บทที่ 6 ขั้นตอนวิธีทฤษฎีจำนวน Algorithmic Number Theory

6.1 จำนวนเฉพาะ

นิยาม จำนวนเฉพาะ(Prime) คือจำนวนเต็มบวก p ถ้า $p>1$ แล้ว p หารด้วย $\pm$ 1 และ $\pm p$ เท่านั้นลงตัว

นิยาม ค่าจำนวนเต็มบวกมากกว่า 1 ที่ไม่ใช่จำนวนเฉพาะเป็นจำนวนประกอบ

ทฤษฎีบท 6.1 จำนวนเต็มบวกมากกว่า 1 สามารถเขียนอยู่ในรูปผลคูณของจำนวนเฉพาะแสดงได้ดังนี้

$$N = \prod_{i=1}^{t} p_i^{a_i} \qquad (6.1)$$

ตัวอย่างที่ 6.1 แสดง 3600 อยู่ในรูปของค่ายกกำลังของจำนวนเฉพาะ

$$\begin{aligned} 3600 &= 36 \times 100 \\ &= 4 \times 9 \times 2 \times 2 \times 5 \times 5 \\ &= 2^4 \times 3^2 \times 5^2 \end{aligned}$$

6.2 การทดสอบจำนวนเฉพาะ

การทดสอบจำนวนเฉพาะมีความจำเป็นสำหรับการแยกค่า $N = pq$ ในระบบระบบรหัสลับ RSA หรือ Rabin และค่ามอดุโลของระบบรหัสลับของ ElGamal และการสร้างกุญแจของ Diffie-Hellman ซึ่งทั้งหมดเป็นการทดสอบจำนวนเฉพาะขนาดใหญ่และต้องให้แน่ใจว่าค่าที่ผ่านการทดสอบเป็นจำนวนเฉพาะจริงๆ มิฉะนั้นแล้วอาจทำให้ระบบรหัสลับล้มเหลวได้ โดยวิธีทดสอบแบบต่างๆ มีดังต่อไปนี้

6.2.1 วิธีทดสอบจำนวนเฉพาะ ของแฟร์มาต์

จากทฤษฎีของแฟร์มาต์ ถ้า p เป็นจำนวนเฉพาะโดย $\gcd(a, p) = 1$ และ $\Phi(p) = p - 1$ แล้ว

$$a^{p-1} \equiv 1 (mod\ p) \qquad (6.2)$$

ดังนั้นจึงสามารถทดสอบว่า N เป็นจำนวนเฉพาะหรือไม่โดยแสดงตัวอย่างดังตาราง

n	$2^{n-1} \equiv x \bmod N$	$N \quad is \quad prime$
3	$2^2 \equiv 1 \bmod 3$	Yes
4	$2^3 \equiv 0 \bmod 4$	No
5	$2^4 \equiv 1 \bmod 5$	Yes
6	$2^5 \equiv 2 \bmod 6$	No
7	$2^6 \equiv 1 \bmod 7$	Yes
8	$2^7 \equiv 0 \bmod 8$	No
9	$2^8 \equiv 4 \bmod 9$	No
10	$2^9 \equiv 2 \bmod 10$	No
11	$2^{10} \equiv 1 \bmod 11$	Yes

สำหรับขั้นตอนวิธีของแฟร์มาต์จากสมการ (6.2) แสดงได้ดังนี้

Input N
Output N *is prime ?*
Choose $a \in \{2 \le a \le N-1\}$
IF $a^{N-1} \neq 1 \bmod N$
Then N is composite
Else
N is Prime

ถ้าหาก N ที่ต้องการทดสอบมีจำนวน k บิตแล้วขนาดความซับซ้อนของขั้นตอนวิธีขึ้นอยู่กับการยกกำลังมีขนาด $O(k^3)$

ตัวอย่างที่ 6.4 ทดสอบจำนวน 341 $(341 = 11 \cdot 31)$

$$2^{340} = 1 \bmod 341$$
$$3^{340} = 56 \bmod 341$$

จากตัวอย่างค่า 341 ไม่ใช้จำนวนเฉพาะแต่ $2^{340} = 1 \bmod 341$ ทำให้การทดสอบแบบแฟร์มาต์ล้มเหลว ในกรณีนี้เรียกเลขจำนวนเต็มที่ผ่านการทดสอบว่าจำนวนเฉพาะเทียมของแฟร์มาต์ ฐาน b โดยสมบัติคือ $b^{n-1} = 1 \bmod N$

ตัวอย่างที่ 6.5 จำนวนเฉพาะเทียมของแฟร์มาต์ฐานต่าง ๆแสดงได้

341 ฐาน 2
91 ฐาน 3
15 ฐาน 4
31 ฐาน 5
35 ฐาน 6
25 ฐาน 7

จำนวนประกอบที่สามารถผ่านการตรวจสอบ $b^{n-1} = 1 \bmod N$ ทุกฐาน b เรียกว่า จำนวนคาร์ไมเคิล (Carmichael) ถ้า N เป็นจำนวนคาร์ไมเคิลแล้วทุก $p|N$ ได้ $p-1|N-1$

6.2.2 วิธีทดสอบจำนวนเฉพาะของ Solovay-Strassen

การทดสอบจำนวนเฉพาะของ Solovay-Strassen[1] ใช้การทดสอบค่าสัญลักษณ์เลอเจอค์ (Legendre) ร่วมกับทฤษฎีของแฟร์มาต์ จากสัญลักษณ์เลอเจอค์

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \; if \; a \in Q_R \\ -1 \; if \; a \in Q_{NR} \end{cases} \tag{6.3}$$

และจากสมการของแฟร์มาต์ (6.2) สามารถเขียนได้

$$\left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \; mod \; p \tag{6.4}$$

จากสมการเป็นจริงเมื่อ a เป็นค่าส่วนตกค้างกำลังสองหรือ $a = x^2$ ทำให้

$$a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \; mod \; p \tag{6.5}$$

ซึ่งเป็นจริงทุกๆกรณีเมื่อ $a \in Q_R$ ดังนั้น

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \; mod \; p \tag{6.6}$$

ทำให้เงื่อนไขข้างต้นเป็นเกณฑ์ออย์เลอร์ที่สามารถใช้ทดสอบค่า N ว่าเป็นจำนวนเฉพาะหรือไม่โดย

$$\left(\frac{a}{N}\right) \equiv a^{\frac{n-1}{2}} \; mod \; N \tag{6.7}$$

ถ้าหากค่า N เมื่อมีขนาดใหญ่แล้วการคำนวณ $\left(\frac{a}{N}\right)$ กระทำได้ใช้สมบัติของสัญลักษณ์จาโคบี

สมบัติสัญลักษณ์จาโคบี(Jacobi)

1. ถ้า n เป็นจำนวนเต็มคี่และ $m_1 \equiv m_2 \bmod n$ ดังนั้น

$$\left(\frac{m_1}{n}\right) = \left(\frac{m_2}{n}\right) \tag{J.1}$$

2. ถ้า n เป็นจำนวนเต็มคี่และผลคูณจาโคบีแสดงได้

$$\left(\frac{m_1 m_2}{n}\right) = \left(\frac{m_1}{n}\right)\left(\frac{m_2}{n}\right) \tag{J.2a}$$

ถ้าค่า $m = 2^k t$ โดย t เป็นจำนวนคี่ ดังนั้น

$$\left(\frac{m}{n}\right) = \left(\frac{2}{n}\right)^k \left(\frac{t}{n}\right) \tag{J.2b}$$

3. ถ้า n เป็นจำนวนเต็มคี่แล้ว

$$\left(\frac{2}{n}\right) = (-1)^{\frac{(n^2-1)}{8}} = \begin{cases} 1 & if\ n \equiv \pm 1 \bmod 8 \\ -1 & if\ n \equiv \pm 3 \bmod 8 \end{cases} \tag{J.3}$$

4. กฎภาวะส่วนกลับกำลังสองถ้า n เป็นจำนวนเต็มคี่แล้ว

$$\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)(-1)^{\frac{(m-1)(n-1)}{4}}$$

หรือ

$$\left(\frac{m}{n}\right) = \begin{cases} -\left(\frac{n}{m}\right) & if\ m \equiv n \equiv 3 \bmod 4 \\ \frac{n}{m} & otherwise \end{cases} \tag{J.4}$$

ตัวอย่างที่ 6.7 แสดงค่าจาโคบีของ $\left(\frac{384}{443}\right)$

$$\left(\frac{384}{443}\right)=\left(\frac{2}{443}\right)^7\left(\frac{3}{443}\right) \qquad \text{สมบัติข้อ J.2b}$$

$$=(-1)^7\left(\frac{3}{443}\right)=-\left(\frac{3}{443}\right) \qquad \text{สมบัติข้อ J.3}$$

$$=-\left(-\frac{443}{3}\right) \qquad \text{สมบัติข้อ J.4}$$

$$=\left(\frac{2}{3}\right) \qquad \text{สมบัติข้อ J.1}$$

$$=-1 \qquad \text{สมบัติข้อ J.3}$$

จากสมบัติของจาโคบีสามารถแสดงขั้นตอนวิธีได้

Input m, n
Output $\left(\frac{m}{n}\right)$
Jacobi (m, n)
If $(m = 1)$ Return 1
If $(2|m)$)
  a. If $(2|\frac{n^2-1}{8}$ return Jacobi $(m/2, n))$
  b. **return** $-$ Jacobi $(m/2, n)$
If $(2|(m-1)(n-1)/4$ **return** Jacobi $(n \bmod m, m))$
  return $-$ Jacobi $(n \bmod m, m)$

ฟังก์ชันที่ใช้ทดสอบค่าจาโคบีคือ Jacobi() เป็นฟังก์ชันเรียกตัวเอง ขั้นแรกถ้าหากค่า m เป็นเลขคู่ใช้สมบัติข้อที่ 2 และ 3 ด้วยการหารข้อมูลอินพุตที่รับเข้ามาด้วย 2 ต่อจาก นั้น เมื่อค่า m เป็นจำนวนคี่แล้วจึงใช้สมบัติข้อ 4 เพื่อลดการค่ามอดุโล วนกระทำจนกระทั่ง m มีค่าเป็น 1

ตัวอย่างที่ 6.8 หาค่าจาโคบีของ $\left(\frac{384}{443}\right)$ โดยใช้ขั้นตอนวิธี Jacobi (m,n)

$$\begin{aligned}
\text{Jacobi}\,(384,443) &= -\text{Jacobi}(192,443) && \text{ขั้นตอน J.2b}\\
&= \text{Jacobi}(96,443) && \text{ขั้นตอน J.2a}\\
&= -\text{Jacobi}(48,443) && \text{ขั้นตอน J.2b}\\
&= \text{Jacobi}(24,443) && \text{ขั้นตอน J.2a}\\
&= -\text{Jacobi}(12,443) && \text{ขั้นตอน J.2b}\\
&= \text{Jacobi}(6,443) && \text{ขั้นตอน J.2a}\\
&= -\text{Jacobi}(3,443) && \text{ขั้นตอน J.2b}\\
&= \text{Jacobi}(2,3) && \text{ขั้นตอน J.3}\\
&= -\text{Jacobi}(1,3) && \text{ขั้นตอน J.4}\\
&= -1
\end{aligned}$$

ขั้นตอนวิธีทดสอบจำนวนเฉพาะของ Solovay-Strassen แสดงได้

Input N
Output N *is prime ?*
Choose $a \in \{2 \le a \le n-1\}$

If $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \bmod n$ Then
N is prime
Else N is composite

ขนาดความซับซ้อนขั้นตอนวิธีขึ้นอยู่กับการยกกำลังโดยถ้าหาก N ที่ต้องการทดสอบมีจำนวน k บิตแล้ว ขนาดความซับซ้อนมีขนาด $O(k^3)$

ตัวอย่างที่ 6.9 ทดสอบจำนวนประกอบ 341

$$\left(\frac{2}{341}\right) = -1$$

$$2^{340} = 1 \bmod 341$$

การทดสอบแบบ Solovay-Strassen พบว่า 341 ไม่เป็นจำนวนเฉพาะ

ตัวอย่างที่ 6.10 ทดสอบจำนวน 91

$$\left(\frac{10}{91}\right)=-1$$

$$10^3 \bmod 91 = -1$$

ที่จริงแล้ว 91 เป็นจำนวนประกอบ $(91 = 7 \cdot 13)$ แต่การทดสอบแบบ Solovay-Strassen พบว่า 91 เป็นจำนวนเฉพาะ ค่าจำนวนประกอบ N ที่ผ่านการทดสอบนี้เรียกว่าจำนวนเฉพาะเทียมของออย์เลอร์ฐาน *b* ถ้า

$$\left(\frac{b}{N}\right) \equiv b^{\frac{n-1}{2}} \bmod N \qquad (6.8)$$

6.2.3 วิธีทดสอบจำนวนเฉพาะของ Miller-Rabin

ขั้นตอนวิธีเสนอโดย[3] ประกอบด้วยขบวนการสองส่วนคือการทดสอบของ Miller ที่อยู่พื้นฐานของทฤษฎีบทแฟร์มาต์และการทดสอบซ้ำของ Rabin เพื่อให้แน่ใจว่าค่าที่ทดสอบไม่เป็นจำนวนเฉพาะเทียมของคาร์ไมเคิลซึ่งเป็นจำนวนประกอบที่ผ่านการทดสอบ วิธีการการทดสอบของ Miller อาศัยทฤษฎีบทแฟร์มาต์ที่สามารถแยก

$$\left(a^{p-1} - 1\right) = \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \; mod \; p$$

ถ้าหากเทอม $\frac{p-1}{2}$ มีค่าเป็นจำนวนคู่แล้วยังคงสามารถแยกเทอม$\left(a^{\frac{p-1}{2}} - 1\right)$ ออกเป็นผลต่างกำลังสองได้อีกจนกระทั่งเทอม $\frac{p-1}{2}$ มีค่าเป็นจำนวนคี่ ดังนั้นถ้าหากค่า N เป็นจำนวนเฉพาะแล้ว ค่า $N-1$ สามารถเขียนได้ $N-1 = 2^s m$ โดยค่า m เป็นจำนวนคี่ จาก a เป็นค่าฐานมีค่าระหว่าง $1-(N-1)$ เขียนสมการอธิบายได้

$$\left(a^{2^s m} - 1\right) = \left(a^{2^{s-1} m} + 1\right)\left(a^{2^{s-2} m} + 1\right) \ldots (a^m + 1)(a^m - 1) \equiv 0 \; mod \; n$$

เพื่อให้สมการดังกล่าวเป็นจริงต้องมีค่า

$$a^m \equiv \pm 1 \; mod \; N \qquad (6.9)$$

หรือ

$$a^{2^j m} \equiv -1 \; mod \; N \qquad (6.10)$$

โดย j เป็นค่าบางค่าที่อยู่ระหว่าง $1 \leq j < s$ Miller ใช้เงื่อนไขดังกล่าวเพื่อทดสอบว่า N เป็นจำนวนเฉพาะหรือไม่ โดยถ้าหาก N เป็นจำนวนเฉพาะฐาน a แล้วการทดสอบต้องอยู่ภายใต้สมการ (6.9) หรือ (6.10)

ตัวอย่างที่ 6.11 แสดงค่า 97 เป็นจำนวนเฉพาะโดยเลือกค่าฐาน $a = 2$
ค่า $N - 1 = 96 = 2^k m = 2^5 \times 3$ ค่า $k = 5, m = 3$

$$(2^{97-1} - 1) = (2^{48} + 1)(2^{48} - 1) \equiv 0 \; mod \; 97$$

$$= (2^{48} + 1)(2^{24} + 1)(2^{12} + 1)(2^6 + 1)(2^3 + 1)(2^3 - 1) \equiv 0 \; mod \; 97$$

จากสมการ (6.10) เมื่อ $m = 3$ ค่า $j = 3$ ทำให้ $2^{2^3 3} = 2^{24} \equiv -1 mod 97$ ทำให้ $(2^{24} + 1)$ มีค่าเป็น 0 ส่งผลทำให้สมการทดสอบ(6.10) เป็นจริง

ตัวอย่างที่ 6.12 ทดสอบค่า 2047 ที่เป็นจำนวนเฉพาะเทียมผ่านทดสอบแบบแฟร์มาต์ที่ฐาน 2

$$2^{2046} \equiv 1 mod 2047$$

การทดสอบของ Miller ที่ฐาน $a = 2$ ค่า $N - 1 = 2046 = 2^s m = 2^1 \times 1023$ ค่า $k = 1, m = 1023$

$$(2^{2046} - 1) = (2^{1023} + 1)(2^{1023} - 1) \equiv 0 \; mod \; 2047$$

จากสมการ (6.9) เมื่อ $m = 1023$ ทำให้ $2^m = 2^{1023} \equiv 1 \; mod \; 2047$ ส่งผลให้ $(2^{1023} - 1)$ มีค่าเป็น 0 ทำให้สมการทดสอบเป็นจริงซึ่งถือเป็นข้อผิดพลาด

นิยาม การทดสอบของ Rabin ถ้า N เป็นเลขจำนวนเต็มคี่และหากเลือกฐาน a ต่างๆกันขนาดจำนวน i ที่มีค่าระหว่าง $0 < a < N$ โดย $\gcd(a, N) = 1$ ในการทดสอบแบบ Miller ถ้าหาก N เป็นจำนวนประกอบแล้ว โอกาสที่ N ผ่านการทดสอบมีโอกาสน้อยกว่า $\left(\frac{1}{4}\right)^i$ แสดงขั้นตอนวิธีของ Miller-Rabinได้

Input N
Output N *is prime ?*
Set $N - 1 = 2^s m$
Do i time (#)
Choose $a \in \{2 \leq a < N\}$
Set $b \equiv a^m mod\ N$
If $b \equiv 1 mod\ N$ Then loop on i (#)
Do s time
If $b \equiv -1 mod\ N$ Then loop on i (#)
If $b \equiv 1 mod\ N$ Then N is composite **Stop**
$b \equiv b^2 mod\ N$
loop on s (s time)
N is composite **Stop**
loop on i
N is prime
End

ขั้นตอนวิธี เริ่มต้นให้ค่า $N - 1 = 2^s m$ จากนั้นจึงเริ่มทดสอบเงื่อนไขตามสมการ (6.9) และสมการ (6.10) ตามลำดับ การทดสอบค่า N กระทำซ้ำจำนวน i รอบ ขนาดความซับซ้อนของขั้นตอนวิธีขึ้นอยู่กับการวนรอบของการยกกำลังถ้าให้ k เป็นขนาดของบิตอินพุต N ที่ต้องการทดสอบแล้วค่าความซับซ้อนมีขนาด $O(ik^3)$

ตัวอย่างที่ 6.13 ทดสอบ 561 ที่เป็นจำนวนเฉพาะเทียมของคาร์ไมเคิลโดยขั้นตอนวิธีแบบ Miller-Rabin

แสดงการทดสอบโดย $N - 1 = 2^s m = 2^4 \times 35$ และ a เป็นค่าฐาน $b \equiv a^{35} mod\ 561$ เป็นค่าฐาน ดังนั้นในการวนลูปย่อยจำนวน $s = 4$ จึงประกอบด้วยการหา

ค่า $b_1 \equiv a^{35} mod\ 561$, $b_2 \equiv a^{70} mod\ 561$, $b_3 \equiv a^{140} mod\ 561$, และ $b_4 \equiv a^{280} mod\ 561$ แสดงตัวอย่างสุ่มค่า a ฐานต่างๆ ได้ในตาราง

a	b_1	b_2	b_3	b_4	test
2	263	166	67	1	
5	23	529	463	67	
10	439	298	166	1	
30	21	441	375	375	
50	560	1	1	1	Fail
101	560	1	1	1	Fail
200	395	67	1	1	
251	89	67	1	1	
300	243	144	540	44	
460	1	1	1	1	Fail

จากตัวอย่าง ถ้าหากสุ่มเจอค่าฐาน 2,10,200,251 การทดสอบพบขั้นตอนทดสอบ **If** $b \equiv 1 mod\ N$ และถ้าสุ่มเจอค่าฐาน 5,30,300 การทดสอบกระทำในลูป **Do** s time จนกระทั้ง N is composite **Stop** ส่วนถ้าหากสุ่มเจอค่าฐาน 50,101,460 การทดสอบเป็นการผิดพลาดโดยการแก้ปัญหากระทำได้โดยวนทดสอบซ้ำดังที่ได้กล่าวมา

6.3 การแยกจำนวนประกอบ

จากที่ทราบว่าความแข็งแกร่งระบบรหัสของ RSA และ Rabin ขึ้นอยู่กับความสามารถของการแยกจำนวนประกอบโดยปัญหาการแยกจำนวนเฉพาะจากจำนวนประกอบขนาดใหญ่นี้เป็นปัญหาที่นักคณิตศาสตร์ ได้พัฒนามาก่อนมีระบบรหัสลับแบบกุญแจสาธารณะ [3-4] และหลังจากมีระบบรหัสลับของ RSA แล้วแล้วผู้คิดค้นรหัส RSA ได้ประกาศท้าทายให้นักวิจัยทั่งโลกทำการแยกจำนวนประกอบขนาดใหญ่ ดังนั้นจึงมีผู้พัฒนาขั้นตอนวิธี เพื่อแยกจำนวนประกอบขนาดใหญ่ที่ค่าความซับซ้อนในการทำงานเป็นที่ยอมรับได้โดยใช้การประมวลผลแบบขนานกันของคอมพิวเตอร์ ขั้นตอนวิธีแยกจำนวนประกอบตั้งแต่ยุคก่อนพัฒนาวิทยาการรหัสลับกุญแจสาธารณะจนถึงช่วงประกาศท้าทายจาก RSA มีตัวอย่างดังนี้

6.3.1 การแยกจำนวนประกอบแบบแฟร์มาต์

การแยกจำนวนประกอบของแฟร์มาต์อาศัยพื้นฐานที่ถ้าหากค่า N สามารถแยกค่าประกอบได้แล้ว ค่า N ต้องมีค่าคำตอบในรูปผลต่างกำลังสองแสดงได้

$$N = x^2 - y^2 \qquad (6.11)$$

$$N = (x + y)(x - y) \qquad (6.12)$$

เพื่อให้ได้ค่าประกอบของ N จากสมการ (6.11) ขั้นตอนวิธีของแฟร์มาต์ทำการหาค่า $y = x^2 - N$ เริ่มต้นให้ค่า x เริ่มต้นเท่ากับ $\lceil\sqrt{N}\rceil$ จนกระทั่งได้ค่า y เป็นเลขจำนวนเต็ม

Input(N)
Output($a \times b$)
$x = \lceil\sqrt{N}\rceil$
Do
$y = x^2 - N$
$x = x + 1$
until $\sqrt{y} =$ integer
$N = (x + y)(x - y)$

วิธีนี้มีประสิทธิภาพถ้าหากค่าจำนวนเฉพาะมีขนาดใกล้เคียงกัน การวนลูปเพื่อหาค่า x มีขนาดสูงสุดคือ $\frac{1}{2}\left(p+\frac{N}{P}\right)-\sqrt{N}$ หรือเท่ากับ $\frac{(\sqrt{N}-p)^2}{2p}$ ถ้าให้ค่าที่แยกคือ $p=k\sqrt{N}$ แล้ว การวนลูปมีขนาด $\frac{(1-k^2)}{2P}\sqrt{N}$ ดังนั้นขนาดความซับซ้อนของขั้นตอนวิธีมีขนาด $O(\sqrt{N})$ หรือเติบโตเป็นแบบเอกซ์โพเนนเชียล $O(exp\left(\frac{1}{2}logN\right))$ เช่นเดียวกับแบบทดลองหาร

ตัวอย่างที่ 6.14 แยกจำนวนประกอบ 3071

$x=\lceil\sqrt{3071}\rceil=56$

$x^2-n=y^2$

$56^2-3071=65$

$57^2-3071=178$

$58^2-3071=293$

$59^2-3071=410$

$50^2-3071=529 \qquad \sqrt{529}=23$

$N=(60+23)(60-23)=83\times 37$

6.3.2 การแยกจำนวนประกอบของ Pollard แบบ P-1

จากทฤษฎีของแฟร์มาต์ $a^{p-1} \equiv 1(mod\ p)$ ได้ $p|(a^{p-1}-1)$ ทุกค่าของ a และถ้า N เป็นจำนวนประกอบเกิดจาก p แล้ว สามารถหาค่าตัวประกอบได้จาก $\gcd(a^{p-1}, N)$ โดย Pollard [3] ใช้สมมุติฐานที่คาดว่าจากค่า N ถ้าหากค่าจำนวนเฉพาะที่แยกได้คือ p แล้วค่า $p-1$ เป็นจำนวนประกอบแสดงได้คือ

$$p-1 = p_1^{e_1} \times p_2^{e_2} \times p_1^{e_3} .. \times p_k^{e_k} \quad (6.13)$$

ถ้าให้ B เป็นค่าขอบเขตโดยถ้า $B = p_k^{e_k}$ แล้วต้องมีเทอมที่ $p-1|B!$ หรือได้ว่า $B! \equiv k(p-1)$ ดังนั้นถ้า $0 < a < p$ แล้ว

$$a^{B!} \equiv (a^{(p-1)})^k \equiv 1(mod\ p) \quad (6.14)$$

หรือเขียนได้ $p|a^{B!}-1$ และจาก N เป็นจำนวนประกอบเกิดจาก p ทำให้สามารถหาค่าตัวประกอบนี้ได้จาก $\gcd(a^{B!}-1, N)$ สำหรับขั้นตอนวิธีแสดงได้ในหน้า 6-17

จากขั้นตอนวิธีการวนลูปยกกำลังของการแฟกทอเรียล $(..((a^2)^3)^4)..)^B$ เพื่อหา $\gcd(a^{B!}-1, N)$ ให้จำนวนการวนรอบคือค่า B มากกว่าค่าจำนวนเฉพาะที่เป็นตัวประกอบของ $p-1$ แล้วขนาดความซับซ้อนของขั้นตอนวิธีขึ้นอยู่กับการวนรอบของการยกกำลังของการแฟกทอเรียล คือเท่ากับขนาด $O(B(logN)^2)$

Input N **Output** p
$a = 2$
For $j = 2\ to\ B$
  $a = a^j mod\ N$
  $p = \gcd(a-1, N)$
  If $p \neq 1\ and\ p \neq N$
    Then p *is factor of* N
End

ตัวอย่างที่ 6.15 หาตัวประกอบของ 2041 กำหนดให้ $B = 10$

จากค่า $N = 2041$ ประกอบด้วย 13×157 โดยที่ $p = 13$, $p - 1 = 12 = 2^2 \times 3$ ดังนั้นเมื่อ $B = 4!$ ทำให้ $p - 1 | B!$ เป็นจริง

$j = 2, a = (2^2 - 1) mod\ 2041, \gcd(3,2041) = 1$
$j = 3, a = (4^3 - 1) mod\ 2041, \gcd(63,2041) = 1$
$j = 4, a = (64^4 - 1) mod\ 2041, \gcd(195,2041) = 13$

6.3.3. การแยกจำนวนประกอบของ Pollard แบบ Rho

วิธีการแยกจำนวนประกอบของ Pollard, แบบ Rho[4] ใช้การสร้างค่าลำดับ x_k จากฟังก์ชันสุ่มพหุนาม $f(x_k) mod\ p$ ถ้า p เป็นจำนวนเฉพาะที่หารได้ลงตัวแล้ว $p|N$ สามารถสร้างค่าลำดับ $z_k = x_k\ mod\ p$ ได้เมื่อ z_k มีค่าอยู่ระหว่าง $0 - (p-1)$ และ $p \le \sqrt{N}$ แล้วลำดับของ z_k น้อยกว่าลำดับ x_k และในลำดับ z_k ถ้ามีค่า $z_i = z_j\ (j > i)$ แล้วทำให้ได้ $x_i \equiv x_j\ mod\ p$ ซึ่งจาก $p|N$ ทำให้ $p|gcd(x_i - x_j, n)$ ดังนั้น $\gcd(x_i - x_j, n)$ เป็นค่าจำนวนประกอบของ N

ตัวอย่างที่ 6.16 ให้ $N = 341 = 11 \times 31$ เลือกฟังก์ชันสุ่มพหุนาม $f(x) = x^2 + 1$ หาลำดับ

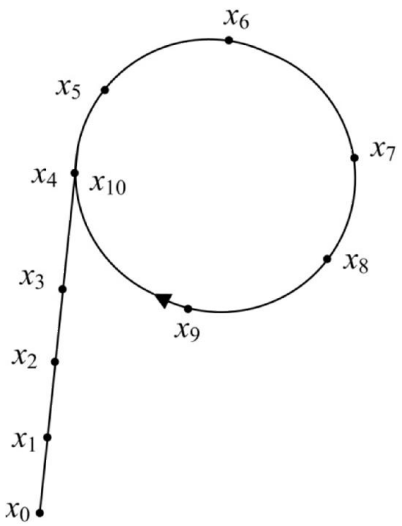
$x_k = f(x_{k-1}) mod\ 341$ กำหนดค่าเริ่มต้นให้ $x_0 = 3$

x_0	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}
3	10	101	313	103	39	158	72	70	127	103

คำนวณ $z_k = x_k\ mod\ 11$

z_0	z_1	z_2	z_3	z_4	z_5	z_6	z_7	z_8	z_9	z_{10}
3	10	2	5	4	6	4	6	4	6	4

จากลำดับ x_k ได้ $x_{10} = x_4$ ลำดับมีการซ้ำตั้งแต่ $x_4 - x_9$ และจากลำดับ z_k ได้ค่า $z_4 = z_6$ หมายถึง $x_4 \equiv x_6 \ mod\ 11$ หรือ $103 - 158 = -55$ หารด้วย 11 ลงตัวหรือค่า $\gcd(x_4 - x_6, n) = \gcd(-55, 341) = 11$ เป็นค่าจำนวนประกอบของ 341



การหาคู่ x_i ในทางปฏิบัติไม่สามารถสร้างลำดับ z_k ได้เนื่องจากไม่ทราบค่า p ดังนั้นจึงใช้การหาค่าตรงกันของคู่ลำดับ $x_i \equiv x_j$ โดยหาค่า x_i จากฟังก์ชันพหุนาม $f(x)$ และค่า x_j จากฟังก์ชันพหุนาม $f(y)$ และให้ $f(y) = f\big(f(y)\big)$ และหลังจากนั้นจึงหาค่าตัวประกอบ N จาก $\gcd(x - y, N)$

$y_0 = x_0$
$x = f(x_0)$
$y = f(y_0)$
Do
  $x_i = f(x_{i-1}) mod\ N$
  $y_i = f\big(f(y_{i-1})\big) mod\ N$
  $p = \gcd(x_i - y_i, N)$
Until $p \neq 1$

ขนาดความซับซ้อนของขั้นตอนวิธีขึ้นอยู่กับโอกาสการชนกันคู่ลำดับ อยู่ภายใต้ $\sqrt{p}$ ถ้าหากขนาด p มีขนาดกึ่งหนึ่งของ N แล้วความซับซ้อนเท่ากับ $O(N^{\frac{1}{4}})$ เติบโตเป็นแบบเอกซ์โพเนนเชียล $O(exp\left(\frac{1}{4}logN\right))$

ตัวอย่างที่ 6.16 แยกจำนวนประกอบ $N = 8051$

ใช้ $f(x) = x^2 + 1$ โดย $x_0 = 1$

i	x_i	y_i	$\gcd(y-x,n)$
0	1	1	1
1	2	5	1
2	5	677	1
3	26	2839	97

6. 4 วิธีหาค่าดิสครีตลอการิทึม

เป็นที่ทราบว่ารหัสลับแบบ ElGamal และการสร้างกุญแจแบบ Diifie-Hellman เป็นปัญหาหาดิสครีตลอการิทึม ที่ผู้วิเคราะห์รหัสได้ตัวแปรสาธารณะคือ (g, Y, p) โดย g เป็นรากปฐมฐานของจำนวนเฉพาะขนาดใหญ่ p ผู้วิเคราะห์ต้องหาให้ได้ว่าค่าลับ x ที่ทำให้ $Y = g^x mod p$ มีค่าเท่าใดโดยค่า x เป็นกุญแจลับของระบบ วิธีการหาค่าดิสครีตลอการิทึมแสดงแบบต่างๆได้ดังนี้

6.4.1 วิธีหาค่าดิสครีตลอการิทึมของ Shank

จากการหาคำตอบของการยกกำลังภายใต้มอดุโล

$$\beta \equiv \alpha^x \bmod p$$

เมื่อให้ α, x แล้วการหา β เป็นการหาคำตอบทำได้ง่ายแต่การหาคำตอบ

$$x = \log_\alpha \beta \bmod p$$

หรือปัญหาค่าดิสครีตลอการิทึมกระทำได้ยาก การแก้ปัญหาโดยการทดลองยกกำลัง $\alpha^x \bmod p$ เพื่อให้ได้ค่า β ต้องทำในขอบเขตขนาด p นั้นขั้นตอนของ Shank[6] ลดขอบเขตการหาลงเหลือเพียงขนาด $\sqrt{p}$ แสดงขั้นตอนวิธีได้ โดยให้ $m = \sqrt{p}$

$$\begin{aligned} \beta &= \alpha^x = \alpha^{i+jm} \\ &= \beta\alpha^{-jm} = \alpha^i \end{aligned} \qquad (6.18)$$

ถ้าที่ค่า i และ j ภายใต้ m ทำให้ $\beta(\alpha^{-m})^j = \alpha^i$ แล้วได้ว่า $x = i + jm$
ขั้นตอนวิธีหาค่า x แสดงได้

Set $m = \lceil \sqrt{p} \rceil$ compute $\alpha^{-m} mod\ p$
For $i = 0\ to\ m-1$
$mod\ p$
For $j = 0\ to\ m-1$

$B[i] = \beta(\alpha^{-m})^j mod\ p$

Compare $A[i] = B[i]$

If $A[i] = B[i]$

Return $x = i + jm$

End

ความซับซ้อนของขั้นตอนวิธี ของการคำนวณหาและเปรียบเทียบค่ามีขอบเขตขนาด $\sqrt{p}$ หรือความซับซ้อนเท่ากับ $O(\sqrt{p})$ และหน่วยความจำที่ใช้เก็บข้อมูลในการเปรียบ เทียบ มีขนาด $2\sqrt{p}$

ตัวอย่างที่ 6.19 หาค่า x จาก $2^x \equiv 5 mod\ 29$

1. $m = \lceil p \rceil = 6$ คำนวณ $\alpha^{-m} = 2^{-6} \equiv (2^{-1})^6 mod\ 29 = 5$

2. คำนวณตาราง α^i

i	0	1	2	3	4	5	6
α^i	0	2	4	8	16	3	6

3. จากสมการ (6.18) คำนวณ $\beta(\alpha^{-m})^j = 5(5)^j$

j	0	1	2	3	4	5
$5(5)^j$	5	25	9	16	22	23

4. $\alpha^i = 2^4 = \beta(\alpha^{-m})^i = 5(2^{-6})^3 = 16$

5. $x = i + jm = 4 + 3(6) = 22$ หรือ $2^{22} = 5 \bmod 29$

6.4.2 วิธีหาค่าอิลลิปติกดิสครีตลอการิทึมของ Shank

จากการจุดค่า P บนเส้นโค้งอิลลิปติกด้วยจำนวนเต็ม d หรือ $Q = dP$ การหาคำตอบของ Q ทำได้ง่าย แต่ถ้าหากให้จุด P และ Q แล้ว การหาค่าจำนวนเต็ม d ทำได้ยาก การใช้ขั้นตอนวิธีแบบ Shank เพื่อหาค่า d จากการให้ค่า P, Q บนสมการเส้นโค้งที่มีขนาดอันดับ $\#E(a,b) = N$ ทำได้โดยให้

$$Q = iP + jmP$$

ได้ว่า

$$iP = Q - jmP$$

ทำการหาค่า iP, jmP ในขอบเขตของ m ถ้าหากจุดทั้งสองข้างมีค่าเท่ากันแล้ว $d = i + jm$ สำหรับขั้นตอนวิธีเลียนแบบขั้นตอนในหัวข้อ 6.4.1แสดงได้

Set $m > \sqrt{N}$ compute mP
For $i = 0$ *to* $m - 1$
    $A[i] = iP$
For $j = 0$ *to* $m - 1$
    $B[i] = Q - jmP$
Compare
If $A[i] = B[i]$
    Return $d = i + jm$
End

ตัวอย่างที่ 6.20 ให้ $P = (3,10), Q = (0,22)$ เป็นจุดบนเส้นโค้งอิลลิปติก $y^2 = x^3 + x + 1 \; mod 23$ มีอันดับเท่ากับ 28 หาค่า d จาก $Q = dP$

1. กำหนด $m > \sqrt{N} = \sqrt{28}, m = 6$ และ $mP = 6(3,10) = (12,4)$
2. หาค่า iP ตั้งแต่ $i = 0$ ถึง $i = 5$

i	iP
0	O_∞
1	(3,10)
2	(7,12)
3	(19,5)
4	(17,3)
5	(9,16)

3. หาค่า $Q - jmP$ ตั้งแต่ $j = 0$ ถึง $j = 5$

j	jmP	$-jmP$	$Q - jmP$
0	∞	$-\infty$	∞
1	(12,4)	(12,19)	(1,7)
2	(5,4)	(5,19)	(11,13)
3	(6,19)	(6,4)	(3,10)
4	(17,20)	(17,3)	(9,7)
5	(7,12)	(7,11)	(18,3)

4. ที่ $iP = Q - jmP$ เมื่อ $i = 1, j = 3$ ดังนั้น $d = i + jm = 19$