3341.211 Number Theory

Wonseok Shin

2021/03/09

Last Compile : 2021/03/09 at 23:14:12

Contents

Number Theory	**[3341.211 Spring 2021]**
Lecture I: Divisibility	
March 2, 2021	
Lecturer: Jung Hee Cheon	Scribe : Wonseok Shin

HW) Niven 1.2 - 2, 13, 16, 24, 43, 49, 51

Divisibility

Definition 1.1 (Common Divisor). $a|b$ 이고 $a|c$ 이면 a 를 b, c의 공약수라고 정의한다. b와 c의 공약수 중 가장 큰 수를 $\gcd(b, c)$ 또는 (b, c) 라고 쓰고, 최대공약수라고 정의한다.

Theorem 1.2 (Extended Euclidean Algorithm). $g = (b, c)$ 에 대해, $^{\exists}x_0, y_0 \in \mathbb{Z}$, $g = bx_0 + cy_0$. 보다 정확하게, $g = \min \{ bx + cy > 0 \mid x, y \in \mathbb{Z} \}$.

Proof. $\min \{ bx + cy > 0 \mid x, y \in \mathbb{Z} \}$ 을 l 이라 하고, $b = lq + r$ 이라고 하자. 이때 l이 b를 나누지 않는다고 하자. 따라서, $0 < r < l$. 이때, $r = b - lq = b(1 - x_0 q) + c(-y_0 q)$ 이므로 r 또한 b, c의 선형결합이다. $r < l$ 이 모순이므로, l은 b를 나눈다. 같은 방법으로 $l|c$이다.
l이 b, c의 약수이므로 gcd를 g라 하면 $l \leq g$이다. 그러나, $g|(bx_0 + cy_0)$ 이므로, $g \leq l$ 이 되어 $l = g$. □

Problem. Show that $(a, m) = (b, m) = 1 \Rightarrow (ab, m) = 1$.

Lemma 1.3 (Euclid Lemma). $c|ab$, $(b, c) = 1$ 이면 $c|a$ 이다.

Algorithm 1.4 (Euclid Algorithm). a, b에 대해, 다음과 같은 수순을 반복한다.

- $a = bq_1 + r_1$
- $b = r_1 q_2 + r_2 \ldots$
- $r_{j-2} = r_{j-1} q_j + r_j$
- $r_{j-1} = r_j q_{j+1}$

이때, $(a, b) = (b, r_1) = \ldots (r_{j-1}, r_j) = r_j$

실제 선형결합 표현을 찾고자 한다면, 다음 표현을 사용한다. $r_0 = b, r_{-1} = a$ 처럼 생각하고,

$$\begin{pmatrix} r_{j-1} \\ r_j \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_j \end{pmatrix} \begin{pmatrix} r_{j_2} \\ r_{j_1} \end{pmatrix} = \cdots = \begin{pmatrix} 0 & 1 \\ 1 & -q_j \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{j-1} \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = M_j \begin{pmatrix} a \\ b \end{pmatrix}$$

- 이 알고리즘의 step 수를 $\lambda \leq \dfrac{\log b}{\log \phi} + 1$ 이라는 바운드를 잡을 수 있다.
- 실제 비트 연산의 횟수는 $O(\log a \log b)$ 정도이다.

Computational Cost

- Logic gate로 $ab \mod 2$와 $a+b \mod 2$를 계산하는 gate가 있다고 할 때 (AND, XOR), Full adder를 만들 수 있다. Full adder $FA(a,b,c) = (a+b+c \mod 2, \left\lfloor \frac{a+b+c}{2} \right\rfloor)$ 를 기준점으로 생각하자.
- 예를 들어, n 비트 수의 덧셈은 n 번의 FA 연산을 요구한다.
- 이때, n비트 수의 덧셈과 뺄셈은 Linear time, 곱셈과 나눗셈은 Quadratic time임을 어렵지 않게 알 수 있다. 특히 곱셈은 $O(\log a \log b)$, 나눗셈은 $O(\log b \log q)$ 시간.
- Euclidean algorithm의 경우, 나눗셈은 $j+1$번 해서 $O(\log^2 b \log q)$ 알고리즘일 것 같지만, 실제로는 나눗셈을 하는 수들의 비트가 계속 줄어들어서 $O(\log a \log b)$ 시간에 수행된다.
- $a^b \mod c$, 행렬곱셈 AB 등은 Cubic complexity.
- 인수분해 등은 Exponential (w.r.t, input bit size) complexity.

Number Theory	**[3341.211 Spring 2021]**

Lecture II: Primes / Binomial Coefficient

March 4, 2021

Lecturer: Jung Hee Cheon Scribe : Wonseok Shin

HW) Niven 1.3 - 16, 41, 42, 43, 44, 48, Euclid

Definition 2.1 (Prime). 정수 $p > 1$ 에 대해, $1 < d < p$ 인 약수 d가 존재하지 않으면 p 를 소수 (prime) 이라 한다. 소수가 아닌 수를 합성수 (composite) 라고 한다.

Theorem 2.2 (Fundamental theorem of arithmetic). 모든 $n > 1$ 인 정수는 소수의 곱으로 유일하게 표현된다. (w/ perhaps only one factor)

Proof. Existence 와 Uniqueness를 따로 나누어 본다.

- Existence : n이 소수이면 증명할 것이 없다. n이 합성수이면, 약수 d가 존재하고, n/d와 d를 표현하고 합칠 수 있다. 재귀적으로 이를 반복할 수 있다.
- Uniqueness : $n = \prod_i p_i^{e_i} = \prod_j q_j^{d_j}$ 라 하자. 이때 p_i와 q_j가 같음을 보이면 충분하다. q_j에 포함되지 않는 p_i가 존재한다고 하고, 이를 p라 하자. $p \mid \prod_i p_i^{e_i}$ 이므로 $p \mid \prod_j q_j^{d_j}$ 여야 하고, $p \mid ab$ 이고 p가 소수이면 $p \mid a$ 또는 $p \mid b$ 이므로 $p \mid q_j^{d_j}$ 인 q_j가 존재해야 한다. 그러나 서로 다른 소수인 p, q_j에 대해 이것이 성립하지 않으므로 모순.

$\square$

정수와 비슷한 성질을 갖는 집합 - 예를 들어, $a + b\sqrt{-6}, a, b \in \mathbb{Z}$ 들의 집합을 생각하자.

- 이 집합이 UFD(소인수분해가 유일한 공간) 인가?
- 이 위의 Norm을 $a^2 + 6b^2$ 처럼 생각하자. $N(a)N(b) = N(ab)$ 이게.
- Unit : $a+b\sqrt{-6}$ 에 대해, $c+d\sqrt{-6}$ 이 존재하여 $(a+b\sqrt{-6})(c+d\sqrt{-6}) = 1$ 이면 UNIT이라고 부른다. 여기서는 1과 -1이 unit임이 자명.
- Prime : 여기서 소수는, $p = (a + b\sqrt{-6})(c + d\sqrt{-6})$ 일 때 둘 중 하나가 반드시 unit이어야 하는 수 p 들을 소수라고 정의한다. 예를 들어, 여기서는 2와 5가 prime임을 안다.
- 첫 질문으로 돌아가서, UFD가 아님을 알 수 있다. $10 = 2 \cdot 5 = (2+\sqrt{-6})(2-\sqrt{-6})$ 이라서, 소인수분해가 유일하지 않으므로.

Note. 언제 $\mathbb{Z}[\sqrt{d}]$ 가 UFD인가? $d = -163, -67, -43, -19, -11, -7, -3, -2, -1\cdot$ ref : Heeger Numbers

Theorem 2.3 (Euclid). 소수의 개수는 무한하다.

Theorem 2.4 (Prime gap). There are arbitrarily large gap between primes.

Proof. Consider $(k+1)!+2$, $(k+1)!+3$, $\cdots$, $(k+1)!+(k+1)$. □

Note (Prime Number Theorem). $\pi(x)$ 를 x보다 작거나 같은 소수의 개수라고 하자. 이때, 소수의 비율은 어떻게 변화하는가? 즉, $\dfrac{\pi(x)}{x}$ 는 어떻게 변화하는가?
Gauss : $\dfrac{1}{\log x}$ 정도 비율. 증명 X
19C : $\displaystyle\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1$. 보다 정확히는, $\pi(x) = \dfrac{x}{\log x} + \mathcal{O}\left(\dfrac{x}{\log^2 x}\right)$. 또한, logarithmic integral $\mathrm{li}(x) = \displaystyle\int_0^x \frac{1}{\log t}\,\mathrm{dt}$ 가 $\dfrac{x}{\log x}$ 에 가까워서, 실제로는 $\mathrm{li}(x)$ 도 π의 approximation.

Conjecture (리만 가설).

$\pi(x)$와 $\mathrm{li}(x)$ 사이의 오차항이 생각보다 더 작다.

$$\left|\pi(x) - \int_0^x \frac{1}{\log t}\,\mathrm{dt}\right| < \frac{1}{8\pi}\sqrt{x}\log x$$

Definition 2.5 (이항 계수). 다음과 같이 이항계수를 정의한다.

$$\binom{\alpha}{k} = \frac{\alpha(\alpha-1)(\alpha-2)\cdots(\alpha-k+1)}{k!}$$

특히, α가 자연수일 때 팩토리얼을 이용하여,

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Theorem 2.6 (이항계수의 조합론적 정의).
n개의 원소 중 k개를 선택하는 경우의 수는 $\binom{n}{k}$ 이다.

Corollary 2.7. k개의 연속된 자연수의 곱은 $k!$의 배수이다.

Theorem 2.8 (Binomial Theorem). $n \geq 1, n \in \mathbb{Z}$에 대해, 다음이 성립한다.

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

Number Theory	**[3341.211 Spring 2021]**

Lecture III: Congruence

March 9, 2021

Lecturer: Jung Hee Cheon | Scribe : Wonseok Shin

HW : 20, 27, 36

Definition 3.1 (Congruence). $a, b, m \in \mathbb{Z}$, $m \neq 0$에 대해, $a \equiv b \mod m \iff m \mid (a-b)$.

이때, a를 m으로 나눈 나머지를 $[a]_m$으로 나타낸다.

Theorem 3.2 (Properties of congruence).

- 위 Congruence relation은 equivalence이다.
- 덧셈, 뺄셈, 곱셈은 잘 보존된다. 즉, $a \equiv b, c \equiv d$이면 $a+b \equiv c+d$이고, $ab \equiv cd$.
- $ac \equiv bc$이고, $(c, m) = 1$이면 $a \equiv b$.

  Proof. $m \mid (bc - ac)$, $(c, m) = 1$이면 유클리드 보조정리에 의해 $m \mid (b-a)$.

Corollary 3.3. 정수계수 다항식 f에 대해, $a \equiv b$ 이면 $f(a) \equiv f(b)$.

Definition 3.4 (Residue).

- y가 x의 $\mod m$에 대한 residue : $y \equiv x \mod m$
- $\{x_1, \ldots x_n\}$ complete residue system : 임의의 정수 y에 대해, $y \equiv x_i \mod m$인 x_i가 유일하게 존재

  Example. Complete residue system $\{0, 1, \ldots m-1\}$

- $\{\, a - km \mid k \in \mathbb{Z} \,\}$ 를 residue class(잉여류) 라고 부른다.
- m과 서로소인 수들의 residue system $\{x_1, \ldots x_{\phi(m)}\}$을 reduced residue system이라고 부른다. 즉, $x_i \neq x_j$, $(x_i, m) = 1$.
- 이때, m과 서로소이면서 m 이하인 자연수의 개수를 $\phi(m)$ 이라고 쓰고, 이를 Euler totient function 이라고 부른다.

Theorem 3.5 (페르마의 소정리). p가 소수일 때, $a^{p-1} \equiv 1 \mod p$이다.

Theorem 3.6 (오일러 정리 (페르마 소정리의 일반화)). $(a, m) = 1$ 일 때, $a^{\phi(m)} \equiv 1$ 이다.

Proof. RRS(Reduced residue system)의 성질을 이용한다.

- RRS $\{r_1, \ldots r_\phi(m)\}$ 에 대해, $\left\{ar_1, ar_2, \ldots ar_{\phi(m)}\right\}$ 이 RRS임을 쉽게 알 수 있다.
- 이때, $r_i = ar_j$인 j가 각 i에 대해 유일하게 존재한다. 이를 이용하여 reindexing하자.
- mod m의 세상에서, 자명하게 $\displaystyle\prod_{j=1}^{\phi(m)} ar_j = \prod_{i=1}^{\phi(m)} r_i$
- 따라서, $a^{\phi(m)} \equiv 1$.

Proposition 3.7 (합동선형방정식).

- $(a, m) = 1$ 이면, $^\exists x, ax \equiv 1 \mod m$. 특히, 이러한 x들은 반드시 mod m에서 같은 잉여류에 속한다.
- $(a, m) > 1$ 이면, 그러한 x가 존재하지 않는다.

Proof. Case를 나눠서 보이자.

- (a, m) 이 1이면, $^\exists x, y \in \mathbb{Z}$, $ax + my = 1$. 이때 $ax \equiv 1 \mod m$ 이다.
- $ax \equiv 1$ 인 x가 존재하면, $ax + my = 1$ 인 y가 존재하므로, $(a, m) = 1$ 이다.

Proposition 3.8. p가 소수일 때, $x^2 \equiv 1 \mod p$ if and only if $x \equiv \pm 1 \mod p$

Theorem 3.9 (윌슨의 정리). p가 소수일 때, $(p-1)! \equiv -1 \mod p$

Proof. 앞서의 정리에 의해, $1 < a < p - 1$ 인 a에 대해 $^{\exists!}\bar{a}$, $a\bar{a} \equiv 1 \mod p$. 이를 이용하여, p가 odd prime 인 경우에는 $(p-1)!$을 순서를 바꾸어 rearrange함으로써 $(p-1)! = 1 \times \left(\displaystyle\prod_{i=2}^{p-2} a\right) \times (p-1) \equiv -1 \mod p$.

Corollary 3.10. 소수 p에 대해 $x^2 \equiv -1 \mod p$ 는 $p = 2$ 또는 $p = 4k + 1$일 때 해를 갖는다.

Proof. $p = 2$일 때의 해는 $x = 1$로 자명하다. $p > 2$가 홀수 소수일 때, p는 $4k + 1$ 또는 $4k + 3$ 이다. 이때 $4k+3$의 경우 $\dfrac{p-1}{2}$가 홀수인데, $x^2 \equiv -1$ 이면 $(x^{p-1}) \equiv (x^2)^{\frac{p-1}{2}} \equiv -1$ 이므로 페르마의 소정리에 모순이다. $p = 4k+1$ 이면, 윌슨의 정리로부터 $-1 \equiv (p-1)! = \displaystyle\prod_{j=1}^{\frac{p-1}{2}} j(p-j)$. 이는 $(-1)^{\frac{p-1}{2}} \left(prod_{j=1}^{\frac{p-1}{2}} j\right)^2$ 이므로 주어진 정리가 성립한다.