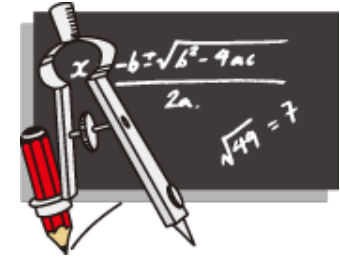


応用数学III

(14)Nを法とする合同式

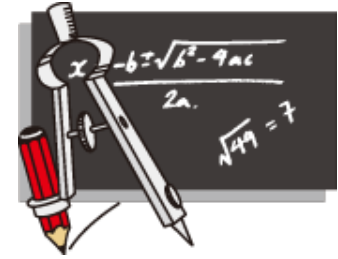
木村真一

講義のスケジュール



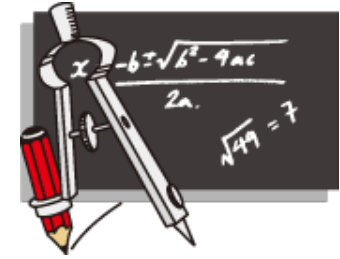
- | | |
|------------------|-----------------------|
| (1) 確率の基礎 | (8) フーリエ解析 |
| (2) 確率変数と確率分布 | (9) フーリエ変換の性質 |
| (3) いろいろな確率分布 | (10) 相関解析 |
| (4) 多次元確率分布 | (11) 不確定信号の相関解析 |
| (5) 大数の法則と中心極限定理 | (12) 群・環・体の定義 |
| (6) 確率過程の基礎 1 | (13) 準同型写像 |
| (7) 確率過程の基礎 2 | (14) Nを法とする合同式 |

割った「あまり」



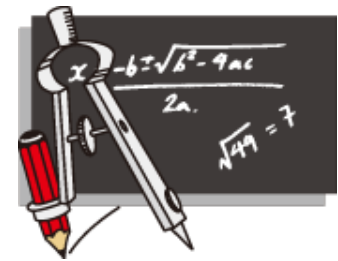
- ある整数を答えを整数として別の整数で割ったときに、「あまり」が出ることがあります。
- この「あまり」を求めるという計算は、いろいろと便利ながあります。
 - 今日が金曜日で、30日後は何曜日？
 - $30 \div 7 = 4 \cdots 2$ 。日曜日。
 - コンピューターのプログラムで変数nを0から5を巡回させたい。
 - $n = (i++) \% 5$;
- 割ったあまりを求めるという関係式は
何と環になるのだっ！！

剰余を扱う準備



- 二つの整数 a, b の最大公約数を (a, b) と書きます。
- (a, b) は正の整数とします。
- $(a, b) = 1$ の時、つまり a と b が公約数を持たないとき、
「 a と b は互いに素である」といいます。
- 2つの整数 a, b に対して、 a が b の倍数であるとき
 $b \mid a$ と書きます。

Nを法とする合同



- 整数 a, b に対して、 $N \mid (a-b)$ であるとき、
「 a と b は N を法として合同である」
と言います。

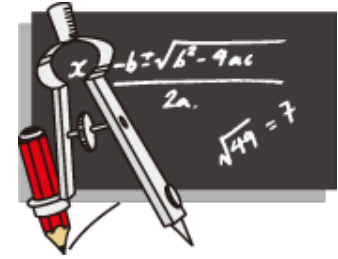
$$a \equiv b \pmod{N}$$

- 例

$$5 \equiv -1 \equiv 23 \pmod{3}$$

$$3 \equiv 25 \equiv -30 \pmod{??} \quad ?? = 11$$

合同式の基本的な性質



- (1) $a \equiv b \pmod{N}$ かつ $b \equiv c \pmod{N}$ ならば

$$a \equiv c \pmod{N}$$

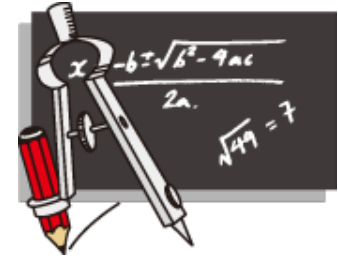
- (2) $a \equiv b \pmod{N}$ かつ $c \equiv d \pmod{N}$ ならば

$$a + c \equiv b + d \pmod{N}$$

$$ac \equiv bd \pmod{N}$$

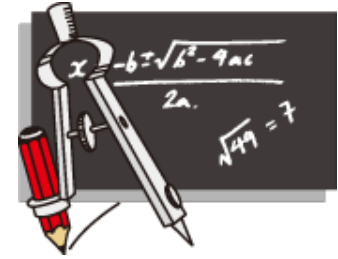
- 何と合同式は普通の等式と同じように、加法・乗法が出来る！！

例題 1



- 4283065591 を9で割ったあまりはいくつでしょう。
- 同じく、4283065591 を11で割ったあまりはいくつでしょう。
- 答え
 - $4283065591 \equiv 4+2+8+3+0+6+5+5+9+1=43$
 $\equiv 4+3=7 \pmod{9}$
 - $4283065591 \equiv 1-9+5-5+6-0+3-8+2-4=-9$
 $\equiv 2 \pmod{9}$

例題 2

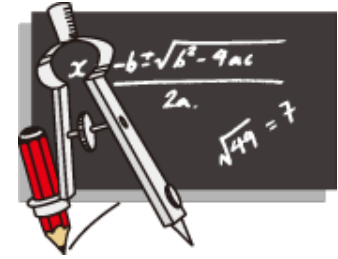


- 4283065591 を37で割ったあまりはいくつでしょう。
- 同じく、4283065591 を7で割ったあまりはいくつでしょう。

- 答え

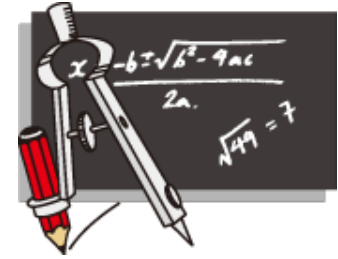
- $4283065591 \equiv 4+283+065+591 \equiv 943$
 $\equiv 18 \pmod{37}$
 - $4283065591 \equiv -4+283-065+591 \equiv 805$
 $\equiv 0 \pmod{7}$

合同類



- 合同式を「環」という考え方で考えてみましょう。
- ある整数 N が設定されると、 N で割ったあまりと言うのは $0, 1, \dots, N-1$ の N 個しかありません。
- 2つの整数が合同になるというのは、 N で割ったときに同じあまりをもつということですから、これを使って整数をグループ分けしてみます。
- N で割ったときに同じあまりを持つ数の集合を
 N を法とする合同類
 といいます。

合同類 (つづき)



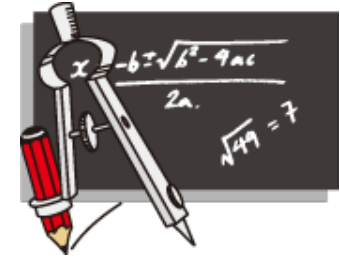
- Nの倍数は符号を変えてもNの倍数です。
- Nの倍数とNの倍数を足したものもNの倍数です。
- ということは、
 Nの倍数の集合は整数の加法に関する部分群
- この部分群をNZと書きます

$$NZ = \{\dots, -2N, -N, 0, N, 2N, \dots\}$$

- Nで割ったときにaと同じあまりを持つ数の集合：合同類
 ：剰余類ともいいます

$$\bar{a} = a + NZ = \{\dots, a - 2N, a - N, a, a + N, a + 2N, \dots\}$$

合同類と合同式



- この表記の仕方を合同式と対応づけてみましょう。

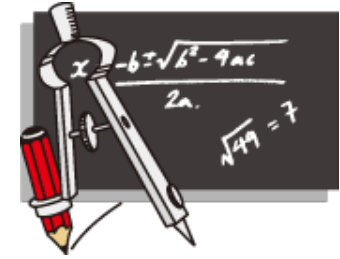
$$\bar{a} = \bar{b} \Leftrightarrow a \equiv b \pmod{N}$$

$$\bar{a} = \bar{b}, \bar{b} = \bar{c} \Rightarrow \bar{a} = \bar{c}$$

$$\bar{a} = \bar{b}, \bar{c} = \bar{d} \Rightarrow \overline{a+c} = \overline{b+d}$$

$$\bar{a} = \bar{b}, \bar{c} = \bar{d} \Rightarrow \overline{ac} = \overline{bd}$$

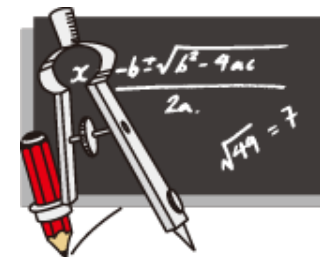
代表元と合同類全体の集合



- 合同類は複数（無限）の数の集合体です。
- その中の一つを選んで代表として扱うことが出来ます。
- だって、どれを代表にしても足したり、かけたりした結果は変わらないからです。
- この代表のことを代表元といいます。
- 合同類全体からなる集合を $Z/(N)$ と呼びます。
- 定義は次の通りです。

$$Z(N) = \{\bar{a} | a \in Z\} = \{\bar{0}, \bar{1}, \dots, \overline{N-1}\}$$

合同類全体の集合は環だ！！

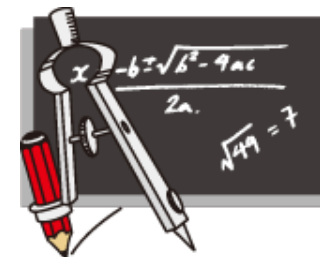


- 合同類の代表元はどれを選んでも同じでしたから、合同類と合同類の加法と乗法は次のように定義できます。

$$\begin{aligned}\bar{a} + \bar{b} &= \overline{a + b} \\ \bar{a}\bar{b} &= \overline{ab}\end{aligned}$$

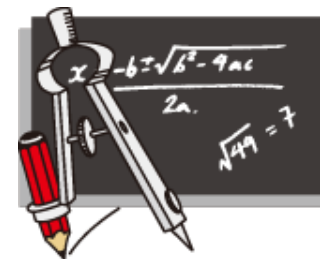
- すると、 $Z(N)$ は環になります。
 - 加法単位元： $\bar{0}$
 - 乗法単位元： $\bar{1}$

合同類の環は不思議な環



- 個数は有限です。
 - N個しかない。
- 有限の要素で環であるためには、計算が巡回します。
 - $\bar{1}$ をN回足し合わせると $\bar{0}$!!
- $\bar{0}$ でない元を掛け合わせて $\bar{0}$ となることがある。
 - $Z(12)$ について $\bar{4} \cdot \bar{3} = \bar{8} \cdot \bar{9} = \bar{6}^2 = \bar{0}$
 - ある環において $y \neq 0$ の y に対して $xy = 0$ となる x が存在するとき、 x の事を「零因子 (れいいんし)」と言います。
 - $n > 0$ に対して $a^n = 0$ となる $a \neq 0$ の事を「幂零元 (べきれいげん)」と言います。

合同類の環は不思議な（つづき）



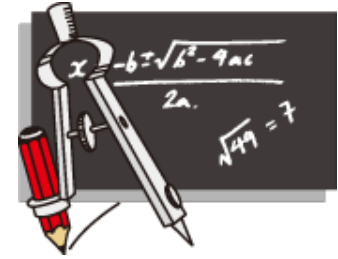
- ・ 零因子が存在するとこんな困ったことが発生します。

- $Z(12)$ について

$$\bar{3} \cdot \bar{5} = \bar{3} \cdot \bar{9} = \bar{3} \quad \text{しかーし！！} \quad \bar{5} \neq \bar{9}$$

- ・ げ！！ということは方程式が解けない！！

何故できる零因子

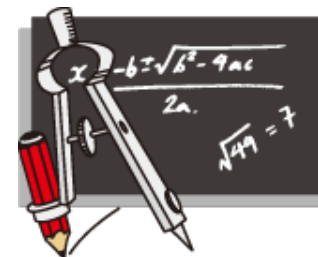


- $(a, N) = 1$ だとしましょう。(Nとaは互いに素)
 - $b \in \mathbb{Z}, \overline{ab} = 0$ のとき $N \mid ab$ ですが、一方で $(a, N) = 1$ ですから、aの因数分解をしてもNは含みません。
 - ということは $N \mid ab$ のNはbが持っていなければなりません。
 - だから $N \mid b$ つまり $\overline{b} = 0$ が言えます。
- もし、 $(a, N) = d > 1$ なら。
 - 少なくとも $b = N/d$ とおくと $\overline{b} \neq 0, \overline{ab} = 0$ が成り立ちます



aが $\mathbb{Z}/(N)$ の零因子 $\longleftrightarrow (a, N) > 1$

逆元の存在



- $(a, N) = 1$ の時、
 $\bar{b}$ に対して $\overline{ab}$ を対応づける写像は全単射

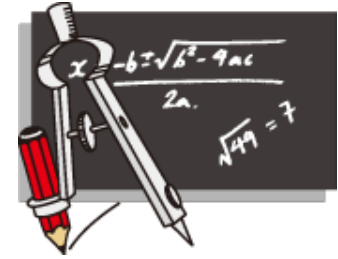


- $(a, N) = 1$ のとき、 $\overline{ab} = \bar{1}$ となる $b \in \mathbb{Z}$ が存在する。

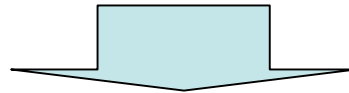


- $\bar{a}$ は乗法に関して逆元を持つ。

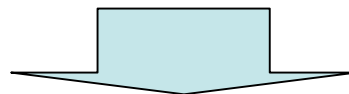
素体



- $N=p$ が素数の場合を考えます。
- p の倍数以外は、全て p と互いに素になります。

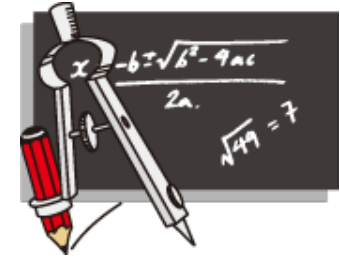


- $\mathbb{Z}/(p)$ の0以外の元は、全て乗法についての逆元を持つ。



- $\mathbb{Z}/(p)$ は体になる！！
- $\mathbb{Z}/(p)$ の事を「素体」と言います。

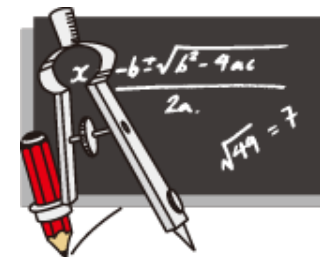
フェルマーの小定理



- p が素数の時、 p の倍数でない任意の整数 a に対して、以下の関係が成り立つ。

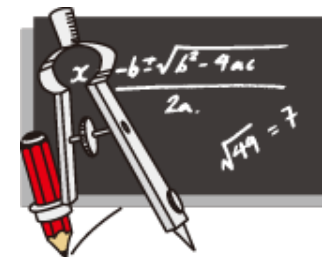
$$a^{p-1} \equiv 1 \pmod{p}$$

循環小数について



- 分数は、割り切れない場合、小数で表すと循環小数になります。
- ところで循環小数をしげしげと眺めてみたことがあります？
 - $1/7 = 0.14285714285714\dots = 0.\dot{1}4285\dot{7}$
 - $2/7 = 0.28571428571428\dots = 0.\dot{2}8571\dot{4}$
 - $3/7 = 0.42857142857142\dots = 0.\dot{4}2857\dot{1}$
 - $4/7 = 0.57142857142857\dots = 0.\dot{5}7142\dot{8}$
 - $5/7 = 0.71428571428571\dots = 0.\dot{7}1428\dot{5}$
 - $6/7 = 0.85714285714285\dots = 0.\dot{8}5714\dot{2}$
- ね。おもしろいでしょ。

何故7桁？



- ・ 循環小数は次のような無限等比級数の和であると考えられます。

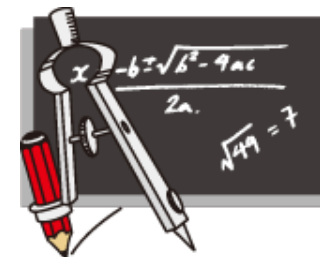
$$\frac{3}{7} = 0.\dot{4}28571 = 0.428571(1 + 10^{-6} + 10^{-12} + \dots)$$

- ・ ここで次の無限等比級数の公式を使って

$$\sum_{k=0}^{\infty} a \cdot r^k = \frac{a}{1-r} \quad (-1 < r < 1)$$

$$\frac{3}{7} = \frac{0.428571}{1 - 10^{-6}} = \frac{0.428571}{10^{-6} - 1}$$

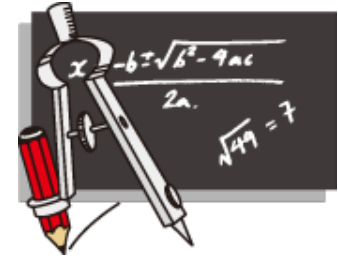
何故7桁？（つづき）



- 7が $10^6 - 1$ の約数。
- もし7より小さいkについて $10^k - 1$ が7で割り切れれば、循環小数はk桁で循環する。
- ここで、 $7 \mid 10^k - 1$ となる最小のkは7

$$7 \mid 10^k - 1 \quad \longleftrightarrow \quad 10^{7-1} \equiv 1 \pmod{7}$$
$$a^{p-1} \equiv 1 \pmod{p}$$

まとめ



- Nを法とする合同式
- 合同類
- 零因子
- 素体
- フェルマーの小定理