Number Theoretic Algorithms

최대공약수와 $\mathbb{Z}_p$의 성질

March 20, 2019

1 시작

아무 것도 믿지 않고서는 아무 것도 할 수 없습니다.

우리는 일반적인 논리계를 믿습니다. 우리는 가장 기초적인 것들, 예를 들어 정수의 덧셈, 뺄셈, 곱셈이 가능하고 그 값이 정수라는 사실을 믿습니다. 우리는 정수의 덧셈, 뺄셈, 곱셈을 하는 방법을 알고 있습니다.

우리는 정수 a와 영이 아닌 정수 b가 존재하여

$$a = bq + r, \quad 0 \leq r < |b|$$

를 만족시키는 정수 q와 r이 유일하게 존재한다는 것을 믿습니다. 이 사실은 우리가 이야기를 시작할 수 있게 해 주는 가장 큰 원동력이 됩니다. 우리는 또한 q와 r을 빠르게 찾는 방법을 알고 있습니다.

수리논리학 과목과 대수학(추상대수) 과목을 들으면, 위 사실들을 증명하게 됩니다. 그때에는 기초적인 논리계조차 부정하여 무엇을 할 수 있는지 살펴봅니다. 이 스터디의 목적은 그것이 아니므로, 우리는 고등학교 때까지 배운 "수학"을 모두 믿기로 합니다.

2 최대공약수

모두 영인 것은 아닌 두 정수 a와 b에 대해 g가 a와 b를 모두 나누어떨어뜨릴 때, 그러한 g 중 가장 큰 것을 a와 b의 최대공약수라 하고, $\gcd(a, b)$로 씁니다.

a와 b에 대해 다음 소인수분해를 생각합니다:

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$$
$$b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$

이때 a_i 혹은 b_i들은 음이 아닌 정수이며, 0도 허용합니다. 그러면

$$\gcd(a, b) = p_1^{c_1} p_2^{c_2} \cdots p_n^{c_n} \qquad c_i := \min(a_i, b_i)$$

인 것이 잘 알려져 있습니다. 그러나 이 방법은 소인수분해를 필요로 하기 때문에, 시간이 상당히 많이 걸리는 방법입니다.

일반성을 잃지 않고 $a > b > 0$이라고 합시다. 그러면 $a = bq + r, \quad 0 \le r < b$인 정수 q와 r이 존재합니다. 이때 $\gcd(a, b) = \gcd(b, r)$인 것이 알려져 있습니다.

증명은 다음과 같이 합니다. $\gcd(a, b) =: g$, $\gcd(b, r) =: g'$이라 하면, r이 g로 나누어떨어짐을 보여 $g \le g'$을 보입니다. 또 a가 g'으로 나누어떨어짐을 보여 $g' \le g$를 보입니다. 따라서 $g = g'$입니다.

나눗셈을 이용해서 계산하면, 최대공약수를 구하는 데 시간이 얼마나 걸릴까요? 이것을 나눗셈 횟수를 통해 확인해 봅시다. b보다 큰 정수 a에 대해 $\gcd(a, b)$를 구하는 데 걸리는 최대 나눗셈 횟수를 T_b라 합니다. 가장 간단히 생각할 수 있는 것은, $r < b$이므로 $T_b \le 1 + \max_{0 \le i < b} T_i$입니다. 그러나 $r > b/2$일 때 다음 단계를 고려하면 $\gcd(b, r) = \gcd(r, b - r)$이 되고, $b - r < b/2$이므로

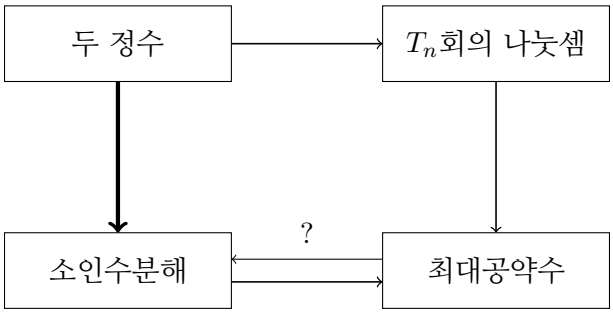
$$T_b \le \max\left(1 + \max_{0 \le i \le b/2} T_i, 2 + \max_{0 \le i < b/2} T_i\right) \le 2 + \max_{0 \le i \le b/2} T_i$$

입니다. 이제 수학적 귀납법 등을 사용하여

$$T_n \le 2 \log_2 n + 1 = \log_{\sqrt{2}} n + 1$$

를 증명할 수 있습니다.

우리가 지금 떠올려야 하는 diagram은 다음과 같습니다:



그럼 반대로 정수를 받았을 때, 어떤 정수를 잘 생성해서 최대공약수를 구하면 소인수분해 시간을 줄일 수 있지 않을까요?[1] 이를 위해서 빠른 나눗셈 방법이 필요합니다! 따라서, 큰 수의 가감승제, 소수 여부의 판단 및 소수의 분포를 구하는 방법과 더불어 소인수분해를 빠르게 하는 방법을 이 스터디의 앞부분에서 다루게 됩니다.

3 체

가감승제가 자유로운 집합을 체라 합니다.

가감승제라 함은 더하기, 빼기, 곱하기, 나누기를 일컫습니다. 자유롭다 함은 다음을 일컫습니다:

[1] 이런 식으로 사고하도록 연습하십시오!

- 더하기, 곱하기를 한 연산의 결과가 집합 안에 있습니다.
- 더하기끼리 혹은 곱하기끼리는 연산[2]이나 피연산자[3]의 순서에 상관없이 값이 같습니다.
- 더하기와 곱하기 사이에 분배 법칙이 성립합니다.
- 집합 내에 0과 1이 존재하며, 서로 다릅니다.[4]
- 어떤 수 a를 가져와도 $(-a)$와 a^{-1}가 집합 내에 존재합니다. 단 0^{-1}은 없고 이것은 예외로 합니다.

예를 들어, 유리수는 체입니다. 실수와 복소수도 체가 됩니다.

4 유한 체

어떤 체 F가 주어졌을 때, F의 원소의 개수 $|F|$가 1 이하일 수는 없습니다. 체의 정의에 따라 $0 \in F$, $1 \in F$이고 $0 \neq 1$이어야 하기 때문입니다.

체 F에는 0, 1의 두 원소가 주어지고, 반드시 다음 연산표를 만족해야 합니다.

$+$	0	1
0	0	1
1	1	x

$\times$	0	1
0	y	0
1	0	1

y는 $0 \cdot 0 = (0+0) \cdot 0 = 0 \cdot 0 + 0 \cdot 0$에 의해 반드시 0이어야 합니다. x가 1이라면, $1+1 = 0+1$, 즉 $0 = 1$이라고 주장하는 셈이기 때문에 안 됩니다. 그런데 만약 $x \neq 1$이면, 한번 $x = 0$으로 놓아 봅시다.

계산하면 할수록 $x = y = 0$으로 놓았을 때 체의 모든 성질이 만족되는 것 같습니다. 이 집합은 실제로 체가 되며, 이 체는 컴퓨터들이 뛰노는 체입니다. 이 체의 이름은 $\mathbb{Z}_2$입니다.

이제 x를 0과 1과 모두 다른 수로 생각하고, 연산표를 확장해서 2개보다 많은 수의 원소를 가지는 체를 만들어 봅시다.

$+$	0	1	x
0	0	1	x
1	1	x	y
x	x	y	z

$\times$	0	1	x
0	0	0	0
1	0	1	x
x	0	x	w

$0 \cdot x$가 0인 것은 위에서와 비슷한 이유입니다.

이번에 우리가 정해야 하는 것은 y, z, w의 세 변수입니다. 이 변수들을 0, 1 혹은 x로 두어 체의 모든 정의들을 만족하도록 시도해 봅시다! 이렇게 하여 원소의 개수가 3개인 체를 구성할 수 있습니다. 이 체의 이름은 $\mathbb{Z}_3$입니다.

[2] 결합 법칙.
[3] 교환 법칙.
[4] 0은 덧셈의 항등원, 1은 곱셈의 항등원이라는 특징이 있어야 합니다.

비슷한 방법으로 원소의 개수가 4개인 체, 즉 "$\mathbb{Z}_4$"를 만들 수 있습니까?[5] 못 만들 것은 없지만, 이제 y, z, w 중 어떤 것을 포함시킬까를 궁리해야 합니다. 또 채워야 하는 칸의 수도, 가능한 경우도 많아집니다. 따라서, 유한 체를 구성하는 일반적인 방법이 필요해 보입니다.

5 $\mathbb{Z}_p$

소수 p가 있을 때 p로 나눈 나머지에 덧셈과 곱셈의 연산 구조를 잘 준 체를 $\mathbb{Z}_p$라 합니다.

a와 b의 합은 $(a+b)$를 p로 나눈 나머지, a와 b의 곱은 ab를 p로 나눈 나머지로 주어집니다. 표기를 남용하여 이것을 그냥 $a+b$, ab로 사용합니다. 이제 교환 법칙, 결합 법칙, 분배 법칙 등은 거저 얻어집니다.

거저 얻어지지 않는 것은 a의 곱셈에 대한 역원인데, 이것은 영이 아닌 수 $a \in \mathbb{Z}_p$에 대해 $ab = np + 1$이 되는 정수 $b \in \mathbb{Z}_p$와 n이 반드시 존재한다는 것입니다. "증명"이 필요하게 되었습니다.

증명은 $p = 2$인 경우 자명하므로 $p > 2$라 합니다. 먼저 귀류법을 사용하여, 그런 b와 n이 존재하지 않는다고 합시다. 다음을 받아들입니다:

> 영이 아닌 $\mathbb{Z}_p$의 원소 b에 대해 ab를 p로 나눈 나머지는 0일 수 없습니다.

귀류법 가정에 의해 b가 0이 아닌 경우 ab를 p로 나눈 나머지가 1일 수도 없으므로, $b = 1, 2, \cdots, p-1$에 대해 ab의 나머지 $r = 2, 3, \cdots, p-1$이 가능합니다. 비둘기집 원리에 의해 서로 다른 b, b'에 대해 ab와 ab'의 나머지가 r로 같은 경우가 있고, 이를 다음

$$ab = np + r$$
$$ab' = n'p + r$$

과 같이 쓰고, 일반성을 잃지 않고 $b > b'$이라 하겠습니다. 그럼

$$a(b - b') = (n - n')p$$

가 되고, $b - b' \in \mathbb{Z}_p$이며 $b - b' \neq 0$이므로 맨 처음 받아들인 사실에 모순입니다.

우리는 이제 임의의 소수 p에 대해 그로부터 체 $\mathbb{Z}_p$를 얻을 수 있습니다. 사실, 우리가 이전에 고생해서 얻은 $\mathbb{Z}_3$는 여기서 얻은 $\mathbb{Z}_3$와 이름만 다를 뿐 동등하다는 것을 알 수 있습니다. 대수학에서는 이것을 isomorphic하다 혹은 up to isomorphic 같다고 합니다.

$\mathbb{Z}_p$는 그 수가 유한하고, 체를 구성하며, 직관적인 더하기 및 곱하기가 성립하기 때문에 수많은 아름다운 정리 및 알고리즘이 존재합니다. 이들은 이 스터디의 뒷부분에서 다루게 됩니다.

[5] 이렇게 해서 만들어진 원소 4개짜리 체를 우리는 $\mathbb{Z}_4$로 부르지 않습니다.

6 문제

1. $a > b > 0$인 두 정수 a, b에 대해 $a = bq + r$인 정수 q와 r이 존재하여 $0 \le r < b$를 만족할 때, $\gcd(a, b)$가 r을 나누고, $\gcd(b, r)$이 a를 나눔을 보이세요.

2. (a) 수학적 귀납법을 이용해서 $T_n \le 2\log_2 n + 1 = \log_{\sqrt{2}} n + 1$을 보이세요.

   (b) 일반적으로 $T_n \le \log_u n + \mathcal{O}(1)$이 성립하는 실수 u들을 생각할 때, $u = \sqrt{2}$는 tightest bound가 아닙니다. 우리의 결론이 $u = \sqrt{2}$로 지어진 데는

   $$\gcd(a, b) = \gcd(b, r) = \gcd(b, b - r)$$

   에서 나눗셈을 두 번 거쳤음에도 $b - r$이 b의 반이 되었다고 생각한 것에 있습니다. 이제, 경우를 잘 나누어, $b - r < b/u^2$이 되도록 하는 실수 $u > 1$의 범위를 구하세요.[6] 이 범위에서 u를 골라 $\sqrt{2}$보다 크게 할 수 있습니까?

   (c) (b)에서 구한 실수를 φ라 합시다. $T_n \le \log_\varphi n + 1$이 성립함을 보이고, 이 bound는 tight함을 보이세요. 즉 아무리 큰 N이 주어져도 $T_n = \lfloor \log_\varphi n + 1 \rfloor$를 만족하는 $n > N$이 존재함을 보이면 됩니다. (Hint: Fibonacci Sequence를 이용하세요.)

3. 이 문제가 흥미롭게 느껴지신다면 생각해 보세요. 아니면 건너뛰어도 좋습니다.

   (a) 체 F가 주어졌을 때, 0과 1은 유일합니까? 어떻게 증명할 수 있습니까?

   (b) 체 F와 체의 원소 a가 주어졌을 때, $(-a)$는 유일합니까? a가 0이 아니면 a^{-1}는 유일합니까? 어떻게 증명할 수 있습니까?

   (c) 0^{-1}가 없다는 조건을 제거해도, 0^{-1}가 없음을 증명할 수 있습니까?

4. (a) 원소의 개수가 23개인 체가 있음을 설명하세요.

   (b) 다음 연산표는 원소의 개수가 8개인 체를 표현합니다. 이 연산표가 정말로 체가 됨을 증명하세요. 결합/분배 법칙, 덧셈의 역원과 곱셈의 역원을 확인하면 됩니다.[7]

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

×	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

[6] 이때 실제로 b를 r로 나눈 나머지가 $b - r$이 됨도 확인해 보셔야 합니다!

[7] 교환 법칙 및 덧셈의 항등원과 곱셈의 항등원은 눈으로도 확인할 수 있어서 뺐습니다. 노가다를 하려면 $3 \cdot 8^3 + 2 \cdot 8^2 = 1664$가지를 전부 확인하셔야 합니다. 코딩을 통해 확인하세요.

(c) 원소의 개수가 6개인 체 F_6가 존재합니까? F_6를 구성하려고 노력해 보고, "존재하지 않을 것 같다"는 확신을 가지세요.

5. (a) 소수 p와 영이 아닌 $\mathbb{Z}_p$의 원소 a가 주어졌을 때, 다음을 증명하세요.

   영이 아닌 $\mathbb{Z}_p$의 원소 b에 대해 ab를 p로 나눈 나머지는 0이 아니다.

   (Hint: 소인수분해의 일의성을 이용하세요. b가 영이 아닌 것은 어디에서 쓰였습니까?)

   (b) p가 합성수이면, $\mathbb{Z}_p$의 곱셈에 대한 역원의 존재성 증명 어디에 문제가 있습니까? 문제가 되는 부분을 고친 명제를 증명하세요. 합성수 n에 대해서 "$\mathbb{Z}_n$"의 원소 중 몇 개가 곱셈에 대한 역원을 가집니까? 곱셈에 대한 역원을 가지는 원소들만 모은 대수적 구조를 $\mathbb{Z}_n^\times$로 씁니다.

6. 영이 아닌 $\mathbb{Z}_p$의 원소 a를 고정하고, $\mathbb{Z}_p$에서 함수 $f : \mathbb{Z}_p \to \mathbb{Z}_p$가 정의역의 모든 x에 대해 $f(x) = ax$를 만족한다 합시다.

   (a) f가 bijection임을 보이세요. 이를 위해서 $f(x) = f(y)$이면 $x = y$임을 보이고(injective), 임의의 $\mathbb{Z}_p$의 원소 y에 대해 $f(x) = y$를 만족하는 x가 있음을 보이면 됩니다(surjective).

   (b) (Fermat) 위 사실과 $f(0) = 0$에서부터 $a^{p-1} = 1$을 유도하세요. 따라서 임의의 영이 아닌 $\mathbb{Z}_p$의 원소 a에 대해, a의 $(p-1)$제곱을 p로 나눈 나머지는 1입니다. (Hint: $f(1), \cdots, f(p-1)$에는 1부터 $p-1$까지가 모두 한 번씩 나타나므로, 곱하면 $(p-1)!$과 같습니다.)

   (c) a^{-1}를 어떻게 빨리 계산할 수 있습니까?

7. 이 문제가 흥미롭게 느껴지신다면 생각해 보세요. 아니면 건너뛰어도 좋습니다.
   $a \in \mathbb{Z}_p$가 영이 아닐 때, 함수 $f(a, r)$을 "$\mathbb{Z}_p$에서 $ab = r$을 만족하는 b의 개수"로 정의합니다.

   (a) $\sum_{r=0}^{p-1} f(a, r) = p$임을 보이세요.

   (b) 3.(b)에 따라 $f(a, r) \leq 1$이어야 합니다. 이제 $f(a, 1) = 0$이라 놓고 모순을 이끌어내어, $f(a, 1) = 1$임을 보이세요. 따라서 a에 대해 역원 a^{-1}는 존재하고 유일합니다.

   (c) 이 증명은 왜 틀렸습니까?