第3章　整数の性質

第1節　約数と倍数

研究　割り算の余りの性質

発展　合同式

最初に申しますが,『合同式』の扱いにはある程度の慣れと経験が必要です．見よう見まねでよいから，いろいろ式をいじくってみることです．その過程において，式変形のコツを掴んでください．

合同式の基本事項については犬プリ「整数問題原則編」にまとめてあるので，必ず見といてください．

250 このような問題で『合同式』が威力を発揮します．『合同式』の典型的な計算方法なので，式変形をボ〜ッと眺めるのではなく，なぜ，そうするのか，なぜ，そうすればうまくいったのか，をしっかりと考えてください．

(1)　パッと見た瞬間に，$37 \equiv 1 \pmod 6$ であることに気づくと思います (ていうか気づいてほしい)．となれば，合同式の計算法則にしたがって計算するだけです．

$$37^{100} \equiv 1^{100} \equiv 1 \pmod 6$$

このように「1 と合同になる」というのがポイントで，(2) 以降，そのようなポイントを自分で探すことになります．

(2) は (1) と違って，見た瞬間に計算はできませんが，5^2，5^3，$\cdots$，を順番に計算して 8 で割った余りを考えると，$5^2 \equiv 1 \pmod 8$ であることが分かります．この関係を利用します．

$$5^{80} \equiv (5^2)^{40} \equiv 25^{40} \equiv 1^{40} \equiv 1 \pmod 8$$

(3) も (2) と同様に，まずは，3^2，3^3，$\cdots$，を順番に計算して 13 で割った余りを考えると $3^3 \equiv 1 \pmod{13}$ であることが分かります．この関係を利用します．ただ今回は 100 乗なので，$100 = 3 \times 33 + 1$ より 1 個余ることに注意しよう．

$$\begin{aligned} 3^{100} &\equiv 3^1 \cdot (3^3)^{33} && \pmod{13} \\ &\equiv 3^1 \cdot 27^{33} && \pmod{13} \\ &\equiv 3 \cdot 1^{33} && \pmod{13} \\ &\equiv 3 && \pmod{13} \end{aligned}$$

(4) も (3) と全く同様です．これは自分で考えてください．

大切なことは，このように，自分で計算して余りが 1 と合同になるタイミングを探すことです．

251 (1)　n が 8 で割って余る数なので，合同式を用いて表すと $n \equiv 3 \pmod 8$ となります．したがって，

$$\begin{aligned} n^2 + 2n + 5 &\equiv 3^2 + 2 \cdot 3 + 5 \\ &\equiv 20 \equiv 4 \pmod 8 \end{aligned}$$

となります．

注 もし『合同式』用いないなら，$n = 8k+3$ とおいて，

$$\begin{aligned} n^2 + 2n + 5 &= (8k+3)^2 + 2(8k+3) + 5 \\ &= 64k^2 + 48k + 9 + 16k + 6 + 5 \\ &= 64k^2 + 64k + 20 \\ &= 8(8k^2 + 8k + 2) + 4 \end{aligned}$$

したがって，$n^2 + 2n + 5$ を 8 で割った余りは 4 だと分かります．この解答からもわかるように，合同式の計算は，余りの部分だけに注目して計算しただけのことです．

(2)　普通に考えれば，$n \equiv 15 \pmod{17}$ あるいは $n = 17k + 15$ ということになるでしょうが，ちょっと工夫すれば少し計算を軽くすることができます．例えば 3 で割った余りで分類するとき，

$$3k, \quad 3k+1, \quad 3k+2$$

とする代わりに

$$3k, \quad 3k+1, \quad 3k-1$$

しましたね．あの感覚です．

(3) は別にやらなくても良いでしょう．(1)(2) と全く同じなので．

252 (1)　$214n + 120 \equiv 0 \pmod 9$ をみたす n を求めよ，ということなので，まずは係数を小さくしてみます．$214 = 9 \cdot 23 + 7$，$120 = 9 \cdot 13 + 3$ なので，

$$7n + 3 \equiv 0 \pmod 9$$

ですが，もう少し係数を小さくして変形してみます．

$$\begin{aligned} 7n &\equiv -3 \pmod 9 \\ -2n &\equiv -3 \pmod 9 \\ 2n &\equiv 3 \pmod 9 \end{aligned}$$

これはある意味，『合同式の 1 次方程式』なんですが，『合同式』の世界では割り算が出来ないので，最後の式で，「両辺を 2 で割る」なんてことは絶対にできません．でも，係数の 2 を消したい！ではどうするのか？

それは，割り算ではなく掛け算のチカラを借りて，n の係数 2 を消去します．つまり両辺に 5 をかけます．すると，

$$\begin{aligned} 10n &\equiv 15 \pmod 9 \\ n &\equiv 6 \pmod 9 \end{aligned}$$

となります．よって，n は 9 で割ると 6 余る数なので，求める最小の自然数は 6 です．

(2) (1) と同様に係数をどんどん小さくしていきます．

$$\begin{aligned} 374n+142 &\equiv 0 \pmod{15} \\ 13n+7 &\equiv 0 \pmod{15} \\ 13n &\equiv -7 \pmod{15} \\ -2n &\equiv -7 \pmod{15} \\ 2n &\equiv 7 \pmod{15} \end{aligned}$$

最後の式の両辺にある数をかけて，n の係数が 1(または −1) になるようにします．何をかければよいのか分かりますよね．

✎注 $\boxed{272}$ を参照のこと．

$\boxed{253}$ う～ん，この問題は『合同式』使うべきではないと思いますね．使わない方が簡単だし，無理に『合同式』を使おうとするから，『合同式はむつかしい』という先入観を与えてしまうんですね．

なので，まずは使わないでやってみます．

(1) の場合，123^{122} の一の位の数は 3^{122} の一の位の数と同じです．よって，3^1，3^2，3^3，…，の一の位を順番に並べると

$$3, 9, 7, 1, 3, 9, 7, 1, \cdots$$

と周期 4 でくり返すことがわかります．

したがって，$122 = 4\cdot 30 + 2$ なので，3^{122} の一の位の数は 9 となります．

(2) の場合，7^1，7^2，7^3，…，の下 2 桁を順番に並べると

$$07, 49, 43, 01, 07, 49, 43, 01, \cdots$$

と周期 4 でくり返すことがわかります．

したがって，$251 = 4\cdot 62 + 3$ なので，7^{251} の一の位の数は 43 となります．

個人的にはこれらの解答で十分だと思いますし，最初にこのように考えるのが普通です．

でも，文句を言う人がいるんですね．「これはあくまでも予想にすぎないじゃないか」と．

そう思う人は『合同式』で証明してください．

もう一度言いますが，この問題はまずは上のような解答を自分で考えてから，その後で『合同式』で証明するのです．何も考えずにいきなり『合同式』を利用するのではありません．

いちおう，(1) だけ『合同式』でやってみます．一の位の数字を求めるには 10 で割った余りを考えればよいので，(mod 10) で計算します．$\boxed{250}$ の計算と全く同じ手法です．

$3^4 \equiv 1 \pmod{10}$ がポイントです．

$$\begin{aligned} 123^{122} &\equiv 3^{122} \pmod{10} \\ &\equiv 3^2\cdot(3^4)^{30} \pmod{10} \\ &\equiv 9\cdot 81^{30} \pmod{10} \\ &\equiv 9\cdot 1^{30} \pmod{10} \\ &\equiv 9 \pmod{10} \end{aligned}$$

よって，123^{122} の一の位の数は 9.

(2) は下 2 桁の数なので 100 で割った余りを考えればよいので，(mod 100) で計算します．これまた $\boxed{250}$ と同じ手法です．7 を何回か書けたら 100 で割った余りが 1 になりませんかね？

$\boxed{254}$ とりあえずやってみてから感想を述べます．

$$\begin{aligned} 2^{6n-5}+3^{2n} &\equiv 2\cdot(2^6)^{n-1}+9^n \pmod{11} \\ &\equiv 2\cdot 64^{n-1}+9\cdot 9^{n-1} \pmod{11} \\ &\equiv 2\cdot 9^{n-1}+9\cdot 9^{n-1} \pmod{11} \\ &\equiv 11\cdot 9^{n-1} \pmod{11} \\ &\equiv 0 \pmod{11} \end{aligned}$$

よって，$2^{6n-5}+3^{2n}$ は 11 で割り切れる．

$$\begin{aligned}
4^{n+1}+5^{2n-1} &\equiv 4^2\cdot 4^{n-1}+5\cdot(5^2)^{n-1} && \pmod{21}\\
&\equiv 16\cdot 4^{n-1}+5\cdot 25^{n-1} && \pmod{21}\\
&\equiv 16\cdot 4^{n-1}+5\cdot 4^{n-1} && \pmod{21}\\
&\equiv 21\cdot 4^{n-1} && \pmod{21}\\
&\equiv 0 && \pmod{21}
\end{aligned}$$

よって，$4^{n+1}+5^{2n-1}$ は 21 で割り切れる．

う〜ん，この 2 つの変形ですが，いずれも一番最初の変形がポイントのようです．しかし「そう言われたらそうやけど，こんなん思いつかんわ」と言うのが正直なところではないでしょうか．確かに，うまく行き過ぎている感がありますね．でも，こうするしかないんですね．

✐**注**　数学 B の『数列』で学習する「数学的帰納法」という証明方法を用いればこのようなわけの分からん変形をしなくても解けます．「合同式を用いて」という指定があればダメですけど．

本原稿の最初に述べたように，合同式の計算は，とりあえず自分でいろいろ式をいじくってみること必要です．必ずうまくいくようになっているので，試行錯誤してコツをつかんでください．いきなり模範解答のようにサクサクとはできません．

「うまいことなってんな〜すごいな〜」と楽しんで解くことが重要かと思います．