

บทที่ 4 การวิเคราะห์ข้อมูล

โครงการเรื่อง การแก้หาผลเฉลย 2 ตัวแปรบนระบบสมภาคโดยใช้ระเบียบวิธีของนิวตันเป็นโครงการประเภทการสร้างทฤษฎี คณะผู้จัดทำนำเสนอผลการศึกษาโดยแบ่งเป็นทฤษฎีที่สร้างขึ้นและตัวอย่างการคำนวณโดยใช้รหัสโปรแกรมดังนี้

4.1 ทฤษฎีและสูตรทั่วไป

ทฤษฎีที่ทางได้คณะผู้จัดทำสร้างขึ้น คือ

ถ้าให้ $\alpha > 0$ และสมมติให้มี x_i, y_i ที่ทำให้ $ax_i + by_i \equiv 1 \pmod{p^\alpha}$ และ $cx_i + dy_i \equiv 1 \pmod{p^\alpha}$ เมื่อ $a, b, c, d \in \mathbb{Z}$ และ $d - b = 1$ จะได้ว่าจะมี x_{i+1} และ y_{i+1} ที่ทำให้ $ax_{i+1} + by_{i+1} \equiv 1 \pmod{p^{2\alpha}}$ และ $cx_{i+1} + dy_{i+1} \equiv 1 \pmod{p^{2\alpha}}$ เมื่อ x_{i+1} และ y_{i+1} สอดคล้องกับสมการ $x_{i+1} = x_i^2(cb - ad) + 2x_i$ และ $y_{i+1} = y_i - x_i(day_i - bcy_i + c - a)$ เมื่อ $i \geq 0$

4.2 ตัวอย่างการคำนวณ

ให้ $a = 2, b = 3, c = 5, d = 4, p = 5$ และ $n = 16$ เราต้องการหาค่า x และ y ที่ทำให้

$$2x + 3y \equiv 1 \pmod{5^{16}} \text{ และ } 5x + 4y \equiv 1 \pmod{5^{16}}$$

ขั้นตอนที่ 1 การกำหนด initial guess

เราจะเรียก x_0 และ y_0 ว่าเป็น initial guess โดย x_0 และ y_0 จะทำให้

$$2x_0 + 3y_0 \equiv 1 \pmod{5} \text{ และ } 5x_0 + 4y_0 \equiv 1 \pmod{5}$$

โดยการหา initial guess ทางคณะผู้จัดทำได้ทำการสรุปสูตรออกมาเป็น

$$x_0 = [(ad - bc) \% p]^{p-2} ((d \% p) + (-b \% p)) \% p$$

$$y_0 = [(ad - bc) \% p]^{p-2} ((-c \% p) + (a \% p)) \% p$$

เมื่อ $\% p$ คือการเอาเศษที่ได้จากการหารด้วย p

ดังนั้นจากโจทย์เราจะได้ x_0 และ y_0 เป็น 2 และ 4 ตามลำดับ

ขั้นตอนที่ 2 การหา x_{i+1} จากทฤษฎีที่สร้างขึ้น

จากทฤษฎีที่คณะผู้จัดทำได้สร้างขึ้นจะได้ว่า

$$2x_1 + 3y_1 \equiv 1(\text{mod } 5^2) \text{ และ } 5x_1 + 4y_1 \equiv 1(\text{mod } 5^2)$$

และจากสูตรทั่วไป จะได้ x_1 และ y_1 เป็น 32 และ 54 ตามลำดับ และเมื่อทำซ้ำเราจะได้

$$2x_2 + 3y_2 \equiv 1(\text{mod } 5^4) \text{ และ } 5x_2 + 4y_2 \equiv 1(\text{mod } 5^4)$$

และจากสูตรทั่วไป จะได้ x_2 และ y_2 เป็น 7232 และ 12054 ตามลำดับ และเมื่อทำซ้ำเราจะได้

$$2x_3 + 3y_3 \equiv 1(\text{mod } 5^8) \text{ และ } 5x_3 + 4y_3 \equiv 1(\text{mod } 5^8)$$

และจากสูตรทั่วไป จะได้ x_3 และ y_3 เป็น 36612723 และ 610212054 ตามลำดับ และเมื่อทำซ้ำเราจะได้

$$2x_4 + 3y_4 \equiv 1(\text{mod } 5^{16}) \text{ และ } 5x_4 + 4y_4 \equiv 1(\text{mod } 5^{16})$$

และจากสูตรทั่วไป จะได้ x_4 และ y_4 เป็น 938344050816127232 และ 1563906751360212054 ตามลำดับ

```
Enter coefficients a, b, c, d separated by spaces: 2 3 5 4
Enter mod value as p:5
Enter number of p raise to the power of n as n : 16
2 4 1 1
32 54 1 1
7232 12054 1 1
366127232 610212054 1 1
938344050816127232 1563906751360212054 1 1
```

รูปที่ 4.1 การแสดงค่าผลเฉลยของการแก้หาคำตอบ

ในบรรทัดที่ 1 จะเป็นการรับค่า a, b, c, d คือสัมประสิทธิ์ข้างหน้าตัวแปร

ในบรรทัดที่ 2 จะเป็นการรับค่า p ตัวที่ต้องการนำมาหาเศษ

ในบรรทัดที่ 3 จะเป็นการรับค่า n หรือเลขชี้กำลังของ p

ในบรรทัดที่ 4-8 เป็นการแสดงค่าต่างๆ โดยจะแสดง $x_i, y_i, (ax_i + by_i) \% p, (cx_i + dy_i) \% p$ ตามลำดับ