

## 離散数学及び演習 講義 6 2016. 5.26(木)

約数・倍数  
(教科書 pp.101-106, 113-116)

## 整数論 (number theory)



$$28 = 1 + 2 + 4 + 7 + 14$$

### 整数の基本的性質

$\mathbf{Z}$ : すべての整数からなる集合  
 $\mathbf{N}$ : すべての自然数からなる集合  
 $\mathbf{N}_0 = \mathbf{N} \cup \{0\}$ : すべての非負整数からなる集合

任意の  $m, n \in \mathbf{Z}$  に対して,

- $m+n \in \mathbf{Z}$
- $m-n \in \mathbf{Z}$ 
  - $0-n = -n \in \mathbf{Z}$
- $m \cdot n \in \mathbf{Z}$
- 一般に,  $m/n \notin \mathbf{Z}$ 
  - $\mathbf{Z}$  は加法, 減法, 乗法について閉じている.
  - $\mathbf{Z}$  は除法について閉じていない.
    - 剰余のある除法

3

### 除法定理 (division theorem)

- (1) 任意の  $m \in \mathbf{N}_0, n \in \mathbf{N}$  に対して, 順序対  $(q, r) \in \mathbf{N}_0^2$  が唯一存在して,  $m = q \cdot n + r$  ( $0 \leq r < n$ )
- (2) 任意の  $m, n \in \mathbf{Z}$  ( $n \neq 0$ ) に対して, 順序対  $(q, r) \in \mathbf{Z}^2$  が唯一存在して,  $m = q \cdot n + r$  ( $0 \leq r < |n|$ )

- $q$  ... 商 (quotient)
- $r$  ... 剰余 (remainder)  $r = \text{mod}(m, n)$

例:

$117 = 2 \cdot 51 + 15$	
$\times 117 = 1 \cdot 51 + 66$	$r = 66 \geq  51 $
$\times 117 = 3 \cdot 51 + (-36)$	$r = -36 < 0$
$-117 = 3 \cdot (-51) + 36$	
$\times -117 = 4 \cdot (-51) + 87$	$r = 87 \geq  -51 $
$\times -117 = 2 \cdot (-51) + (-15)$	$r = -15 < 0$

4

### 証明

- (1) 任意の  $m \in \mathbf{N}_0, n \in \mathbf{N}$  に対して, 順序対  $(q, r) \in \mathbf{N}_0^2$  が唯一存在して,  $m = q \cdot n + r$  ( $0 \leq r < n$ )
  - a) 「 $(q, r) \in \mathbf{N}_0^2$  が存在する」を示す.
  - b) 「 $(q, r) \in \mathbf{N}_0^2$  は唯一である」を示す.

- a-1)  $m < n$  のとき. このとき,  $0 \leq m < n$ .  
 $q=0, r=m$  とおくと,  $m = 0 \cdot n + m$  だから,  $m = q \cdot n + r$  ( $0 \leq r < n$ )
- a-2)  $m \geq n$  のとき.  $m$  に関する帰納法により示す.  
 任意の  $k < m$  ( $k \in \mathbf{N}_0$ ) に対して,  $(q', r') \in \mathbf{N}_0^2$  が存在して,  
 $k = q' \cdot n + r'$  ( $0 \leq r' < n$ ) と仮定する (帰納法の仮定).  
 ここで,  $m' = m - n$  ( $\geq 0$ ) とおくと,  $m' - m = -n < 0$  だから,  $m' < m$ .  
 帰納法の仮定から,  $m'$  と  $n$  に対して,  $(q', r') \in \mathbf{N}_0^2$  が存在して,  
 $m' = q' \cdot n + r'$  ( $0 \leq r' < n$ ).  
 $m' = m - n = q' \cdot n + r'$  だから,  $m = (q'+1) \cdot n + r'$ .  
 $q = q'+1, r = r'$  とおくと,  $(q, r) \in \mathbf{N}_0^2$  で,  $m = q \cdot n + r$  ( $0 \leq r < n$ ).

5

### 証明 (続き2)

- (1) 任意の  $m \in \mathbf{N}_0, n \in \mathbf{N}$  に対して, 順序対  $(q, r) \in \mathbf{N}_0^2$  が唯一存在して,  $m = q \cdot n + r$  ( $0 \leq r < n$ )
  - b) 「 $(q, r) \in \mathbf{N}_0^2$  は唯一である」を示す.

- b) 任意の  $m \in \mathbf{N}_0, n \in \mathbf{N}$  に対して,  $(q_1, r_1), (q_2, r_2) \in \mathbf{N}_0^2$  ( $q_1 \neq q_2$ ) が存在して,  $m = q_1 \cdot n + r_1$  ( $0 \leq r_1 < n$ ),  $m = q_2 \cdot n + r_2$  ( $0 \leq r_2 < n$ ) と仮定する.
- b-1)  $q_1 > q_2$  のとき.  
 このとき,  $0 = (q_1 - q_2) \cdot n + (r_1 - r_2)$ . すなわち,  $r_2 - r_1 = (q_1 - q_2) \cdot n$ .  
 $q_1 - q_2 > 0$  で,  $q_1 - q_2 \in \mathbf{Z}$  だから,  $q_1 - q_2 \geq 1$ .  
 $n > 0$  だから,  $(q_1 - q_2) \cdot n \geq n$ .  
 一方,  $r_2 < n, r_1 \geq 0$  だから,  $r_2 - r_1 < n$ .  
 $r_2 - r_1 = (q_1 - q_2) \cdot n < n$  となるから, これは矛盾.
- b-2)  $q_2 > q_1$  のとき. 同様に矛盾.  
 ゆえに,  $q_1 = q_2$ .  
 このとき,  $r_2 - r_1 = (q_1 - q_2) \cdot n = 0$  だから,  $r_1 = r_2$ .

6

### 証明(続き3)

- (1) 任意の  $m \in \mathbb{N}_0, n \in \mathbb{N}$  に対して, 順序対  $(q, r) \in \mathbb{N}_0^2$  が唯一存在して,  $m = q \cdot n + r$  ( $0 \leq r < n$ )
- (2) 任意の  $m, n \in \mathbb{Z}$  ( $n \neq 0$ ) に対して, 順序対  $(q, r) \in \mathbb{Z}^2$  が唯一存在して,  $m = q \cdot n + r$  ( $0 \leq r < |n|$ )
- a) 「 $(q, r) \in \mathbb{Z}^2$  が存在する」を示す.
  - b) 「 $(q, r) \in \mathbb{Z}^2$  は唯一である」を示す.
  - a-1)  $n > 0$  のとき.
    - a-1-1)  $m \geq 0$  のとき. ... (1)から明らか.
    - a-1-2)  $m < 0$  のとき.
  - a-2)  $n < 0$  のとき.
    - a-2-1)  $m \geq 0$  のとき. } (1)に帰着させる.
    - a-2-2)  $m < 0$  のとき.
  - b) (1)と同様に証明できる.

7

### 証明(続き4)

- (2) 任意の  $m, n \in \mathbb{Z}$  ( $n \neq 0$ ) に対して, 順序対  $(q, r) \in \mathbb{Z}^2$  が唯一存在して,  $m = q \cdot n + r$  ( $0 \leq r < |n|$ )
- a) 「 $(q, r) \in \mathbb{Z}^2$  が存在する」を示す.
- a-1)  $n > 0$  のとき. このとき,  $|n| = n$ .
- a-1-1)  $m \geq 0$  のとき. (1)から明らか.
- a-1-2)  $m < 0$  のとき.  
 $m' = -(m+1)$  とおくと,  $m < 0$  だから,  $m' > -1$ .  
 $m' \in \mathbb{Z}$  だから,  $m' \geq 0$ .  
 (1)から,  $m', n$  に対して,  $(q', r') \in \mathbb{Z}^2$  が存在して,  $m' = q' \cdot n + r'$  ( $0 \leq r' < n$ )
- このとき,  $m = -m' - 1 = -(q' \cdot n + r') - 1 = (-q' - 1) \cdot n + (n - 1 - r')$ .  
 ここで,  $q = -q' - 1, r = n - 1 - r'$  とおくと,  $(q, r) \in \mathbb{Z}^2$  で,  $m = q \cdot n + r$ .  
 また,  $r' \in \mathbb{Z}$  だから,  $0 \leq r' \leq n - 1$ .  
 ゆえに,  $0 \leq n - 1 - r' \leq n - 1$ .  
 したがって,  $0 \leq r \leq n - 1$  だから,  $0 \leq r < n = |n|$ .

8

### 証明(続き5)

- (2) 任意の  $m, n \in \mathbb{Z}$  ( $n \neq 0$ ) に対して, 順序対  $(q, r) \in \mathbb{Z}^2$  が唯一存在して,  $m = q \cdot n + r$  ( $0 \leq r < |n|$ )
- a) 「 $(q, r) \in \mathbb{Z}^2$  が存在する」を示す.
- a-2)  $n < 0$  のとき. このとき,  $|n| = -n > 0$ .
- a-2-1)  $m \geq 0$  のとき.  
 $n' = -n$  とおくと,  $n' > 0$ .  
 (1)から,  $m, n'$  に対して組  $(q', r') \in \mathbb{Z}^2$  が存在して,  $m = q' \cdot n' + r'$  ( $0 \leq r' < n'$ )
- このとき,  $m = q' \cdot (-n) + r' = (-q') \cdot n + r'$ .  
 ここで,  $q = -q', r = r'$  とおくと,  $(q, r) \in \mathbb{Z}^2$  で,  $m = q \cdot n + r$ .  
 さらに,  $n' = -n = |n|$  だから,  $0 \leq r' < |n|$ .

9

### 証明(続き6)

- (2) 任意の  $m, n \in \mathbb{Z}$  ( $n \neq 0$ ) に対して, 順序対  $(q, r) \in \mathbb{Z}^2$  が唯一存在して,  $m = q \cdot n + r$  ( $0 \leq r < |n|$ )
- a) 「 $(q, r) \in \mathbb{Z}^2$  が存在する」を示す.
- a-2)  $n < 0$  のとき. このとき,  $|n| = -n > 0$ .
- a-2-2)  $m < 0$  のとき.  
 $m' = -(m+1), n' = -n$  とおくと,  $m' \geq 0, n' > 0$ .  
 (1)から,  $m', n'$  に対して組  $(q', r') \in \mathbb{Z}^2$  が存在して,  $m' = q' \cdot n' + r'$  ( $0 \leq r' < n'$ )
- このとき,  $m = -m' - 1 = -(q' \cdot (-n) + r') - 1 = (q' + 1) \cdot n + (-n + r' - 1)$ .  
 ここで,  $q = q' + 1, r = -(n + r' + 1)$  とおくと,  $(q, r) \in \mathbb{Z}^2$  で,  $m = q \cdot n + r$ .  
 さらに,  $0 \leq r' < n'$  だから,  $1 \leq r' + 1 < n' + 1 = -n + 1$ .  
 ゆえに,  $0 < r' + 1 \leq -n$  だから,  $0 \leq -(n + r' + 1) < -n = |n|$ .  
 すなわち,  $0 \leq r < |n|$ .

10

### 約数・倍数

- $n, k \in \mathbb{Z}$  に対して,
- $k$  は  $n$  の約数(divisor)である
  - $n$  は  $k$  の倍数(multiple)である
  - $k$  は  $n$  を割り切る(divide) ( $n$  は  $k$  で割り切れる(divisible))
- ...  $k \mid n$
- ある  $q \in \mathbb{Z}$  が存在して,  $n = q \cdot k$

例:

- $19 \mid 38$  (19は38の約数, 38は19の倍数)
  - $38 = 2 \cdot 19$
- $-19 \mid 38$  (-19は38の約数, 38は-19の倍数)
  - $38 = (-2) \cdot (-19)$

11

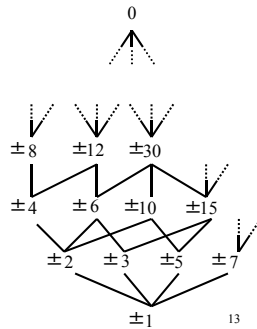
### 約数・倍数(続き)

- $n, k \in \mathbb{Z}$  に対して,
- $k$  は  $n$  の約数(divisor)である,  $n$  は  $k$  の倍数(multiple)である
  - $k$  は  $n$  を割り切る(divide) ( $n$  は  $k$  で割り切れる(divisible)) ...  $k \mid n$ 
    - ある  $q \in \mathbb{Z}$  が存在して,  $n = q \cdot k$
  - 任意の  $n \in \mathbb{Z}$  に対して,  $n = n \cdot 1, n = (-n) \cdot (-1)$  ( $\pm n \in \mathbb{Z}$ )
    - $\pm 1$  は任意の  $n \in \mathbb{Z}$  の約数である. 任意の  $n \in \mathbb{Z}$  は  $\pm 1$  の倍数である
    - $\pm 1$  は任意の  $n \in \mathbb{Z}$  を割り切る ( $\pm 1 \mid n$ )
  - 任意の  $k \in \mathbb{Z}$  に対して,  $0 = 0 \cdot k$  ( $0 \in \mathbb{Z}$ )
    - 任意の  $k \in \mathbb{Z}$  は  $0$  の約数である,  $0$  は任意の  $k \in \mathbb{Z}$  の倍数である
    - 任意の  $k \in \mathbb{Z}$  は  $0$  を割り切る ( $k \mid 0$ )
    - 特に,  $0$  は  $0$  の約数である,  $0$  は  $0$  の倍数である
    - $0$  は  $0$  を割り切る ( $0 \mid 0$ )
  - 任意の  $n \in \mathbb{Z}$  ( $n \neq 0$ ) に対して,  $n = q \cdot 0$  となる  $q \in \mathbb{Z}$  は存在しない
    - $n \neq 0$  に対して,  $0 \mid n$  とはならない.

12

## 整除関係 (divisibility relation)

- $\mathbb{Z}$  上の整除関係  $|$  ( $| \subseteq \mathbb{Z}^2$ )**
  - $k | n$  iff ある  $q \in \mathbb{Z}$  が存在して,  $n = q \cdot k$
  - $|$  は反射的かつ推移的である
  - $|$  は反対称的でない  
 $1 | -1$ かつ $-1 | 1$ であるが,  $1 \neq -1$
- $\mathbb{N}_0$  上の整除関係  $|$  ( $| \subseteq \mathbb{N}_0^2$ )**
  - $|$  は半順序
- 1 は  $\mathbb{N}_0$  上の整除関係  $|$  の最小元**
  - 任意の  $n \in \mathbb{N}_0$  に対して,  $1 | n$ .
- 0 は  $\mathbb{N}_0$  上の整除関係  $|$  の最大元**
  - 任意の  $k \in \mathbb{N}_0$  に対して,  $k | 0$ .



13

## 定理

任意の  $m, n, k \in \mathbb{Z}$  に対して, 次の(1)~(4)が成り立つ.

- $m | m$ .
- $m | n$  かつ  $n | m$  ならば,  $|m| = |n|$ .  
 特に,  $m, n \in \mathbb{N}_0$  のとき,  
 $m | n$  かつ  $n | m$  ならば,  $m = n$ .
- $m | n$  かつ  $n | k$  ならば,  $m | k$ .
- $k | m$  かつ  $k | n$  ならば, 任意の  $a, b \in \mathbb{Z}$  に対して,  
 $k | am + bn$ .

- 整除関係  $|$  は  $\mathbb{N}_0$  上の半順序である.

14

## 証明

- $m | m$ .
- $m | n$  かつ  $n | m$  ならば,  $|m| = |n|$ .

- 
- $1 \in \mathbb{Z}$  に対して,  $m = 1 \cdot m$  だから, 明らか.
  - $m | n$  だから,  $q_1 \in \mathbb{Z}$  が存在して,  $n = q_1 \cdot m$ .  
 $n | m$  だから,  $q_2 \in \mathbb{Z}$  が存在して,  $m = q_2 \cdot n$ .  
 ゆえに,  $n = q_1 q_2 n$ .  
 a)  $n \neq 0$  のとき,  $q_1 q_2 = 1$ .  
 $q_1, q_2 \in \mathbb{Z}$  だから,  $q_1 = q_2 = 1$  または  $q_1 = q_2 = -1$ .  
 すなわち,  $m = n$  または  $m = -n$  だから,  $|m| = |n|$ .  
 b)  $n = 0$  のとき,  $m = q_2 \cdot 0 = 0$ .  
 ゆえに,  $m = n = 0$  だから,  $|m| = |n|$ .

15

## 証明(続き)

- $m | n$  かつ  $n | k$  ならば,  $m | k$ .  
 「ある  $q \in \mathbb{Z}$  が存在して,  $k = q \cdot m$ 」を示す.

---

$m | n$  だから,  $q_1 \in \mathbb{Z}$  が存在して,  $n = q_1 \cdot m$ .  
 $n | k$  だから,  $q_2 \in \mathbb{Z}$  が存在して,  $k = q_2 \cdot n$ .  
 ゆえに,  $k = q_2 \cdot q_1 \cdot m$ .  
 $q_2 \cdot q_1 \in \mathbb{Z}$  だから,  $m | k$ .

16

## 証明(続き2)

- $k | m$  かつ  $k | n$  ならば, 任意の  $a, b \in \mathbb{Z}$  に対して,  
 $k | am + bn$ .  
 「ある  $q \in \mathbb{Z}$  が存在して,  $am + bn = q \cdot k$ 」を示す.

---

$k | m$  だから,  $q_1 \in \mathbb{Z}$  が存在して,  $m = q_1 \cdot k$ .  
 $k | n$  だから,  $q_2 \in \mathbb{Z}$  が存在して,  $n = q_2 \cdot k$ .  
 ゆえに,  $am + bn = aq_1 k + bq_2 k = (aq_1 + bq_2)k$ .  
 $aq_1 + bq_2 \in \mathbb{Z}$  だから,  $k | am + bn$ .

17

## 定理

$n, m \in \mathbb{Z}$  に対して,  
 $m \neq 0$  かつ  $n | m$  ならば,  $|n| \leq |m|$ .

特に,  $n, m \in \mathbb{N}$  に対して,  $n | m$  ならば,  $n \leq m$ .

18

### 証明

$n, m \in \mathbb{Z}$  に対して,  $m \neq 0$  かつ  $n \mid m$  ならば,  $|n| \leq |m|$ .

$n \mid m$  だから,  $q \in \mathbb{Z}$  が存在して,  $m = q \cdot n$ .

$m \neq 0$  だから,  $q \neq 0$  かつ  $n \neq 0$ .

ゆえに,  $1 \leq |q|$ .

$|n| \geq 0$  だから,  $|n| \leq |q| \cdot |n| = |q \cdot n| = |m|$ .

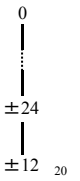
19

### 公倍数

$n, k \in \mathbb{Z}$  に対して,

- $m \in \mathbb{Z}$  は  $n, k$  の公倍数 (common multiple) である
  - $n \mid m$  かつ  $k \mid m$ .
- $m \in \mathbb{N}_0$  は  $n, k$  の最小公倍数 (least common multiple) である
  - ...  $m = \text{lcm}(n, k) = [n, k]$
- $m$  は  $n, k$  の公倍数で, かつ,  $n, k$  の任意の公倍数  $m'$  に対して,  $m \mid m'$  ( $m'$  は  $m$  の倍数).
- $m$  は  $n, k$  のすべての非負公倍数からなる集合上での整除関係に関する最小元

- 例: 4 の倍数 :                    ..., -12, -8, -4, 0, 4, 8, 12, ...
- 6 の倍数 :                    ..., -18, -12, -6, 0, 6, 12, 18, ...
- 4 と 6 の公倍数 :            ..., -24, -12, 0, 12, 24, ...
  - 4 と 6 の最小公倍数 : 12 ( $\in \mathbb{N}_0$ )
    - 12  $\mid$  0, 12  $\mid$  12, 12  $\mid$  24



20

### 定理

- 任意の  $n, k \in \mathbb{Z}$  に対して,  $\text{lcm}(n, k) = \text{lcm}(k, n)$ .
- 任意の  $n \in \mathbb{Z}$  に対して,  $\text{lcm}(n, 0) = 0$ .
  - 0 は  $n, 0$  の唯一の公倍数で, かつ,  $0 \mid 0$ .
- $n, k \in \mathbb{N}$  の最小公倍数は  $n, k$  の公倍数の中で (大小関係に関して) 最小である.
  - $m$  を  $n, k$  の任意の公倍数とすると,  $\text{lcm}(n, k) \mid m$ , かつ,  $m > 0$ ,  $\text{lcm}(n, k) > 0$  だから, 定理より,  $\text{lcm}(n, k) \leq m$ .

21

### 公倍数(続き)

$k_1, \dots, k_n \in \mathbb{Z}$  に対して,

- $m \in \mathbb{Z}$  は  $k_1, \dots, k_n$  の公倍数である
  - $k_1 \mid m, \dots, k_n \mid m$ .
- $m \in \mathbb{N}_0$  は  $k_1, \dots, k_n$  の最小公倍数である
  - ...  $m = \text{lcm}(k_1, \dots, k_n) = [k_1, \dots, k_n]$
- $m$  は  $k_1, \dots, k_n$  の公倍数で, かつ,  $k_1, \dots, k_n$  の任意の公倍数  $m'$  に対して,  $m \mid m'$ .

22

### 公約数

$n, k \in \mathbb{Z}$  に対して,

- $d \in \mathbb{Z}$  は  $n, k$  の公約数 (common divisor) である
  - $d \mid n$  かつ  $d \mid k$ .
- $d \in \mathbb{N}_0$  は  $n, k$  の最大公約数 (greatest common divisor) である
  - ...  $d = \text{gcd}(n, k) = (n, k)$
  - $d$  は  $n, k$  の公約数で, かつ,  $n, k$  の任意の公約数  $d'$  に対して,  $d' \mid d$  ( $d'$  は  $d$  の約数).
  - $d$  は  $n, k$  のすべての非負公約数からなる集合上での整除関係に関する最大元

- 例: 8 の約数 :                    -8, -4, -2, -1, 1, 2, 4, 8                    ±4
- 12 の約数 :                    -12, -6, -4, -3, -2, -1,                    ±2
- 1, 2, 3, 4, 6, 12
- 8 と 12 の公約数 : -4, -2, -1, 1, 2, 4
  - 8 と 12 の最大公約数 : 4 ( $\in \mathbb{N}_0$ )
    - 1  $\mid$  4, 2  $\mid$  4, 4  $\mid$  4                    ±1

23

### 定理

- 任意の  $n, k \in \mathbb{Z}$  に対して,  $\text{gcd}(n, k) = \text{gcd}(k, n)$ .
- 任意の  $n \in \mathbb{Z}$  に対して,  $\text{gcd}(n, 0) = |n|$ .
  - 特に,  $\text{gcd}(0, 0) = 0$ .
  - 任意の整数は 0 の約数である.
  - ゆえに,  $n, 0$  の公約数は  $n$  の約数である.
  - $|n|$  は  $n, 0$  の公約数で, かつ,  $n, 0$  の任意の公約数  $d'$  に対して,  $d' \mid |n|$ .
- $n, k \in \mathbb{N}$  の最大公約数は  $n, k$  の公約数の中で (大小関係に関して) 最大である.
  - $d$  を  $n, k$  の任意の公約数とすると,  $d \mid \text{gcd}(n, k)$  かつ  $\text{gcd}(n, k) > 0$ ,  $d > 0$  だから, 定理より,  $d \leq \text{gcd}(n, k)$ .

24

## 公約数(続き)

$k_1, \dots, k_n \in \mathbb{Z}$  に対して,

- $d \in \mathbb{Z}$  は  $k_1, \dots, k_n$  の公約数である
  - $d \mid k_1, \dots, d \mid k_n$ .
- $d \in \mathbb{N}_0$  は  $k_1, \dots, k_n$  の最大公約数である
  - ...  $d = \gcd(k_1, \dots, k_n) = (k_1, \dots, k_n)$
- $d$  は  $k_1, \dots, k_n$  の公約数で、かつ、 $k_1, \dots, k_n$  の任意の公約数  $d'$  に対して、 $d' \mid d$ .

25

## 互いに素

- $n, k \in \mathbb{Z}$  は互いに素である  
(relatively prime, coprime)
- $\gcd(n, k) = 1$

26

## 定理

任意の  $m, n \in \mathbb{Z}$  に対して、 $x, y \in \mathbb{Z}$  が存在して、  
 $mx + ny = \gcd(m, n)$ .

例:  $\gcd(10, 15) = 5 = 10 \cdot (-1) + 15 \cdot 1$   
 $\gcd(30, 77) = 1 = 30 \cdot 18 + 77 \cdot (-7)$

27

## 証明

任意の  $m, n \in \mathbb{Z}$  に対して、 $x, y \in \mathbb{Z}$  が存在して、  
 $mx + ny = \gcd(m, n)$ .

$mu + nv$  ( $u, v \in \mathbb{Z}$ ) という形の最小の自然数を  $d = mx + ny$  とする。  
このとき、 $x, y \in \mathbb{Z}$ .

- $d = \gcd(m, n)$  を示す.
  - 1) 「 $d \mid m$  かつ  $d \mid n$ 」を示す.
  - 2) 「 $m$  と  $n$  の任意の公約数  $d'$  に対して、 $d' \mid d$ 」を示す.
- 1)  $d \mid m$  でないと仮定する。  
このとき、除法定理から、 $q, r \in \mathbb{Z}$  が存在して、 $m = q \cdot d + r$  ( $0 < r < d$ ).  
ゆえに、 $r = m - q \cdot d = m - q \cdot (mx + ny) = m(1 - q \cdot x) + n(-q \cdot y)$ .  
 $1 - q \cdot x, -q \cdot y \in \mathbb{Z}$  だから、 $r$  は  $mu + nv$  という形の自然数である。  
ところが、 $r < d$  だから、 $d$  の選び方に矛盾する。  
ゆえに、 $d \mid m$ .  
同様に、 $d \mid n$ .

28

## 証明(続き)

任意の  $m, n \in \mathbb{Z}$  に対して、 $x, y \in \mathbb{Z}$  が存在して、  
 $mx + ny = \gcd(m, n)$ .

$mu + nv$  ( $u, v \in \mathbb{Z}$ ) という形の最小の自然数を  $d = mx + ny$  とする。

- $d = \gcd(m, n)$  を示す.
  - 2) 「 $m$  と  $n$  の任意の公約数  $d'$  に対して、 $d' \mid d$ 」を示す.
- 2)  $d'$  は  $m$  と  $n$  の公約数だから、 $m', n' \in \mathbb{Z}$  が存在して、  
 $m = m' \cdot d'$  かつ  $n = n' \cdot d'$ .  
ゆえに、 $d = mx + ny = m' \cdot d' \cdot x + n' \cdot d' \cdot y = (m' \cdot x + n' \cdot y) \cdot d'$ .  
 $m' \cdot x + n' \cdot y \in \mathbb{Z}$  だから、 $d' \mid d$ .  
以上から、 $d = \gcd(m, n)$ .

29

## 系

任意の  $m, n, k \in \mathbb{Z}$  に対して、  
 $\gcd(m, n) = 1$  かつ  $m \mid nk$  ならば、 $m \mid k$ .

30

### 証明

任意の  $m, n, k \in \mathbb{Z}$  に対して,  
 $\gcd(m, n) = 1$  かつ  $m \mid nk$  ならば,  $m \mid k$ .

定理から,  $m, n \in \mathbb{Z}$  に対して,  $x, y \in \mathbb{Z}$  が存在して,  
 $mx + ny = \gcd(m, n) = 1$ .  
 このとき,  $k(mx + ny) = k$ .  
 一方,  $k(mx + ny) = mkx + nky$ .  
 $m \mid nk$  だから,  $m \mid nky$ .  
 また, 明らかに,  $m \mid mkx$ .  
 ゆえに, 定理より  $m \mid mkx + nky$  だから,  $m \mid k(mx + ny)$ .  
 $mx + ny = 1$  だから,  $m \mid k$ .

31

### 定理

任意の  $n, k \in \mathbb{Z}$  に対して,  $\gcd(n, k) \cdot \text{lcm}(n, k) = n \cdot k$ .

32

### 証明

任意の  $n, k \in \mathbb{Z}$  に対して,  $\gcd(n, k) \cdot \text{lcm}(n, k) = n \cdot k$ .

- a)  $n=0$  または  $k=0$  のとき.
- b)  $n, k \neq 0$  のとき.

a)  $n=0$  または  $k=0$  のとき.  
 $\text{lcm}(n, k) = 0, n \cdot k = 0$  だから,  $\gcd(n, k) \cdot \text{lcm}(n, k) = n \cdot k$ .

33

### 証明(続き)

任意の  $n, k \in \mathbb{Z}$  に対して,  $\gcd(n, k) \cdot \text{lcm}(n, k) = n \cdot k$ .

b)  $n, k \neq 0$  のとき.  
 $\gcd(n, k) = d$  とおく. すなわち,  $d \cdot \text{lcm}(n, k) = n \cdot k$  を示す.  
 このとき,  $q, q' \in \mathbb{Z}$  が存在して,  $n = q \cdot d$  かつ  $k = q' \cdot d$ .  
 ( $\gcd(q, q') = 1$ )

ゆえに,  $n \cdot k = q \cdot d \cdot q' \cdot d = d \cdot qq'd$ .  
 $qq'd = m$  とおく. すなわち,  $n \cdot k = d \cdot m$ .

- $m = \text{lcm}(n, k)$  を示す.
- b-1) 「 $n \mid m$  かつ  $k \mid m$ 」を示す.
- b-2) 「 $n, k$  の任意の公倍数  $m'$  に対して,  $m \mid m'$ 」を示す.

b-1)  $m = q \cdot d = q \cdot n$  だから,  $n \mid m$ .  
 また,  $m = q \cdot d = q \cdot k$  だから,  $k \mid m$ .

34

### 証明(続き2)

b)  $n, k \neq 0$  のとき.  
 $\gcd(n, k) = d$  とおく. すなわち,  $d \cdot \text{lcm}(n, k) = n \cdot k$  を示せばよい.  
 このとき,  $q, q' \in \mathbb{Z}$  が存在して,  $n = q \cdot d$  かつ  $k = q' \cdot d$ .  
 ゆえに,  $n \cdot k = q \cdot d \cdot q' \cdot d = d \cdot qq'd$ .  
 $qq'd = m$  とおく. すなわち,  $n \cdot k = d \cdot m$ .  
 ▪ b-2) 「 $n, k$  の任意の公倍数  $m'$  に対して,  $m \mid m'$ 」を示す.

b-2)  $n, k$  の任意の公倍数を  $m'$  とする.  
 このとき,  $q_1 \in \mathbb{Z}$  が存在して,  $m' = q_1 \cdot n = q_1 \cdot q \cdot d$ .  
 一方,  $q_2 \in \mathbb{Z}$  が存在して,  $m' = q_2 \cdot k = q_2 \cdot q' \cdot d$ .  
 ゆえに,  $q_1 \cdot q \cdot d = q_2 \cdot q' \cdot d$ .  
 $d \neq 0$  だから,  $q_1 \cdot q = q_2 \cdot q'$  であり,  $q' \mid q_1 \cdot q$ .  
 ところが,  $\gcd(q, q') = 1$  だから,  $q' \mid q_1$ .  
 ゆえに,  $q' \cdot n \mid q_1 \cdot n$  だから,  $q' \cdot q \cdot d \mid q_1 \cdot n$ .  
 すなわち,  $m \mid m'$ .

35

### 定理(Euclidの互除法の原理)

任意の  $m, n, q, r \in \mathbb{Z}$  に対して,  $m = qn + r$  ならば,  
 $\gcd(m, n) = \gcd(n, r)$ .

例:  $\gcd(117, 51)$

$$\begin{aligned} &= \gcd(51, 15) && \dots 117 = 2 \cdot 51 + 15 \\ &= \gcd(15, 6) && \dots 51 = 3 \cdot 15 + 6 \\ &= \gcd(6, 3) && \dots 15 = 2 \cdot 6 + 3 \\ &= \gcd(3, 0) && \dots 6 = 2 \cdot 3 + 0 \\ &= 3 && \dots \text{定理} \end{aligned}$$



Euclid  
 (ギリシャ, 330?-275? B.C.)

36

## Euclid の互除法 (Euclidean Algorithm)

- 入力:  $m, n \in \mathbb{Z}$
- 出力:  $\gcd(m, n)$
- 手順:
 

$\gcd(m, n)$	
$= \gcd(n, r_1)$	$r_1 = \text{mod}(m, n) \quad (0 \leq r_1 <  n )$
$= \gcd(r_1, r_2)$	$r_2 = \text{mod}(n, r_1) \quad (0 \leq r_2 <  r_1  = r_1)$
$= \gcd(r_2, r_3)$	$r_3 = \text{mod}(r_1, r_2) \quad (0 \leq r_3 <  r_2  = r_2)$
⋮	
$= \gcd(r_{k-1}, r_k)$	$r_k = \text{mod}(r_{k-2}, r_{k-1})$ $(0 \leq r_k <  r_{k-1}  = r_{k-1})$
$= \gcd(r_k, 0)$	$0 = \text{mod}(r_{k-1}, r_k)$
$= r_k$	

37

## 証明

任意の  $m, n, q, r \in \mathbb{Z}$  に対して,  $m = qn + r$  ならば,  
 $\gcd(m, n) = \gcd(n, r)$ .

- 「 $m$  と  $n$  のすべての非負公約数からなる集合  $D_{m,n}$  と,  
 $n$  と  $r$  のすべての非負公約数からなる集合  $D_{n,r}$  は等しい  
 $(D_{m,n} = D_{n,r})$ 」を示す.
- 等しい集合上の整除関係に関する最大元は等しい.

$m$  と  $n$  のすべての非負公約数からなる集合を  $D_{m,n}$  とし,  
 $n$  と  $r$  のすべての非負公約数からなる集合を  $D_{n,r}$  とする.  
 任意の  $d \in D_{m,n}$  に対して,  $d \mid m$  かつ  $d \mid n$  だから,  $d \mid m - qn$ .  
 ゆえに,  $d \mid r$  だから,  $d$  は  $n$  と  $r$  の非負公約数でもあり,  $d \in D_{n,r}$ .  
 したがって,  $D_{m,n} \subseteq D_{n,r}$ .  
 一方, 任意の  $d' \in D_{n,r}$  に対して,  $d' \mid n$  かつ  $d' \mid r$  だから,  $d' \mid qn + r$ .  
 ゆえに,  $d' \mid m$  だから,  $d'$  は  $m$  と  $n$  の非負公約数でもあり,  $d' \in D_{m,n}$ .  
 したがって,  $D_{n,r} \subseteq D_{m,n}$ .  
 以上から,  $D_{m,n} = D_{n,r}$  だから,  $\gcd(m, n) = \gcd(n, r)$ .

38

## Euclid の互除法の実現

- 入力:  $m, n \in \mathbb{Z}$
- 出力:  $\gcd(m, n)$
- 手順:
 

```

procedure gcd(m, n);
begin
  if n=0 then return(|m|);
  s := m;
  s' := n;
  while s' ≠ 0 do
    begin
      t := s;
      s := s';
      s' := mod(t, s');
    end;
  return(s);
end
            
```

39

## Euclid の互除法の実現(続き)

- 入力:  $m, n \in \mathbb{Z}$
- 出力:  $\gcd(m, n)$
- 手順:
 

```

procedure gcd(m, n);
begin
  if n=0
    then return(|m|)
    else return(gcd(n, mod(m, n))) ← 再帰呼び出し
end
            
```

40

## 定理(停止性と正当性, 計算量)

- Euclid の互除法は, 有限回の計算ステップで停止し,  
 任意の  $m, n \in \mathbb{Z}$  に対して,  $\gcd(m, n)$  を正しく計算する.
- $m, n \in \mathbb{Z} (m \geq n)$  に対して, Euclid の互除法は  
 最大  $\lceil \log_\phi(n) \rceil$  回以下の除法で計算を停止する.  
 ただし,  $\phi = \frac{1+\sqrt{5}}{2}$ 
  - $u \in \mathbb{R}$  に対して,  $\lceil u \rceil$  は  $u$  の小数点以下を切り上げた整数.
- $m, n \in \mathbb{Z} (m > n)$  に対して,  $n$  が10進  $s$  桁ならば,  
 Euclid の互除法は最大  $5s$  回以下の除法で計算を停止する.

41

## まとめ

- 今回の講義
  - 約数・倍数
- 次回の講義
  - 素数(教科書 pp.106-113)
- 今回の演習
  - 束

42