

ゼミレポート

Kiyoshi Ohashi, Syogo Osumi

2023 年 4 月 7 日

Prop 1. $n > 1$ 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。 \square

この命題の対偶を取れば、次のような表現となる

Prop 2. \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 \square

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調べるのが、考察の手立てとなる。

Prop 3. 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, \dots, 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、 $p \neq p_1, \dots, p_n$ より、素数が有限個と仮定したことが誤りである． \square

次に、合同式について定義する．

Def 1. $m \in \mathbb{Z} \setminus \{0\}$ 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 4. $a, b \in \mathbb{Z}, b \neq 0$ ならば、 $\exists! q, r \in \mathbb{Z}, \text{ s.t. } a = bq + r, 0 \leq r < |b|$

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、 $r \geq 0$ 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、 $\exists q, r \in \mathbb{Z} \text{ s.t. } |a| = |b|q + r, 0 \leq r < |b|$ 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

$$a = -bq + r = b(-q) + r \text{ となり成立.}$$

2. $a < 0, b > 0$ のとき

$$-a = bq + r \iff a = b(-q) - r \text{ となる. ここで、} r \neq 0 \text{ のとき、} a = b(-q-1) + b - r \text{ であり、} \\ 0 \leq b - r < b \text{ となり成立. また、} r = 0 \text{ のときも成立する.}$$

3. $a < 0, b < 0$ のとき

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

(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． \square

この命題において、 q, r を求めることを割り算といい、 q 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 5. $a, b \in \mathbb{Z}, m \in \mathbb{Z} \setminus \{0\}$ 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. (\Leftarrow) は自明．

(\Rightarrow)

$a \equiv b \pmod{m} \iff m \mid a - b$ 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、 $r = r'$ \square

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 6. 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 1. $m \in \mathbb{Z} \setminus \{0\}, a, b, x, y \in \mathbb{Z}$ 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 2. 整数 $x > 0$ の l 進法による表記とは, $0 \leq a_0, \dots, a_n < l$ として, $x = a_0 + a_1l + \dots + a_nl^n$ 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, $(a_0 - b_0) + (a_1 - b_1)l + \dots + (a_N - b_N)l^N = 0$ 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 7. 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, $x = a_0 + 10a_1 + \dots + 10^n a_n = a_0 + 10(a_1 + \dots + 10^{n-1}a_n)$ となる．

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

□

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

$$\begin{aligned} 16^2 &\equiv 3 \pmod{23} \\ 16^4 &\equiv 9 \pmod{23} \\ 16^8 &\equiv 12 \pmod{23} \\ 16^{16} &\equiv 6 \pmod{23} \\ 16^{32} &\equiv 13 \pmod{23} \\ 16^{64} &\equiv 8 \pmod{23} \\ 16^{64} \cdot 16^{32} &\equiv 12 \pmod{23} \\ 16^{64} \cdot 16^{32} \cdot 16^4 &\equiv 16 \pmod{23} \end{aligned} \tag{1}$$

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 $\lceil \log_2 n \rceil + 1$ 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, $N = \lceil \log_2 n \rceil + 1$ となる. 従って, $a^n \pmod{b}$ を求める時には, n の桁数からおおよそ $\log_2 n$ 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, 計算の回数はおおよそ $2 \log_2 n$ 回となる.