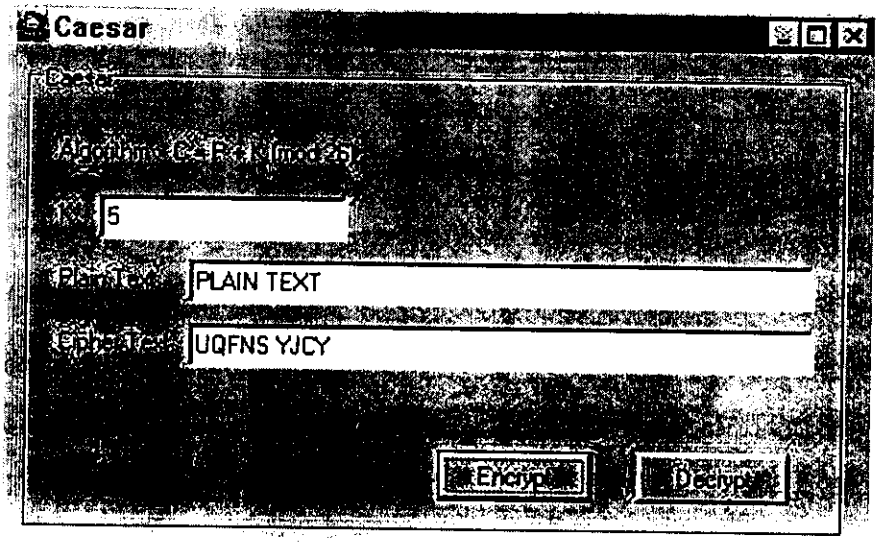
3.1 จากตัวอย่างเป็นการเปลี่ยนจำนวนอตรรกยะซึ่งอยู่ในรูปแบบ $\frac{A+\sqrt{B}}{C}$ ซึ่งในตัวอย่างนี้คือค่า $\frac{7+\sqrt{2}}{5}$ เป็นเศษส่วนต่อเนื่อง

3.2 ป้อนค่า A, B, C ที่ต้องการลงในช่องรับค่า

3.3 คลิกที่ปุ่ม Run เพื่อตรวจสอบคำตอบและขั้นตอนการคำนวณ

3.4 คำตอบและขั้นตอนการคำนวณจะปรากฏในช่อง Result

4. การเข้ารหัสแบบซีซาร์ คือการเข้ารหัสแบบเลื่อน ค่าคีย์ที่ใช้ในการเข้ารหัสเป็นเลขจำนวนเต็มบวกซึ่งเป็นเลขจำนวนที่ใช้บอกการเลื่อนของตัวอักษรว่าให้เลื่อนถัดไปอีกกี่ตัวอักษร เช่น A หากค่าคีย์เป็น 1 คือให้เลื่อนไป 1 ตัวอักษรเป็น B และหากค่าคีย์เป็น 2 ก็จะเลื่อนไปเป็น C ดังภาพประกอบที่ ก.4



ภาพประกอบที่ ก.4 การเข้ารหัสแบบซีซาร์

4.1 การเข้ารหัสแบบซีซาร์เป็นการเข้ารหัสแบบเลื่อน ดังตัวอย่างค่าคีย์ของการเข้ารหัสคือ 5

4.2 จากตัวอย่าง ข้อความก่อนการเข้ารหัสคือ Plain Text และข้อความหลังการเข้ารหัสคือ Cipher Text ค่าคีย์ที่ใช้เข้ารหัสคือค่า K

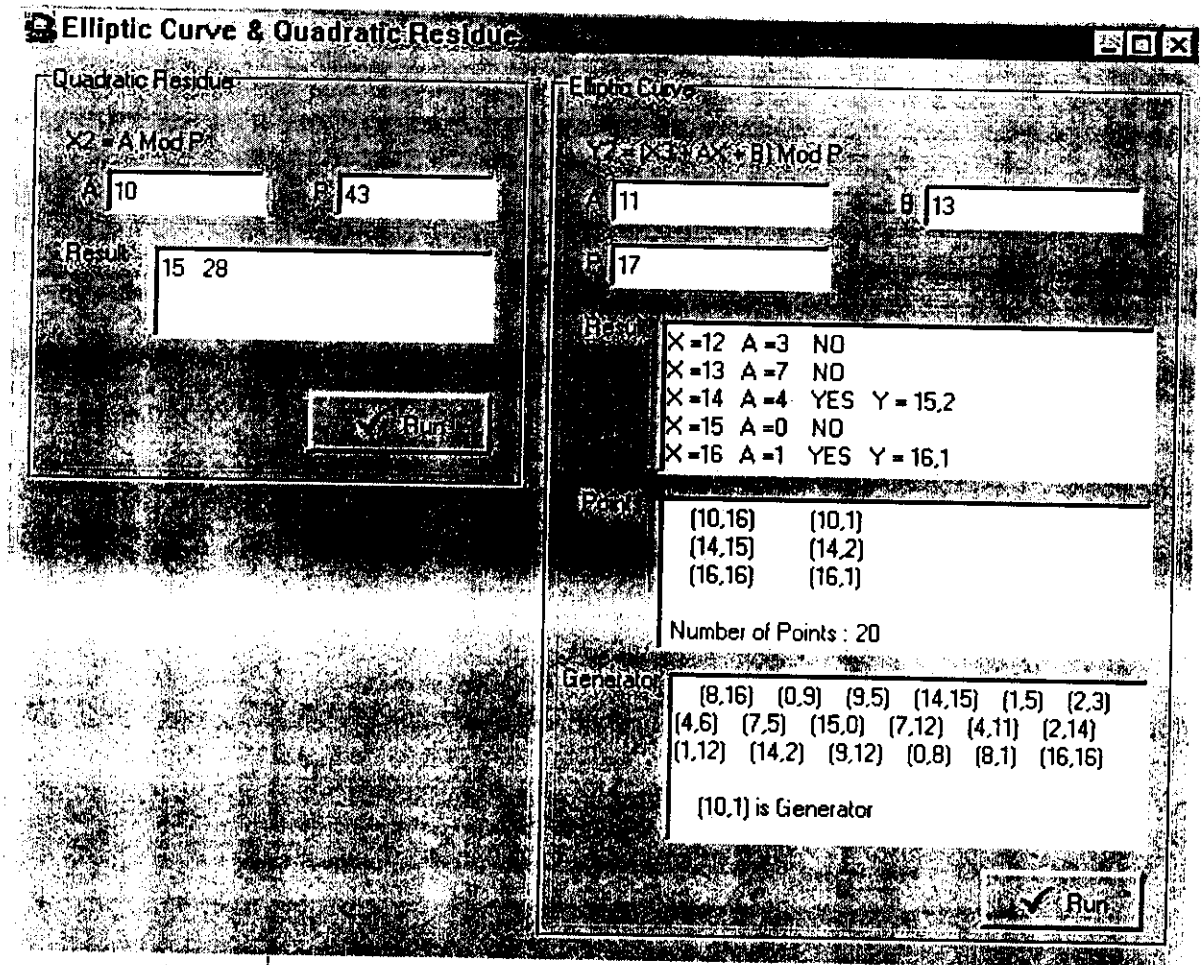
4.3 ป้อนค่าคีย์ที่ใช้เข้ารหัสในช่องค่า K

4.4 ใส่ Plain text ที่ต้องการเข้ารหัสในช่อง Plain text จากนั้นจึงคลิกที่ปุ่ม Encrypt เพื่อเข้ารหัสข้อความ ข้อความที่เข้ารหัสจะปรากฏในช่อง Cipher text

4.5 ในทางกลับกัน หากต้องการถอดรหัสก็ให้ใส่ค่าคีย์ลงในช่องค่า K

4.6 ใส่ Cipher text ลงในช่อง Cipher text จากนั้นจึงคลิกปุ่ม Decrypt เพื่อถอดรหัสข้อความ ข้อความที่ถูกถอดรหัสจะปรากฏในช่อง Plain text

5. Elliptic Curve และ Quadratic Residue ดังภาพประกอบที่ ก.5



ภาพประกอบที่ ก.5 Elliptic Curve & Quadratic Residue

5.1 ในโปรแกรมย่อยนี้ประกอบด้วยเมนูย่อย 2 เมนูคือส่วนของ Elliptic Curve และ Quadratic Residue ซึ่งทั้งสองเมนูย่อยนี้มีเนื้อหาที่เกี่ยวข้องกัน

5.2 ป้อนค่าข้อมูลนำเข้าต่างๆ เข้าสู่ช่องว่างที่รอรับค่าต่างๆ จากนั้นจึงคลิกที่ปุ่ม Run ในเมนูย่อยที่ต้องการทราบค่า ในที่นี้ขอกล่าวถึงเฉพาะ Elliptic Curve

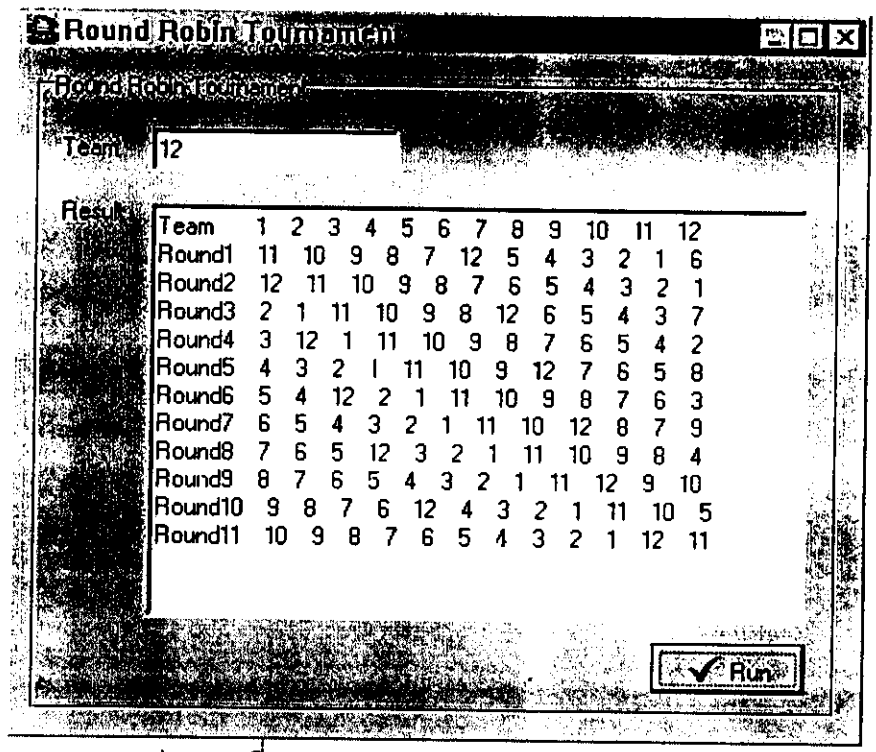
5.3 หลังจากป้อนค่าต่างๆ และคลิกปุ่ม Run แล้ว ผลลัพธ์การคำนวณต่างๆ จะแสดงในช่องแสดงผลลัพธ์ต่างๆ

5.4 ในช่อง Result จะแสดงผลลัพธ์การคำนวณของค่าตั้งแต่ 0 จนถึงค่าจำนวนเฉพาะที่ป้อนเข้ามา –1 พร้อมแสดงว่าสามารถหาคำตอบที่เป็นตัวเลขจำนวนเต็มได้หรือไม่

5.5 ในช่อง Points จะแสดงคู่อันดับของผลลัพธ์ที่สามารถคำนวณได้ ซึ่งเป็นผลลัพธ์ต่อเนื่องจากช่อง Result

5.6 ในช่อง Generator จะแสดงการหา generator ของคู่อันดับที่เป็นผลลัพธ์ต่อเนื่องจากช่อง Points ซึ่งหาคู่อันดับใดสามารถเป็น generator ได้ก็จะแสดงผลลัพธ์บอกออกมาว่าเป็น generator

6. Round Robin Tournament เป็นโปรแกรมย่อยที่ประยุกต์ใช้ระบบคอนกรูเอนซ์มาใช้ในชีวิตประจำวัน คือการจัดตารางการแข่งขันกีฬาแบบพบกันหมด ดังแสดงตามภาพประกอบที่ ก.6



ภาพประกอบที่ ก.6 Round Robin Tournament

6.1 จากตัวอย่างเป็นการจัดตารางการแข่งขันแบบพบกันหมด โดยมีทีมเข้าร่วมการแข่งขันจำนวน 12 ทีม

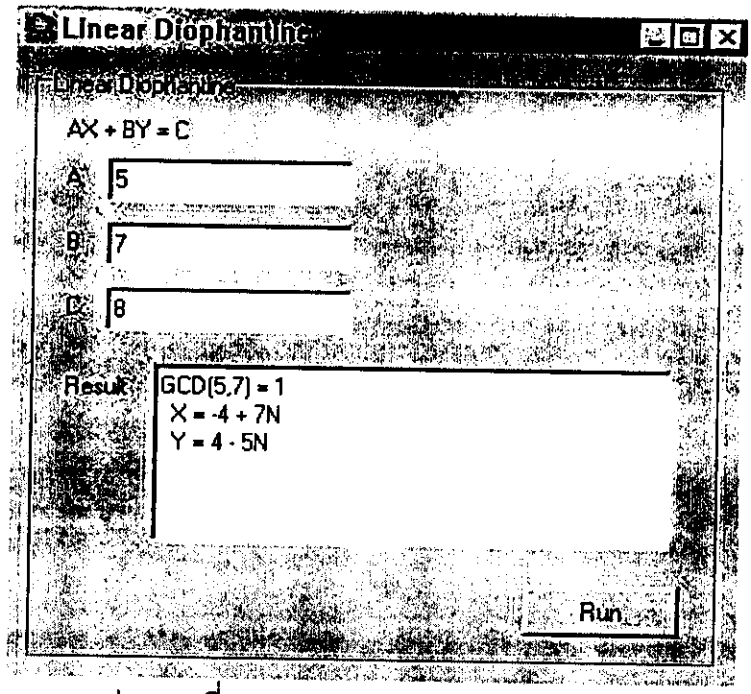
6.2 การใช้งานส่วนโปรแกรมย่อยนี้เพียงป้อนค่าจำนวนทีมที่ต้องการลงในช่องว่างจำนวนทีม

6.3 จากนั้นจึงคลิกที่ปุ่ม Run เพื่อให้ส่วนของโปรแกรมทำการคำนวณ และจัดตารางการแข่งขัน

6.4 ผลการจัดตารางการแข่งขันจะปรากฏในช่อง Result ค่าตัวเลขตามแนวนอนคือหมายเลขทีมที่จับคู่แข่งขันกันในแต่ละรอบการแข่งขัน ค่าตัวเลขตามแนวตั้งจะเป็นหมายเลขทีมที่ทีมหมายเลขที่หัวสดมภ์จะพบในแต่ละรอบ เช่น ใน

รอบที่ 1 ทีมหมายเลข 1 พบทีมหมายเลข 11 เช่นเดียวกันทีมหมายเลข 11 ก็จะพบกับทีมหมายเลข 1 ในรอบที่ 1 เช่นกัน หรือทีมหมายเลข 2 พบทีมหมายเลข 10 ในรอบที่ 1 ทีมหมายเลข 3 พบทีมหมายเลข 9 เป็นต้น

7. Linear Diophantine คือ โปรแกรมย่อยที่ใช้หาคำตอบสมการ 1 สมการแต่มี 2 ตัวแปร โดยมีรูปแบบสมการทั่วไปคือ AX + BY = C เมื่อ A, B และ C เป็นจำนวนเต็ม โดยคำตอบที่ได้จะอยู่ในรูปแบบสมการ 1 ตัวแปรซึ่งสามารถแทนค่าตัวแปรที่ได้ด้วยจำนวนเต็ม ดังภาพประกอบที่ ก.7



ภาพประกอบที่ ก.7 Linear Diophantine

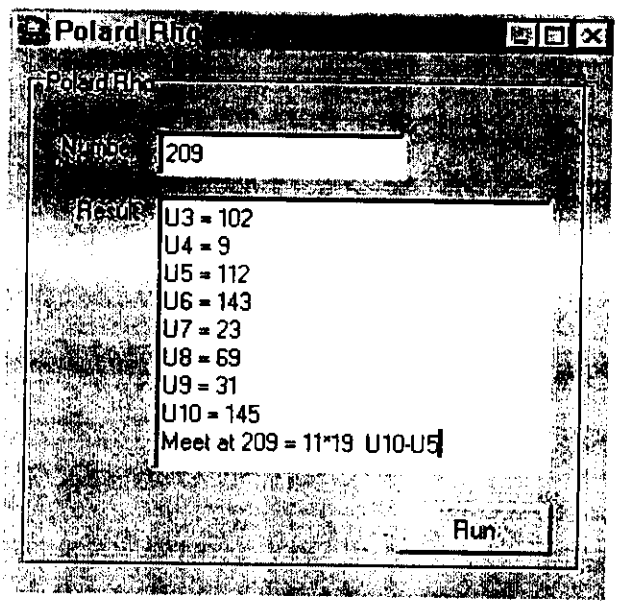
7.1 จากภาพประกอบเป็นการหาคำตอบของสมการ 5X + 7Y = 8

7.2 ป้อนค่าตัวแปร A, B และ C ลงในช่องรับค่า จากนั้นจึงคลิกที่ปุ่ม Run

7.3 ผลลัพธ์การคำนวณจะปรากฏในช่อง Result ซึ่งในส่วนแรกของผลลัพธ์จะเป็นการตรวจสอบก่อนว่าสมการที่ผู้ใช้ป้อนค่าต่างๆ เข้ามานั้นสามารถหาคำตอบได้หรือไม่ โดยการตรวจสอบค่าตัวหารร่วมมากระหว่าง A และ B หากค่าตัวหารร่วมมากที่ได้สามารถหาร C ลงตัว แสดงว่าสมการนี้สามารถหาคำตอบได้ แต่หารค่าตัวหารร่วมมากที่ได้ไม่สามารถหาร C ได้ลงตัว แสดงว่าสมการดังกล่าวไม่สามารถหาคำตอบได้

7.4 ผลลัพธ์การคำนวณต่อมาคือค่าของตัวแปร X และ Y ที่ส่วนของโปรแกรมคำนวณได้ ซึ่งติดอยู่ในรูปตัวแปร N ซึ่งเป็นตัวแปรจำนวนเต็ม

8. Polard Rho เป็นการส่วนของโปรแกรมที่ใช้ทำงานในหัวข้อเรื่องของการแยกตัวประกอบโดยวิธีการของ Polard ดังภาพประกอบที่ ก.8



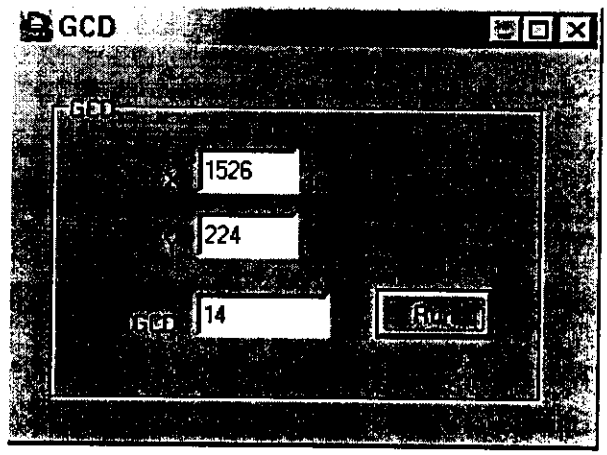
ภาพประกอบที่ ก.8 Polard Rho

8.1 จากภาพประกอบจะเป็นตัวอย่างการแยกตัวประกอบของจำนวน 209 โดยใช้วิธีของ Polard

8.2 ป้อนค่าตัวเลขที่ต้องการแยกตัวประกอบลงในช่อง Number จากนั้นจึงคลิกที่ปุ่ม Run เพื่อให้ส่วนของโปรแกรมทำการหาคำตอบ

8.3 คำตอบการคำนวณจะปรากฏในช่อง Result ซึ่งจะแสดงค่าต่างๆ ที่เกี่ยวข้องในการแยกตัวประกอบ พร้อมทั้งแสดงผลลัพธ์

9. Greatest Common Divisor เป็นการส่วนของโปรแกรมที่ใช้ทำงานในหัวข้อเรื่องของการหาค่าตัวหารร่วมมากของจำนวนสองจำนวน ดังภาพประกอบที่ ก.9



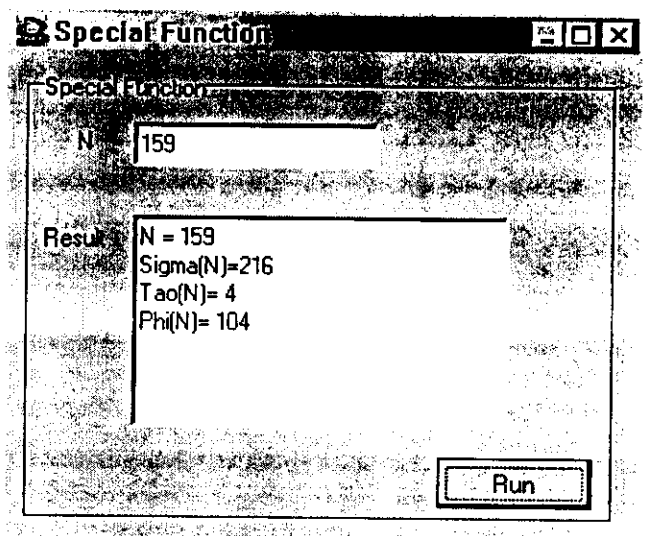
ภาพประกอบที่ ก.9 การหาค่าตัวหารร่วมมากของจำนวนสองจำนวน

9.1 ส่วนโปรแกรมนี้ต้องการข้อมูลที่ใช้ในการคำนวณเป็นตัวเลขจำนวนเต็มสองจำนวน จากภาพประกอบจะเป็นตัวอย่างการหาค่าตัวหารร่วมมากระหว่าง 1526 และ 224

9.2 ป้อนค่าข้อมูลที่ต้องการลงในช่องรับค่า ซึ่งในที่นี้คือ 1526 และ 224 จากนั้นจึงคลิกที่ปุ่ม Run เพื่อให้ส่วนของโปรแกรมทำการคำนวณ

9.3 คำตอบผลการคำนวณจะปรากฏในช่อง GCD ซึ่งก็คือค่าตัวหารร่วมมากระหว่างค่าข้อมูลเข้าทั้งสอง

10. Special Function เป็นส่วนของโปรแกรมที่ใช้ในการหาค่าฟังก์ชันพิเศษต่างๆ ที่เกี่ยวข้องกับวิชาทฤษฎีจำนวน ดังภาพประกอบที่ ก.10



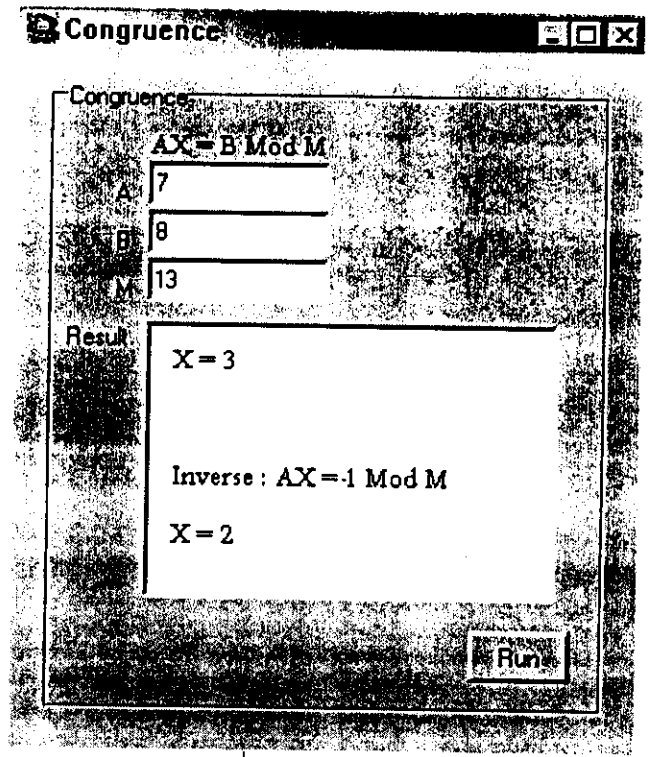
ภาพประกอบที่ ก.10 การหาค่าฟังก์ชันพิเศษต่างๆ

10.1 จากภาพประกอบเป็นการหาค่าฟังก์ชันพิเศษต่างๆ เมื่อค่าข้อมูลรับเข้าที่ต้องการหาคือ 159

10.2 ป้อนค่าข้อมูลที่ต้องการหา ซึ่งในที่นี้คือ 159 ลงในช่องรับข้อมูลเข้า จากนั้นจึงคลิกที่ปุ่ม Run เพื่อให้ส่วนของโปรแกรมทำการคำนวณคำตอบ

10.3 ผลการคำนวณจะปรากฏในช่อง Result ซึ่งก็คือค่า Sigma, Tao และ Phi ของค่าข้อมูลเข้า

11. Congruence คือส่วนของโปรแกรมที่ทำการคำนวณเกี่ยวกับระบบคอนกรูเอนซ์ ดังภาพประกอบที่ ก.11



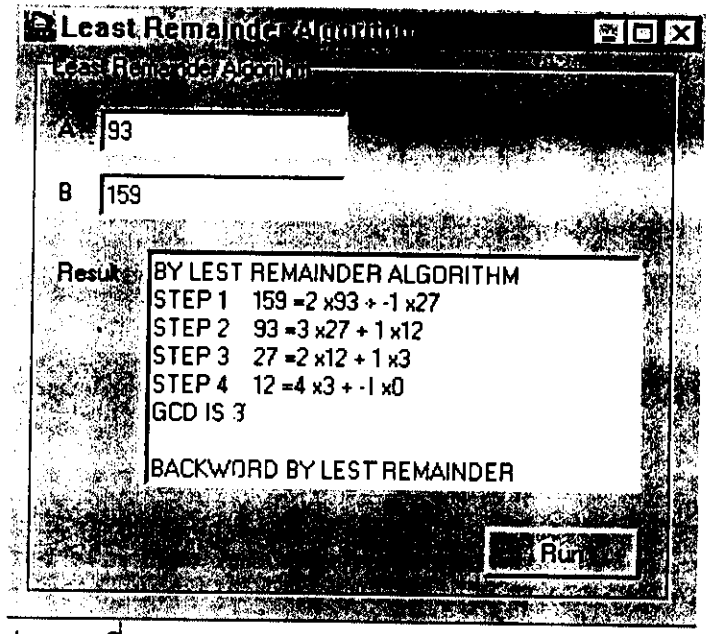
ภาพประกอบที่ ก.11 ระบบคอนกรูเอนซ์

11.1 ส่วนของโปรแกรมนี้ต้องการค่าข้อมูลเข้าคือค่า A, B และ M เพื่อให้สอดคล้องกับสมการที่แสดงไว้ จากตัวอย่างเป็นการหาค่าตัวแปรที่ต้องการเมื่อค่า A, B และ M คือ 7, 8 และ 13 ตามลำดับ

11.2 ป้อนค่าข้อมูลเข้าที่ต้องการลงในช่องรับข้อมูลเข้า จากนั้นจึงคลิกที่ปุ่ม Run เพื่อให้ส่วนของโปรแกรมทำการคำนวณผลลัพธ์

11.3 ผลลัพธ์การคำนวณจะปรากฏในช่อง Result ซึ่งคือค่าของตัวแปรที่ต้องการ พร้อมทั้งหาค่าผกผันของตัวแปรดังกล่าวที่สอดคล้องกับสมภาคที่กำหนดด้วย

12. Least Remainder Algorithm คือการหาค่าตัวหารร่วมมากโดยวิธีเศษเหลือน้อยที่สุด เป็นวิธีการหาค่าตัวหารร่วมมากอีกวิธีหนึ่ง ค่าข้อมูลเข้าคือตัวเลขจำนวนเต็มสองจำนวน การใช้งานแสดงตามภาพประกอบที่ ก.12



ภาพประกอบที่ ก.12 การหาค่าตัวหารร่วมมากโดยวิธีเศษเหลือน้อยที่สุด

12.1 จากภาพประกอบเป็นการหาค่าตัวหารร่วมมากระหว่าง 93 และ 159 ป้อนค่าตัวเลขที่ต้องการหาค่าตัวหารร่วมมากสองค่าลงในช่องรับค่า ในที่นี้คือ 93 และ 159 จากนั้นจึงคลิกที่ปุ่ม Run

12.2 ผลลัพธ์ที่คำนวณได้จะแสดงในช่อง Result ซึ่งเป็นขั้นตอนการคำนวณแต่ละขั้นตอนเพื่อจะให้ได้คำตอบซึ่งก็คือค่าตัวหารร่วมมากของจำนวน จากนั้นส่วนของโปรแกรมจึงแสดงผลการทำงานย้อนกลับของผลลัพธ์ที่ได้เพื่อให้ผู้ใช้ทราบอีกด้วย

13. การเปลี่ยนเลขฐานในส่วนของโปรแกรมต้องการค่าข้อมูลเข้าคือตัวเลขฐานสิบที่เป็นค่าตัวเลขที่ต้องการเปลี่ยนเป็นฐานอื่นๆ และค่าของฐานที่ต้องการให้เปลี่ยน การใช้งานดังแสดงในภาพประกอบที่ ก.13