모듈러 역원 연산 기법

https://youtu.be/rhySIBWUwKs

정보컴퓨터공학과 송경주

Fermat’s Little Theorem (FLT)

- **Fermat's Little Theorem (페르마의 소정리, FLT)**
  - RSA, ECC 등에서 역원 계산과 모듈러 연산 최적화에 사용됨
  - 정수 a의 역원 $a^{-1} \bmod p$ 를 구하는건 어려움
  - FLT(페르마 소정리) 를 사용하면 쉽게 연산 가능

  - FLT(페르마 소정리)는 정수 a 와 소수 p 에 대해 다음과 같은 관계를 만족:

$$a^{p-1} \equiv 1 \pmod{p}$$

ex) a=3, p =7 이면, $3^6 = 729 \bmod 7 = 1$

  - 소수 p로 나눌 수 없는 정수 a에 대해, a^{p-1}을 p로 나눈 나머지는 항상 1
  - 이를 응용하여 역원 계산에 사용할 수 있음(즉, 양 변에 a^{-1} 을 곱함)

$$a^{-1} \equiv a^{p-2} \pmod{p}$$

Fermat's Little Theorem (FLT)

- 소수 p =7 일 때, 정수 $a = 4$의 역원 a^{-1} =?

1) FTL 공식에 따라 값 대입

$$a^{-1} \equiv a^{p-2} \pmod{p} \quad = \quad 4^{-1} \equiv 4^5 \pmod{7}$$

2) 연산

$$4^{-1} \equiv 1024\,(mod\ 7)$$
$$4^{-1} \equiv 2\ (mod\ 7)$$

3) 결과 및 검산

결과 : $4^{-1} \equiv 2\ (mod\ 7)$
검산 : $4 \times 2 = 8 \equiv 1\ (mod\ 7)$

Fermat's Little Theorem (FLT) 응용

- RSA

- RSA에서 개인키 d는 공개지수 e에 대해 다음과 같이 계산됨

$$d \equiv e^{-1}\ mod\ \phi(n) \quad \text{이때, } \phi(n) = (p-1)(q-1), n = pq$$

- 즉, 개인키 d는 공개지수 e의 모듈러 역원임
- $e \times d \equiv 1 \text{ mod } \phi(n)$
- 하지만 $\phi(n)$가 소수가 아니므로 FLT를 직접 사용하지는 못함

  → Euler's Theorem (FLT 확장판) 이용

  - gcd(a,n)=1 이면 $a^{\phi(n)} \equiv 1 \text{ mod } n$
  - $a^{-1} \equiv a^{\phi(n)-1} \mod n$
  - 따라서 이론적으로는 FLT처럼 제곱으로 역원을 계산할 수 있음

Fermat’s Little Theorem (FLT) 응용

항목	FLT	Euler 정리
정리 공식	$a^{p-1} \equiv 1 \bmod p$	$a^{\phi(n)} \equiv 1 \bmod n$ $* \ \phi(n) = (p-1)(q-1), n = pq$
조건	p은 소수, $\gcd(a, p) = 1$	$\gcd(a, n) = 1$, n은 임의의 자연수
역연산 계산	$a^{-1} \equiv a^{p-2} \bmod p$	$a^{-1} \equiv a^{\phi(n)-1} \bmod n$
RSA 사용 여부	직접 사용 불가 $(\phi(n) \neq p-1)$	적용 가능

Fermat's Little Theorem (FLT) 응용

- ECC

- ECC 핵심 연산인 point addition과 point doubling에서 두 점의 기울기를 구할때, 역원 계산이 필요함
- 두 점 P=(x_1, y_1), Q=(x_2, y_2), $\mathrm{P} \neq Q$ 에 대해 Point addition 결과 R=(x_3, y_3)를 계산할 때 기울기 $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ mod p연산에 역원이 필요함

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \text{ mod p} = (y_2 - y_1) \times (x_2 - x_1)^{-1} \text{ mod p}$$

- 즉, $(x_2 - x_1)^{-1}$ 연산에 FLT 적용 가능

Fermat's Little Theorem (FLT) 양자회로 적용

- 페르마 소정리를 ECC 양자회로에 적용시, x의 역원을 구할 때, Modular squaring 을 (p-1)번 동작해야 함 → prime field ECC 비효율적

- 따라서 확장 유클리드 알고리즘 (Extended Euclidean Algorithm, EEA) 활용

확장 유클리드 알고리즘 (Extended Euclidean Algorithm, EEA)

- 정수 a, p에 대해서 gcd$(a, p) = 1$ 이라면, 모듈러 역원 $a^{-1} = x$은 다음을 만족함

$$\boxed{a \cdot x \equiv 1 \; mod \; p}$$

- 유클리드 알고리즘을 확장하면 다음 관계를 가짐:

$$\text{gcd}(a, p) = ax + py$$

- 여기서 gcd$(a, p) = 1$이면, 1 = $ax + py$ → $\boxed{ax \equiv 1 \; mod \; p}$
- 즉, x가 역원이 됨

확장 유클리드 알고리즘 (EEA)

- 소수 p =7 일 때, 정수 $a = 4$의 역원 a^{-1} =?

1) 수식 대입

$\text{gcd}(a, p) = ax + py$ → $\boxed{4x + 7y = 1}$

2) 유클리드 알고리즘 역추적 $\text{gcd}(a, p) \rightarrow \text{gcd}(\text{b}, a \bmod \text{p})$

단계	p / a	몫(q)	나머지(r)	식
1	7 / 4	1	3	7 = 4*1 + 3
2	4 / 3	1	1	4 = 3*1 + 1
3	3 / 1	3	0	종료

3) 역추적: gcd(4, 7) = 4x + 7y → $x \equiv 4^{-1}$ mod 7 을 만족하는 x 찾기

- 1 단계 수식: 3 = 7 - 4*1
- 2 단계 수식: 1 = 4 - 3*1

→수식 합치기 (수식 2에 수식 1 대입) : 1 = 4 – (7-4*1)*1 = $\boxed{\text{4*2+(-1)*7}}$

- $a = 4, p = 7, x = 2, y = -1$
- 즉 $x = a^{-1}$ = 2

Kaliski's algorithm

- 확장 유클리드 알고리즘과 유사한 원리를 따름
- 유클리드 알고리즘 기반의 역원 계산을 바탕으로 다음 특징을 가짐
  - Binary 방식 (짝수/홀수에 따라 분기)
  - 모든 연산을 덧셈/뺄셈/비트 쉬프트(2로 나눔)로 처리 → 곱셈보다 빨라 하드웨어 유리

- 동작
  - 짝수 분기:
    - If u is even : $u \leftarrow u/2$, $r \leftarrow r/2$
    - If v is even : $v \leftarrow v/2$, $s \leftarrow s/2$
  - 홀수 분기
    - If $u > v$: $u \leftarrow u - v$, $r \leftarrow r - s$
    - Else: $v \leftarrow v - u$, $s \leftarrow s - r$
  - 루프 종료: $u = 0$ 또는 $v = 0$
    - $u = 0$: 역원이 s에 저장됨 $s \bmod m$
    - $v = 0$: 역원이 r에 저장됨 $r \bmod m$

Kaliski's algorithm

- 소수 $\mathrm{m} = 7$ 일 때, 정수 $a = 4$의 역원 $a^{-1} =?$

1) 초기값 설정

$$u = 4, v = 7, r = 1, s = 0$$

- u, v: GCD 추적용 r, s: 계수 추적용 (역원 계산 결과가 저장됨)

단계	조건	연산	결과
1	$u = 4$ (짝수)	$u \leftarrow u/2, r \leftarrow r/2$	$u = 2, \mathrm{r} = 4$
2	$u = 2$ (짝수)	$u \leftarrow u/2, r \leftarrow r/2$	$u = 1, r = 2$
3	$v = 7$ (홀수), $u < v$	$v \leftarrow v - u, s \leftarrow s - r$	$v = 6, s = -2$
4	$v = 6$ (짝수)	$v \leftarrow v/2, s \leftarrow s/2$	$v = 3, s = 2$
5	$v = 3$ (홀수), $u < v$	$v \leftarrow v - u, s \leftarrow s - r$	$v = 2, s = 0$
6	$v = 2$ (짝수)	$v \leftarrow v/2, s \leftarrow s/2$	$v = 1, s = 0$
7	$u = 1$, $v = 1$	$u \leftarrow u - v, r \leftarrow r - s$	$\boldsymbol{u = 0, r = 2}$

종료 조건: u=0
역원(r) = 2

Q & A