

基礎数学 A 定期試験解答例

1. 1, 2, 3, 6, 7, 14, 21, 42. □

本文はサービス問題です. all or nothing で採点しました. 過不足があるもの, および問題文の指示に従っていないもの(小さい順から並べていないもの) はすべて 0 点としました.

2. (1) 3, (2) 37. □

(1) はサービス問題で, ユークリッドの互除法を用いるまでもなかったと思います. (2) はユークリッドの互除法を用いる問題です.

$$1591 = 1073 \times 1 + 518, \quad 1073 = 518 \times 2 + 37, \quad 518 = 37 \times 14$$

ですので, 求める最大公約数は 37 ということになります. 計算回数あまり膨れ上がらないように問題を作成しました.

3. (1) 存在しない, (2) $(x, y) = (80, -25)$. □

(1) 全ての整数の組 (x, y) に対し $8x + 2y$ は 2 で割れるが, 右辺の 3 は 2 で割れないことに注意します. すると, (1) の答えは「存在しない」となります.

(2) ユークリッドの互除法を活用します. 割り算を繰り返して,

$$51 = 16 \times 3 + 3, \tag{1}$$

$$16 = 3 \times 5 + 1, \tag{2}$$

$$3 = 1 \times 3.$$

となります. 式 (2) の 3×5 を左辺に移項して,

$$1 = 16 - 3 \times 5 \tag{3}$$

を得ます. 次に式 (1) の 16×3 を左辺に移項して $3 = 51 - 16 \times 3$. これを式 (3) に代入して,

$$\begin{aligned} 1 &= 16 - (51 - 16 \times 3) \times 5 \\ &= 16 - 51 \times 5 + 16 \times 3 \times 5 \\ &= 16 \times (1 + 3 \times 5) + 51 \times (-5) \\ &= 16 \times 16 + 51 \times (-5) \end{aligned} \tag{4}$$

を得ます. 求めたかったのは $16x + 51y = 5$ の整数解だったので, 式 (4) の辺々を 5 倍して,

$$16 \times 80 + 51 \times (-25) = 5$$

を得ます. つまり, $16x + 51y = 5$ の整数解の一つとして $(x, y) = (80, -25)$ を得ます.

4. (1) 4, (2) 66. □

(1) はフェルマーの小定理を活用する問題でした. フェルマーの小定理は, 素数 p と $\gcd(a, p) = 1$ なる a に対し,

$$a^{p-1} \equiv 1 \pmod{p}$$

を主張するものでした. 今, 67 は素数, $\gcd(2, 67) = 1$ ですので, フェルマーの小定理から,

$$2^{66} \equiv 1 \pmod{67} \tag{5}$$

が成り立ちます. あとは $200 = 66 \times 3 + 2$ に注意すれば, 指数法則と式 (5) から,

$$2^{200} = 2^{66 \times 3 + 2} = 2^{66 \times 3} \times 2^2 = (2^{66})^3 \times 2^2 \equiv 1^3 \times 4 = 4 \pmod{67}$$

となります.

(2) はウィルソンの定理を活用する問題でした. ウィルソンの定理は, 素数 p に対し,

$$(p-1)! \equiv -1 \pmod{p}$$

を主張するものでした. 67 は素数ですので, ウィルソンの定理から,

$$66! \equiv -1 \pmod{67}$$

を得ます. $-1 \equiv -1 + 67 = 66 \pmod{67}$ ですので,¹ 答えは 66 となります.

(2) の答えとして -1 としたものがありません. しかし, 問題文は「0, 1, ..., 65, 66 から選べ」となっていて, 選択肢に -1 はありません. 答えを -1 としたものは残念ながら 0 点です.

5. 93. □

まず, a の末尾二桁を求めることは, $a \equiv a' \pmod{100}$ となる高々 2 桁の非負整数 a' を求めることと同等であることに注意します. だから, 93^{2013} を法 100 で計算したい, ということになります. ヒントにあるとおり, 小さい n に対し 93^n を法 100 で計算してみると,²

$$\begin{aligned} 93^2 &\equiv (-7)^2 = 49 \pmod{100}, \\ 93^3 &\equiv (-7)^3 = -343 \equiv -343 + 400 = 57 \pmod{100}, \\ 93^4 &\equiv (-7)^4 = 49^2 = 2401 \equiv 1 \pmod{100} \end{aligned} \tag{6}$$

となります. 合同式 (6) に気づくことができれば, あとは問題 4(1) と同じ要領で,

$$93^{2013} = 93^{4 \times 503 + 1} = (93^4)^{503} \times 93 \equiv 1^{503} \times 93 = 93 \pmod{100}$$

となり, 答えは 93 であることが分かります.

¹一般に, 正の整数 m と整数 a, k に対し, $a \equiv a + mk \pmod{m}$ が成り立ちます. これは合同式の定義を思い出してみると当たり前です.

² $93 \equiv -7 \pmod{100}$ に気づくと計算はより楽になります. 下ではこの合同式を用いて計算しています.

注意 (発展). フェルマーの小定理は法 p が素数の場合のみ使える合同式でした. 実は, フェルマーの小定理を拡張したオイラーの定理というものがあり, オイラーの定理は法が合成数の場合でも使うことができます. ここでオイラーの定理を簡単に説明したいと思います.

まず, 一つ記号を準備します. 正の整数 m に対し,

$$\varphi(m) = (1 \text{ 以上 } m \text{ 以下で, } m \text{ と互いに素な整数全体の個数})$$

とおき, これをオイラーの φ 関数と言います. 例えば, $\varphi(6)$ を求めてみることを考えてみます. 1以上6以下で, 6と互いに素な整数は1, 5の2つですので, $\varphi(6) = 2$ となります. 次に, p が素数のとき $\varphi(p)$ の値を考えてみましょう. 1以上 p 以下で, p と互いに素な整数は $1, 2, \dots, p-1$ の $(p-1)$ 個ですので, $\varphi(p) = p-1$ となります.

上の記号の下, オイラーの定理は, 正の整数 m と $\gcd(a, m) = 1$ となる整数 a に対し,

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

を主張するものです. $m = p$ (素数) の場合, $\varphi(p) = p-1$ でしたので, この場合, オイラーの定理は $a^{p-1} \equiv 1 \pmod{p}$ となり, フェルマーの小定理と一致することが分かります. つまり, オイラーの定理はフェルマーの小定理を含む主張になっているのです.

さて, 定期試験の問題に戻ってみて, オイラーの定理の $m = 100$ の場合を考えてみます. これは, $\gcd(a, 100) = 1$ となる整数 a に対し,

$$a^{\varphi(100)} \equiv 1 \pmod{100} \tag{7}$$

を主張しています. $\varphi(100)$ を計算するには, 1以上100以下で100と互いに素でない整数の総数を求めればよく,

$$\varphi(100) = 100 - 50 - 20 + 10 = 40$$

となります.³ つまり, オイラーの定理の $m = 100$ の場合, 即ち合同式 (7) は,

$$a^{40} \equiv 1 \pmod{100} \quad (a \text{ は } \gcd(a, 100) = 1 \text{ なる整数}) \tag{8}$$

ということになります. 実は, 合同式 (8) よりも強く,

$$a^{20} \equiv 1 \pmod{100} \quad (a \text{ は } \gcd(a, 100) = 1 \text{ なる整数}) \tag{9}$$

を証明することができます. ただし, これを示すには代数学 (群論および環論) と呼ばれる分野の知識が必要になります.

³100 と互いに素でない数は, 2 の倍数または 5 の倍数です. 上式の 50 は 1 以上 100 以下で 2 の倍数の総数, 上式の 20 は 1 以上 100 以下で 5 の倍数の総数, 上式の 10 は 1 以上 100 以下で 2 の倍数かつ 5 の倍数 (= 10 の倍数) の総数を表しています.

合同式 (8) または合同式 (9) を用いると, $\gcd(a, 100) = 1$ なる整数 a に対し,

$$a^{2013} = a^{40 \times 50 + 13} \equiv a^{13} \pmod{100}$$

となることが分かります. $a = 93$ の場合は合同式 (9) よりも強く, 合同式 (6) が分かったので, 比較的楽に 93^{2013} の末尾 2 桁を計算できたわけです.

オイラーの定理に興味のある人は, 教科書の 9 章をご覧ください.

6. n に関する数学的帰納法により,

$$\sum_{j=1}^n j^3 = \left(\frac{n(n+1)}{2} \right)^2 \quad (10)$$

を証明する.

$n = 1$ のとき,

$$(\text{左辺}) = \sum_{j=1}^1 j^3 = 1^3 = 1, \quad (\text{右辺}) = \left(\frac{1(1+1)}{2} \right)^2 = 1^2 = 1$$

となり, 等式 (10) が成立する.

k を正の整数とし, $n = k$ の場合, 等式 (10) が成立すると仮定する. つまり,

$$\sum_{j=1}^k j^3 = \left(\frac{k(k+1)}{2} \right)^2 \quad (11)$$

が成り立つと 仮定する. このとき, $n = k + 1$ のとき等式 (10), つまり,

$$\sum_{j=1}^{k+1} j^3 = \left(\frac{(k+1)\{(k+1)+1\}}{2} \right)^2 \quad (12)$$

が成り立つことを 証明したい. \sum 記号の意味を考えると, 式 (12) の左辺は,

$$\sum_{j=1}^{k+1} j^3 = \sum_{j=1}^k j^3 + (k+1)^3$$

と変形できる. これに数学的帰納法の仮定 (11) を代入して,

$$\begin{aligned} \sum_{j=1}^{k+1} j^3 &= \left(\frac{k(k+1)}{2} \right)^2 + (k+1)^3 = \frac{k^2(k+1)^2 + 4(k+1)^3}{4} \\ &= \frac{(k+1)^2\{k^2 + 4(k+1)\}}{4} = \frac{(k+1)^2(k^2 + 4k + 4)}{4} \\ &= \frac{(k+1)^2(k+2)^2}{4} = \left(\frac{(k+1)\{(k+1)+1\}}{2} \right)^2. \end{aligned} \quad (13)$$

つまり, 等式 (12) が成り立つ. よって, 示したい等式 (10) について, $n = k$ のとき等式 (11) が成り立つと仮定すると, $n = k + 1$ のとき等式 (12) が成り立つことが分かった.

以上より, 数学的帰納法からすべての正整数 n に対し, 等式 (10) が成り立つ. \square

本問は, $n = 1$ の場合をチェックしていて 3 点, 数学的帰納法の仮定である等式 (11) を用いている場所を明らかにして 6 点, 式 (13) の計算部分に 6 点, という基準で採点しました. 次に該当するものは減点しました.

- 数学的帰納法の仮定の式, 示したい式, 論理的に正しい式が明確に区別されていない答案. 上の解答例の下線を引いている部分のように, 何が仮定で何を示したいのか, きちんと区別しないと証明していることにはなりません. 例えば, 式 (11) と式 (12) を羅列して書いていて, 上の解答例の下線部分のような説明がないものは大幅に減点しました.
- 式 (13) の計算の方針が見えない答案. 等式 (12) を示したいことは分かっているので,

$$\sum_{j=1}^{k+1} j^3 = \left(\frac{k(k+1)}{2} \right)^2 + (k+1)^3 = \frac{(k+1)^2(k+2)^2}{4}$$

などを書いてあると, 必要な計算をしていないと疑わざるを得ません. 計算していることをきちんとアピールするようにしましょう.

7. 背理法で証明する. 即ち, 素数が有限個しかないとし矛盾を示す. p_1, \dots, p_n を素数全体とし,

$$N = p_1 \times \dots \times p_n + 1$$

を考える. N を素因数分解したときに現れる素数の一つを p とする. このとき, N は p で割り切れる.

一方, p_1, \dots, p_n が素数全体だったので, p は p_1, \dots, p_n のいずれかと一致する. そこで $p = p_j$ とすると, $N \div p_j$ の余りは 1 なので, N は $p_j (= p)$ で割り切れない.

下線部は相反する. つまり, 素数は無数に存在することが分かった. □

素数が有限個しかないと仮定すると, 素数すべての積を整数 (または自然数) の中で考えることができ矛盾が起こる, というのが基本的な考え方でした. 上ぐらいの答案が書けていれば正解です. 勿論, 授業プリントのように, N を割る素数の存在について議論する以下のような解答でも正解です.

より詳しい解答例. 背理法で証明する. 即ち, 素数が有限個しかないとし矛盾を示す. p_1, \dots, p_n を素数全体とし,

$$N = p_1 \times \dots \times p_n + 1$$

を考える. N は p_1, \dots, p_n のいずれよりも真に大きいので, N は合成数である. よって, N の 1, N 以外の正の約数が存在する. その中で最小のものを p とする.

p が素数であることを背理法で証明するため, p が合成数と仮定する. このとき, $k \mid p$ かつ $k \neq 1, p$ なる正の整数 k が存在する. $k \mid p, p \mid N$ なので, $k \mid N$ が成り立つ. $k \neq p$ なので $k < p$. これは p が N を割る 1, p 以外の正整数であることに反する. よって, p は素数である. 以上より, p は素数で $p \mid N$ を満たすことが分かった.

一方, p_1, \dots, p_n が素数全体だったので, p は p_1, \dots, p_n のいずれかと一致する. そこで $p = p_j$ とすると, $N \div p_j$ の余りは 1 なので, N は $p_j (= p)$ で割り切れない.

下線部は相反する. つまり, 素数は無数に存在することが分かった. □

エラトステネスの篩は, 与えられた数以下の有限個の自然数の中から素数をすべて拾い出す方法です. それだけでは素数が無数にあることの説明になっていません.

上の解答例以外で正しいと判断できる答案はありませんでしたが, 素数が無数にあることの証明は他にもいくつか知られています. 興味のある人は教科書の 4-3 節をご覧ください.

平均点, 成績

この試験の平均点は下の通りとなりました (小数点第 3 桁四捨五入).⁴

	1	2	3	4	5	6	7	合計
平均点	9.34	19.15	18.77	17.18	5.23	9.96	0.61	80.24
配点	10	20	20	20	10	15	15	110

また, 最高点は 108 点 (2 名), 6 名の方が 100 点以上の点数をとりました.

試験前に説明したとおり, 以下の要領で成績をつけることにします.

- 裏面の学生番号, 氏名に記入漏れのあった人は 5 点減点する.
- 100 点以上の方は, 100 点を成績とする.
- 60 点以上 100 点未満の方は, 試験の点数を成績とする.
- 60 点未満の方は, 定期試験の点数に $5 \times (\text{出席票を出した回数})$ を加える. これで 60 点以上になった人は 60 点を成績とする. 60 点未満だった人は定期試験の点数と出席点の合計を成績とする.
- 定期試験未受験の方は, 0 点を成績とする.

⁴定期試験の点数そのものの統計です. つまり, 100 点を超えている人や 60 点未満の人, 解答用紙裏面の氏名等に記入漏れのある人について, 点数を調整・減点する前のもので集計しています. また, 未受験者は統計に加えていません.