代数入門
まとめのレポート問題　その1

(中野 伸)

問題提示：2021 年 7 月 23 日 10:00

提出〆切：2021 年 7 月 26 日 15:00

注意: 数値を求める問題についても，結果に至る考え方を書くこと

[1]　自然数 n に対して

$$A(n) = 4^n - 3^n, \qquad B(n) = 4^n + 3^n$$

とおくとき，以下の問いに答えよ．

(1)　すべての自然数 n に対して，$A(n)$ と $B(n)$ は互いに素であることを示せ．

(2)　$A(n)$ が素数ならば，n は素数であることを証明せよ．

(3)　$B(724)$ を 175 で割った余りを求めよ．

(4)　$A(10)$ の最小の素因数を p とし，最大の素因数を q とするとき，平方剰余記号 $\left(\dfrac{p}{q}\right)$ を計算せよ．

代数入門
まとめのレポート問題　その2

(中野 伸)

問題提示：2021 年 7 月 23 日 10:00

提出〆切：2021 年 7 月 26 日 15:00

注意: 数値を求める問題についても，結果に至る考え方を書くこと

[2]　以下の問いに答えよ．

(1)　連立合同式

$$\begin{cases} 5x - 2 \equiv 33 \pmod{63} \\ 3x + 7 \equiv 53 \pmod{67} \end{cases}$$

をみたす最小の自然数 x を求めよ．

(2)　連立合同式

$$\begin{cases} 5x - 2y + 3z \equiv 13 \pmod{17} \\ 3x + 7y - 10z \equiv 0 \pmod{17} \\ 2x - y + 8z \equiv -5 \pmod{17} \end{cases}$$

をみたす整数の組 x, y, z を求めよ．ただし，$|x|$, $|y|$, $|z| \leq 8$ とする．

(3)　2 次合同式

$$3x^2 + 5x + 7 \equiv 0 \pmod{127}$$

が整数解を持つかどうか判定せよ．

(4)　法 2021 に関する零因子 n で，$900 < n < 1000$ をみたすものをすべて求めよ．

代数入門
まとめのレポート問題　その3

(中野 伸)

問題提示：2021 年 7 月 23 日 10:00

提出〆切：2021 年 7 月 26 日 15:00

注意: 数値を求める問題についても，結果に至る考え方を書くこと

[3]　$N = 2425481$ は異なる 2 つの素数の積である．愛し合う太郎さんと花子さんは，これを用いて RSA 暗号システムを構築しメッセージ交換をしていた．以下のストーリーに沿って，N を素因数分解し，$\varphi(N)$ と d の値を求めよ．

(A) 最初に示した $N = 2425481$ は，花子さんが異なる素数 p, q を選んで $N = pq$ として定めた数です．p と q は秘密ですが，$N = 2425481$ は秘密にしなくてもＯＫです．

(B) 花子さんは，N のオイラー関数の値 $\varphi(N)$ を計算し，それと互いに素な e を選んで，公開鍵 (N, e) を太郎さんに伝えました．

(C) ところが，花子さんは飲み友達である伸さんに，N の素因数のひとつ 1217 をうっかり教えてしまいました．

(D) ずる賢い伸さんは，N を素因数分解し，$\varphi(N)$ の値を計算しました．

(E) 実際には，花子さんは $e = 1357$ を選んでいたのですが，それを知った伸さんは，秘密鍵 d も見つけてしまいました．あぁ〜，伸さんはなんて悪いやつなんでしょう．