정보보호개론(CSE441)
www.facebook.com/KoreaTech.Crypto

암호수학

Note 09 addon

한국기술교육대학교 컴퓨터공학부 김상진

sangjin@koreatech.ac.kr
www.facebook.com/sangjin.kim.koreatech

교육목표

- 암호기술을 이해하기 위한 수학
  - 정수론
  - 응용대수
    - 군(group), 환(ring), 체(field), 다항식체(polynomial field)
- 타원곡선
- 겹선형 사항(bilinear pairing)
- 암호기술 관련 수학 문제
  - RSA 문제
  - 이산대수 문제

암호에서 정수론과 응용대수의 역할

- 공개키 암호알고리즘은 일방향 트랩도어 함수가 필요함
- 보통 수학에서 어렵다고 알려진 문제들을 일방향 트랩도어 함수를 이용함
  - 이 함수들은 주로 정수론, 응용대수와 관련된 문제임
  - 가장 많이 사용하는 문제는 인수분해 문제와 이산대수 문제임
    - 이 문제는 아직 다차 시간 알고리즘을 발견하지 못한 NP 문제임
    - 하지만 양자 컴퓨팅을 이용하면 다차 시간에 해결할 수 있는 문제임

표기법

표기	의미
$\mathbb{Z}$	정수 집합, $\mathbb{Z}^+$: 양의 정수 집합 {1,2,3,…}
$\mathbb{Z}_n$	$\{0, 1, \ldots, n-1\}$
$\mathbb{Z}_n^*$	$\mathbb{Z}_n$의 원소 중 n과 서로소인 원소의 집합
$\gcd(a, b)$	정수 a와 b의 최대공약수
$a \mid b$	두 정수 a와 b에 대해 $b = ac$를 만족하는 c가 존재한다는 것을 나타내고, a가 b를 나눌 수 있다고 함(연산자가 아님) 여기서 a는 약수(divisor, factor)라 하고, b를 a의 배수라 함

모든 정수는 0을 나눔. 하지만 0 나눗셈은 존재하지 않음

나눗셈

- 모든 공집합이 아닌 양의 정수 집합은 최소 원소가 존재함
- (나눗셈 알고리즘) 정수 a와 $b(>0)$가 주어지면 다음이 성립하면 독특한 정수 q와 r이 존재함

$$a = bq + r, \qquad 0 \le r < b$$

  - 여기서 a를 피제수(dividend)와 b를 제수(divisor, modulist), q를 몫(quotient)와 r를 나머지(remainder, residue)라 함
- d가 정수 a와 b의 최대공약수이기 위한 조건
  - 조건 1. (공약수): $d|a$, $d|b$
  - 조건 2. (최대): $\forall c$ s.t $c|a \wedge c|b \rightarrow c \le d$
- 두 정수 a와 b의 최대공약수는 $\gcd(a, b) = ax + by$ 형태로 표현할 수 있음. (여기서 a와 b는 동시에 0이 아니어야 함)
- 참고. 정수에 대한 정리를 접할 때 해당 정수가 0도 포함하는지 주의 있게 살펴보아야 함
  - $\gcd(a, 0) = a, \gcd(0, 0)$은 존재하지 않음

소수

- $p \ge 2$인 양의 정수의 양의 인수가 1과 p이면 p를 소수(prime)라 함
  - 소수가 아니면 합성수($n \ge 2$)라 함
  - 0, 1은 소수도 합성수도 아님
- 모든 정수 $n \ge 2$는 다음과 같이 소수의 곱으로 표현되며, 소수의 순서를 무시하면 그 표현은 유일함

$$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$$

  - 여기서 p_i는 서로 다른 소수임
- 소수의 수는 무한함
- $n(\ge 2)$이 합성수이면 n은 $\sqrt{n}$는보다 작은 인수를 가짐
- $\gcd(a, b) = 1$이면 a와 b는 서로 소(relatively prime, coprime)라 함

유크리드 알고리즘

- 유크리드 알고리즈: $a = bq + r$이면 $\gcd(a, b) = \gcd(b, r)$임
  - $\gcd(a, b) = \gcd(b, a \bmod b), a > b$
  - 예) gcd(27, 6) = gcd(6, 3) = gcd(3, 0) = 3
  - 유크리드 알고리즘의 복잡성: $O(\log n)$
    - Why? $a \bmod b < (a/2)$

합동

- 정수 a, b, n이 있을 때 a와 b를 n으로 나눈 나머지가 같으면a와 b는 n을 법(modulus)으로 합동(congruent)이라 하고, $a \equiv b \pmod{n}$으로 표현함
- 정수 a, b, n이 있을 때 $a \equiv b \pmod{n}$이면 b는 법 n에서 a의 잉여(residue)라 함. 만약 $0 \leq b \leq n - 1$이면 b는 법 n에서 a의 최소 양의 잉여(least non-negative residue)라 함
- $\mathbb{Z}$는 n을 법으로 n개의 잉여류(residue class, equivalence class, congruent class)로 분활됨
- 예) {0, 1, 2, 3, 4}: 법 5에서 최소 양의 잉여들의 집합
- 예) {-2, -1, 0, 1, 2}: 법 5에서 최소 절대 잉여들의 집합
- 최소 양의 잉여들의 집합을 표준잉여계라 함
- 잉여계의 부분집합 중 n가 서로소인 수들만 구성된 집합을 기약잉여계(reduce residue system)라 함
- 예) {1, 2, 3, 4}: 법 5에서 기약잉여계

법 연산

- 법 연산에서는 뺄셈, 나눗셈은 정의되어 있지 않음
  - 뺄셈: 덧셈에 대한 역원을 통해 유사한 기능을 할 수 있음
  - 나눗셈: 곱셈에 대한 역원을 통해 유사한 기능을 할 수 있음
- 법 연산은 중간에 언제든지 법 연산을 취하여도 최종 결과는 같음
- 주어진 양의 정수의 모든 자리 수를 더한 것이 9로 나누어지면 해당 정수도 9로 나누어짐
  - 주어진 정수 n은 $n = \sum_{i=0}^{k} d_i \times 10^k$로 표현할 수 있음
  - $9|n \rightarrow n \bmod 9 = 0 \rightarrow 9|\sum_{i=0}^{k} d_i \times 10^k$
  - $10^k \equiv 1 \pmod 9 \rightarrow \sum_{i=0}^{k} d_i \times 10^k \equiv \sum_{i=0}^{k} d_i \pmod 9$
- 7|5432 ?
  - 5432 = (((0+5)x10+4)x10+3)x10+2
    - 위 세부 연산 중 언제든지 나머지 연산을 취할 수 있음

곱셈에 대한 역원

- $ab \equiv 1 \pmod n$이면 b는 법 n에서 a의 곱셈에 대한 역원 (multiplicative inverse, reciprocal)임
  - 예) 2와 3은 법 5에서 서로 곱셈에 대한 역원임
- a가 법 n에서 곱셈에 대한 역원이 존재하기 위한 필요충분조건은 $\gcd(a, n) = 1$임
- $a, b, c, n (> 0)$에 대해 $\gcd(c, n) = 1$이고 $ac \equiv bc \pmod n$이면 $a \equiv b \pmod n$임
- $a, b, c, d, n (> 0)$에 대해 $a \equiv b \pmod n$이고 $c \equiv d \pmod n$이면 $a \pm c \equiv b \pm d \pmod n$과 $ac \equiv bd \pmod n$가 성립함

연립합동식 (1/3)

- (중국인 나머지 정리, Chinese Remainder Theorem) $n_1, n_2, \ldots, n_k$이 각각 서로 소인 양의 정수이면 다음 연립합동식은 법 $M = n_1 n_2 \cdots n_k$에서 유일한 해를 가짐

$$\begin{aligned} x &\equiv a_1 \ (mod\ n_1) \\ x &\equiv a_2 \ (mod\ n_2) \\ &\ \ \vdots \\ x &\equiv a_k \ (mod\ n_k) \end{aligned}$$

  - 그 해는 다음과 같음
    - $x_0 = a_1 M_1 y_1 + \cdots + a_k M_k y_k,\ \ M_i = \frac{M}{n_i}, y_i \equiv M_i^{-1} \ (\mathrm{mod}\ n_i)$
- 정수에 대한 CRT 표현
  - 예) $739 \equiv 3 \ (\mathrm{mod}\ 4), 739 \equiv 1 \ (\mathrm{mod}\ 9), 739 \equiv 14 \ (\mathrm{mod}\ 25),$
    - $739 \equiv \ (3, 1, 14) \ (\mathrm{mod}\ (4, 9, 25))$
      - 0부터 899까지의 정수는 모두 CRT 법 $(4, 9, 25)$에서 독특한 표현을 가짐

연립합동식 (2/3)

- 예) 다음 연립합동식의 해를 구하시오

$$\begin{aligned} x &\equiv 1 \ (\mathrm{mod}\ 5) \\ x &\equiv 2 \ (\mathrm{mod}\ 6) \\ x &\equiv 3 \ (\mathrm{mod}\ 7) \end{aligned}$$

  - 첫 식의 해는 $5t + 1$ 형태임. 이것을 둘째 식에 대입하면 $5t + 1 \equiv 2 \ (mod\ 6)$임. 따라서 $t \equiv 5 \ (mod\ 6)$임. 즉, $t = 6u + 5$ 형태이므로 첫 두 식을 만족하는 해는 $30u + 26$ 형태임. 이것을 마지막 식에 대입하면 $30u + 26 \equiv 3 \ (mod\ 7)$임. 즉, $u = 7v + 6$ 형태이므로 위 연립합동식의 해는 $210v + 206$ 형태임. 즉, $x \equiv 206 \ (mod\ 210)$임
  - 중국인 나머지 정리
    - $M = 5 \cdot 6 \cdot 7 = 210, M_1 = 42, M_2 = 35, M_3 = 30$
    - y_1: $42y_1 \equiv 1 \ (\mathrm{mod}\ 5) \to 2y_1 \equiv 1 \ (\mathrm{mod}\ 5) \to y_1 \equiv 3 \ (\mathrm{mod}\ 5)$
    - y_2: $35y_2 \equiv 1 \ (\mathrm{mod}\ 6) \to 5y_1 \equiv 1 \ (\mathrm{mod}\ 6) \to y_2 \equiv 5 \ (\mathrm{mod}\ 6)$
    - y_3: $30y_3 \equiv 1 \ (\mathrm{mod}\ 7) \to 2y_3 \equiv 1 \ (\mathrm{mod}\ 7) \to y_3 \equiv 4 \ (\mathrm{mod}\ 7)$
    - $x \equiv 1 \cdot 42 \cdot 3 + 2 \cdot 35 \cdot 5 + 3 \cdot 30 \ \cdot 4 \equiv 206 \ (mod\ 210)$

연립합동식 (3/3)

- CRT 법의 원소들 간에 일반 연산을 수행할 수 있음
- 예) CRT 법 $(3,4,5)$, $N=60$
  - $v = 40 \cdot R_1 + 45 \cdot R_4 + 36 \cdot R_1$
  - $23 \equiv (2,3,3)\ (\text{mod}\ (3,4,5)), 46 \equiv (1,2,1)\ (mod\ (3,4,5))$
  - $(2,3,3)+(1,2,1) \equiv (3,5,4) \equiv (0,1,4)(\text{mod}\ 60)$
  - $2 \cdot (2,3,3) \equiv (4,6,6) \equiv (1,2,1)\ (\text{mod}\ 60)$
  - $(2,3,3) \cdot (1,2,1) \equiv (2,6,3) \equiv (2,2,3)\ (\text{mod}\ 60)$
  - $(2,3,3)^{-1} \equiv (2^{-1},3^{-1},3^{-1}) \equiv (2,3,2)\ (\text{mod}\ 60)$
    - 확장 유크리드 알고리즘과 비교
  - $23^3 \equiv (2^3,3^3,3^3) \equiv (8,27,27) \equiv (2,3,2)\ (\text{mod}\ 60)$
    - RSA 계산에 활용 가능

곱셈에 대한 역원 구하기

- 서로소인 a와 n이 주어지면 $\gcd(a,n) = ax + ny$를 만족하는 x와 y를 구할 수 있다고 하자. 그러면 $ax \equiv 1\ (\text{mod}\ n)$이 성립하므로 x는법 n에서 a의 곱셈에 대한 역원임
- $ax \equiv 1\ (\text{mod}\ n) \rightarrow a[i]x \equiv r[i]\ (\text{mod}\ n)$
- $\gcd(n,a) = \gcd(a, n\ \text{mod}\ a)$: 일반 유크리드 알고리즘
  - $\gcd(r[0], r[1]) = \gcd(r[1], r[0]\ \text{mod}\ r[1])$
  - $r[i] = r[i-2]\ \text{mod}\ r[i-1]$
- $q[i] = \frac{r[i-2]}{r[i-1]}, r[i-2] = q[i]r[i-1] + r[i]$
- $r[i] \equiv r[i-2] - q[i]r[i-1]\ (\text{mod}\ n)$
- $a[i]x \equiv a[i-2]x - q[i]a[i-1]x\ (\text{mod}\ n)$
- $a[i] \equiv a[i-2] - q[i]a[i-1]\ (\text{mod}\ n)$
  - $a[0]x \equiv r[0]\ (mod\ n)$
  - $a[1]x \equiv r[1]\ (mod\ n)$

	q_n	r_n	a_n
0		11	0
1		7	1
2	1	4	10
3	1	3	2
4	1	1	8

특수 합동

- (페르마의 작은 정리) p가 소수이고 $\gcd(a, p) = 1$이면 $a^{p-1} \equiv 1 \pmod{p}$가 성립함
  - a^{p-2}은 법 p에서 a의 곱셈에 대한 역원임
- 정수 $n > 0$에 대해 의 오일러 파이 함수(Euler pi(phi, totient) function)는 n보다 작은 서로 소인 양의 정수의 개수를 말함

$$\phi(n) = |\{a | 1 \le a < n \wedge \gcd(a, n) = 1\}|$$

  - 예) $\phi(5) = 4$, $\phi(6) = 2$
- (오일러 정리) 정수 $n > 0$과 $1 \le a < n$에 대해 $\gcd(a, n) = 1$이면 $a^{\phi(n)} \equiv 1 \pmod{n}$이 성립함
- $\phi(n)$ 계산법
  - p가 소수이면 $\phi(p) = p - 1$임
  - p가 소수이면 모든 $i \ge 1$에 대해 $\phi(p^i) = p^i - p^{i-1}$임
  - $\gcd(m, n) = 1$이면 $\phi(mn) = \phi(m)\phi(n)$임
  - 예) $\phi(7) = 6$, $\phi(8) = 8 - 4 = 4$, $\phi(10) = \phi(5)\phi(2) = 4$

Square-and-Multiply

- 예) $3^{17} \bmod 31$
  - 일반적 계산: 16번의 곱셈 필요
  - $3^{17} = 3^{16} \cdot 3 = 3^{2^{2^{2^2}}} \cdot 3$: 5번의 곱셈 필요
- $12345^{6789} \bmod 143$?
  - $12345 \equiv 47 \pmod{143} \rightarrow 12345^{6789} \equiv 47^{6789} \pmod{143}$
  - $\gcd(47, 143) = 1, \phi(143) = 120 \rightarrow 47^{6789} \equiv 47^{69} \pmod{143}$
  - $69 = 64 + 4 + 1 \rightarrow 47^{69} \equiv 47^{64} \cdot 47^4 \cdot 47 \pmod{143}$

카마이클 수, 보편 지수

- 양의 정수 n의 보편지수(universal exponent, Carmichael number): 모든 $1 \leq a < n$이고 $\gcd(a, n) = 1$인 a에 대해 $a^{\lambda} \equiv 1 \pmod{n}$을 만족하는 가장 작은 양의 정수 λ를 말함
  - $\lambda \leq \phi(n)$
- p와 q가 서로 다른 소수이고, $n = pq$이면
  - $\phi(pq) = \phi(p)\phi(q) = (p-1)(q-1)$
  - $\lambda = \mathrm{lcm}(p-1, q-1)$

군 (1/4)

- (군) 공집합이 아닌 집합 $\mathbb{G}$가 이항 연산 $\circ$에 대해 닫혀 있고, 다음 조건들을 만족하면 $\langle \mathbb{G}, \circ \rangle$를 군이라 함
  - (결합법칙) 모든 $a, b, c \in \mathbb{G}$에 대해 $(a \circ b) \circ c = a \circ (b \circ c)$가 성립해야 함
  - (항등원) 모든 $a \in \mathbb{G}$에 대해 다음을 만족하는 e가 존재함
$$a \circ e = e \circ a = a$$
  - (역원) 모든 $a \in \mathbb{G}$에 대해 다음을 만족하는 a^{-1}가 존재함
$$a \circ a^{-1} = a^{-1} \circ a = e$$
- (아벨군) 군 $\langle \mathbb{G}, \circ \rangle$가 추가적으로 교환법칙이 성립하면 아벨군(abelian group, commutative group)이라 함
  - (교환법칙) 모든 $a, b \in \mathbb{G}$에 대해 $a \circ b = b \circ a$가 성립해야 함
- 이항 연산이 덧셈 계열이면 덧셈군(additive group)이라 하고, 곱셈 계열이면 곱셈군(multiplicative group)이라 함
- 군을 구성하는 집합이 유한 집합이면 유한군(finite group)이라 하고, 아니면 무한군(infite group)이라 함

군 (2/4)

- $\langle \mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}, \times \bmod 7 \rangle$: 유한 곱셈군
  - 닫힘 특성: 집합의 임의 두 개 원소에 대한 이항연산의 결과는 항상 $\mathbb{Z}_7^*$에 속함
  - 결합법칙 성립
  - 항등원 존재: 1
  - 역원 존재: (1, 1), (2, 4), (3, 5), (6, 6)
  - 교환법칙 성립: 아벨군

군 (3/4)

- 유한군의 원소 개수를 군의 **위수**(order)라 함
  - 위수가 n인 유한군을 $\mathbb{G}_n$으로 표기함
- (**부분군**) $\langle \mathbb{G}, \circ \rangle$가 군이고, 공집합이 아닌 $\mathbb{H}$가 $\mathbb{G}$의 부분집합이고, $\mathbb{H}$가 이항연산 $\circ$에 대해 군을 형성하면 $\langle \mathbb{H}, \circ \rangle$를 $\langle \mathbb{G}, \circ \rangle$의 부분군이라 함
- 예) $\langle \{1, 2, 4\}, \times \bmod 7 \rangle$는 $\langle \mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}, \times \bmod 7 \rangle$의 부분군임
- 각 $\mathbb{G}$의 원소를 이용하여 부분군을 생성할 수 있음
  - 예) $2^1 = 2, 2^2 = 4, 2^3 = 1 \rightarrow \{1, 2, 4\}$
- 군의 이항연산은 명백하면 앞으로 생략하고 집합만 이용하여 군을 나타냄
- $\mathbb{G}$가 군이고 $a \in \mathbb{G}$이면 $\mathbb{H} = \{a^n | n \geq 1\}$는 a를 포함하는 $\mathbb{G}$의 가장 작은 부분군임
  - 이 군은 a를 이용하여 생성된 순환군(cyclic group)이며, a를 이 군의 **생성자**(generator, primitive root)라 하고, 이 군을 $\langle a \rangle$로 표기함
- 곱셈군이 생성자를 가지면 이 군을 순환군이라 함. 예) $\mathbb{Z}_7^* = \langle 3 \rangle$

군 (4/4)

- 군 $\mathbb{G}$의 원소 a에 대해 $a^x = e$를 만족하는 가장 작은 양의 정수 x를 군 $\mathbb{G}$에서 a의 위수라 함
  - 예) $2^1 = 2, 2^2 = 4, 2^3 = 1$이므로 $\mathbb{Z}_7^*$에서 2의 위수는 3임
- 군 $\mathbb{G}$의 원소 a의 위수가 n이면 a^m의 위수는 $n/\gcd(n,m)$임
- 예) $\mathbb{Z}_7^* = \langle 3 \rangle$, 3^2의 위수는? $\frac{6}{\gcd(6,2)} = 3$
- 위수가 n인 유한 순환군 $\mathbb{G}$의 모든 부분군은 순환군이며, 부분군의 위수는 n의 약수임
  - 위수가 n인 유한 순환군 $\mathbb{G}$의 원수 a의 위수도 n의 약수임
- 유한 순환군 $\mathbb{G}$의 위수가 n이면 n의 모든 약수 d에 대해 위수가 d인 독특한 부분군이 존재함
- 예) $\mathbb{Z}_7^* = \langle 3 \rangle$, $|\mathbb{Z}_7^*| = 6$
  - 약수: 1, 2, 3, 6 → {1}, {1,6}, {1,2,4}, {1,2,3,4,5,6}
- 순환군의 위수가 소수이면 항등원을 제외한 군의 모든 원소는 군의 생성자임

$\mathbb{Z}_n$와 $\mathbb{Z}_n^*$

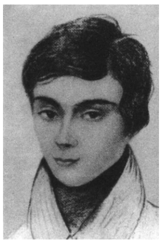
- $\mathbb{Z}_n$: 위수가 인 덧셈군
- $\mathbb{Z}_n^*$: 위수가 인 곱셈군
  - 이 군이 순환군이 되기 위한 필요충분조건은 p가 소수이고 $k \geq 1$일 때 $n = 2, 4, p^k, 2p^k$임
- $\mathbb{Z}_p^*$: 위수가 $p-1$인 순환 곱셈군
- $\mathbb{G}_q$: $\mathbb{Z}_p^*$의 위수가 소수 q인 부분군
  - 1을 제외한 모든 원소가 군의 생성자임
- 예) $\mathbb{Z}_{13}^* = \langle 2 \rangle$
  - 이 군의 위수는 12, 12의 약수는 1, 2, 3, 4, 6, 12임
  - 약수 중 소수는 2와 3
  - $\frac{12}{\gcd(12,m)} = 3 \rightarrow m = 4, 2^4 = 3$
  - $3^1 = 3, 3^2 = 9, 3^3 = 1 \rightarrow \{1,3,9\} = \langle 3 \rangle = \langle 9 \rangle$

환 (1/2)

- (환) 집합 $\mathbb{R}$에 두 개의 이항 연산 $+, \circ$이 정의되어 있고 다음 조건들을 만족하면 $< \mathbb{R}, +, \circ >$을 환(ring)이라 함
  - A. $< \mathbb{R}, + >$는 아벨군이어야 함
    - A.1 (결합법칙): $(a+b)+c = a+(b+c)$
    - A.2 (교환법칙): $a+b = b+a$
    - A.3 (항등원): $\mathbb{R}$의 모든 원소 a에 대해 $a+0=a$인 0 요소가 $\mathbb{R}$에 있어야 함
    - A.4 (역원): $\mathbb{R}$의 모든 원소 a는 $a+(-a)=0$을 만족하는 $-a$가 $\mathbb{R}$에 있어야 함
  - M.1 (결합법칙): $(a \circ b) \circ c = a \circ (b \circ c)$
  - M.2 (항등원): $\mathbb{R}$의 모든 원소 a에 대해 $a \circ 1 = 1 \circ a = a$인 1 요소가 $\mathbb{R}$에 있어야 함
  - D. (분배법칙): $a \circ (b+c) = a \circ b + a \circ c$, $(b+c) \circ a = b \circ a + c \circ a$

환 (2/2)

- (가환환) $< \mathbb{R}, +, \circ >$이 환이고, 다음이 추가적으로 만족하면 가환환(commutative ring)이라 함
  - M.3 (교환법칙): $a \circ b = b \circ a$
- (정역) 환 $\mathbb{R}$이 다음을 만족하면 정역(integral domain)이라 함
  - M.4: $a \circ b = 0$이면 $a = 0$ 또는 $b = 0$이어야 함
- (체) $< \mathbb{R}, +, \circ >$ 이 가환환이고, 0을 제외한 모든 원소가 $\circ$에 대한 역원을 가지고 있으면 체(field)라 함
  - 다른 말로 나눗셈환(division ring)이라고도 함
  - 예) 모든 소수 p에 대해 $\mathbb{Z}_p$는 체임. 다른 표기법: $GF(p), F_p$
    - 갈로아 체(Galois field)



다항식환 (1/4)

- $\mathbb{R}$이 가환환일 때 계수(coefficient)가 $\mathbb{R}$의 원소가 되는 다음과 같은 다항식을 정의할 수 있음

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots$$

  - 여기서 $a_i \in \mathbb{R}$이고 유한개의 i를 제외하고는 $a_i = 0$이다.
  - a_0, $a_1 x$ 등을 항(term)이라 하고, 이 중 a_0를 상수항이라 함
- 상수다항식(constant polynomial): a_0를 제외한 모든 $a_i = 0$인 다항식
- 영다항식(zero polynomial): 모든 $a_i = 0$인 다항식
- 최고차항 계수(leading coefficient): 모든 $i > n$에 대해 $a_i = 0$이면 a_n을 최고차항 계수라 하고, n을 다항식의 차수(degree)라 하고 $\deg f(x)$로 표기함
  - 최고차항 계수가 1이면 이 다항식을 모닉 다항식(monic polynomial)이라 함

다항식환 (2/4)

- 다항식 연산
  - 예) 일반 다항식 연산: $f(x) = x^3 + x^2 + 1$, $g(x) = x^2 + x + 1$
    - $f(x) + g(x) = x^3 + 2x^2 + x + 2$
    - $f(x) - g(x) = x^3 - x$
    - $f(x) \times g(x) = x^5 + 2x^4 + x^3 + 2x^2 + 2x + 1$
    - $f(x) = xg(x) + (-x + 1)$
  - 예) $GF(2)$에서 다항식 연산
    - $f(x) + g(x) = x^3 + x$
    - $f(x) - g(x) = x^3 + x$
    - $f(x) \times g(x) = x^5 + x^3 + 1$
    - $f(x) = xg(x) + (x + 1)$

$$\begin{array}{r} x \\ x^2+x+1 \overline{\smash{\big)}\, x^3+x^2 \qquad +1} \\ \underline{x^3+x^2+x} \\ -x \ +1 \end{array}$$

$$\begin{array}{r} x \\ x^2+x+1 \overline{\smash{\big)}\, x^3+x^2 \qquad +1} \\ \underline{x^3+x^2+x} \\ x \ +1 \end{array}$$

다항식환 (3/4)

- (다항식환) 가환환 $\mathbb{R}$의 원소를 계수로 하는 모든 다항식에 대해 다항식 덧셈과 곱셈에 대해 환을 만족하면 이 환 $\mathbb{R}[x]$을 다항식환(polynomial ring)이라 함
- 체 $\mathbb{F}$의 다항식환 $\mathbb{F}[x]$는 다음을 특성을 가지는 정역임
  - 모든 $f(x), g(x) \in \mathbb{F}[x]$에 대해 다음이 성립함
  $$\deg f(x)g(x) = \deg f(x) + \deg g(x)$$
  - (나눗셈 알고리즘) 모든 다항식 $f(x), \neq 0\ g(x) \in \mathbb{F}[x]$에 대해 다음을 만족하는 독특한 다항식 $q(x), r(x) \in \mathbb{F}$에 가 존재함
  $$g(x) = f(x)q(x) + r(x)$$
    - 여기서 $r(x) = 0$ 또는 $0 \leq \deg r(x) < \deg f(x)$임
- $\deg p(x) \geq 1$인 $p(x) \in \mathbb{F}[x]$에 대해 다음이 성립하면 $p(x)$를 기약 다항식(irreducible polynomial)이라 함
  - $f(x)|p(x)$일 필요충분조건은 $f(x) = a$이거나 $f(x) = ap(x)$임
- 기약 다항식이 아니면 가약 다항식(reducible polynomial)이라 함

다항식환 (4/4)

- (인수분해 정리) 모든 $\deg f(x) \geq 1$인 $f(x) \in \mathbb{F}[x]$는 다음과 같이 표현될 수 있음
$$f(x) = ap_1(x)^{e_1}p_2(x)^{e_2}\cdots p_k(x)^{e_k}$$
  - 여기서 $p_1(x), \ldots, p_k(x)$는 모닉 기약 다항식이고, e_i는 양의 정수임
  - 만약 곱셈 순서를 무시하면 이 인수분해는 독특함
- 예) $f(x) \in \mathbb{Z}_2[x]$
  - 가약다항식: $f(x) = x^2$, $f(x) = x^2 + 1$, $f(x) = x^2 + x$
  - 기약다항식: $f(x) = x^2 + x + 1$
- 예) $x^2 + 1 \in \mathbb{Z}_7[x]$는 기약 아니면 가약?
  - $f(0) = 1$, $f(1) = 2$, $f(2) = 5$, $f(3) = 3$, $f(4) = 3$, $f(5) = 5$, $f(6) = 2$이기 때문에 기약 다항식임

$\mathbb{Z}_2[x]$ (1/2)

- 모든 계수가 0 아니면 1이기 때문에 비트 문자열로 표현할 수 있음
- 이 문자열을 다시 일반 정수로 표현 가능

0(000)	1(001)	2(010)	3(011)	4(100)	5(101)	6(110)	7(111)
0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1

- 덧셈 연산
  - 계수들을 더하는 형태로 계산되기 때문에 XOR 연산으로 구현 가능
  - 예) $a(x) = x^6 + x^4 + x^2 + x + 1, b(x) = x^7 + x + 1$
    - $a(x) + b(x) = x^7 + x^6 + x^4 + x^2$
    - $(0101\ 0111) \oplus (1000\ 0011) = (1101\ 0100)$, 57+83=D4
- 기약 다항식을 이용하여 특정 차수 이하에 다항식으로만 구성된 체를 만들 수 있음

$\mathbb{Z}_2[x]$ (2/2)

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

일반 연산

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	3	1	7	5
3	0	3	6	5	7	4	1	2
4	0	4	3	7	6	2	5	1
5	0	5	1	4	2	7	3	6
6	0	6	7	1	5	3	2	4
7	0	7	5	2	1	6	4	3

$\mathbb{Z}_2[x]_{x^3+x+1}$

$$x \cdot (x^2 + 1) = x^3 + x$$

$$x^3 + x \bmod x^3 + x + 1 = 1$$

곱셈 연산: 이동 연산과 XOR 연산으로 구현 가능

타원곡선 (1/6)

- 가장 널리 사용하는 공개키 암호알고리즘은 인수분해 문제나 이산대수 문제에 의존함
  - 문제. 컴퓨팅 기술의 발달로 이 문제를 해결하는데 소요되는 시간이 점점 단축되고 있으며, 이 때문에 지속적으로 이들 알고리즘에서 사용하는 키 길이가 늘어나고 있음
- 타원곡선(elliptic curve) 기반 암호알고리즘은 이와 같은 문제를 해결하기 위해 연구된 결과임
  - 같은 안전성을 제공하면서 키 길이를 줄일 수 있음
  - 타원곡선은 기존 이산대수 기반 알고리즘을 대체할 수 있음
    - 이산대수 기반 알고리즘에서는 곱셈군을 사용하지만 타원곡선은 덧셈군을 사용함

타원곡선 (2/6)

- 타원곡선 기반 순환군은 다음과 같은 형태의 식을 사용함

$$y^2 + axy + by = x^3 + cx^2 + dx + e$$

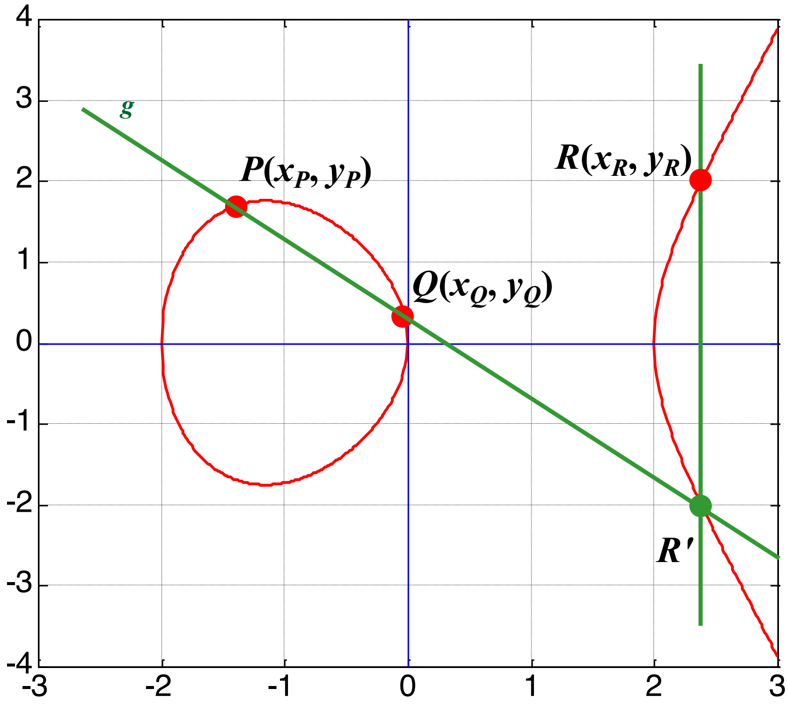
  - 이 식은 $y^2 = x^3 + ax + b$로 단순화할 수 있음
- $y^2 = x^3 + ax + b$을 이용하여 타원곡선 기반 군을 형성하기 위해서는 $x^3 + ax + b$가 여러 개의 근이 없어야 함. 이것은 $4a^3 + 27b^2 \neq 0$을 검사하여 확인할 수 있음. 예) $a = -12, b = 16$
- 이 곡선에 있는 점들이 군 원소가 됨
  - 이 군에서 항등원은 무한대 있는 점 $O(x, \infty)$을 사용함
- 표준 곡선
  - P-256 (FIPS 186-4에 제시된 15개 중 하나, secp256r1)
  - Curve25519 (RFC 7748)

$$y^2 = x^3 + 486662x^2 + x \mod p, p = 2^{555} - 1$$
$$|G| = 2^{252} + 27742317777372353535851937790883648493$$

  - Secp256k1 (비트코인에서 사용 중)

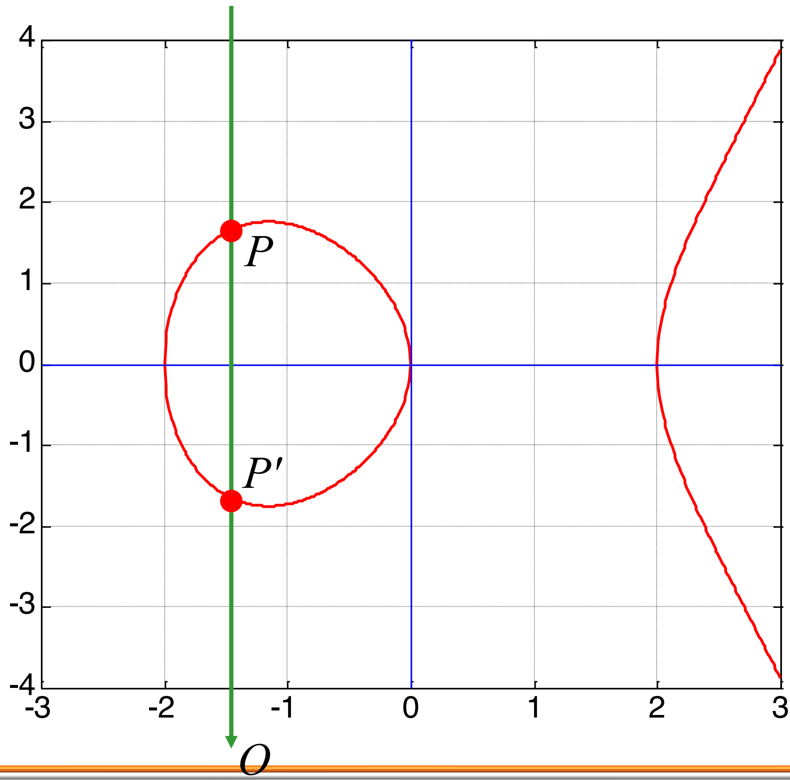
타원곡선 (3/6)

- $R = P + Q$



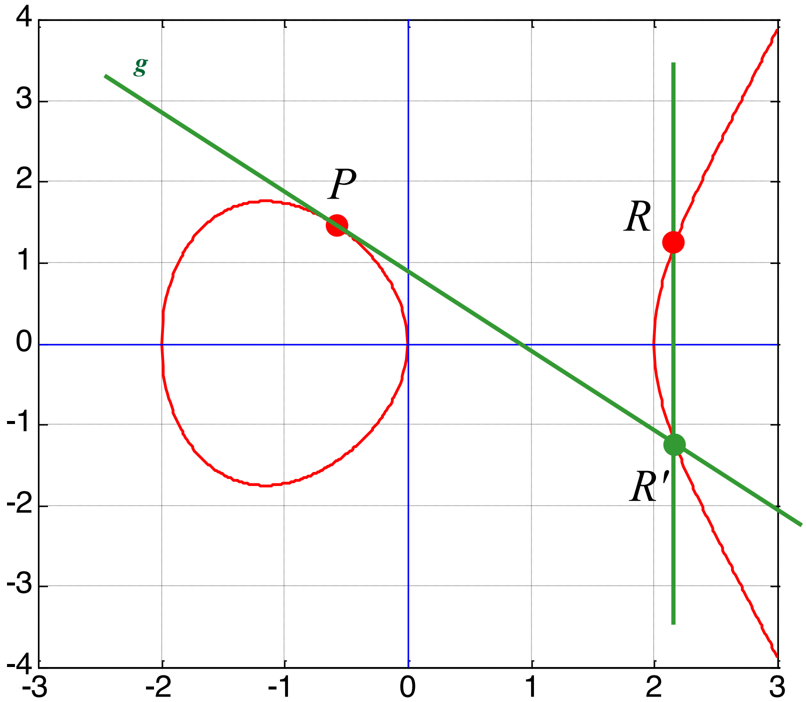
타원곡선 (4/6)

- $P + O = P$
- $O + O = O$



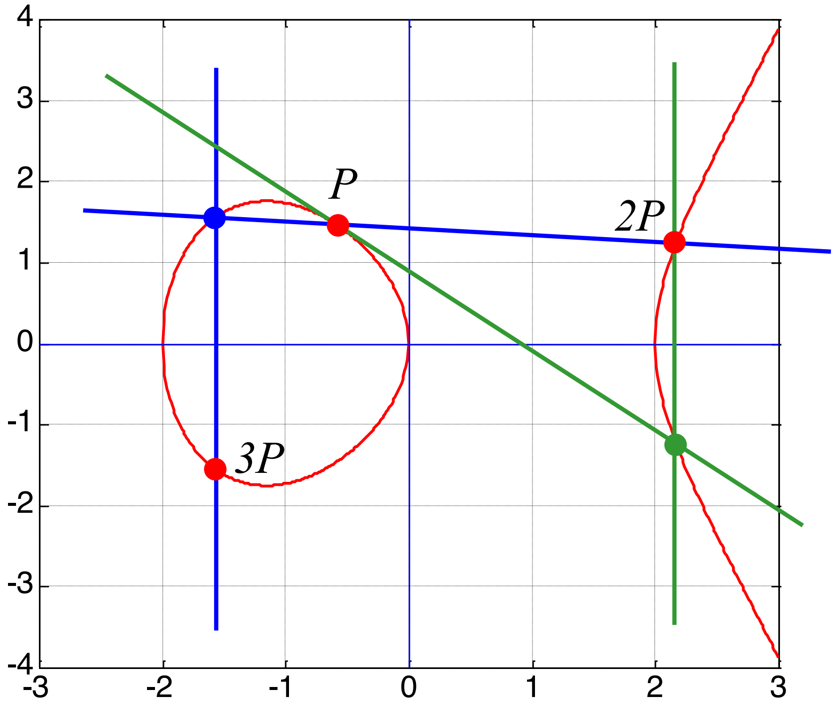
타원곡선 (5/6)

- $P + P = 2P$



타원곡선 (6/6)

- $P + P + \cdots + P = kP$



겹선형 사상 (1/2)

- 겹선형 사상(bilinear pairing): 원래 타원곡선 공개키 기술을 공격하기 위해 개발됨
- 그 이후 목적이 바뀌어 현재는 암호기술로 사용하고 있음
- 특히, 이것을 이용하면 3자간 자체 강화 방식의 키 동의 프로토콜을 수행할 수 있음
- (겹선형 사상) G_1이 타원곡선 기반 유한 순환군이고, G_2는 유한 순환 곱셈군이며, 두 군의 위수가 같을 때, 사상 $\hat{e}$: $G_1 \times G_1 \rightarrow G_2$가 다음 조건을 만족하면 사용가능 겹선형 사상이라 함
  - 겹선형: $P, Q, R \in G_1$에 대해 다음이 성립함
    $\hat{e}(P+Q, R) = \hat{e}(P, R) \cdot \hat{e}(Q, R)$, $\hat{e}(P, Q+R) = \hat{e}(P, Q) \cdot \hat{e}(P, R)$
  - Non-degenerate: 대다수의 $P, Q \in G_1$에 대해 $\hat{e}(P, Q)$는 G_2의 항등원으로 매핑하지 않아야 함
  - 계산 가능: 모든 $P, Q \in G_1$에 대해 $\hat{e}(P, Q)$를 효과적으로 계산할 수 있어야 함

겹선형 사상 (2/2)

- 겹선형 특성 때문에 다음을 만족함

$$\hat{e}(aP, bQ) = \hat{e}(P, bQ)^a = \hat{e}(aP, Q)^b = \hat{e}(P, Q)^{ab}$$
$$= \hat{e}(abP, Q) = \hat{e}(P, abQ)$$

- 겹선형 사상 때문에 더 이상 타원곡선 기반 결정 DH 문제는 어려운 문제가 아님

$$\hat{e}(aP, bQ)? = \hat{e}(cP, Q)$$

- (BDHP, Bilinear DH Problem) 타원곡선 기반 유한 순환군 $G = \langle P \rangle$와 $P, aP, bP, cP \in G$가 주어지면 $\hat{e}(P, P)^{abc}$를 찾는 문제
  - 이 문제는 a, b, c 중 하나를 알면 계산할 수 있음
    $$\hat{e}(aP, bP)^c = \hat{e}(aP, cP)^b = \hat{e}(bP, cP)^a = \hat{e}(P, P)^{abc}$$
  - 이 문제는 타원곡선 기반 DH 계산 문제를 해결할 수 있어도 해결할 수 있음
    $$\hat{e}(aP, bcP) = \hat{e}(bP, acP) = \hat{e}(cP, abP) = \hat{e}(P, P)^{abc}$$

암호기술에 사용되는 어려운 문제

- 공개키 암호알고리즘은 안전한 일방향 트랩도어 함수를 이용함
- 일방향 트랩도어 함수란 트랩도어 정보를 알고 있으면 주어진 함수의 역을 구할 수 있고, 모르면 일방향인 함수를 말함
- 보통 수학적 어려운 문제를 일방향 트랩도어 함수로 활용함
  - 대표적인 문제: 인수분해 문제, 이산대수 문제
- 왜 인수분해 문제가 일방향 트랩도어 함수인가?
  - 매우 큰 같은 크기의 두 개의 소수 p와 q를 입력으로 받는함수 $f(p,q) = p \times q = n$
    - n으로부터 p와 q를 찾는 것은 계산적으로 어려운 문제임
    - 여기서 트랩도어? p와 q
      - 트랩도어로부터 p와 q 를 계산하는 것이 아니라 역 자체가 트랩도어임. 조금 특이?

인수분해 문제

- (인수분해 문제) 정수 n이 주어졌을 때 다음을 만족하는 서로 다른 소수 p_i와 지수 e_i를 찾는 문제를 말함
$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$
- (소수판별 문제) 주어진 정수 n이 소수인지 판단하는 문제는 쉬운 문제 (다항시간 알고리즘 존재)임
- 가장 직관적인 인수분해 방법
  - 가능한 모든 인수로 나누어 보는 것
    - 최악의 경우: $\sqrt{n}$보다 작은 모두 정수를 시도해 보아야 함. $O(\sqrt{n})$
  - 참고. 주어진 정수 n이 합성수이면 n은 $\sqrt{n}$보다 작은 소인수를 가짐
- 효과적인 인수분해 알고리즘의 기본 생각
  - 랜덤한 $\sqrt{n}$보다 작은 모두 임의 정수 a를 선택한 후 $\gcd(n, a)$을 계산하여 n의 약수를 찾음

- RSA에서 사용하는 $n = pq$에 대한 인수분해 속도

bit length of *n*	time duration	machine	memory
430	Under 5 minutes	105	-
760	600 month	4300	4 GB
1020	342,000,000 years	114	170 GB
1620	1.6×10^5 years		120 TB

	current	until 2030	after 2031
Symmetric key	80 bits	112 bits	128 bits
n	1024 bits	2048 bits	3072 bits

From RSA Laboratories, Factoring Challenge FAQ

RSA 문제

- (RSA 문제) 두 개의 소수 p와 q의 곱인 양의 정수 n과 $\gcd(e, \phi(n)) = 1$인 양의 정수 e, 양의 정수 $c(< n)$가 주어졌을 때, $m^e \equiv c \ (mod\ n)$를 만족하는 양의 정수 m을 찾는 문제를 말함
  - n을 인수분해할 수 있으면 이 문제를 해결할 수 있음
  - 하지만 RSA 문제를 해결이 인수분해 해결을 의미하지는 않음. 아직 이것은 증명되어 있지 않지만 많은 학자들은 두 문제가 등가인 문제로 생각하고 있음
- 유사문제
  - 이차 잉여(quadratic residue) 문제. 주어진 수가 이차잉여인지 여부를 결정하는 문제
    - 이차 잉여. 양의 정수 $a(< n)$가 법 n에서 이차 잉여이면 $x^2 \equiv a \ (mod\ n)$인 x가 존재함
  - 제곱근 구하기 문제. 이차 잉여가 주어졌을 때 그것의 제곱근을 구하는 문제
    - 제곱근 구하기 문제는 인수분해 문제와 등가 문제임

소수 생성

- RSA나 이산대수 기반 암호알고리즘들은 모두 일정한 크기의 소수를 생성할 필요가 있음
  - 보통 소수는 랜덤하게 일정한 크기의 수를 생성한 다음 소수 판별 문제를 이용하여 해당 수가 소수인지 판단함
    - 매우 많은 수의 검사가 필요할 수 있음
    - 150자리 정수: 350개, 600자리 정수: 1400개 검사 필요 $(1/\ln(N))$
  - 참고. 이산대수에서 필요한 생성자도 유사하게 생성
    - 군의 원소를 랜덤하게 선택한 후 위수 검사

소수 판별

- 페르마의 작은 정리 이용: p가 소수이고 $\gcd(a, p) = 1$이면 $a^{p-1} \equiv 1 \pmod{p}$가 성립함
  - n이 소수? 임의의 $a(< n)$를 선택한 후 a^{n-1}를 계산하여 법 n에서 1과 합동인지 검사
    - 카마이클 수는 이 테스트를 통과함
- Miller와 Rabin 방법
  - n이 소수이면 1의 제곱근은 1 또는 -1이어야 함
    - 법 n에서 1, -1이 아닌 1의 제곱근이 존재하면 n은 소수가 아님
  - $a^{n-1} \equiv 1 \pmod{n}$이 성립한다는 가정하에 $n - 1 = 2^s d$를 계산한 후, a^d를 이용하여 법 n에서 1, -1이 아닌 1의 제곱근을 찾음
  - 예) 561 (가장 작은 카마이클 수)
    - $560 = 2^4 \cdot 35, a = 7$
      - $7^{35} \equiv 241 \pmod{561}, 241^2 \equiv 298 \pmod{561}, 298^2 \equiv 166 \pmod{561}, 166^2 \equiv 67 \pmod{561}, 67^2 \equiv 1 \pmod{561},$

이산대수 (1/2)

- (이산대수) $\mathbb{G} =< g >$가 유한 순환군이라 하자. 기저 g에 대한 $y \in \mathbb{G}$에 대한 이산대수(discrete logarithm)는 $y = g^x$를 만족하는 정수 $x(1 \le x \le |\mathbb{G}|)$를 말하며, $\log_g y$로 표기함
  - 이산대수를 기저 g에 대한 $y \in \mathbb{G}$의 색인(index)이라고도 함
- 이산대수의 특징
  - 독특성. 색인이 x가 되는 $\mathbb{G}$의 원소는 유일함
- 법 세계에서 이산대수는 로그의 일반적 성질을 만족히지 않음
  - 예) $\mathbb{Z}_7^* =< 3 >, 3^1 = 3, 3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5, 3^6 = 1$
    - $\log_3 10 \equiv \log_3 3 \equiv 1 \pmod 7$
      - $\log_3 10 \equiv \log_3(2 \cdot 5) \not\equiv \log_3 2 + \log_3 5 \equiv 2 + 5 \equiv 0 \pmod 7$
    - $\log_3 4^2 \equiv \log_3 16 \equiv \log_3 2 \equiv 2 \pmod 7$
      - $\log_3 4^2 \not\equiv 2 \cdot \log_3 4 \equiv 2 \cdot 4 \equiv 8 \equiv 1 \pmod 7$

참고. 자연로그, 상용로그
$\ln x = \log_e x, e = 2.718 \ldots$
$\log x = \log_{10} x$

일반 로그와 이산 로그의 차이점.
일반 로그에서 $x > y$ 이면 $\log x > \log y$이지만
이산 로그에서는 이것이 성립하지 않음

이산대수 (2/2)

- $x \equiv y \pmod{\phi(n)} \rightarrow b^x \equiv b^y \pmod n$
- 즉, 지수들은 다른 법 세계에서 동작하기 때문에 일반 로그 성질을 적용할 때 신중해야 함
- $\log_3 10 \equiv \log_3(2 \cdot 5) \equiv \log_3(3^2 \cdot 3^5) \equiv \log_3 3^{2+5} \equiv \log_3 3^7 \equiv \log_3 3^1$
- (이산대수 문제) 유한 순환군 $\mathbb{G} =< g >$와 $y \in \mathbb{G}$가 주어졌을 때, $y = g^x$를 만족하는 정수 $x(1 \le x \le |\mathbb{G}|)$를 찾는 문제를 말함
  - 이 문제를 해결하는 다항시간 알고리즘은 아직 발견되지 않음
  - 이 문제를 해결하는 다항시간 알고리즘이 존재하지 않는다고 증명되어 있지 않음