整数の下二桁の値のちょっとした小手技

札幌旭丘高等学校　中村文則

○まなぶライクな合同式の扱い方

<先　生> 今日は、今年の年号にちなんだ問題を考えてみようか。

> $N=2013^{2013}$ について次の数を求めよ。
> (1) 一の位の数
> (2) 十の位の数

<アリス> わっ、マニアックですね。今年は 2013 年だから、その累乗ということですか。
<まなぶ> だからといって、年号をさらにその年号の数だけ累乗する必要はないと思う。ここまでしてしまうと重箱の隅をほじくるようなマニアックさで、変質的オタク側の境界線に近づいている。
<よしお> でも、常用対数を用いて桁数や最高位の数を求める問題で似たようなものがありましたね。
<まなぶ> 全然違うだろ。桁数問題は指数の底を 10 にすることで数の大きさを大雑把に調べることができるから、近似という意味で価値があるけど、この問題は一や十の位の数だろ。そんなゴミみたいに小さな数を調べていったい何の得があるわけ。
<かず子> 数学はまなぶのように損得を考えて打算的にするものではないでしょ。あんたの方がよっぽどゴミみたいに小さいと思うけど。問題の(1)にしてもよく桁数問題では最高位の数とペアと出題されている問題だし。
<アリス> 確か累乗をすると一の位がどのように変化していくか調べたのですよね。この場合は、

$2013^1=2013 \quad 2013^2=4052169$

何か計算が大変そう。
<よしお> 正確に計算する必要はないと思うよ。調べればいいのは一の位だけだから、その位の数の変化だけ追っていけばいい。2 乗は、2013 の 3 同士を掛ければいいから $3^2=9$ になる。次の 3 乗は、9 に 2013 の 3 を掛けた一の位だから 7 が得られる。
<まなぶ> ということは、4 乗は 7 に 3 を掛けると、おっ、1 になったぞ。これで数字のサイクルがみえてきた。

$3 \Rightarrow 9 \Rightarrow 7 \Rightarrow 1 \Rightarrow 3 \Rightarrow 9 \Rightarrow 7 \Rightarrow 1 \Rightarrow \cdots$

4 乗する度に 1 が現れるってことだな。
<かず子> 解答のいいところだけはしっかりキープするのね。そうすると、

$2013=4\times503+1$

だから、503 回繰り返した後の 1 回目だから 3 が答えですね。
<先　生> OK。では(2)はどう解く。
<アリス> 今度は、累乗したときの十位までの数の規則性を調べればいいということですね。
<かず子> でもそれは大変よ。一の位だと長くてもそのサイクルは 10 の間隔だけど、この場合はどれだけ長くなるか見当もつかないわ。それをやっていたら本当に数字のオタクになっちゃう。
<先　生> そうだね。そこで(2)を考えるために、もう一度(1)の一位の数の求め方を整理してみよう。数 N に対して、一の位の数を次のように考えてみる。

> N を 10 で割ったときの余りが N の一位の数である。

<まなぶ> N から十の位以上を除けばいいわけだから、もっともではある。
<かず子> なに偉そうにいっているの。そうかぁ、このことから一位の数を求めることは余りの問題として処理できるということですね。
<よしお> ということは、

$$N\equiv 2013^{2013} \pmod{10}$$

である N を求めればいいことになる。ずいぶん見方が変わってきますね。

$$2013=10\times201+3$$

だから、$N\equiv 3^{2013} \pmod{10}$
すっきり整理できますね。
<まなぶ> なるほど、これだと簡単な問題だ。

$3^2=9,\ 3^3=27,\ 3^4=81$　より、$3^4\equiv 1 \pmod{10}$

これが先ほどの 4 乗のサイクルということか。

$$N\equiv 3^{2013}\equiv (3^4)^{503}\cdot 3\equiv 3 \pmod{10}$$

言葉での説明がいらないから解答も随分ラクになった。

<かず子> まなぶの思考の行き着く先は、結局はラクであるかどうかなのね。この方法は(2)でも使えますね。

N を 100 で割ったときの余りが N の十位以下(下 2 桁)の数である。

この考え方だと、(1),(2)の両方が同時に求められるから、ラクしたいまなぶにとっては最高よね。

<先　生> 確かに「まなぶライク」な方法かもしれない。これを合同式で表すとどうなる。

<まなぶ> なに、その「まなぶライク」って。先生もだんだん「かず子ライク」になってきてるんじゃない。さてと、

$$N \equiv 2013^{2013} \pmod{100}$$

ここで、$2013 = 20 \times 100 + 13$ だから、

$$N \equiv 13^{2013} \pmod{100}$$

でも、13 の累乗か。これもまた面倒だなあ。

<かず子> そうでもないと思うわ。

$13^2 = 169$　だけど、$169 = 100 + 69$ だから、

$$13^2 \equiv 69 \pmod{100}$$

百位以上は切り捨ててしまえばいいってことよね。

<アリス> なるほどね。後はサイクルを見つけるために 100 を法として累乗と 1 に合同になるものを見つければいいのね。

69 の平方は一位が 1 になるのがすぐ分かるから、

$$13^4 \equiv 69^2 \equiv 61 \pmod{100}$$

残念、1 にならないわ。

<よしお> 頑張って続けるしかないね。13^4 の一位は 1 なのだから、これからひたすら平方の値を計算してみよう。

$$13^8 \equiv 61^2 \equiv 21 \pmod{100}$$

$$13^{16} \equiv 21^2 \equiv 41 \pmod{100}$$

$$13^{32} \equiv 41^2 \equiv 81 \pmod{100}$$

うーん、厳しいな。

<先　生> 少し十位の数の規則性を考えてみてはどうかな。一位は 1 であるから、あとは十位が 0 になればいい。

一位が 1 である 2 桁の整数は、

$10a+1, 10b+1$（a, b は一桁の自然数）

と表される。その積はどうなる。

<まなぶ>　$(10a+1)(10b+1) = 100ab + 10(a+b) + 1$

ということは合同式で表すと、

$$(10a+1)(10b+1) \equiv 10(a+b) + 1 \pmod{100}$$

そうか、十位の和が 10 になればいいということか。

<アリス> それだったらすぐ見つかるわ。よしおが計算した式をみると、

$13^8 \equiv 21 \pmod{100}$ 、$13^{32} \equiv 81 \pmod{100}$

これから、$13^{40} \equiv 1 \pmod{100}$　だわ。

<かず子> アリスが最初に計算した式を使った方がもっといいと思う。

$13^4 = 61 \pmod{100}$, $13^{16} \equiv 41 \pmod{100}$

だから、$13^{20} \equiv 1 \pmod{100}$

<よしお>　これで循環サイクルの長さが分かりました。

$$2013 = 20 \times 100 + 13$$

より、$13^{2013} \equiv 13^{13} \pmod{100}$

ですね。最後に 13 の 13 乗を求めればいい。

<まなぶ> これもさきほどの計算結果が使える。

$$13^{12} \equiv 13^4 \cdot 13^8 \equiv 61 \cdot 21 \equiv 81 \pmod{100}$$

これより、

$$13^{13} \equiv 13^{12} \cdot 13 \equiv 81 \cdot 13 \equiv 53 \pmod{100}$$

できた！。十位の数は 5 で一位の数は 3 だ。

でも、(2)の結果は(1)を含んでいるから、(1)を先に解いたことが何か損したような気分になる。

<先　生>　(2)の問題はは(1)の考え方を応用してるのだし、(2)だけではその考え方を理解するのは難しい。

それにこの方法は、言葉による説明を省略し合同式の記号を用いて簡潔に計算できるわけだから、

実に「まなぶライク」な解法といえる。

<アリス> そうですね。でも、「まなぶライク」と「まなびライク」は似て非なるものですよね。たった一字しか違わないのにどうしてこんなに合同からかけ離れているのかしら。不思議ですね。

<まなぶ> ……

<かず子> ……、アリスって、キツイ娘だったのね。

あとがき

平成 24 年、ゆとりを残しつつ生きる力を育むことを目標に改訂された学習指導要領に則り、生きることを許されなかった分野、生きることを引き続きあるいは新たに許された分野で数学は再編成され、先行実施することになった。

行列は消え、替わって複素数平面が復活したが、数学Ⅲの限られた選択者に対してのものである。その内容も、点の変換のみを扱い行列による図形変換の面白みはなく以前の複素数平面の完全復活には至っていない。これに対して、整数の性質は、過去の学習指導要領の履修内容にかなり近づいたものといえる。

昔のある大学受験参考書の「はしがき」を読んでみると、「整数」に関しては次のように記述があった。

整数のもつ美しい性質の紹介と、それを保証する理論展開の面白さを伝えることである……、整数問題は毎年どこかの大学で出題される……、1977 以降の大学の入試問題を材料として解説し……、整数の理論を進める上で、どうしても欠かせないものは「合同式」であり、この合同式から「フェルマーの定理」「オイラーの定理」が導かれることを説明した。

かつて整数論は大学入試問題の花形であり、その内容はまさに美しく、面白いものであった。今回の改訂では合同式は「発展」の扱いではあるが、それでも教科書に掲載されているのだから現場は指導するだろうし今後は堰を切ったように入試では出題されるかもしれない。そこで、本文でも、かる〜く合同式の小手技を扱ってみた。

実は、小手技としては 3^{20} の下二桁の数について 2000 年に執筆した「対数の桁数問題の小手技」で触れている。この頃の学習指導要領はもちろん合同式はないため、電卓や近似式を用いての解法であった。これも合同式を用いると、「まなぶライク」な姿勢で解答が導けることになる。本文の問題もその観点からもう少し深めて考察してみよう。

まず、2013^{2013} の十位以下の数であるが、

$$N \equiv 2013^{2013} \equiv 13^{2013} \pmod{100}$$

として本文は進めている。ここで、二項定理

$$(a+b)^n = a^n + {}_nC_1 a^{n-1}b + {}_nC_2 a^{n-2}b^2 + \cdots + {}_nC_{n-1} ab^{n-1} + b^n$$

より、$a=3, b=10, n=2013$ とすると、

$$N \equiv 13^{2013} \equiv 3^{2013} + 2013 \cdot 3^{2012} \cdot 10 \pmod{100} \qquad \cdots\cdots(*)$$

となる。結局 N は 3 の累乗の下 2 桁の数を求める問題に帰結する。

$$3^2 \equiv 9 \pmod{100}\ ,\ 3^4 \equiv 81 \pmod{100}$$

を用いると、

$$3^8 \equiv 81 \cdot 81 \equiv 61 \pmod{100}\ ,\ 3^{12} \equiv 3^4 \cdot 3^8 \equiv 81 \cdot 61 \equiv 41 \pmod{100}$$

これから、

$$3^{20} \equiv 3^8 \cdot 3^{12} \equiv 61 \cdot 41 \equiv 1 \pmod{100}$$

よって、$3^{2012} \equiv \left(3^{20}\right)^{100} \cdot 3^{12} \equiv 41 \pmod{100}$

$$3^{2013} \equiv 3^{2012} \cdot 3 \equiv 41 \cdot 3 \equiv 23 \pmod{100}$$

(*)に代入すると、

$$N \equiv 23 + 2013 \cdot 41 \cdot 10 \equiv 53 \pmod{100}$$

本文に較べ多少難しくなった印象はあるかもしれないが、この方法は下 3 桁の数を求める場合も有効である。

$$N \equiv 2013^{2013} \equiv 13^{2013} \pmod{1000}$$

二項定理より

$$N \equiv 3^{2013} + 2013 \cdot 3^{2012} \cdot 10 + 2013 \cdot \frac{2012}{2} \cdot 3^{2011} \cdot 100 \pmod{1000}$$

あとは、

$$3^{\alpha} \equiv 1 \pmod{1000}$$

となる α を見つければよい。ここで、

$3^{10} = 59049$　すなわち、　$3^{10} \equiv 49 \pmod{1000}$

これより、

$$3^{20} \equiv 49^2 \equiv 401 \pmod{1000}$$

下 2 桁が 01 である 3 桁の 2 つの数を

$100a+1, 100b+1$（a, b は 1 桁の自然数）

とするとその積は、

$$(100a+1)(100b+1) \equiv 100(a+b)+1 \pmod{1000}$$

したがって、3^{20} を 5 回掛けると、

$$\left(30^{20}\right)^5 \equiv (41)^5 \equiv 1 \pmod{1000}$$

$$\therefore\quad 3^{100} \equiv 1 \pmod{1000}$$

これから、

$3^{2011} \equiv \left(3^{100}\right)^{20} \cdot 3^{10} \cdot 3 \equiv 49 \cdot 3 \equiv 147 \pmod{1000}$

$3^{2012} \equiv 3^{2011} \cdot 3 \equiv 147 \cdot 3 \equiv 441 \pmod{1000}$

$3^{2013} \equiv 3^{2012} \cdot 3 \equiv 441 \cdot 3 \equiv 323 \pmod{1000}$

以上より、

$N \equiv 323 + 2013 \cdot 441 \cdot 10 + 2013 \cdot 1006 \cdot 147 \cdot 100 \equiv 323 + 330 + 600 \equiv 253 \pmod{1000}$

N の下 3 桁は 253 である。。

次に、さらに「まなぶライク」な解法を探ってみよう。

Ex1) 7^{77} を 13 で割った余りを求めよ。

解) 指数の 77 を 2 進数展開をすると、

$77 = 1001101_{(2)}$

これから、$77 = 2^6 + 2^3 + 2^2 + 1$ となる。ここで、

$7^1 \equiv 7 \pmod{13}$

$7^2 \equiv 49 \equiv 10 \pmod{13}$

$7^4 \equiv 10^2 \equiv 100 \equiv 9 \pmod{13}$

$7^8 \equiv 9^2 \equiv 81 \equiv 3 \pmod{13}$

$7^{16} \equiv 3^2 \equiv 9 \pmod{13}$

$7^{32} \equiv 3 \pmod{13}$

$7^{64} \equiv 3^2 \equiv 9 \pmod{13}$

これより、

$7^{77} \equiv 7^{64+8+4+1} \equiv 9 \cdot 3 \cdot 9 \cdot 7 \equiv 9 \pmod{13}$

このように指数を 2 進数に展開し、べき乗の積を求めると計算は容易になる。2013 乗についても、

$2013 = 11111011101_{(2)}$

であるから、$2013 = 2^{10} + 2^9 + 2^8 + 2^7 + 2^6 + 2^4 + 2^3 + 2^2 + 1$

そして、13 の累乗である $13^2, 13^4, 13^8, \cdots 13^{1024}$ を 100 で割った余りを規則正しく、そして根気強く計算していけばよい。

同じようにすると下 3 桁の数も求めることは可能である。しかし、ここで

$3^{\alpha} \equiv 1 \pmod{1000}$

となる α を見つけることができれば、もっと「まなぶライク」な解法といえる。

実は、その値は、次の定理から得ることができる。

> $n > 1, a > 0$ のとき、$(a, n) = 1$ であれば、
>
> $a^{\varphi(n)} \equiv 1 \pmod{n}$

この性質をオイラーの定理という。

なお、$(a, n) = 1$ は、a と n は互いに素であることを表す。

また、$\varphi(n)$ は、n を自然数とするとき、n と互いに素である n 以下の自然数の個数を表し、

この関数 $\varphi(n)$ をオイラー関数という。

Ex2) $\varphi(12)$ を求めよ。

解) 分母が 12 で分子が 1～12 の分数を考える。

$$\frac{1}{12}\ \frac{\cancel{2}}{\cancel{12}}\ \frac{\cancel{3}}{\cancel{12}}\ \frac{\cancel{4}}{\cancel{12}}\ \frac{5}{12}\ \frac{\cancel{6}}{\cancel{12}}\ \frac{7}{12}\ \frac{\cancel{8}}{\cancel{12}}\ \frac{\cancel{9}}{\cancel{12}}\ \frac{\cancel{10}}{\cancel{12}}\ \frac{11}{12}\ \frac{\cancel{12}}{\cancel{12}}$$

この中で既約分数でないものの個数を求めると、$\varphi(12) = 4$

オイラー関数の値は、n を素因数分解して、

$n = a^{p_1} \cdot b^{p_2} \cdot c^{p_3}$

となるとき、

$\varphi(n) = n(1-a)(1-b)(1-c)$

で与えられる（証明はそれほど難しいものではない）。

Ex2 の場合は、

$12 = 2^2 \cdot 3$ であることから、$\varphi(12) = 12 \times \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 4$ である。

さて、ここで $N \equiv 13^{2013} \pmod{1000}$ の話に戻し、オイラーの定理を用いて考察してみよう。

$100 = 2^2 \cdot 5^2$ より、$\varphi(100) = 100 \times \left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 40$ である。

また、13 と 100 は互いに素であるから、オイラーの定理より、

$$13^{40} \equiv 1 \pmod{100}$$

である。同様に、13 と 1000 は互いに素より、

$$\varphi(1000) = 1000\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 400$$

これから、 $13^{400} \equiv 1 \pmod{1000}$ が見つかる。

すなわち、

$$N \equiv 13^{2013} \equiv \left(13^{400}\right)^5 \cdot 13^{13} \equiv 13^{13} \pmod{1000}$$

次に、$13 = 1101_{(2)} = 2^3 + 2^2 + 1$ であるから、

$13^1 \equiv 13 \pmod{1000}$

$13^2 \equiv 169 \pmod{1000}$

$13^4 \equiv (169)^2 \equiv 561 \pmod{1000}$

$13^8 \equiv (561)^2 \equiv 721 \pmod{1000}$

この累乗の値を用いると、

$13^{13} \equiv 13^8 \cdot 13^4 \cdot 13^1 \equiv 721 \cdot 561 \cdot 13 \equiv 253 \pmod{1000}$

このように合同式の性質を用いることで簡単に下 3 桁が求められるのである。
もちろんこれは 2013 年という年号の特殊性に依るところは大きい（1000 と互いに素であることや、百位が 0）。
しかし、整数の性質を理解しておけばまた別のアプローチやいろいろな問題への応用も可能になるのである。

オイラーの定理において、自然数 n を素数 p としてみる。

$$\varphi(p) = p - 1$$

は明らかであるから、

> p は素数で、$(a, p) = 1$ であれば、
> $a^{p-1} \equiv 1 \pmod{p}$

この性質をフェルマーの定理という。

Ex3) n を自然数とする。$N = n^5 - n$ は 30 の倍数であることを証明せよ。

証明) 5 は素数であるから、フェルマーの定理より、

$$n^4 \equiv 1 \pmod{5}$$

これから、$n^5 - n \equiv 0 \pmod{5}$

よって、$n^5 - n$ は 5 の倍数である。

また、$n^5 - n = (n-1)n(n+1)(n^2+1)$ から、

$(n-1)n(n+1)$ は連続する 3 つの整数の積より 6 の倍数でもある。

5 と 6 は互いに素であるから、以上より、N は 30 の倍数である

Q.E.D

合同(記号≡,congruent)の考えと、その法(modulo)を表す記号 mod を考案したのはドイツの大数学者ガウス(1777-1855)である。ガウスは整数の性質を整数そのものをみるのではなく、整数全体をある数で割った余り(剰余)の集合に分類することから考察した。合同式を用いると、「p を奇数の素数とするとき、p の倍数より 1 だけ少ない平方数」は、まなぶライクに $x^2 \equiv -1 \pmod{p}$ と表すことができる。この解の存在を含めガウスは 19 歳のときに、その著書「数論研究」で、ある条件のもとでは合同式の法と剰余を入れ替えることが可能である性質を用いて導いている。その美しい性質が平方剰余の相互法則であり、「初等整数論の中の宝石」と称される。ガウスは生涯、相互法則に 7 通りの異なる証明を与えている。そして、合同式の考え方は代数的整数論のみならず、幾何学・代数学にも大きな影響を与えていくのである。

過去の学習指導要領の元での教科書にはオイラーやフェルマーの定理を載っているわけではない。しかし、その当時の大学受験の問題集や参考書では、入試で出題されることもあり、当然の如く解説されていたし、またそれはガウスのような大数学者の業績に触れることのできる嬉しい機会でもあった。数理重視の切り札の一つとして復活した整数の性質は、随分昔に扱われたものであり、現場で指導したことのない教師が大多数かもしれない。その指導法もまだまだ未開拓といえる。

この古くて新しい素晴らしい分野に対し、本研究会においても多くの先生方の指導実践とそのあいのりを望みたいと思う。