今までの主なレポート課題の例 (12/15 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よ。また、(心得のある人は) 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 $\boldsymbol{Z}$ 上の関係 $\sim$ を次で定める :

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

(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。
(5) $\overline{a} \in \boldsymbol{Z}/m\boldsymbol{Z}$ に対し、乗法に関する逆元 ($\overline{a} \cdot \overline{x} = \overline{1}$ となる元) が存在する条件は ?

問 5. (Fermat の小定理) p を素数とする。p と互いに素な整数 a に対し、

$$a^{p-1} \equiv 1 \pmod{p} \qquad (a^p \equiv a \pmod{p} \text{ と言っても同じ})$$

が成り立つ。これを次の 2 つの方法で示せ。

(1) (加法的方法) 二項定理により $(a+b)^p \equiv a^p + b^p \pmod{p}$ を示し、帰納法を用いる。
(2) (乗法的方法) $x = 1, \ldots, p-1$ に対して、$ax \bmod p$ が全て異なり 1 回づつ現れることから、$(p-1)!$ を 2 通りに計算して比較する。

問 6. 秘密分散の数理技術において、授業で紹介した 2 人が協力すれば秘密を復元できる方法についてまとめると共に、$k > 2$ に対し、 k 人が協力すれば秘密を復元できる方法を構成せよ。

問 7. (本問は Mathematica などの計算代数ソフトウェアを用いると良い。)
$N = 1316383$, $e = 3617$ とし、自分の学生番号の先頭のアルファベットを除いた 7 桁の数字で出来る自然数を P とする。

(1) N を法、e を暗号化鍵 (公開鍵) として、RSA 暗号で P を暗号化し、暗号文 C を求めよ。
(2) N を素因数分解して、これから復号鍵 (秘密鍵) d を求めよ。
(3) 求めた復号鍵 d を用いて、暗号文 C から平文 P を復元せよ。

問 8. 暗号・符号など、数理が利用されている実用技術について調べて述べよ。

問 9. 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 10. 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 11. D を平方数でない正整数とする。

(1) 色々な D に対し、$\sqrt{D}$ の (正則) 連分数展開 (の循環節) を求めよ。
(2) $D = n^2 + 1, n^2 + 2$ ($n \in \boldsymbol{N}$) の場合には規則性が見られる。それを観察して予想を立て (出来れば証明せ) よ。
(3) 他にも規則性の見られる場合があるか。観察・予想・証明せよ。
(4) 循環節が特に長くなるような D を見付けよ。

問 12. 前問の状況で、$\sqrt{D}$ の連分数展開を途中で打切って得られる分数 ($\sqrt{D}$ の近似分数という) を p/q とする。

(1) $\sqrt{D} \fallingdotseq p/q$ であるので、$p^2 - Dq^2$ は小さい整数になると考えられる。各 D に対し、幾つかの近似分数 p/q について $p^2 - Dq^2$ を計算せよ。何か規則性はないか。
(2) 特に $p^2 - Dq^2 = \pm 1$ となる p, q を見付けることが出来るか。

問 13. 方程式の代数解法 (係数から四則演算と冪根とを有限回用いて解を表す公式) の探求について、数学的・歴史的なことを含めて調べて述べよ。

問 14. n 次多項式 $f(X) = X^n + a_1 X^{n-1} + \cdots + a_{n-1} X + a_n$ に対し、その根を (重複度を込めて) $w_1, \ldots, w_n$ とする。根の差積の平方

$$D(f) := \prod_{1 \le i < j \le n} (w_i - w_j)^2$$

を f の**判別式 (discriminant)** という。

(1) 根 $w_1, \ldots, w_n$ を用いた f の因数分解を考えることにより、n 次多項式の根と係数の関係を求めよ。特に 3 次多項式 $f(X) = X^3 + pX + q$ の場合はどうなるか。
(2) 判別式 $D(f)$ は根の対称式であるので、基本対称式で表して根と係数の関係を用いることにより、f の係数で表せる。$f(X) = X^3 + pX + q$ の場合に $D(f)$ を具体的に p, q で表せ。
(3) Fontana-Cardano の公式の 3 乗根の中に現れる平方根の中身と $D(f)$ とを比べよ。

問 15. 上問の結果より、実数を係数とする 3 次方程式が 3 つの実数解を持つとき、その解の公式には負数の平方根が必ず現れる。これを「不還元の場合 (Casus Irreducibilis)」と呼び、これが歴史上で複素数 (虚数) を扱った (扱わざるを得なかった) 最初と言われている。このことを含めて、複素数に関して数学的・歴史的なことを含めて調べて述べよ。

問 16. 4 次多項式 $f(X) = X^4 + pX^2 + qX + r$ の根を $w_1, \ldots, w_4$ とし、

$$t_1 := w_1 w_4 + w_2 w_3, \qquad t_2 := w_1 w_3 + w_2 w_4, \qquad t_3 := w_1 w_2 + w_3 w_4$$

とおく。

(1) t_1, t_2, t_3 を根とする 3 次多項式 $g(T)$ を作り、その係数を f の係数 p, q, r で表せ。
(2) Ferrari の解法で現れる f の 3 次分解式と、上の $g(T)$ とを比べよ。

レポート提出について

- 締切：**2016 年 2 月 1 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。
- 年明けに今後の分のレポート課題の例を配布する予定。