岡山高等学校　公開授業

合同式と友達になろう！

～数学 A『整数』～

2016 年2月12日(金)　14:40～15:30　於　岡山中学校・岡山高等学校

授業者　岩手県立大野高等学校　下町　壽男

INDEX

本時の目標

■　自然な考えから「和の余りは余りの和、「積の余りは余りの積」を納得し合同式の理解につなげる。

■　合同式の性質を用いて不定方程式、剰余の問題を解決する。

■ Chapter Ⅰ　アイスブレイク

■ ChapterⅡ　ウォーミングアップ問題

(1)　7777710 を7で割った余りを求めよ。また 777777723 を7で割った余りを求めよ。

(2)　A=7777710 ， B=777777723 とすると、2A＋B＋AB を7で割った余りはどうなるだろうか。
グループで考えてみよう。

(3)　x の整式 $f(x)$ を$x-1$ で割った余りが4、を x^2+x+1 で割った余りが x である。
このとき、$f(x)$ をx^3-1 で割った余りを求めよ。

■ Chapter Ⅲ　合同式の定義・性質

1　合同式の定義

m は自然数とする。2つの整数 a, b について $a-b$ が m の倍数であるとき、

「a と b は法 m（moduras）について合同(congruence)である」

（「a と b は m を法として合同」）といい、 $\boldsymbol{a \equiv b \pmod{m}}$ と表す。

このような式を**合同式**という。

この式は、「a を m で割った余りと、b を m で割った余りが等しい」

とイメージしておけばよい。

合同式については次の「**同値関係**」が成り立つ。

[1]　$a \equiv a \pmod{m}$（反射律）

[2]　$a \equiv b \pmod{m}$ のとき $b \equiv a \pmod{m}$　（対称律）

[3]　$a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$ のとき $a \equiv c \pmod{m}$　（推移律）

※つまり「≡」は「＝」と同じ「同値関係」なので、「＝」で行うことと

ほぼ同じことが「≡」でもできる。

2　合同式の性質

$a \equiv c \pmod{m}$, $b \equiv d \pmod{m}$ のとき

① $a+b \equiv c+d \pmod{m}$

② $a-b \equiv c-d \pmod{m}$

③ $ab \equiv cd \pmod{m}$

③の系 $a^k \equiv c^k \pmod{m}$

※ $ca \equiv cb \pmod{m}$ のとき

$$a \equiv b \left(\mathrm{mod}\ \frac{m}{d}\right)$$

（ただし d は c と m の最大公約数

3　覚えておきたい定理

p を素数，m, n を整数とするとき

$(m+n)^p \equiv m^p + n^p \pmod{p}$

p を素数，a を自然数とし，$(a, p)=1$ とすると

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

注 $(a, p)=1$ とは a と p の最大公約数が１であること

【メモ】

■ Chapter Ⅳ　問題に挑戦

【べき乗の余りの問題】

(1)　23^{2016} を 7 で割ったときの余りを求めよ。★

(2)　$10^{100}+11^{100}$ を 7 で割ったときの余りを求めよ。★★

(3)　整数a, b, c に対して $a^2+b^2-6ab=c^2$ が成り立つとき、a, b の少なくとも一方は 3 の倍数であることを示せ。★★★

【不定方程式】 ★★

(1)　よしひろさんは、1個 300 円のケーキと、1個 350 円のケーキを合せて  個買い、3300 円はらいました。300 円のケーキと 350 円のケーキをそれぞれ何個買ったのでしょう(どちらも少なくとも 1 個は買っています)。　（「東京書籍　中学数学 2 年」の問題より一部改題）

(2)　不定方程式 $92x+197y=1$ を満たす整数 x, y の組の中でx の絶対値が最小のものを求めよ。
（2016　センター試験）

※　不定方程式(ベズーの等式)の問題は後でユークリッドの互除法を学んだあとに出てきます。ここでは、合同式を用いて解く手法を考えます。

COFFEE　BREAK

私の薦めるこの一冊

博士の愛した数式／小川洋子(新潮社)

80 分しか記憶が持たない数学者「博士」と「私」と「ルート」のピュアで，知的で，そして切ない愛の物語．博士の愛した数式はご存知 $e^{\pi i}+1=0$ だが，このストーリー全体のモチーフとして「完全数」を中心とした数論の面白さが取り上げられている．生徒に読ませたいし，この本を使って授業を展開するのも面白い．尚，著者と藤原正彦氏の対談集「世にも美しい数学入門」(ちくまプリマー)もお薦め．

＜抜粋　完全数の話＞

「一つ、私の発見について、お話しても構わないでしょうか」小枝が動きを止め、沈黙が戻ってきた時、自分でも思いがけないことを口走っていた。レース模様の美しさに心を奪われ、自分もそこに加わってみたくなったのかもしれない。そして私は、博士がその幼稚すぎる発見を、決して粗末に扱ったりはしないと確信していた。

「28 の約数を足すと、28 になるんです」

「ほう…」

博士はアルティン予想についての記述の続きに、

28＝1+2+4+7+14　　と書いた。

「完全数だ」

「カンゼン、数」　揺るぎない言葉の響きを味わうように、私はつぶやいた。

「一番小さな完全数は6。6=1+2+3」

「あっ、本当だ。別に珍しくないんですね」

「いいや、とんでもない。完全の意味を真に体現する、貴重な数だよ。28 の次は 496。

496=1+2+4+8+16+31+62+124+248。その次は　8128。その次は 33550336。次は 8589869056。数が大きくなればなるほど、完全数を見つけるのはどんどん難しくなる」

億の桁の数字を博士が苦もなく導き出しているのに、私は驚いた。

「当然、完全数以外は、約数の和がそれ自身より大きくなるか、小さくなるかだ。大きいのが過剰数、小さいのが不足数。実に明快な命名だと思わないかい？18 は 1+2+3+6+9=21 だから過剰数だね。14 は 1+2+7=10 で、不足数になるわけだ」

私は 18 と 14 を思い浮かべた。博士の説明を聞いたあとでは、それらは最早ただの数字ではなかった。人知れず 18 は過剰な荷物の重みに耐え、14 は欠落した空白の前に、無言でたたずんでいた。

「1だけ小さい不足数はいくらでもあるのだが、1だけ大きい過剰数は一つも存在しない。いや、誰も見つけられずにいる、というのが正しい言い方かもしれん」

「何故見つからないんでしょう」

「理由は、神様の手帳にだけに書いてある」

日差しは柔らかく、目に映るものすべてに平等に降り注いでいた。噴水に浮かぶ虫の死骸さえ、輝いて見えた。胸元の一番大事なメモ＜僕の記憶は 80 分しかもたない＞が外れそうになっているのに気づき、私は手をのばしクリップを留め直した。

「もう一つ、完全数の性質を示してみよう」

博士は小枝を握り直し、両足をベンチに引っ込ませて空いた地面を確保した。

「完全数は連続した自然数の和であらわすことができる」

6=1+2+3

28=1+2+3+4+5+6+7

496=1+2+3+4+5+6+7+8+9+10+11+12+13+14+15+16+17+18+19+20+21+22+23+24+25+26+27+28+29+30+31

博士は腕を一杯にのばし、長い足し算を書いた。それは単純で規則正しい行列だった。どこにも無駄がなく、研ぎ澄まされ、痺れるような緊張感に満たされていた。　(「博士の愛した数式」／小川洋子　より抜粋)

チャレンジ問題

$A=2^{p-1}(2^p-1)$　(2^p-1は素数) のとき，A は完全数であることを証明せよ．
また偶数の完全数はA の形に限ることを示せ．