ゼミレポート

Kiyoshi Ohashi, Syogo Osumi

2023 年 4 月 7 日

1　整数の基本性質

$\mathbb{Z}$ には和と積が定義でき, 結合法則・交換法則・分配法則が成り立つ. つまり $a, b, c \in \mathbb{Z}$ ならば

$(a+b)+c = a+(b+c), (ab)c = a(bc),$
$a+b = b+a, ab = ba,$
$a+0 = 0+a = a, a1 = 1a = a,$
$a(b+c) = ab+ac$

である.

$x \in \mathbb{N}$ は $x \in \mathbb{N}$ であるときに $x \geqq 0$ と定義する.
さらに正の整数を $x \geqq 0$ であって $x \neq 0$, 同様に負の整数を $x \leq 0$ であって $x \neq 0$ と定義する.
$x, y \in \mathbb{Z}, x-y > 0 (x-y \geqq 0)$ なら,$x > y (x \geqq y)$ と定義する.
$x, y \in \mathbb{Z}$ なら,$x > y, x = y, x < y$ のどれか一つが必ず成り立つ.$x \geqq y$ なら,
$max\{x, y\} = x, min\{x, y\} = y$ と定義する.
$x \leq y$ である場合も同様で,n が正の整数ならば,n 以下の正の整数の数は有限であることを認める.
整数の大小関係について以下が成り立つ.
$a, b, c \in \mathbb{Z}, c > 0$ なら $a > b \iff a+c > b+c \iff ac \neq bc$ が成り立つ.(1.3.1)
なお,$c < 0$ なら $ac < bc$ である. 特に $c \neq 0$ ならば,
$a \neq b \iff ac \neq bc$(1.3.2)

また $x \in \mathbb{R}$ に対して,

$$|x| = \begin{cases} x & x \geqq 0 \\ -x & x \leq 0 \end{cases} \tag{1}$$

と絶対値を定義する.n が正の整数なら,$|x| \leq n$ である整数の個数は $2n+1$ 個であり, 有限である.

公理として次の性質を述べる.

Axm. 1.3.3 *1* は最小の正の整数である

この公理を認めると,$n \in \mathbb{N}, n < m$ である最小の m が $n - m > 0$ より,$n - m = 1$ を満たす. よって n より大きい整数の中で最小のものは $n + 1$ とわかる。

Prop 1. 1.3.4　$a > 0$ を整数とするとき, 次の（*1*）〜（*3*）が成り立つ
(1)$b \in \mathbb{Z}$,$|b - a| < 1$ なら,$b = a$ である.
(2)$|b| < 1$ なら,$b = 0$ である.
(3)$b, b' \in \mathbb{Z}, 0 \leq b, b' \leq a$, なら,$|b - b'| < a$

Proof. (1)　$c = b - a$ とおく,$c \in \mathbb{Z}, |c| < 1$ である,$c > 0$ なら $0 < c < 1$ となり, この整数 c は正の 1 より小さい整数なので,**Axm1.3.3** に矛盾する.$c < 0$ ならば $-1 < c < 0$ なので $0 < -\mathrm{c} < 1$ となりこれも公理 1.3.3 に矛盾する. 従って $c = 0$, つまり $b = a$ である.
(2)　$|b| < 1$ で $b > 0$ なら $0 < b < 1$ となり、**Axm1.3.3** に矛盾, と（1）と同様に $b = 0$ が示される. また, この命題「$|b| < 1$ なら $b = 0$」の対偶をとると「$b \neq 0$ ならば $|b| \geqq 1$」も導かれる.
(3)　$b' \geqq 0$ と $b < a$ より $b - b' \leq b < a$, また,$b \geqq 0$ と $b' < a$ より $b - b' \geqq -b' > -a$ 従って $-a < b - b' < a$ となる. □

Axm. 1.3.5 アルキメデスの公理　$x > 0$ が実数なら,x 以下の正の整数の数は有限個である.

Axm1.3.5 を認めると, 正の実数 x に対して,x 以下の整数で最大のものが存在すると分かる. これを $[x]$ と書く.$[x]$ の定義より,$x < [x] + 1$ である.$y \in \mathbb{Z}$ で $x < y$ ならば,$[x] < y$ なので $[x] + 1 \leq y$ である. 逆に $[x] + 1 \leq y$ なら,$x < [x] + 1$ なので,,$x < [x] + 1 \leq y$ から $x < y$ である. よって $y = [x] + 1$ が $x < y$ である最小の整数である. 負の場合も x 以下の最大の整数が存在することがわかる. この $[x]$ をガウス記号と呼ぶ. $[x]$ の定義より,$[x] \leq x < [x] + 1$ である.$x > 0$ の場合と同様に $y = [x] + 1$ は $y > x$ である最小の整数である.

2　整数の合同

Def 1. 1.4.1 $a, b \in \mathbb{Z}$ とする.
(1)$a \neq 0$ であるとき,$b = an$ となる $n \in \mathbb{Z}$ があるなら,b を a の倍数,a を b の約数といい,$a|b$ と書く.b が a の倍数でないなら,$a \not| b$ と書く
(2)a, b の共通の約数を a, b の公約数と呼ぶ
(3)$a \neq 0$ かつ $b \neq 0$ であるとき,a, b の共通の倍数を a, b の公倍数という

Prop 2. 1.4.2 $a, b \in \mathbb{Z} \setminus \{0\}$ で $b|a$ ならば,$|b| \leq |a|$ である. よって a の約数の個数は有限である $a = bn$ となる $n \in \mathbb{N}$ がある.$a \neq 0$ なので,$n \neq 0$ である.$|n| > 0$ は整数なので,***Axm1.3.3*** より $|n| \geqq 1$ である, よって,$|a| = |b||n| \geqq |b|$ である

絶対値が 1 以下である整数は,$\pm 1, 0$ だけなので, 次の系を得る.

Cor 1. 1.4.3　1 の約数は ± 1 である

Cor 2. 1.4.4　p が素数なら $p \not| 1$

Proof. **Cor1.4.3** より,1 の約数は ± 1 のみなので,p が素数であれば,p は 1 の約数ではない, つまり 1 は p で割り切れない. □

Def 2. 1.4.5 $a,b \in \mathbb{Z}$ とする
(1)$a \neq 0$ または $b \neq 0$ であるとき,a,b の正の公約数の中で最大のものを最大公約数といい,$gcd(a,b)$ と書く,$gcd(a,b)=1$ ならば,a,b は互いに素であるという
(2)$a,b \neq 0$ なら,a,b の正の公倍数の中で最小のものを最小公倍数といい,$lcm(a,b)$ と書く

Prop1.4.2 より約数の個数は有限個であり, 従って a,b の公約数の個数も有限個である. これにより有限個の公約数の中に最大のものがあるので,**Dfn1.4.5**(1) は正当化される.(2) では,$|ab|$ は a,b の公倍数であり,$|ab|$ 以下の正の整数の個数は有限なので, その中に $|ab|$ の約数であって最小のものが存在する. よって Dfn1.4.5(2) も正当化される.

Prop 3. 1.4.7 *(1)* $a|b, b|c$ なら,$a|c$ である
(2) $m \neq 0$ なら,$a|b \iff am|bm$

Proof. (1) $a|b, b|c$ より,$b=an, c=bm$ となる $n,m \in \mathbb{Z}$ が存在する. 代入して,$c=anm$ よって $a|c$
(2) まず $a|b \implies am|bm$ を示す.
$a|b \implies b=an(n \in \mathbb{Z})$ この両辺に $m \neq 0$ をかけて $bm=anm$,$n \in \mathbb{Z}$ より $am|bm$ 次に $am|bm \implies a|b$ を示す.$am|bm \implies bm=amn(n \in \mathbb{Z})$ この両辺を $m \neq 0$ で割ると $b=an$ よって $a|b$
従って $m \neq 0$ なら,$a|b \iff am|bm$ □

数学的帰納法についての復習をしておこう. P_n を自然数 n に対し与えられた数学的主張とするとき, 次のような論法を数学的帰納法, または単に帰納法という.
数学的帰納法１　P_0 が正しく,P_n が正しいなら P_n+1 が正しいとき,P_n は全ての n に対して正しい.
また次のように使うこともある
数学的帰納法２　P_0 が正しく,「全ての $m<n$ に対し P_m が正しい」なら P_m が正しいとき,P_n は全ての n に対して正しい.

Prop 4. 1.4.8 $n>1$ が整数なら,n の約数で素数であるものがある

Proof. n が素数でなければ,$1<m<n$ を n の約数にもつ. ここで P_n を
P_n「$n>1$ が整数なら,n の約数で素数であるものがある」とする.P_2 は 2 が約数に素数 2 を持つので正しい. ここで $n>1$ を整数とし,「全ての $m<n$ に対し,P_m が正しい」と仮定する. このとき P_n が正しいことを示す.
仮定より全ての $m<n$ に対し P_m が正しい, つまり n より小さい整数 m は素数 p を約数にもつ. 今.m は n の約数としてとってきたので,**prop1.4.7**(1) から n も p を約数に持つ. □

Prop 5. $n>1$ が合成数ならば，$\sqrt{n}$ 以下の素数の約数を持つ

Proof. n が合成数と仮定すると，$^{\exists}l \in \mathbb{Z}$ s.t. $l \mid n$ である．ただし，$n>1$ の合成数より，$l \neq 1, n$．ここで，$m=n/l$ とおくと，$l, m \neq 1, n$，$n=lm$ である．(合成数の定義から $l>0$)．もし，$l, m > \sqrt{n}$ であるとき，$lm>n$ となり矛盾する．よって，$l \leq \sqrt{n}$ または $m \leq \sqrt{n}$ となるため，n は $\sqrt{n}$ 以下の約数 l を持つ.
Prop 1.4.8 より，l は素数の約数を持ち，それを p と置くと $p \mid l$ であり，**Prop 1.4.7** より，推移律から $p \mid n$ となる.
したがって，$p \leq l \leq \sqrt{n}$ であるから，n は $\sqrt{n}$ 以下の素数の約数を持つ. □

この命題の対偶を取れば，次のような表現となる

Prop 6. $\sqrt{n}$ 以下の素数の約数を持たないならば，n は素数である．

「割り切れる（割り算）」の概念を規定するのは **Prop 1.4.15** とまだ先であるが，その概念を用いて説明するならば，本命題が主張することは ある正の整数 n が与えられた時，$\sqrt{n}$ 以下の素数全てで n を割り切れない時，n が素数であることを主張する．すなわち，n が素数であることを調べる際に，n 回ではなく $\sqrt{n}$ 回のステップのみで充分であることを意味する．

また，次の補題についても確認しよう．

Lem 1. $m, n \in \mathbb{Z}$ のとき，$n \mid m,\ n \neq \pm 1 \implies n \nmid m+1$

Proof. 仮定より $^{\exists}a \in \mathbb{Z}$ s.t. $m = na$ である．もし，$n \mid m+1$ ならば，$^{\exists}b \in \mathbb{Z}$ s.t. $m+1 = nb$ であり，$1 = (m+1) - m = n(b-a)$ である．**Cor 1.4.3** より，$n = \pm 1$ であるが，これは矛盾 □

今回のゼミにおいて，個人的に疑問に思ったのは $n \mid m$ によって $n \neq \pm 1 \implies n \nmid m+1$ を束縛しているのではないか，という点である．この事については，束縛させても仮定に用いても，帰結されるものに変わりはない．むしろ，今回の場合には $n \mid m+1$ を仮定した際に，$n \nmid m$ または $n = \pm 1$ を考え，それぞれの命題変数の成立の可否をを調べることが，考察の手立てとなる．

Prop 7. 素数は無限個存在する

Proof. 素数が有限個存在すると仮定し，それを $p_1, p_2, ..., p_n$ とおく．$q = (p_1 p_2 \cdots p_n) + 1$ とすれば，**Prop 1.4.8** より，q は素数を約数にもつ．その素数の 1 つを p とおくと，$^{\exists}i \in \mathbb{Z}$, s.t. $0 \leq i \leq n, p = p_i, p \mid p_1 \cdots p_n$ である．一方，**Lem 1.4.10** より，$\gcd(p_1 \cdots p_n, q) = 1$ であるが，これはどの素数も約数に持たない事を意味するため矛盾する．よって，$p \neq p_1, ..., p_n$ より，素数が有限個と仮定したことが誤りである． □

次に，合同式について定義する．

Def 3. $m \in \mathbb{Z} \setminus \{0\}$ とする．$a, b \in \mathbb{Z}$ で，$m \mid a-b$ であるとき，$a \equiv b \pmod{m}$ とかき，a, b は m を法として合同であるという．

また，$\mathbb{Z}$ における割り算の概念についても確認する．割り算は次の命題によって正当化される．

Prop 8. $a, b \in \mathbb{Z}, b \neq 0$ ならば，$^{\exists!}q, r \in \mathbb{Z},\ s.t.\ a = bq + r, 0 \leq r < |b|$

Proof. 段階に分けて証明していく．
（存在すること）
(i) $a \geq 0, b > 0$ のとき
アルキメデスの公理より，$bq \leq a$ をみたす $q \in \mathbb{N}$ は有限個である．q をその中の最大値とする．$r = a - bq$ とおくと，$r \geq b$ のとき，$r - b \geq 0$ より，$a - b(q+1) = r - b \geq 0$ で，q が最大の値であることに反する．よって，$r < b$ であり，$a \geq bq$ より，$r \geq 0$ である．
(ii) a, b が必ずしも正でないとき
(i) より，$^{\exists}q, r \in \mathbb{Z}$ s.t. $|a| = |b|q + r, 0 \leq r < |b|$ である．このとき，絶対値を外した時に条件を満たす q, r が存在することを確認する．

1. $a \geq 0, b < 0$ のとき
   $a = -bq + r = b(-q) + r$ となり成立.
2. $a < 0, b > 0$ のとき
   $-a = bq + r \iff a = b(-q) - r$ となる．ここで，$r \neq 0$ のとき，$a = b(-q-1) + b - r$ であり，$0 \leq b - r < b$ となり成立．また，$r = 0$ のときも成立する．
3. $a < 0, b < 0$ のとき
   $-a = -bq + r \iff a = bq - r$ となる．ここで，$r \neq 0$ のとき，$a = b(q+1) - b - r = b(q+1) + |b| - r$ であり，$0 \leq b - r < |b|$ となり成立．また，$r = 0$ のときも成立する．

（一意的であること）
$a = bq + r = bq' + r', q, q', r, r' \in \mathbb{Z}, 0 \leq r, r' < |b|$ とおくと，$b(q - q') = r' - r$ である．また，**Prop 1.3.4(3)** より，$|r' - r| < |b|$ であるが，$|b(q - q')| \geq |b|$ より矛盾. □

この命題において，q, r を求めることを**割り算**といい，q, r をそれぞれ**商**と**余り**という．
次に，高校で学習した合同式と余りの関係性についても確認しよう．

Prop 9. $a, b \in \mathbb{Z}, m \in \mathbb{Z} \setminus \{0\}$ とするとき，$a \equiv b \pmod{m} \iff a, b$ を m で割ったときの余りが等しい

Proof. ($\Longleftarrow$) は自明.
($\Longrightarrow$)
$a \equiv b \pmod{m} \iff m \mid a - b$ である．a, b の m による割り算の結果を $a = mq + r, b = mq' + r'$ とすると，$a - b = m(q - q') + r - r' = mc$ となる $c \in \mathbb{Z}$ が存在する．よって，$r - r' = m(c + q' - q)$ となる．$r - r' \neq 0$ ならば，$c + q' - q \neq 0$ であり，$|m(c + q' - q)| \geq |m|$ となるが，$|r - r'| < |m|$ であることに矛盾．よって，$r = r'$ □

また，合同式について次の性質が成立する．証明は容易であるため省略する．

Prop 10. 次の諸性質が成立する．

1. $a, a', b, b' \in \mathbb{Z}, m \in \mathbb{Z} \setminus \{0\}$ とするとき，$a \equiv a', b \equiv b' \pmod{m}$ なら，
$$a + b \equiv a' + b', ab \equiv a'b' \pmod{m}$$
2. $a, a', b, b' \in \mathbb{Z}, m, n \in \mathbb{Z} \setminus \{0\}, n \mid m$ とするとき，
$$a \equiv b \pmod{m} \implies a \equiv b \pmod{n}$$
3. $a, a', b, b' \in \mathbb{Z}, m, n \in \mathbb{Z} \setminus \{0\}$ とするとき，
$$a \equiv b \pmod{m} \implies am \equiv bm \pmod{nm}$$

Cor 3. $m \in \mathbb{Z} \setminus \{0\}, a, b, x, y \in \mathbb{Z}$ とするとき，$a, b \equiv 0 \pmod{m}$ なら，$ax + by \equiv 0 \pmod{m}$ である．したがって，a, b が m で割り切れるなら，$ax + by$ も m で割り切れる．

少し脇道に逸れるが，高校までに学習した倍数の判定法と l **進法**について確認する．

Def 4. **整数** $x > 0$ **の** l **進法による表記**とは，$0 \leq a_0, ..., a_n < l$ として，$x = a_0 + a_1 l + ... + a_n l^n$ と表すことである．ここで，a_i のことを l^i **の位の数**と呼ぶ.

ここで，l 進法による表記の一意性について確認する．次のように，x が l 進法について二つの表記で書けたとする．

$$x = \sum_{i=0}^{n} a_i l^i = \sum_{i=0}^{m} b_i l^i$$

$N = max\{n, m\}$ とおくと，$(a_0 - b_0) + (a_1 - b_1)l + ... + (a_N - b_N)l^N = 0$ が成り立つ．ここで，l を法とする合同式を考えると，$a_0 - b_0 \equiv 0 \pmod{l} \iff a_0 \equiv b_0 \pmod{l}$ となる．$0 \leq a_i, b_i < l$ であるため，$a = b$ を満たす．これを N 回繰り返すことで，x の l 進法における表記の一意性が確かめられる．

次に，$l = 10$ における有名な命題を紹介する．

Prop 11. *1.* 正の整数が $2, 5$ で割り切れること $\iff$ 正の整数の 1 の位の数がそれぞれ $2, 5$ で割り切れること

2. 正の整数が $3, 9$ で割り切れること $\iff$ 正の整数の各位の数の総和がそれぞれ $3, 9$ で割り切れること

Proof. 1. $x \in \mathbb{N}$ を 10 進法で表すと，$x = a_0 + 10a_1 + ... + 10^n a_n = a_0 + 10(a_1 + ... + 10^{n-1}a_n)$ となる．よって，$x - a_0 = 10(a_1 + ... + 10^{n-1}a_n) \iff x \equiv a_0 \pmod{10}$ である．また，**Prop 1.4.18(2)** より，$2, 5 \mid 10$ なので，$x \equiv a_0 \pmod{2}, x \equiv a_0 \pmod{5}$

2. $x = a_0 + 10a_1 + ... + 10^n a_n = a_0 + a_1 + ... + a_n + (10 - 1)a_1 + ... + (10^n - 1)a_n$ である．ここで，$10^i - 1 \equiv 0 \pmod{9}$ より，$x \equiv a_n = a_0 + a_1 + ... + a_n \pmod{9}$ である．**Prop 1.4.18(2)** より，$3 \mid 9$ なので，$x \equiv a_n = a_0 + a_1 + ... + a_n \pmod{3}$

□

また，高校で学習したように，合同式は剰余の計算において有効的である．特に高い冪の余りの計算について，ここでは確認しよう．

Ex 1. 16^4 を 13 で割ったときの余り

$16 \equiv 3 \pmod{13}$ を用いて，$16 \equiv 3 \pmod{13} \implies 16^2 \equiv 3^2 \pmod{13} \implies 16^4 \equiv 3^4 \equiv 81 \equiv 3 \pmod{13}$ よって，余りは 3 である．

16^4 程度であれば，手計算でも行える範疇であるが，合同式は次のような手計算では行えない大きな数の冪に対して有効である．

Ex 2. 16^{100} を 23 で割ったときの余り

$100 = 2^6 + 2^5 + 2^2$ と 2 進法で表すと，$16^{100} = 16^{2^6+2^5+2^2} = 16^{2^6} \cdot 16^{2^5} \cdot 16^{2^2}$ となる．ここで，

$16^{2^6}, 16^{2^5}, 16^{2^2}$ の余りについて考えていくとよい．具体的には

$$\begin{aligned}
16^2 &\equiv 3 \pmod{23} \\
16^4 &\equiv 9 \pmod{23} \\
16^8 &\equiv 12 \pmod{23} \\
16^{16} &\equiv 6 \pmod{23} \\
16^{32} &\equiv 13 \pmod{23} \\
16^{64} &\equiv 8 \pmod{23} \\
16^{64} \cdot 16^{32} &\equiv 12 \pmod{23} \\
16^{64} \cdot 16^{32} \cdot 16^4 &\equiv 16 \pmod{23}
\end{aligned} \tag{2}$$

となるので，求める余りは 16 である．一般に，整数 n を 2 進法で表すと，桁数は $[\log_2 n] + 1$ である．なぜなら，2 進法における桁数を N とおくと，$2^{N-1} \leq n < 2^N$ である．よって，$N - 1 \leq \log_2 n < N$ より，$N = [\log_2 n] + 1$ となる．従って，$a^n \mod b$ を求める時には，n の桁数からおよそ $\log_2 n$ 回の計算が必要となる．それらを最大 $\log_2 n$ 回掛けるので，計算の回数はおよそ $2\log_2 n$ 回となる．