SEAGULL TIMES

今回のテーマ…「余りの数と合同式!!」

～代数学を添えて～

Step 1 合同式について知ろう!!

合同式とは…

「割り算の余り」に対する公式!!

実際の大学の教科書では、
aをmで割ったときの余りと
bをmで割ったときの余りが同じであるとき、
aとbはmを法として合同であると言い、

合同式

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

(モード)

と表す。

aを12，bを7を例として代入すると，…
12と7は5で割った余りは同じなので，…

$$12 \equiv 7 \pmod{5}$$

そして，17と2も5で割ったときも余りは同じなので…

$$17 \equiv 12 \equiv 7 \equiv 2 \pmod{5}$$

と表す。

合同式の基本性質

＊ $a \equiv c \pmod{m}$，$b \equiv d \pmod{m}$であるとき，

① $a+b \equiv c+d \pmod{m}$，$a-b \equiv c-d \pmod{m}$

② $ab \equiv cd \pmod{m}$

③ $\boxed{a^k \equiv c^k \pmod{m}}$ ← 今回はこれを使用!!

④ $ab \equiv ac \pmod{m}$で，aとmが互いに素なら $b \equiv c \pmod{m}$

Step 2 実践しよう!!

15^{100}を7で割った余りはいくつでしょうか?

15の100乗なので…

普通に計算は無理ですね!!

合同式を利用してみましょう!!

$15 \equiv 1 \pmod{7}$であるから

$$15^{100} \equiv 1^{100} \pmod{7}$$

1は何回かけても1なので…

$$15^{100} \equiv 1 \pmod{\ }$$

よって余りは1である。

Step 3 実際に国公立大学の入試問題をやってみよう!!

合同式を用いて，次のものを求めなさい。

(1) 19^{200}を6で割った余り

今年は2017年なので…

(2) 2^{2017}を7で割った余り

〈解答〉

(1) $19 \equiv 1 \pmod{6}$であるから

$19^{200} \equiv 1^{200} \pmod{6}$ つまり…

$19^{200} \equiv 1 \pmod{6}$

よって余りは1である。

(2) この問題は$2^? \equiv 1 \pmod{7}$を出せば解ける!!

$2^3 \equiv 1 \pmod{7}$であるから，

$2017 = 3 \times 672 + 1$で

$2^{2017} = (2^3)^{672}$ この場合2016になるので

よって$(2^3)^{672} \equiv 1^{672} \pmod{7}$

2017にするために $\boxed{\times 2}$をかける!!

$2^{2017} \equiv 1 \boxed{\times 2}$

$\equiv 2 \pmod{7}$

よって余りは2である

1年2組 石井琢真 永井駿平 矢澤隼斗 東優希
大塚菜夏 小金澤由佳 鈴木愛唯

シーガルタイムズ

合同式 ……「割り算の余りに対する公式」

○「aをmで割ったときの余り」と「bをmで割ったときの余り」が同じであるときaとbはmを法として合同であるといい、

$a \equiv b \pmod{m}$ が成り立つ。

例) $12 \equiv 7 \pmod{5}$　　$12 \div 5 = 2 \cdots 2$、$7 \div 5 = 1 \cdots 2$　余りが2で等しい

また $a^k \equiv b^k \pmod{m}$ も成り立つ

例) 19^{200}を6で割った余りは？

$19 \div 6 = 3 \cdots 1$　よって　$19 \equiv 1 \pmod{6}$

$19^{200} \equiv 1^{200} \pmod{6}$

すなわち　19^{200}を6で割った余りは　1

ーメンバーー
金井 奏太朗
眞下 智也
相場 優奈
金子 実加彩
定方 美樹
高田 ひより
松岡 ももこ

群 … 集合Gとその集合上の演算・の組が次の3つを満たすとき、そのペア$(G, \cdot)$を群という。

① 任意の$a, b, c \in G$に対して$(a \cdot b) \cdot c = a \cdot (b \cdot c)$（結合法則）

② ある$e \in G$が存在して任意の$a \in G$に対して$a \cdot e = e \cdot a = a$を満たす。（単位元）

③ 任意の$a \in G$に対して、$a \cdot b = b \cdot a = e$を満たす$b \in G$が存在する。（逆元）

剰余類 … 合同式を利用することにより、nで割ったときの余りでグループ分けすること。

Z_3

	1	2
1	1	2
2	2	1

群になる

Z_4

	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

群にならない

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

群になる

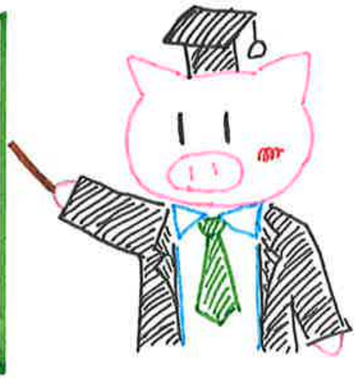
Z_pのPが素数のときは必ず群になる。

シーガルタイムズ

メンバー
粟田 雄空　諸星 和樹
江泉 伽耶　毛塚 利佳子
荒尾 優衣　長谷川 美波

代数学とは!?

数の代わりに文字を用い、計算の法則・方程式の解法などを主に研究する数学の一分野。
現在では、代数系の研究をいう。



例えば・・・

2の2017乗を7で割った余りを求めなさい。

余りが1になるまで累乗する。

$$\begin{cases} 2^1 = 2 \\ 2^2 = 4 \\ 2^3 = 1 \pmod 7 \end{cases}$$

2^3を7で割る余りは1
1を7で割る余りは1

(mod 7) 7で割るという意

$(2^3)^{672} = 1 \pmod 7$

余りが1のものを672乗しても余りは1となる。

$(2^3)^{672}$は2^{2016}なので2^{2017}にするために2をかける。

$$2^{2017} = (2^3)^{672} \times 2$$
$$= 1^{672} \times 2$$

余りが1のものを672乗することと同じ。

よって余りは2

感想

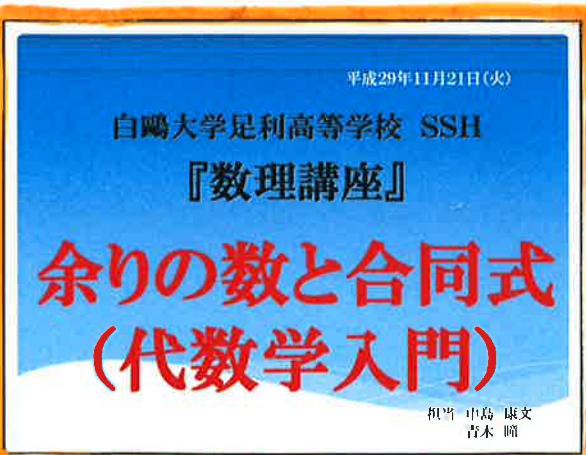
代数学は数学なのに文字が多用されるので、先輩方の中には単位を落とす心配をしている方々がいます。上に挙げた例のような問題は大学1年生で学ぶ、基本的な問題なので、文理選択の際には大学で学ぶ内容に実際に触れてみることが大切だと思いました!!

SSH シーガルタイムズ

久保田 輪
青木 千尋
山崎 日菜乃
河原 涼那
竹内 夏海
茂木 裕太
佐藤 悠

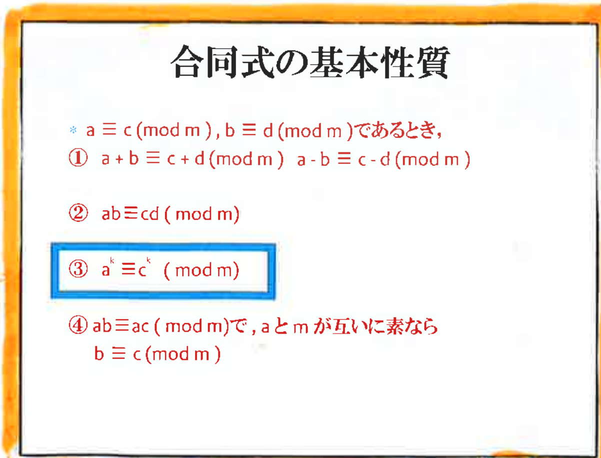
代数学とは，

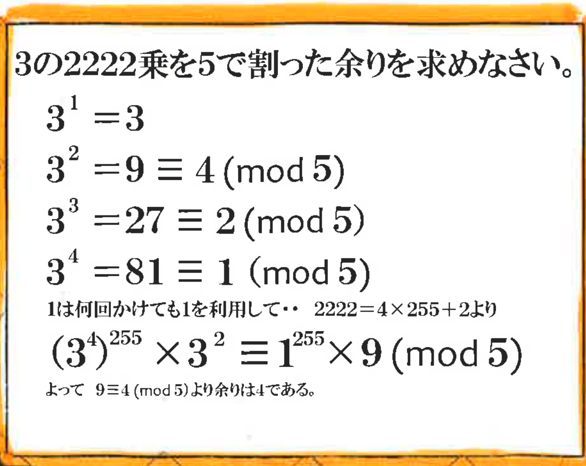
数学の一分野で，「代数」の名の通り数の代わりに文字を用いて方程式の解法を研究する学問。
現代では，代数学はその範囲を大きく広げているため「数の代わりに文字を用いる数学」という理解の仕方は必ずしも適当ではない。



① 私達はSSH「数理講座」で代数学の一分野である合同式について学びました。
合同式とは「割り算の余りの公式」です。

② 合同式の基本性質を利用すると





③ このようにある数を2ケタ以上の数字で累乗したものを，特定の数で割ったときの余りを求めることができます。

シーガルタイムズ

大関拓夢
長竹真吾
渡邉旭
大山美玖
櫻井詩子
関口桜
前川愛友佳

合同式とは？

→割り算の余りの公式

$a \div m$ の余りと
$b \div m$ の余りが同じとき
$a \equiv b \pmod{m}$ と表す

ex) $12 \div 5$ の余りは2
$7 \div 5$ の余りも2
↓
$12 \equiv 7 \pmod{5}$

合同式の性質

$a \equiv c \pmod{m}$ ならば
$a^n \equiv c^n \pmod{m}$

ex) $15 \equiv 1 \pmod{7}$ だから
$15^{100} \equiv 1^{100} \pmod{7}$ となるので
余りは1

3の222乗÷5の余りは $3^1 = 3$
⋮
$3^4 = 81 \equiv 1 \pmod{5}$

$222 = 4 \times 55 + 2$ より
$(3^4)^{55} \times 3^2 \equiv 1^{55} \times 3^2 \pmod{5}$
よって $9 \div 5$ の余りは4なので
余り4

群とは … 今回の場合かけ算のみなので逆元が存在すればよい

逆元 … $a \times \square = 1$ → □にはいる整数があればよい

ex) $a \times \square = 1$ のとき
a の逆元の□は $\frac{1}{a}$ となる
$a = 2$ のとき a の逆元は $\frac{1}{2}$ となり分数なので、これは群ではない

剰余類)

ex) $\mathbb{Z}_3^*$ (3で割ったときの余りのうち0を除いたもの)

	1	2
1	1	2
2	2	1

1の逆元は 1×1 なので1
2の逆元は 2×2 のとき1
→よって群である