通論 6/29

§4 剰余類と同値関係, 同値類
(equivalence class)

$p>0$ 自然数

$a, b \in \mathbb{Z}$

modulo (pを法として)

$$\boxed{a \equiv b \mod p \overset{\text{def}}{\Longleftrightarrow} a-b \text{ が } p \text{ で割り切れる}}$$

例 $p=3$

$a=1,\ b=7$

$a-b=-6=-2\times p$ 割り切れる.

Th 4.1

$a \equiv a' \mod p$

$b \equiv b' \mod p$

$\Rightarrow a \pm b \equiv a' \pm b' \mod p$

$ab \equiv a'b' \mod p$ —— ①

∵ 似ているので①のみ証明

仮定より

$a-a'=sp$ $\quad s, t \in \mathbb{Z}$

$b-b'=tp$ $\quad$ と書ける

∴ $a=a'+sp,\ b=b'+tp$

$ab=(a'+sp)(b'+tp)$

$=a'b'+p\underbrace{(a't+sb'+stp)}_{\text{整数}}$

単に展開
pで整理

$ab-a'b'$ は p の整数倍

∴ $ab \equiv a'b' \mod p$ //

No.

Th4.1より

≡は＝みたいに扱ってO.K.

たとえば移項もO.K.

$a = b + c \Rightarrow a - c = b$

$\underbrace{a}_{a\text{とみたい}} \equiv \underbrace{b + c}_{a'\text{とおきたい}} \mod p$

両辺に$-c$をたす

$a - c \equiv b + c - c = b \mod p$

$x \equiv 2 \mod 3$となるxは？

$\cdots, 2-6, 2-3, 2, 2+3, 2+6, 2+9, \cdots$

$\quad\quad -4 \quad -1 \quad\quad 5 \quad\quad 8 \quad\quad 11$

○このようなxは、3で割った余りが2となる数である

負の数xをpで割った余りとは？

$x = q \cdot p + r \quad \boxed{0 \leq r < p}$

となるq, rが一意的に存在し、このrを"余り"と数学ではよぶ

例 $x = -4$, $p = 3$

$-4 = \underbrace{-2}_{q} \times p + \underbrace{2}_{r}$

~~Java Script~~ --

$x \% p$ はxをpで割った余りを戻す

$-4 \% 3$ の値は2

例 12^{100}を11で割った余りを求めよ。

答 $12 \equiv 1 \mod 11$

Th4.1より

$12 \times 12 \equiv 1 \times 1 \mod 11$

$\vdots$

$12^{100} \equiv 1^{100} = 1 \mod 11$. ∴ 12^{100}を11で割った余りは1

例 10^{100}を11で割った余りを求めよ.

$10 \equiv -1 \mod 11$

$10^{100} = (-1)^{100} = 1 \mod 11$

答 1.

ユークリッドの互除法

最大公約数
(greatest common divisor)
G C D
を求めるアルゴリズム(計算法)

$a > b > 0$

a, b の最大公約数を $\gcd(a, b)$ と書く.

Th.4.2

$a = \underset{\text{商}}{q}b + \underset{\text{余り}}{r}$, $0 \leq r < b$

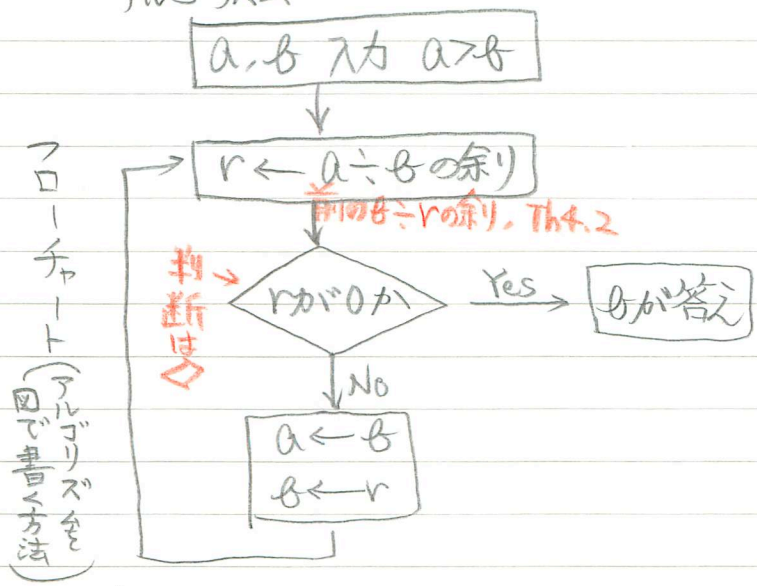
$\gcd(a, b) = \gcd(b, r)$

問6.3

① $d = \gcd(a, b)$
$d' = \gcd(b, r)$ とおく.
dは定義より aもbも割り切る.
$r = \underset{\text{◎}\times d}{a} - q\underset{\triangle\times d}{b}$ とかけるので
dはrも割り切る
よってdは bもrも割り切るので, d'も割る。 ①
(公約数は最大公約数の約数)
逆に, d'は定義より bもrも割り切る
$a = qb + r$と書けるので
d'はaも割り切る
よってd'は aもbも割り切るのでdも割り切る ②
①②より $d = d'$

Th 4.2は互除法の原理

アルゴリズム



例

$a=152$, $b=18$.

$152 = \underset{q}{8} \cdot 18 + \underset{r}{8}$ ——— ①

Th 4.2 $\gcd(152, 18) = \gcd(18, 8)$

$\overset{a}{18} = 2 \cdot \overset{b}{8} + \underset{r}{2}$ ——— ②

Th 4.2 $\gcd(18, 8) = \gcd(8, 2)$

$8 = \boxed{4} \cdot 2 + \boxed{0}$

$\gcd(8, 2) = 2$

答 2

n元連立方程式 の解き方を線形代数で習う.
$x_1, \cdots, x_n$

ここでは

$ax + by = d$ ← 1次不定方程式

$d = \gcd(a, b)$

をみたす整数(x, y)を求めよ

(今の計算の副産物)

という問題の解き方を説明する.

No.

$152x+18y=2$ を解け

②より

$18-2\cdot 8=2$

① $152-8\cdot 18=8$ を代入

$18-2(152-8\cdot 18)=2$

$\underset{x}{-2}\times 152+\underbrace{(1-2\cdot(-8))}_{y}\times 18=2$

$a=4321,\ b=1234$

$\gcd(a,b)=1$

$\overset{a}{4321}=3\cdot\overset{b}{1234}+\overset{r}{619}$ — ①

$1234=1\cdot 619+615$ — ②

$619=1\cdot 615+4$ — ③

$615=153\cdot 4+3$ — ④

$4=1\cdot 3+1$ — ⑤

$4-1\cdot 3=1$

④

$3=615-153\cdot 4$

$4-1\times(615-153\cdot 4)=1$

$(1+153)\times 4-1\times 615=1$

③

$4=619-1\times 615$

$(1+153)\times(619-1\times 615)-1\times 615=1$

$(1+153)\times 619-(1+153+1)\times 615=1$ ← a, bでかける

a, bでかける　　bと619でかける

以下省略

google [15%4] 検索

3と戻す

[cfep/asir] 検索

Mac

KYOKUTO

No.

Th 4.2の系

pを素数

$1 \leq a < p$

$ax \equiv 1 \bmod p$ $1 \leq x < p$

となるxが存在

(不定方程式を解いて求まる)

xをaの逆元という。

∵ $ax + py = 1$ 不定方程式を解く。

を解く(∵ $\gcd(a, p) = 1$)

答えを$\bar{x}, \bar{y}$とする。

$a\bar{x} \equiv 1 \bmod p$

$\bar{x}$をpで割った余りをxとすれば答

例 $p=3$

$1 \times 1 = 1 \bmod 3$

$2 \times 2 = 1 \bmod 3$

1の逆元 1

2 〃 2

問6.1.2

pを素数

aとp 互いに素 つまり

(aは0でなくpの倍数でもない)

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

例) $2^2 \equiv 1 \mod 3$

[問6.1.2の答] $1\cdot a,\ 2\cdot a,\ 3\cdot a,\ \cdots,\ (p-1)\cdot a$　p−1コの数をかんがえる

全部かけると、

$1\times 2\times 3\times \cdots \times (p-1)\times a^{(p-1)} \equiv 1\times 2\times 3\times \cdots \times (p-1) \mod p$

この数をpで割った余りを考えると、集合としては$\{1, 2, 3, \cdots, p-1\}$に等しい

例) $p=5,\ a=2$

$1\times 2 = 2$

$2\times 2 = 4$

$3\times 2 \equiv 1 \mod 5$

$4\times 2 \equiv 3 \mod 5$

(∵) $i \neq j,\ ia \not\equiv ja \mod p$ → 自分で証明を加えよ。

$i, j \in \{1, \cdots, p-1\}$ //

$(1\times 2\times \cdots \times (p-1))\ x \equiv 1 \mod p$

となるxがある（さっきと同様にできる 自分で証明）

①の両辺にxをかけて

$1\times a^{p-1} \equiv 1\cdot 1 \mod p$

$a^{p-1} \equiv 1 \mod p$ //