離散数学演習８　解答例

1. 除法定理から, n, d に対して, 自然数の組 (q, r) が唯一に存在して, $n = qd + r$ $(0 \leq r < d)$ となる. そこで, $a_0 = r$ とおく.
   $q < n$ だから, 帰納法の仮定から, q に対して, 自然数の列 $a_1, \cdots, a_k$ （$0 \leq a_i < d$ $(i = 1, \cdots, k)$, $a_k \neq 0$）が唯一に存在して, $q = a_k d^{k-1} + a_{k-1} d^{k-2} + \cdots + a_2 d + a_1$.
   ゆえに, $n = qd + r = a_k d^k + a_{k-1} d^{k-1} + \cdots + a_2 d^2 + a_1 d + a_0$.

2. $m \mid n$ から、整数 q が存在して, $n = qm$. また, $k \mid l$ から, 整数 q' が存在して, $l = q'k$. ゆえに, $nl = qq'mk$. qq' は整数であるから, $mk \mid nl$.

3. (1)
$$\begin{aligned}
& \gcd(6188, 4709) \\
= \ & \gcd(4709, 1479) && 1479 = \mathrm{mod}\ (6188, 4709) \\
= \ & \gcd(1479, 272) && 272 = \mathrm{mod}\ (4709, 1479) \\
= \ & \gcd(272, 119) && 119 = \mathrm{mod}\ (1479, 272) \\
= \ & \gcd(119, 34) && 34 = \mathrm{mod}\ (272, 119) \\
= \ & \gcd(34, 17) && 17 = \mathrm{mod}\ (119, 34) \\
= \ & \gcd(17, 0) && 0 = \mathrm{mod}\ (34, 17) \\
= \ & 17
\end{aligned}$$

   (2)
$$\begin{aligned}
& \gcd(23843, 29041) \\
= \ & \gcd(29041, 23843) && 23843 = \mathrm{mod}\ (23843, 29041) \\
= \ & \gcd(23843, 5198) && 5198 = \mathrm{mod}\ (29041, 23843) \\
= \ & \gcd(5198, 3051) && 3051 = \mathrm{mod}\ (23843, 5198) \\
= \ & \gcd(3051, 2147) && 2147 = \mathrm{mod}\ (5198, 3051) \\
= \ & \gcd(2147, 904) && 904 = \mathrm{mod}\ (3051, 2147) \\
= \ & \gcd(904, 339) && 339 = \mathrm{mod}\ (2147, 904) \\
= \ & \gcd(339, 226) && 226 = \mathrm{mod}\ (904, 339) \\
= \ & \gcd(226, 113) && 113 = \mathrm{mod}\ (339, 226) \\
= \ & \gcd(113, 0) && 0 = \mathrm{mod}\ (226, 113) \\
= \ & 113
\end{aligned}$$

   (3)
$$\begin{aligned}
& \gcd(6825, -1485) \\
= \ & \gcd(-1485, 885) && 885 = \mathrm{mod}\ (6825, -1485) \\
= \ & \gcd(885, 285) && 285 = \mathrm{mod}\ (-1485, 885) \\
= \ & \gcd(285, 30) && 30 = \mathrm{mod}\ (885, 285) \\
= \ & \gcd(30, 15) && 15 = \mathrm{mod}\ (285, 30) \\
= \ & \gcd(15, 0) && 0 = \mathrm{mod}\ (30, 15) \\
= \ & 15
\end{aligned}$$

4. a', b' に正の公約数 $d' > 1$ が存在すると仮定する.
   このとき, 整数 q, r が存在して, $a' = d'q$, $b' = d'r$. ゆえに, $a = (d'q)d = (d'd)q$, $b = (d'r)d = (d'd)r$. したがって, $d'd$ は a, b の公約数である. $d \mid d'd$ だから, これは d が a, b の最大公約数であることに矛盾する.
   ゆえに, a', b' の正の公約数は 1 である. すなわち, a', b' は互いに素である.

5. (1) 整数 $m, km + n$ に対して, 整数 x, y が存在して, $\gcd(m, km + n) = mx + (km + n)y = (x + ky)m + yn$.
   また, $\gcd(m, n) \mid m$. $\gcd(m, n) \mid n$ だから, 任意の整数 a, b に対して, $\gcd(m, n) \mid am + bn$. 特に, 整数 $x + ky, y$ に対して, $\gcd(m, n) \mid (x + ky)m + yn$.
   ゆえに, $\gcd(m, n) \mid \gcd(m, km + n)$.
   一方, 整数 m, n に対して, 整数 x', y' が存在して,
   $\gcd(m, n) = mx' + ny' = (x' - y'k)m + y'(km + n)$.
   また, $\gcd(m, km + n) \mid m$, $\gcd(m, km + n) \mid km + n$ だから, 任意の整数 a, b に対して,
   $\gcd(m, km + n) \mid am + b(km + n)$.
   特に, 整数 $x' - y'k$, y' に対して, $\gcd(m, km + n) \mid (x' - y'k)m + y'(km + n)$.
   ゆえに, $\gcd(m, km + n) \mid \gcd(m, n)$.
   $\gcd(m, n) \mid \gcd(m, km + n)$, $\gcd(m, km + n) \mid \gcd(m, n)$ だから,
   $|\gcd(m, n)| = |\gcd(m, km + n)|$. $\gcd(m, n) \geq 0$, $\gcd(m, km + n) \geq 0$ だから,
   $\gcd(m, n) = \gcd(m, km + n)$.

（別解）
$m, km+n$ のすべての非負公約数からなる集合を $D_{m,km+n}$ とし, m, n のすべての非負公約数からなる集合を $D_{m,n}$ とする.
このとき, 任意の $d \in D_{m,km+n}$ に対して, $d \mid m$, $d \mid km+n$ だから, $d \mid (km+n) - k \cdot m$. $(km+n) - k \cdot m = n$ だから, $d \mid n$. ゆえに, $d \in D_{m,n}$. すなわち, $D_{m,km+n} \subseteq D_{m,n}$.
一方, 任意の $d \in D_{m,n}$ に対して, $d \mid m$, $d \mid n$ だから, $d \mid k \cdot m + n$. ゆえに, $d \in D_{m,km+n}$. すなわち, $D_{m,n} \subseteq D_{m,km+n}$.
したがって, $D_{m,km+n} = D_{m,n}$.
最大公約数は, それらの集合上の整除関係に関する最大元であるから, $\gcd(m, km+n) = \gcd(m, n)$ [1] .

(2) $\dfrac{m}{d} = m', \dfrac{n}{d} = n'$ とおく. このとき, m', n' は整数だから, 整数 x, y が存在して, $\gcd(m', n') = m'x + n'y = \dfrac{1}{d}(xm + yn)$. ゆえに, $d \cdot \gcd(m', n') = xm + yn$.
また, $\gcd(m, n) \mid m$, $\gcd(m, n) \mid n$ だから, 任意の整数 a, b に対して, $\gcd(m, n) \mid am + bn$. 特に, 整数 x, y に対して, $\gcd(m, n) \mid xm + yn$. ゆえに, $\gcd(m, n) \mid d \cdot \gcd(m', n')$.
一方, 整数 m, n に対して, 整数 x', y' が存在して, $\gcd(m, n) = mx' + ny'$.
また, $\gcd(m', n') \mid m'$, $\gcd(m', n') \mid n'$ だから, 任意の整数 a, b に対して, $\gcd(m', n') \mid am' + bn'$. 特に, 整数 x', y' に対して, $\gcd(m', n') \mid x'm' + y'n'$. ゆえに, $\gcd(m', n') \mid \dfrac{1}{d}(x'm + y'n)$. このとき, $d \cdot \gcd(m', n') \mid mx' + ny'$ であり, $d \cdot \gcd(m', n') \mid \gcd(m, n)$.
$\gcd(m, n) \mid d \cdot \gcd(m', n')$, $d \cdot \gcd(m', n') \mid \gcd(m, n)$ だから, $|\gcd(m, n)| = |d \cdot \gcd(m', n')|$.
$\gcd(m, n) > 0$, $d > 0$, $\gcd(m', n') > 0$ だから, $\gcd(m, n) = d \cdot \gcd(m', n')$. すなわち, $\gcd\left(\dfrac{m}{d}, \dfrac{n}{d}\right) = \dfrac{\gcd(m, n)}{d}$.
（別解）
$\dfrac{m}{d} = m', \dfrac{n}{d} = n'$ とおく. m', n' のすべての非負公約数からなる集合を $D_{m',n'}$ とし, m, n のすべての非負公約数からなる集合を $D_{m,n}$ とする. また, $D'_{m,n} = \{\dfrac{x}{d} \mid x \in D_{m,n}, \dfrac{x}{d}$は整数.$\}$ とする.
このとき, 任意の $d' \in D_{m',n'}$ に対して, $d' \mid m'$, $d' \mid n'$. ゆえに, 整数 q, q' が存在して, $m' = qd'$, $n' = q'd'$. したがって, $m = qdd'$, $n = q'dd'$ であり, $dd' \mid m$, $dd' \mid n$. $dd' \in D_{m,n}$ だから, $d' \in D'_{m,n}$. すなわち, $D_{m',n'} \subseteq D'_{m,n}$.
一方, 任意の $\dfrac{d'}{d} \in D'_{m,n}$ $(d' \in D_{m,n})$ に対して, $d' \mid m$, $d' \mid n$. ゆえに, 整数 q, q' が存在して, $m = qd'$, $n = q'd'$. $d \neq 0$ だから, $m' = q\dfrac{d'}{d}$, $n' = q'\dfrac{d'}{d}$. $\dfrac{d'}{d}$ は整数だから, $\dfrac{d'}{d} \mid m'$, $\dfrac{d'}{d} \mid n'$ であり, $\dfrac{d'}{d} \in D_{m',n'}$. すなわち, $D'_{m,n} \subseteq D_{m',n'}$.
したがって, $D_{m',n'} = D'_{m,n}$.
このとき, $\gcd(m', n')$ は, $D_{m',n'}$ 上での整除関係に関する最大元であるから, $D'_{m,n}$ 上の整除関係に関する最大元 $\dfrac{u}{d}$ に等しい. 一方, u は $D_{m,n}$ 上の整除関係に関する最大元である $\gcd(m, n)$ に等しい. ゆえに, $\gcd(m', n') = \gcd\left(\dfrac{m}{d}, \dfrac{n}{d}\right) = \dfrac{\gcd(m, n)}{d}$.

(3) $m, n \neq 0$ だから, $\gcd(m, n) > 0$. そこで, (2) から,
$\gcd\left(\dfrac{m}{\gcd(m, n)}, \dfrac{n}{\gcd(m, n)}\right) = \dfrac{\gcd(m, n)}{\gcd(m, n)} = 1$.
（別解）$\gcd(m, n) = d$ とおく. $m, n \neq 0$ だから, $d \neq 0$.
$\dfrac{m}{d} = m', \dfrac{n}{d} = n'$ とおき, さらに, $\gcd(m', n') = d'$ とおく. このとき, $d' = 1$ を示せばよい.
$\gcd(m', n') = d'$ だから, $d' \mid m'$, $d' \mid n'$, ゆえに, 整数 q, q' が存在して, $m' = qd'$, $n' = q'd'$.
したがって, $m = m'd = qd'd$, $n = n'd = q'd'd$ だから, $d'd \mid m$, $d'd \mid n$. すなわち, $d'd$ は m, n の公約数である.
ところで, d は m, n の最大公約数だから, $d'd \mid d$. ゆえに, 整数 q'' が存在して, $d = q''d'd$. $d \neq 0$ だから, $1 = q''d'$. q'' は整数で, d' は非負整数だから, $d' = 1$.

(4) i) $k > 0$ のとき.

[1] 厳密には, $D_{m,km+n}$ と $D_{m,n}$ が整除関係に関して同型であることを示す.

k は km, kn の正の公約数だから, (2) から, $\gcd\left(\frac{km}{k}, \frac{kn}{k}\right) = \frac{\gcd(km, kn)}{k}$.
ゆえに, $k \cdot \gcd(m, n) = \gcd(km, kn)$.
ii) $k = 0$ のとき.
左辺=$\gcd(0 \cdot m, 0 \cdot n) = \gcd(0, 0) = 0$. 一方, 右辺=$0 \cdot \gcd(m, n) = 0$. ゆえに, 左辺=右辺.
i), ii) から, $k \cdot \gcd(m, n) = \gcd(km, kn)$.
（別解）
整数 m, n に対して, 整数 x, y が存在して, $\gcd(m, n) = mx + ny$.
このとき, $k \cdot \gcd(m, n) = k \cdot (mx + ny) = x(km) + y(kn)$.
また, $\gcd(km, kn) \mid km$, $\gcd(km, kn) \mid kn$ だから, 任意の整数 a, b に対して,
$\gcd(km, kn) \mid a(km) + b(kn)$. 特に, 整数 x, y に対して, $\gcd(km, kn) \mid x(km) + y(kn)$.
ゆえに, $\gcd(km, kn) \mid k \cdot \gcd(m, n)$.
一方, 整数 km, kn に対して, 整数 x', y' が存在して,
$\gcd(km, kn) = (km)x' + (kn)y' = k \cdot (x'm + y'n)$.
また, $\gcd(m, n) \mid m$, $\gcd(m, n) \mid n$ だから, 任意の整数 a, b に対して, $\gcd(m, n) \mid am + bn$. 特に, 整数 x', y' に対して, $\gcd(m, n) \mid x'm + y'n$. ゆえに, $k \cdot \gcd(m, n) \mid k \cdot (x'm + y'n)$.
したがって, $k \cdot \gcd(m, n) \mid \gcd(km, kn)$.
$\gcd(km, kn) \mid k \cdot \gcd(m, n)$, $k \cdot \gcd(m, n) \mid \gcd(km, kn)$ だから, $|\gcd(km, kn)| = |k \cdot \gcd(m, n)|$.
$\gcd(km, kn) \geq 0$, $k \cdot \gcd(m, n) \geq 0$ だから, $\gcd(km, kn) = k \cdot \gcd(m, n)$.

6. (1) m_1, m_2, n のすべての非負公約数からなる集合を $D_{m_1,m_2,n}$ とし, n, r_1, r_2 のすべての非負公約数からなる集合を D_{n,r_1,r_2} とする.
このとき, 任意の $d \in D_{m_1,m_2,n}$ に対して, $d \mid m_1$, $d \mid m_2$, かつ $d \mid n$ だから, $d \mid m_1 - q_1 n$ であり, $d \mid r_1$. 同様に, $d \mid (m_2 - q_2 n)$ であり, $d \mid r_2$. ゆえに, $d \in D_{n,r_1,r_2}$. すなわち, $D_{m_1,m_2,n} \subseteq D_{n,r_1,r_2}$.
一方, 任意の $d' \in D_{n,r_1,r_2}$ に対して, $d' \mid n$, $d' \mid r_1$, かつ $d' \mid r_2$ だから, $d' \mid q_1 n + r_1$ であり, $d \mid m_1$. 同様に, $d' \mid q_2 n + r_2$ であり, $d \mid m_2$. ゆえに, $d \in D_{m_1,m_2,n}$. すなわち, $D_{n,r_1,r_2} \subseteq D_{m_1,m_2,n}$.
したがって, $D_{m_1,m_2,n} = D_{n,r_1,r_2}$.
最大公約数は, それらの集合上の整除関係に関する最大元であるから, $\gcd(m_1, m_2, n) = \gcd(n, r_1, r_2)$.

(2)
$$
\begin{aligned}
& \gcd(126, 336, 91) \\
= \ & \gcd(336, 126, 91) \\
= \ & \gcd(63, 35, 91) && 63 = \mathrm{mod}\ (336, 91), 35 = \mathrm{mod}\ (126, 91) \\
= \ & \gcd(91, 63, 35) \\
= \ & \gcd(21, 28, 35) && 21 = \mathrm{mod}\ (91, 35),\ 28 = \mathrm{mod}\ (63, 35) \\
= \ & \gcd(35, 28, 21) \\
= \ & \gcd(14, 7, 21) && 14 = \mathrm{mod}\ (35, 21),\ 7 = \mathrm{mod}\ (28, 21) \\
= \ & \gcd(21, 14, 7) \\
= \ & \gcd(0, 0, 7) && 0 = \mathrm{mod}\ (21, 7),\ 0 = \mathrm{mod}\ (14, 7) \\
= \ & 7
\end{aligned}
$$

7.
```
int gcd(int m, int n)
{
    if(n==0){
        return(abs(m));
    }
    else{
        return(gcd(n, m%n));
    }
}
```

または

```
int gcd(int m, int n)
{
    int x, y, z;

    if(n==0){
        return(abs(m));
    }
    x=m;
    y=n;
    while(y!=0){
        z=x;
        x=y;
        y=z%y;
    };
    return(x);
}
```