

สารบัญ

	หน้า
บทคัดย่อ.....	(3)
Abstract	(4)
กิตติกรรมประกาศ.....	(5)
สารบัญ.....	(6)
รายการตาราง.....	(10)
รายการภาพประกอบ.....	(11)
บทที่	
1 บทนำ.....	1
1.1 การตรวจเอกสาร.....	1
1.2 วัตถุประสงค์.....	3
1.3 เป้าหมายและขอบเขตของการดำเนินงาน	3
1.4 ขั้นตอนและระยะเวลาการดำเนินงาน	4
1.5 สถานที่และเครื่องมือที่ใช้	5
1.6 ประโยชน์ที่คาดว่าจะได้รับ	6
2 วิชาทฤษฎีจำนวน	6
2.1 ประวัติความเป็นมาของวิชาทฤษฎีจำนวน	8
2.2 จำนวนเต็ม	9
2.3 ทฤษฎีจำนวนในชุดโปรแกรมทฤษฎีจำนวน	10
2.3.1 ตัวหารร่วมมากและขั้นตอนวิธีของยูคลิด	11
2.3.1 ขั้นตอนวิธีเศษเหลือน้อยที่สุด	13
2.3.3 การทำย้อนกลับ	15
2.3.4 จำนวนเฉพาะ	16
2.3.5 ฟังก์ชันทางทฤษฎีจำนวน	17
2.3.6 การแยกตัวประกอบโดยวิธีของแฟร์มาต์(Fermat Factorization) และการแยกตัวประกอบโดยวิธีของโพลาร์ด (Polard Rho Factorization)	19
จำนวนแฟร์มาต์ และการแยกตัวประกอบโดยวิธีของแฟร์มาต์	19

การแยกตัวประกอบโดยวิธีของโพลาร์ด	21
2.3.7 สมการไดโอแฟนไทน์เชิงเส้น	24
2.3.8 ระบบคอนกรีท	26
คอนกรีท	26
คอนกรีทเชิงเส้น	28
Round-robin Tournament	29
2.3.9 เศษส่วนต่อเนื่อง	30
เศษส่วนต่อเนื่องจำกัด	30
เศษส่วนต่อเนื่องอนันต์	36
2.3.10 การเข้ารหัส	40
หลักการทั่วไปของระบบรหัสลับ	41
ชนิดของระบบรหัสลับ	41
ระบบรหัสลับแบบซีซาร์หรือระบบรหัสลับแบบเลื่อน	42
ระบบรหัสลับแบบแอฟเฟน	43
การเข้ารหัสลับแบบบล็อก	44
การถอดรหัสลับแบบบล็อก	44
การเข้ารหัสแบบ Knapsack	45
การถอดรหัสแบบ Knapsack	47
การเข้ารหัสแบบ RSA	48
2.3.11 Elliptic Curve and Quadratic Residue	50
การบวกสองจุดใดๆ บน Elliptic Curve	51
การบวกสองจุดใดๆ บน Elliptic Curve เชิงพีชคณิต	51
การบวกสองจุดใดๆ ของ Elliptic Curve บน Z_p	52
Quadratic Residue	52
3 การพัฒนาระบบงาน	55
3.1 การวิเคราะห์ระบบงาน	56
3.2 การออกแบบระบบงาน	59
3.2.1 หลักของการออกแบบส่วนแสดงผล	60
3.2.2 หลักของการออกแบบส่วนรับข้อมูลเข้า	62
3.3 การดำเนินการสร้างระบบ	64

3.4 การทดสอบโปรแกรม	64
3.4.1 รูปแบบทั่วไปในการทดสอบระบบงานใหม่	65
3.5 การสนับสนุนภายหลังการติดตั้ง	66
4 ชุดโปรแกรมทฤษฎีจำนวน	67
4.1 การรวบรวมและวิเคราะห์ความต้องการของผู้ใช้	67
4.2 การออกแบบชุดโปรแกรม	72
4.3 การออกแบบส่วนรับข้อมูลเข้าและส่วนแสดงผลการทำงาน	74
4.4 การทำโพรโตไทป์ (Prototype).....	76
4.5 การทำงานของชุดโปรแกรมทฤษฎีจำนวน	77
4.6 การทำงานของส่วนโปรแกรมย่อย	84
4.7 ฟังก์ชันต่างๆ ที่มีการเรียกใช้งานบ่อย	84
4.8 โครงสร้างข้อมูลที่กำหนดพิเศษ	86
4.9 การพัฒนาโปรแกรมสำหรับชุดโปรแกรมทฤษฎีจำนวน	87
4.10 การทำงานติดต่อกับผู้ใช้ (User Interface)	89
5 บทสรุป	90
5.1 ผลการวิจัย	90
5.2 อุปสรรคและปัญหาในการวิจัย	90
5.3 ข้อเสนอแนะ	91
บรรณานุกรม.....	92
ภาคผนวก ก. คู่มือการใช้งานชุดโปรแกรมทฤษฎีจำนวน	93
Prime Number	93
Euclidean Algorithm	94
การแปลงจำนวนอตรรกยะเป็นเศษส่วนต่อเนื่อง	95
การเข้ารหัสแบบซีซาร์	95
Elliptic Curve and Quadratic Residue	96
Round Robin Tournament	98
Linear Diophantine	99
Polard Rho Factorization	100
การหาค่าตัวหารร่วมมาก	100
Special Function	101

Congruence	102
Least Remainder Algorithm	103
การเปลี่ยนเลขฐานสิบเป็นฐานต่างๆ	103
การแปลงจำนวนตรรกยะเป็นเศษส่วนต่อเนื่อง	104
การแปลงเศษส่วนต่อเนื่องเป็นจำนวนตรรกยะ	105
การแปลงเศษส่วนต่อเนื่องเป็นจำนวนอตรรกยะ	106
การแยกตัวประกอบ	107
Fermat Factorization	108
การแยกตัวประกอบโดยใช้เศษส่วนต่อเนื่อง	109
Block Encryption	110
Affine Encryption	111
Knapsack Encryption	112
RSA Encryption	113
ประวัติผู้เขียน	115

รายการตาราง

ตาราง	หน้า
1.1 แสดงระยะเวลาการดำเนินงานวิจัย	5
2.1 แสดงค่าฟังก์ชันทางทฤษฎีจำนวนเมื่อค่า N มีค่าตั้งแต่ 1 ถึง 12	18
2.2 Round – Robin Tournament จำนวน 5 ทีม	30
2.3 ผลเฉลยของ $y^2 \equiv x^3 + x + 1 \pmod{17}$	53
4.1 ส่วนการทำงานหลักที่สำคัญในชุดโปรแกรมทฤษฎีจำนวน	88

รายการภาพประกอบ

ภาพประกอบ	หน้า
4.1 แสดงการทำงานโดยรวมของชุดโปรแกรม.....	74
4.2 แสดงขั้นตอนต่างๆ โดยทั่วไปของโปรแกรมย่อยต่างๆ.....	74
4.3 รูปแบบทั่วไปของหน้าต่างส่วนโปรแกรมย่อย	75
4.4 แสดงโครงสร้างการทำงานของชุดโปรแกรม.....	77
4.5 ส่วนของการลงชื่อเข้าใช้ชุดโปรแกรม.....	78
4.6 ส่วนของการเชื่อมโยงไปยังเนื้อหาส่วนอธิบาย.....	79
4.7 ส่วนของการเชื่อมโยงไปยังเนื้อหาที่ใช้อ้างอิง.....	79
4.8 ส่วนของการเชื่อมโยงไปยังส่วนโปรแกรมย่อย.....	80
4.9 ส่วนของการเชื่อมโยงไปยังส่วนเกี่ยวกับชุดโปรแกรม.....	80
4.10 แสดงคำสั่งการเรียกใช้ยูนิทโปรแกรมย่อย.....	83
4.11 แสดงคำสั่งการเรียกการทำงานโปรแกรมย่อย.....	83
4.12 โครงสร้างโปรแกรมสำหรับชุดโปรแกรมทฤษฎีจำนวน	87
ก.1 Prime Number	93
ก.2 Euclidean Algorithm	94
ก.3 การแปลงจำนวนอตรรกยะเป็นเศษส่วนต่อเนื่อง	95
ก.4 การเข้ารหัสแบบซีซาร์	95
ก.5 Elliptic Curve and Quadratic Residue	96
ก.6 Round Robin Tournament	98
ก.7 Linear Diophantine	99
ก.8 Polard Rho Factorization	100
ก.9 การหาค่าตัวหารร่วมมาก	100
ก.10 Special Function	101
ก.11 Congruence	102
ก.12 Least Remainder Algorithm	103
ก.13 การเปลี่ยนเลขฐานสิบเป็นฐานต่างๆ	103
ก.14 การแปลงจำนวนอตรรกยะเป็นเศษส่วนต่อเนื่อง	104
ก.15 การแปลงเศษส่วนต่อเนื่องเป็นจำนวนอตรรกยะ	105
ก.16 การแปลงเศษส่วนต่อเนื่องเป็นจำนวนอตรรกยะ	106

ก.17 การแยกตัวประกอบ	107
ก.18 Fermat Factorization	108
ก.19 การแยกตัวประกอบโดยใช้เศษส่วนต่อเนื่อง	109
ก.20 Block Encryption	110
ก.21 Affine Encryption	111
ก.22 Knapsack Encryption	112
ก.23 RSA Encryption	113