

『離散構造』 期末試験 解答例

問 1

(a)

P: $A \Rightarrow (\neg B)$.

Q: $(\neg B) \Rightarrow ((\neg C) \wedge (\neg D))$.

または、

Q: $(\neg B) \Rightarrow (\neg(C \vee D))$.

R: $(\neg D) \Rightarrow (\neg A)$.

(b) 真理値表は次のとおり。

A	B	C	D	$\neg B$	$\neg C$	$(\neg B) \Rightarrow (\neg C)$	$\neg D$	P	$C \vee D$	$\neg(C \vee D)$	Q	$\neg A$	R	$P \wedge Q$	$(P \wedge Q) \wedge R$
T	T	T	T	F	F	T	F	F	T	F	T	F	T	F	F
T	T	T	F	F	F	T	F	F	T	F	T	F	F	F	F
T	T	F	T	F	T	T	T	F	T	F	T	F	T	F	F
T	T	F	F	F	T	T	T	F	F	T	T	F	F	F	F
T	F	T	T	T	F	F	F	T	T	F	F	F	T	F	F
T	F	T	F	T	F	F	T	T	T	F	F	F	F	F	F
T	F	F	T	T	T	T	F	T	T	F	F	F	T	F	F
T	F	F	F	T	T	T	T	T	F	T	T	F	F	T	F
F	T	T	T	F	F	T	F	T	T	F	T	T	T	T	T
F	T	T	F	F	F	T	T	T	T	F	T	T	T	T	T
F	T	F	T	F	T	T	F	T	T	F	T	T	T	T	T
F	T	F	F	F	T	T	T	T	F	T	T	T	T	T	T
F	F	T	T	T	F	F	F	T	T	F	F	T	T	F	F
F	F	T	F	T	F	F	T	T	T	F	F	T	T	F	F
F	F	F	T	T	T	T	F	T	T	F	F	T	T	F	F
F	F	F	F	T	T	T	T	T	F	T	T	T	T	T	T

(c) $(P \wedge Q) \wedge R$ の真理値表を見ると、 $(P \wedge Q) \wedge R$ が真のとき、 A は常に偽である。いいかえれば、このとき $\neg A$ は常に真である。したがって、 $((P \wedge Q) \wedge R) \Rightarrow (\neg A)$ は、恒真式である。

(もちろん、 $((P \wedge Q) \wedge R) \Rightarrow (\neg A)$ の真理値表を直接書いて、確かめてもよい。)

問 2

(a)

$$h(2) = f(12, 8, 2) = f(4, 8, 1) = f(4, 4, 0) = 8$$

$$h(3) = f(12, 8, 3) = f(4, 8, 2) = f(4, 4, 1) = f(0, 4, 0) = 4$$

$$h(4) = f(12, 8, 4) = f(4, 8, 3) = f(4, 4, 2) = f(0, 4, 1) = f(0, 4, 0) = 4$$

(b)

関数 h は単射でない。なぜなら、(たとえば) $h(3) = h(4)$ となるから。

関数 h は全射でない。なぜなら、 $k \geq 3$ となる任意の k に対して、 $h(k) = f(0, 4, k-3) = f(0, 4, 0) = 4$ となるので、 $h(\mathcal{N}) = \{20, 12, 8, 4\}$ であり、これは $\mathcal{N}$ と一致しないから。(注: 「 $h(x) = 1$ となる x はないから」といった理由でもよい。)

(c) [本問の解答としてはごく簡単に理由を書けばよく、以下のように詳細に書く必要はないが解答例であるので、念のため、きちんと書いておく。]

$\gcd(x, y)$ は x の約数かつ y の約数なので、 $x = a \cdot \gcd(x, y)$ かつ $y = b \cdot \gcd(x, y)$ となる $a, b \in \mathcal{N}$ が存在する。 $x + y = (a + b) \cdot \gcd(x, y)$ となるので、 $\gcd(x, y)$ は $x + y$ の約数である。

また、 $x > y$ のとき、 $p = \gcd(x - y, y)$ 、 $q = \gcd(x, y)$ とおくと、ある c, d に対して、 $x - y = pc$ かつ $y = pd$ であり、また、ある e, f に対して、 $x = qe$ かつ $y = qf$ である。

そこで、 $x = p(c + d)$ なので、 p は x と y の約数となり、 $p \leq \gcd(x, y) = q$ である。(x と y の両方の約数となっている数のうち最大のものが $\gcd(x, y)$ なので p はそれ以下である。)

また、 $x - y = q(e - f)$ なので、 q は $x - y$ と y の約数となり、 $q \leq \gcd(x - y, y) = p$ である。

以上から $p = q$ である。

(d) 性質「 $\gcd(x, y)$ は $f(x, y, k)$ を割り切る。」を k に関する帰納法で証明する。(注: 厳密には、性質「すべての $x, y \in \mathcal{N}$ に対して、 $\gcd(x, y)$ は $f(x, y, k)$ を割り切る。」を k に関する帰納法で証明しているのである。)

(帰納法の基礎) $k = 0$ のとき、 $f(x, y, k) = x + y$ なので、上記小問 (c) により、 $\gcd(x, y)$ はこれを割り切る。

(帰納法のステップ) 次に、 $k > 0$ に対して上記性質が成立すると仮定する。 $x > y$ かどうかで場合分けする。

(ケース 1: $x > y$ のとき)

$f(x, y, k+1) = f(x-y, y, k)$ である。また、上記小問 (c) により、 $\gcd(x, y) = \gcd(x-y, y)$ である。さらに、帰納法の仮定により、 $\gcd(x-y, y)$ は $f(x-y, y, k)$ を割り切るので、これらをあわせると、 $\gcd(x, y)$ は $f(x, y, k+1)$ を割り切る。

(ケース 2: $x \leq y$ のとき)

$f(x, y, k+1) = f(x, y-x, k)$ である。上記小問 (c) と同様にして、 $\gcd(x, y) = \gcd(y-x, y)$ であることがわかる。帰納法の仮定により、 $\gcd(x, y-x)$ は $f(x, y-x, k)$ を割り切るので、これらをあわせると、 $\gcd(x, y)$ は $f(x, y, k+1)$ を割り切る。

以上より、帰納法を使うと、すべての $k \in \mathcal{N}$ に対して、(すべての $x, y \in \mathcal{N}$ に対して) $\gcd(x, y)$ は $f(x, y, k)$ を割り切る。(証明おわり。)

(e) 解答 1 (言葉による解答-本問では、これで十分。)

k が x, y に比べて十分大きいとする。(注: たとえば $k \leq x + y$ となる k を考えればよいが、具体的に k をいくつ以上にすべきかは、この問題では問わない。)

$f(x, y, k)$ の計算において、 $k > 0$ のときは f が再帰的に呼び出される。このときの引数 x, y の値の変化を見ると、 $x > 0$ かつ $y > 0$ ならば、必ず、 $x + y$ の値が減少する。しかし、 x, y の値は常に非負なので、これが無限に繰返されることはなく、いつか必ず $x = 0$ または $y = 0$ となる。

ひとたび $x = 0$ となれば、 $f(0, y, k) = f(0, y, k-1) = \dots = f(0, y, 0) = y$ となる。同様に $y = 0$ のときも、 $f(x, 0, k) = f(x, 0, k-1)$ なので、これ以上、 x, y の値は変わらない。

以上より、 k が十分大きい値のとき、 $f(x, y, k)$ の値は k によらない。

(注: この一定の値は、 $\gcd(x, y)$ である。ただし $x = y = 0$ のときを除く。)

(e) 解答 2 (上記の解答を厳密にしたもの-論理に興味がある人向け。)

まず、以下の 2 つの事実 (*) を証明する。

$$\forall k, x \in \mathcal{N}. \quad f(x, 0, k) = x$$

$$\forall k, y \in \mathcal{N}. \quad f(0, y, k) = y$$

これらは k に関する帰納法で簡単に証明できる。

次に、

$$\forall k \geq 1, \forall x, y \in \mathcal{N}. ((k \geq x + y \geq 1) \Rightarrow (f(x, y, k) = \gcd(x, y)))$$

を $k \geq 1$ に関する帰納法で証明する。

(base) $k = 1$ のとき、 $(x + y = 1) \Rightarrow (f(x, y, 1) = \gcd(x, y))$ を証明すればよい。 $x + y = 1$ から $(x = 1 \wedge y = 0) \vee (x = 0 \wedge y = 1)$ となる。いずれのケースも、 $f(x, y, 1) = 1$ となり $\gcd(x, y) = 1$ なので両者は一致する。

(step) k に対して上記の命題が成立すると仮定する。すなわち、

$$\forall x, y \in \mathcal{N}. (k \geq x + y \geq 1) \Rightarrow (f(x, y, k) = \gcd(x, y))$$

が成立する (これが帰納法の仮定となる)。

このとき $k+1$ に対しても上記の命題が成立することを証明しよう。すなわち、

$$\forall x, y \in \mathcal{N}. (k+1 \geq x + y \geq 1) \Rightarrow (f(x, y, k+1) = \gcd(x, y))$$

が成立すること証明しよう。

まず、 $x, y \in \mathcal{N}$ と $k+1 \geq x+y \geq 1$ を仮定する。ここで場合分けする。

(case-1: $x=0$) 上記の事実 (*) より、 $f(x, y, k+1) = y$ となり、 $\gcd(x, y) = y$ なので、 $f(x, y, k+1) = \gcd(x, y)$ となる。

(case-2: $x \neq 0 \wedge y=0$) 上記の事実 (*) より、 $f(x, y, k+1) = x$ となり、 $\gcd(x, y) = x$ なので、 $f(x, y, k+1) = \gcd(x, y)$ となる。

(case-3: $x > y > 0$) このとき、 f の定義より $f(x, y, k+1) = f(x-y, y, k)$ である。 k に関する帰納法の仮定を $x-y$ と y にあてはめて使うと、

$$(k \geq (x-y) + y \geq 1) \Rightarrow (f(x-y, y, k) = \gcd(x-y, y))$$

が言える。ところで、 $k+1 \geq x+y$ と $x > y > 0$ より、 $k \geq ((x-y) + y) \geq 1$ が言える。また、 $x > y$ のとき $\gcd(x-y, y) = \gcd(x, y)$ である。以上をまとめると、

$$f(x, y, k+1) = f(x-y, y, k) = \gcd(x-y, y) = \gcd(x, y)$$

である。

(case-4: $y \geq x > 0$) このとき、 f の定義より $f(x, y, k+1) = f(x, y-x, k)$ である。 k に関する帰納法の仮定を x と $y-x$ にあてはめて使うと、

$$(k \geq x + (y-x) \geq 1) \Rightarrow (f(x, y-x, k) = \gcd(x, y-x))$$

が言える。ところで、 $k+1 \geq x+y$ 、 $y \geq x > 0$ より、 $k \geq (x + (y-x)) \geq 1$ が言える。また、 $x \leq y$ のとき $\gcd(x, y-x) = \gcd(x, y)$ である。以上をまとめると、

$$f(x, y, k+1) = f(x, y-x, k) = \gcd(x, y-x) = \gcd(x, y)$$

である。

以上より、いずれのケースも、 $f(x, y, k+1) = \gcd(x, y)$ であるので、帰納法の (step) も言えた。

(base) と (step) がいえたので、帰納法により、

$$\forall k \geq 1. \forall x, y \in \mathcal{N}. (k \geq x+y \geq 1) \Rightarrow (f(x, y, k) = \gcd(x, y))$$

が証明できた。(証明おわり)

(注: 証明した論理式において、 $x+y \geq 1$ という仮定を付加しているのは、 $x=y=0$ の場合は、 $\gcd(x, y)$ という値が定義されないからである。このようなつまらないケースを除けば、「 $f(x, y, k)$ は k が十分大きいとき (k が $x+y$ 以上のとき)、いつでも $\gcd(x, y)$ を返す。」と言える。)