บทที่ 1

บทนำ

ปัจจุบันเราพบว่าเทคโนโลยีคอมพิวเตอร์เข้ามามีบทบาทในงานทุกประเภททุกสาขา เช่นการควบคุมสัญญาณระบบไฟจราจร การพยากรณ์อากาศ การบริหารงานบุคคล การควบคุมเครื่องจักร การวินิจฉัยโรค การวิเคราะห์ข้อมูล การออกแบบสิ่งก่อสร้างและผลิตภัณฑ์ต่างๆ ตลอดจนการเรียนการสอน ทั้งนี้มีเหตุเนื่องจากความสามารถและประสิทธิภาพในการทำงานของระบบคอมพิวเตอร์ที่ทำการประมวลผลข้อมูลได้อย่างถูกต้องแม่นยำและรวดเร็ว

สาขาวิชาทฤษฎีจำนวนเป็นสาขาวิชาหนึ่งทางด้านคณิตศาสตร์ที่ศึกษาถึงคุณสมบัติในด้านต่างๆ ของระบบจำนวนเต็ม การหาคำตอบในโจทย์ปัญหาต่างๆ และในอีกหลายๆ หัวข้อ จากลักษณะการศึกษาและงานวิจัยในสาขาวิชาทฤษฎีจำนวนนี้จำเป็นต้องมีการคำนวณทดสอบและแก้ปัญหาที่เป็นกระบวนการทำงานที่เป็นขั้นตอน หรือในบางส่วนต้องอาศัยการทำงานที่เป็นขั้นตอนที่ซ้ำๆ กัน เช่น การทดสอบจำนวนเฉพาะ การหาตัวหารร่วมมากโดยวิธีของยูคลิด เป็นต้น

ในลักษณะกระบวนการคำนวณดังกล่าวข้างต้นซึ่งเป็นการคำนวณที่เป็นระเบียบขั้นตอนและมีการทำซ้ำในบางขั้นตอน จึงทำให้มองเห็นว่าสามารถนำเทคโนโลยีคอมพิวเตอร์มาประยุกต์ช่วยในการคำนวณเช่นนี้ได้ ซึ่งจะช่วยลดเวลาและไม่เกิดความผิดพลาดในการคำนวณ อีกทั้งยังสามารถตรวจสอบขั้นตอนการคำนวณในแต่ละขั้นตอนได้อีกด้วย

1.1 การตรวจเอกสาร

การนำความรู้ทางคอมพิวเตอร์มาประยุกต์ใช้เพื่อคิดหาวิธีการประมวลผลการแก้ปัญหาใดๆ นั้น สิ่งจำเป็นสิ่งแรกที่ต้องทำความเข้าใจคือ ลักษณะของปัญหาหรืองานนั้นๆ ทั้งนี้เพราะการพิจารณาวิเคราะห์ปัญหาหรืองานได้อย่างเข้าใจโดยถ่องแท้ ทำให้เราสามารถดำเนินการนำเอาคอมพิวเตอร์เข้ามาเป็นเครื่องมือช่วยในการทำงานได้อย่างคุ้มค่าและมีประสิทธิภาพ

เราพบว่าปัญหาส่วนใหญ่ที่มีอยู่ในโลกนี้ ยังไม่สามารถนำคอมพิวเตอร์เข้ามาช่วยในการแก้ปัญหาได้ เมื่อพิจารณาปัญหาต่างๆ ในแง่ของการที่สามารถคำนวณได้ ก็หมายถึงปัญหาต่างๆ เหล่านั้นมีคำตอบที่เป็นผลจากการแก้ปัญหาที่เป็นขั้นตอนวิธี นอกจากนั้นยังมีปัญหาอีกบางปัญหาที่ถือว่าเป็นปัญหาที่สามารถคำนวณได้บางส่วน เช่น ปัญหา $A + B = C$ แล้วถามว่ามีเลข

จำนวนเต็มใดบ้างที่ทำให้สมการนี้ถูกต้อง ปัญหาข้อนี้จะสามารถหาคำตอบได้เพียงบางส่วนเท่านั้น เนื่องจากกลุ่มของคำตอบที่ได้มีจำนวนเป็นอนันต์

เมื่อพิจารณาเฉพาะกลุ่มของปัญหาที่มีคำตอบเป็นขั้นตอนวิธีในแง่ของความซับซ้อน ซึ่งในทางวิทยาการคอมพิวเตอร์จะเป็นการศึกษาในด้านการใช้ทรัพยากรคอมพิวเตอร์ในการคำนวณ เราพบว่าขั้นตอนวิธีที่ใช้ทรัพยากรคอมพิวเตอร์อย่างจำกัดในการทำงานเท่านั้นที่มีประโยชน์และเป็นไปได้ในทางปฏิบัติ โดยที่ทรัพยากรคอมพิวเตอร์ที่น่าสนใจ ได้แก่

1. เวลาที่ใช้ในการคำนวณตั้งแต่ต้นจนจบโดยอาศัยหน่วยประมวลผลกลางของเครื่องคอมพิวเตอร์
2. หน่วยความจำที่ใช้เก็บข้อมูลระหว่างที่ขั้นตอนวิธีนั้นปฏิบัติงาน
3. ฮาร์ดแวร์อื่นๆ ที่ต้องใช้ในการปฏิบัติงานของขั้นตอนวิธี

ทั้งนี้เนื่องจากในการแก้ปัญหาเดียวกัน สามารถมีได้หลากหลายขั้นตอนวิธี ซึ่งอาจจะใช้ทรัพยากรในปริมาณที่แตกต่างกัน ในการลดทรัพยากรประเภทหนึ่งอาจจะเพิ่มทรัพยากรอีกประเภทหนึ่งเป็นการชดเชยก็ได้ ดังนั้นเราจึงต้องหาจุดสมดุลตามความเหมาะสมในขณะนั้นและต้องพิจารณาถึงความเป็นไปได้ในทางปฏิบัติของขั้นตอนวิธีนั้นๆ โดยอาจพิจารณาในแง่ของการใช้เวลาของหน่วยประมวลผลกลางนานเกินไปหรือใช้เนื้อที่ในหน่วยความจำมากเกินไปหรือเกินกว่าที่มีอยู่หรือไม่ แต่ในบางครั้งการหาคำตอบของปัญหาต่างๆ เราต้องลดระดับความต้องการลงมาด้วยวิธีใดวิธีหนึ่ง เช่น

1. การยอมรับคำตอบในเชิงปริมาณ แทนที่จะพยายามหาคำตอบที่แท้จริง เราอาจยอมรับว่าคำตอบที่ได้เป็นคำตอบที่ดี ถึงจะไม่ดีที่สุดแต่ก็เพียงพอต่อการนำไปใช้งานได้ต่อไป
2. ในกรณีข้อมูลบางชุดทำให้ใช้เวลามากเกินไป ก็อาจยอมรับได้ในงานที่ไม่ก่อให้เกิดผลความเสียหายที่รุนแรง
3. ยอมลดหย่อนเงื่อนไขบางอย่างในการทำงาน

ดังนั้นจึงกล่าวสรุปได้ว่า ปัญหาที่เป็นไปได้ในการคำนวณ เป็นกลุ่มปัญหาที่เราสามารถนำคอมพิวเตอร์มาช่วยในการแก้ปัญหาได้เป็นอย่างดี และในการใช้คอมพิวเตอร์ในการแก้ปัญหานั้นจำเป็นต้องลดความต้องการในการค้นหาคำตอบลงบ้าง

วิชาทฤษฎีจำนวนเป็นวิชาที่ศึกษาถึงคุณสมบัติต่างๆ ของจำนวนเต็ม และในหลายๆ หัวข้อของวิชานี้จำเป็นต้องมีการคำนวณ ทดสอบและแก้ปัญหา ที่เป็นกระบวนการทำงานการคำนวณที่เป็นขั้นตอน หรือในบางส่วนก็อาศัยการทำงานที่ซ้ำไปซ้ำมา เช่น การทดสอบจำนวน

เฉพาะ การหาตัวหารร่วมมากระหว่างจำนวนสองจำนวน และตั้งแต่สองจำนวนขึ้นไป การแยกตัวประกอบ การหาฟังก์ชั่นพิเศษต่างๆ การคำนวณในส่วนของเศษส่วนต่อเนื่อง เป็นต้น

ลักษณะกระบวนการดังกล่าวข้างต้นจะเป็นการทำงานที่เป็นระเบียบขั้นตอน จึงทำให้ผู้วิจัยมองเห็นว่า สามารถนำวิชาทางวิทยาการคอมพิวเตอร์มาประยุกต์ใช้กับการทำงานเช่นนี้ได้ ซึ่งทำให้ลดเวลา และทำให้ไม่เกิดข้อผิดพลาดจากการคำนวณโดยมนุษย์ จึงได้พิจารณาเลือกหัวข้อของระบบทฤษฎีจำนวนที่กล่าวมามาสร้างเป็นชุดโปรแกรม

1.2 วัตถุประสงค์

1.2.1 เพื่อใช้ชุดโปรแกรมทฤษฎีจำนวนประกอบการเรียนการสอนสาขาวิชาทฤษฎีจำนวน

1.2.2 เพื่อใช้ชุดโปรแกรมทฤษฎีจำนวนในการคำนวณงานด้านต่างๆ ที่นำสาขาวิชาทฤษฎีจำนวนมาประยุกต์ใช้ เช่น การเข้ารหัสและถอดรหัสข้อมูล

1.2.3 เพื่อใช้ชุดโปรแกรมทฤษฎีจำนวนในการช่วยลดเวลาที่ใช้ในการคำนวณขั้นตอนที่ยุ่งยากในวิชาทฤษฎีจำนวน

1.2.4 เพื่อแสดงถึงความสัมพันธ์ระหว่างสาขาวิชาทฤษฎีจำนวนและสาขาวิชาวิทยาการคอมพิวเตอร์

1.2.5 เพื่อแสดงถึงความสำคัญของระบบคอมพิวเตอร์ในชีวิตประจำวัน

1.3 เป้าหมายและขอบเขตของการดำเนินงาน

1.3.1 จะได้ชุดโปรแกรมสำเร็จรูปที่ใช้ประกอบการเรียนการสอนวิชาทฤษฎีจำนวน

1.3.2 จะได้ชุดโปรแกรมสำเร็จรูปที่ใช้ในการคำนวณงานด้านต่างๆ ที่นำสาขาวิชาทฤษฎีจำนวนมาประยุกต์ใช้ เช่นการเข้ารหัสและถอดรหัสข้อมูล

1.3.3 จะได้ชุดโปรแกรมสำเร็จรูปที่ใช้คำนวณในสาขาวิชาทฤษฎีจำนวนบางส่วน เช่น

1.3.3.1 การหาตัวหารร่วมมากของจำนวนตั้งแต่สองจำนวนขึ้นไป

1.3.3.2 การแจกแจงจำนวนเฉพาะทั้งหมดที่น้อยกว่าหรือเท่ากับจำนวนที่กำหนดขึ้น

1.3.3.3 การแยกตัวประกอบของจำนวนเต็มที่กำหนดขึ้นโดยวิธีการต่างๆ

1.3.3.4การหาคำตอบของสมการไดโอแฟนไทน์เชิงเส้น (Linear Diophantine)

1.3.3.5 การเข้ารหัสและถอดรหัสข้อมูลโดยวิธีการต่างๆ

1.3.3.6 การคำนวณด้านเศษส่วนต่อเนื่องในรูปแบบต่างๆ

1.3.3.7 การหาค่าฟังก์ชั่นพิเศษต่างๆ

1.3.4 Input / Output Specification ส่วนของข้อมูลเข้ามีความแตกต่างกันตามแต่ส่วนของโปรแกรมย่อย เช่น ถ้าเป็นการคำนวณหาตัวหารร่วมมากของจำนวนสองจำนวนก็มีข้อมูลเข้าคือตัวเลขจำนวนเต็มสองจำนวน ถ้าเป็นส่วนของการเข้ารหัสข้อมูลเข้าคือข้อความที่ต้องการเข้ารหัสและค่ากุญแจสำหรับการเข้ารหัส ส่วนของข้อมูลออกก็เช่นเดียวกันที่มีความแตกต่างกันตามแต่ส่วนของโปรแกรมย่อย เช่น ถ้าเป็นการหาตัวหารร่วมมากของจำนวนสองจำนวนก็มีข้อมูลออกคือตัวเลขจำนวนเต็มที่เป็นตัวหารร่วมมากระหว่างตัวเลขข้อมูลเข้าทั้งสองจำนวน ถ้าเป็นส่วนของการเข้ารหัสข้อมูลออกคือข้อความที่ผ่านการเข้ารหัสเรียบร้อยแล้ว

1.3.5 Functional Specification ขอบเขตเนื้อหาการทำงานครอบคลุมเนื้อหาวิชาทฤษฎีจำนวนบางหัวข้อที่เกี่ยวข้องกับระบบเลขจำนวนเต็มเป็นส่วนใหญ่ มีเพียงบางส่วนที่อยู่นอกเหนือระบบเลขจำนวนเต็ม เช่นส่วนเนื้อหาเกี่ยวกับเศษส่วนต่อเนื่องก็มีบรรจุอยู่ในชุดโปรแกรมนี้ด้วย และส่วนของการประยุกต์นำวิชาทฤษฎีจำนวนมาใช้งาน เช่นส่วนของการเข้ารหัสและถอดรหัสข้อมูล

1.3.6 Software Design ชุดโปรแกรมประกอบด้วยส่วนของโปรแกรมหลักที่มีส่วนที่สามารถเชื่อมโยงไปยังส่วนโปรแกรมย่อยที่สามารถคำนวณค่าต่างๆ ในวิชาทฤษฎีจำนวนที่ชุดโปรแกรมมีเนื้อหาครอบคลุมถึง นอกจากนั้นยังสามารถเข้าทำงานส่วนของโปรแกรมย่อยได้จากส่วนของเนื้อหาที่อธิบายหัวข้อต่างๆ ในวิชาทฤษฎีจำนวนที่ชุดโปรแกรมมีเนื้อหาครอบคลุมถึงด้วย

1.4 ขั้นตอนและระยะเวลาการดำเนินงาน

1.4.1 สำรวจข้อมูล ความเป็นไปได้ กำหนดขอบเขตของการพัฒนา เลือกภาษาคอมพิวเตอร์และซอฟท์แวร์พื้นฐานที่ใช้ในการพัฒนา และศึกษาเนื้อหาที่เกี่ยวข้องในเรื่องวิชาทฤษฎีจำนวน

1.4.2 วิเคราะห์ส่วนของระบบพื้นฐานที่ใช้ในการทำงานด้านต่างๆ เช่น ส่วนของโปรแกรมหลักที่มีการเชื่อมโยงการทำงานระหว่างโปรแกรมย่อย ส่วนฟังก์ชันพื้นฐานทางทฤษฎีจำนวนที่มีการเรียกใช้การทำงานบ่อย เช่น การหาตัวหารร่วมมาก การตรวจสอบจำนวนเฉพาะ

1.4.3 ออกแบบส่วนของระบบพื้นฐาน

1.4.4 พัฒนาระบบพื้นฐานและส่วนของโปรแกรมต่างๆ

1.4.5 รวมส่วนของโปรแกรมย่อยต่างๆ เข้าด้วยกันและทดสอบการทำงานร่วมกันของโปรแกรมย่อย

1.4.6 ทดสอบชุดโปรแกรม

1.4.7 จัดทำเอกสารประกอบชุดโปรแกรมและงานวิจัย

ตาราง 1.1 แสดงระยะเวลาการดำเนินงานวิจัย

ขั้นตอนการดำเนินงาน	พ.ย. 2543	ธ.ค. 2543	ม.ค. 2544	ก.พ. 2544	มี.ค. 2544	เม.ย. 2544	พ.ค. 2544	มิ.ย. 2544	ก.ค. 2544
1.4.1	←	—	→						
1.4.2			↔						
1.4.3			↔						
1.4.4			←	—	—	→			
1.4.5				←	—	—	→		
1.4.6					←	—	—	→	
1.4.7								←	→

หมายเหตุ ก่อนหน้าการดำเนินงานวิจัยมีการลงทะเบียนวิชาวิทยานิพนธ์ก่อน แต่ขอกล่าวถึงในส่วนของการดำเนินงานวิจัยเท่านั้น

1.5 สถานที่และเครื่องมือที่ใช้

1.5.1 สถานที่

ห้องปฏิบัติการคอมพิวเตอร์ M. 105

โครงการจัดตั้งภาควิชาวิทยาการคอมพิวเตอร์

คณะวิทยาศาสตร์ มหาวิทยาลัยสงขลานครินทร์

วิทยาเขตหาดใหญ่

1.5.2 **เครื่องมือที่ใช้**

1.5.2.1 เครื่องคอมพิวเตอร์ หน่วยประมวลผลกลาง AMD K6/2 – 450 MHz หน่วยความจำ 32 MB ฮาร์ดดิสก์ 20 GB ระบบปฏิบัติการ Windows 98 SE

1.5.2.2 Borland Pascal Version 7.0

1.5.2.3 Borland Delphi Version 3.0

1.6 ประโยชน์ที่คาดว่าจะได้รับ

1. ได้ชุดโปรแกรมที่สามารถแสดงให้เห็นถึงขั้นตอนการคำนวณแต่ละขั้นตอนเพื่อให้ได้มาซึ่งคำตอบของแต่ละหัวข้อในวิชาทฤษฎีจำนวน
2. เพื่อการคำนวณหาคำตอบต่างๆ ที่ใช้หลักการทางวิชาทฤษฎีจำนวนให้ได้รวดเร็วยิ่งขึ้น
3. สามารถประยุกต์ใช้ในการทำงานอื่นๆ ได้ เช่นการเข้ารหัสและถอดรหัสขั้นพื้นฐาน
4. ได้สื่อการเรียนการสอนในวิชาทฤษฎีจำนวน
5. เป็นแนวทางให้ผู้สนใจเกิดความคิดในการทำวิจัยในลักษณะการพัฒนาโปรแกรมสำเร็จรูปเพื่อการเรียนการสอนและช่วยในการทำงานในสาขาวิชาอื่นๆ