今までの主なレポート課題の例 (12/19 配布)

問 1. 授業の 1 回目に紹介した「思い浮かべた 3 桁の数を 2 つ並べて 6 桁の数を作り、それが 7 で割れれば $\cdots$」という小遊びの別バージョンを作れ。(数学的に別なものでも、別の演出でも良い。)

問 2. 中国の数学書「孫子算経」や日本の江戸時代の数学書である吉田光由「塵劫記」に、現在では「中国式剰余定理 (Chinese Remainder Theorem)」と呼ばれる定理に相当する問題とその解法が掲載されている。これを調べ、その解法を現代の数学の言葉で説明せよ。

問 3. 2 整数 $a, b \in \boldsymbol{Z}$ に対し、その最大公約数 $d := \gcd(a, b)$ を求める Euclid の互除法、および、それと同時に $ax + by = d$ となる整数 $x, y \in \boldsymbol{Z}$ を求める拡張互除法についてまとめると共に、何らかの計算機言語 (表ソフトのマクロなどでも良い) で実装せよ。

問 4. 合同式の理論は、次のように "剰余類のなす世界" $\boldsymbol{Z}/m\boldsymbol{Z}$ を構成することによって、明快に論ずることが出来る。1 以上の整数 m を一つ取って固定し、整数全体の集合 Z 上の関係 $\sim$ を次で定める :

$$a \sim b \overset{\text{def}}{\Longleftrightarrow} \exists t \in \boldsymbol{Z} : a - b = tm.$$

(1) $\sim$ が $\boldsymbol{Z}$ 上の同値関係であることを示せ。$a \in \boldsymbol{Z}$ の属する同値類 (剰余類とも言う) を $\overline{a}$ と書こう。$\overline{a}$ は具体的にはどのような集合か。この関係 $\sim$ による商集合を $\boldsymbol{Z}/m\boldsymbol{Z}$ と書く。
(2) $\boldsymbol{Z}/m\boldsymbol{Z}$ の加法を $\overline{a} + \overline{b} := \overline{a + b}$ で定めると well-defined であることを示せ。
(3) $\boldsymbol{Z}/m\boldsymbol{Z}$ の乗法を $\overline{a} \cdot \overline{b} := \overline{a \cdot b}$ で定めると well-defined であることを示せ。
(4) $\boldsymbol{Z}/m\boldsymbol{Z}$ の加法・乗法に関する結合律・可換律・分配律を示せ。

問 5. 大きな素数を探す候補として、しばしば次のような数が考察される。自然数 n に対し、$F_n := 2^{2^n} + 1$ を **Fermat 数**と呼ぶ。

(1) 自然数 m が奇数ならば、多項式 $X^m + 1$ は整数係数の範囲で既約でない (因数分解される) ことを示せ。
(2) 自然数 m に対し、$2^m + 1$ が素数ならば、$m = 2^n$ の形 (即ち $2^m + 1 = 2^{2^n} + 1$ が Fermat 数) であることを示せ。
(3) $n \leq 4$ のときは F_n は素数であるが、F_5 は素数でない。
(4) 異なる n に対する Fermat 数は、どの 2 つも互いに素であることを示せ。
(5) F_n の素数判定・素因数分解の研究や計算の現状について調べよ。

問 6. 素数 p に対し、$M_p := 2^p - 1$ を **Mersenne 数**と呼ぶ。

(1) 自然数 m に対し、多項式 $X^m - 1$ は $X - 1$ で割り切れることを示せ。
(2) 自然数 m に対し、$2^m - 1$ が素数ならば、m が素数 (即ち $2^m - 1$ が Fermat 数) であることを示せ。
(3) 小さい素数 p については M_p が素数であることも多いが、M_p が素数でないこともある。両方の例を挙げよ。
(4) M_p の素数判定・素因数分解の研究や計算の現状について調べよ。

問 7. 集合 X と写像 $s : X \to X$ と X の元 $0 \in X$ の組 $(X, s, 0)$ が **Peano の公理系**を満たすとは次が成り立つことである :

(1) $\forall n \in X : s(n) \neq 0$
(2) s : 単射 (即ち、$s(n) = s(m) \Rightarrow n = m$)
(3) (数学的帰納法の原理) X の部分集合 $S \subset X$ について、
 (a) $0 \in S$
 (b) $\forall k \in S : s(k) \in S$
 ならば $S = X$

2 つの組 $(X_1, s_1, 0_1), (X_2, s_2, 0_2)$ が共に Peano の公理系を満たすとき、全単射 $f : X_1 \to X_2$ で、$f(0_1) = 0_2$ かつ $f \circ s_1 = s_2 \circ f$ となるものがただ一つ存在することを示せ。

以下では、Peano の公理系を満たす組 $\boldsymbol{N} = (\boldsymbol{N}, s, 0)$ を一つ固定して、自然数の集合とする。$s(n) = n'$ と書き、また必要ならば通常のように $0' = 1, 1' = 2, \ldots$ と書く。

問 8. $\boldsymbol{N}$ の加法を帰納的に次で定義するとき、以下を示せ。

$$n+0:=n, \qquad n+m':=(n+m)'$$

(1) 結合律 : $(a+b)+c=a+(b+c)$
(2) 可換律 : $a+b=b+a$
(3) 消約律 : $a+c=b+c \Longrightarrow a=b$

問 9. $\boldsymbol{N}$ の乗法を帰納的に次で定義するとき、以下を示せ。

$$n\cdot 0:=0, \qquad n\cdot m':=n\cdot m+n$$

(1) 結合律 : $(a\cdot b)\cdot c=a\cdot(b\cdot c)$
(2) 可換律 : $a\cdot b=b\cdot a$
(3) 分配律 : $(a+b)\cdot c=a\cdot c+b\cdot c, a\cdot(b+c)=a\cdot b+a\cdot c$
(4) 消約律 : $a\cdot c=b\cdot c \Longrightarrow a=b$

問 10. $n\in\boldsymbol{N}$ に対し、切片 $S(n)\subset\boldsymbol{N}$ を帰納的に次で定義する :

$$S(0):=\{0\}, \qquad S(n'):=S(n)\cup\{n'\}$$

これを用いて、$\boldsymbol{N}$ の大小関係 $\leq$ を次で定義するとき、以下を示せ。

$$n\leq m \overset{\leftarrow}{\Longleftrightarrow} n\in S(m)$$

(1) $a\leq b \Longleftrightarrow a'\leq b'$
(2) 反射律 : $a\leq a$
(3) 反対称律 : $a\leq b, b\leq a \Longrightarrow a=b$
(4) 推移律 : $a\leq b, b\leq c \Longrightarrow a\leq c$
(5) 全順序性 (比較可能性) : $a\leq b$ または $b\leq a$
(6) $a\leq b \Longleftrightarrow \exists c\in\boldsymbol{N}: a+c=b$

問 11. 自然数の集合 $\boldsymbol{N}$ から 整数の集合 $\boldsymbol{Z}$ を次で構成する。

(1) $X:=\boldsymbol{N}\times\boldsymbol{N}$ に関係 $\sim$ を次で定義すると、同値関係である :

$$(a_1,b_1)\sim(a_2,b_2) \overset{\leftarrow}{\Longleftrightarrow} a_1+b_2=b_1+a_2$$

$\boldsymbol{Z}:=X/\sim$ とし、$(a_1,b_1)\in X$ の同値類を $[a_1,b_1]\in\boldsymbol{Z}$ と書く。
(2) $[a_1,b_1]+[a_2,b_2]:=[a_1+a_2,b_1+b_2]$ により well-defined に $\boldsymbol{Z}$ の加法が定まる。しかるべき性質を示せ。
(3) $\boldsymbol{Z}$ の乗法をしかるべく定義し、しかるべき性質を示せ。
(4) $\boldsymbol{Z}$ の大小関係をしかるべく定義し、しかるべき性質を示せ。

問 12. 整数の集合 $\boldsymbol{Z}$ から 有理数の集合 $\boldsymbol{Q}$ の構成、加法・乗法・大小関係の定義、しかるべき性質の証明など、一連のことを行なえ。

問 13. Newton-Raphson 法により、$n=2,3,\ldots$ などについて、

(1) $\sqrt{n}$ の近似値を小数第 8 位くらいまで求めよ。
(2) $k=3,4,\ldots$ などについて、$\sqrt[k]{n}$ の近似値を小数第 8 位くらいまで求めよ。

(必要なら電卓・表ソフトなどを用いよ。長い桁数が扱えないなら、小数第 6 位くらいまででもよろしい。プログラミングの心得がある人は、プログラムと実行結果を提出しても良い。計算の途中経過も適宜表示させること。)

問 14. 有理数の集合 $\boldsymbol{Q}$ から実数の集合 $\boldsymbol{R}$ を構成する方法として、講義では Cauchy 列を用いた方法を紹介したが、他にも Dedekind の切断を用いる方法もある。この方法について調べて述べよ。

レポート提出について

- 締切 : **2012 年 2 月 6 日 (月)20 時頃**まで
- 内容 : 配布プリントのレポート課題の例のような内容、及び授業に関連する内容で、授業内容の理解または発展的な取組みをアピールできるようなもの
- 分量 : プリントのレポート課題を全部提出する必要はなく、問題の重さによって適宜判断して数問取り組めば良い。内容に関しては、このプリントの例に必ずしも拘らず、意欲的な取組みを望む。