2015 年度後期 基礎数学 B 定期試験　略解

1. (1) 13,　(2) 53.

2. (1) 存在しない,　(2) $(x, y) = (-7, -3)$ など.

3. 1.

4. (1) 25,　(2) 20.

5. $x = -43$ など.
(考え方) $x \equiv 1 \pmod{11}$ を満たす整数 x は,

$$x = 11k + 1, \tag{1}$$

ただし $k \in \mathbb{Z}$, を満たす. さらに $x \equiv 3 \pmod{23}$ も満たすので, $11k + 1 \equiv 3 \pmod{23}$. よって, $(11k + 1) - 3 = 11k - 2$ は 23 で割り切れる. つまり,

$$11k - 2 = 23l, \tag{2}$$

ただし $l \in \mathbb{Z}$, を満たす. ユークリッドの互除法もしくは目算で一次不定方程式 (2) の整数解の一つを探すと, 例えば $(k, l) = (-4, -2)$ が見つかる. これを (1) に代入して, $x = -43$ を得る.

一次不定方程式 (2) の解は $(k, l) = (-4, -2)$ 以外にもある. よって, **5** には他にも解があり $x = 210$, $x = -296$ なども正解である.

本問題は, **中国剰余定理** (もしくは**孫子剰余定理**) と呼ばれる定理を参考に, 一次不定方程式の知識だけで解けるようにして出題しました. 興味のある人は, 参考書で調べてみてください.

6. 背理法で証明する. つまり, $x^3 = 4$ を満たす有理数 x が存在したとして矛盾を導く. $x^3 = 4$ を満たす有理数 x を $x = \frac{m}{n}(m, n$ は整数で $n > 0)$ と書く. 必要なら, $\frac{m}{n}$ を約分した後, 改めて m と n を取り直すことで, m と n は互いに素 となるように選ぶことができる. $x = \frac{m}{n}$ を $x^3 = 4$ に代入して,

$$\left(\frac{m}{n}\right)^3 = 4, \quad \text{即ち}, \quad m^3 = 4n^3. \tag{3}$$

右辺は偶数より, m^3 も偶数. そのためには m も偶数でなくてはいけない. よって, $m = 2k(k$ は整数) と書ける. これを式 (3) に代入して,

$$(2k)^3 = 4n^3, \quad \text{即ち}, \quad 2k^3 = n^3.$$

左辺は偶数より, n^3 も偶数となる. そのためには n が偶数でなくてはいけない. よって, $n = 2l$(l は整数) と書ける.

以上より, m と n は公約数 2 を持つ. しかし, これは下線を引いた「m と n は互いに素」に矛盾する.

よって, $x^3 = 4$ を満たす有理数 x は存在しない.

注意. 式 (3) から, m^3 が 4 で割り切れることが分かります. しかし, この事実から「m が 4 で割り切れる」とするのは誤りです. 例えば, $m = 2$ のとき, $m^3 = 8$ は 4 で割り切れますが, $m = 2$ は 4 で割り切れません. 一般に, m を整数, k を正整数, p を素数とするとき,

$$m^k \text{が } p \text{ で割り切れるならば, } m \text{ は } p \text{ で割り切れる} \tag{4}$$

が成り立ちます. しかし, 「p を素数とするとき」という仮定を外すと主張 (4) は一般に正しくなくなります.

7. (1) $b - a$ が m で割り切れるとき, $a \equiv b \pmod{m}$ と書く.

(2) n に関する帰納法により $a^n \equiv b^n \pmod{m}$ が成り立つことを示す.

$n = 1$ のとき, 仮定 $a \equiv b \pmod{m}$ から $a^n \equiv b^n \pmod{m}$ は正しい.

k を正整数とし, $n = k$ のとき示すべき合同式が正しい, 即ち, $a^k \equiv b^k \pmod{m}$ が成り立つと仮定する. 問題の仮定 $a \equiv b \pmod{m}$ と帰納法の仮定から,

$$b - a = mL, \qquad b^k - a^k = mM \tag{5}$$

を満たす整数 L, M が存在する. $n = k + 1$ のときを考えると,

$$\begin{aligned} b^{k+1} - a^{k+1} &= b^{k+1} - ab^k + ab^k - a^{k+1} \\ &= b^k(b - a) + a(b^k - a^k). \end{aligned}$$

これに式 (5) を代入して,

$$b^{k+1} - a^{k+1} = b^k mL + amM = m(b^k L + aM).$$

a, b, M, L は整数だから $b^k L + aM$ も整数である. よって, $b^{k+1} - a^{k+1}$ は m で割り切れる. 即ち, $a^{k+1} \equiv b^{k+1} \pmod{m}$ が成り立つ. 以上より, $n = k$ のとき示すべき合同式が正しいと仮定すると, $n = k + 1$ のときも示すべき合同式が正しいことが分かった.

以上より, 数学的帰納法から, すべての正整数 n に対し, $a^n \equiv b^n \pmod{m}$ が成り立つことが分かった.

上はあくまで解答の一例です. 満点はつけられませんが, 下のような解答も考えられます.

(別解) 次の事実を認めて証明する.

事実. $A \equiv B \pmod{m}$ かつ $C \equiv D \pmod{m}$ ならば $AC \equiv BD \pmod{m}$.

n に関する帰納法で証明する. $n = 1$ の時は仮定から示すべき合同式は正しい. k を正整数とし, $n = k$ のとき示すべき合同式が正しい, 即ち,

$$a^k \equiv b^k \pmod{m} \tag{6}$$

が成り立つと仮定する. 問題の仮定と帰納法の仮定 (6) から, 事実で $A = a$, $B = b$, $C = a^k$, $D = b^k$ と取ると事実の仮定 (前提条件) を満たす. よって, 事実より

$$a \times a^k \equiv b \times b^k \pmod{m},$$

即ち $a^{k+1} \equiv b^{k+1} \pmod{m}$ が成り立つ. 故に, $n = k$ の場合示すべき合同式が正しいと仮定すると, $n = k + 1$ のときも示すべき合同式は正しい.

以上より, 数学的帰納法から, すべての正整数 n に対し, $a^n \equiv b^n \pmod{m}$ が成り立つことが分かった.

上のように, 問題にある主張はどのような事実から従うものなのか, ということをはっきりさせて証明した場合, 8 点以上の点数をつけたいと思います. 勿論, 上述の事実にも証明がついている場合, 満点にします. 一方, 別解と類似の証明でも, どのような事実を用いているのかが明確でない場合, さらに減点する予定です.