整数問題「基礎の隙間」

整数問題の基礎事項で少し残っている部分があるので，まとめて紹介しておこう．

これで基礎は完ぺき～

1　指数型の扱い方

2^n や 3^n のような指数型の整数を割った余りを考えよう．これには3通りの方法があります．次の例題をそれぞれの方法で解き比べてみよう．

例題 1.
(1) すべての自然数 n に対して 4^n-1 が3で割り切れることを示せ．
(2) 2^n+1 が3で割り切れるような自然数 n の満たすべき条件を求めよ．

1.1　合同式の利用

この方法が最も簡単でベストな解法です．

解 (1) $4\equiv 1 \pmod 3$ なので，
$4^n\equiv 1^n\equiv 1 \pmod 3$
よって，$4^n-1\equiv 0 \pmod 3$．
(2) $2\equiv -1 \pmod 3$ なので，
$2^n+1\equiv (-1)^n+1 \pmod 3$
n が偶数のとき，
$(-1)^n+1\equiv 1+1\equiv 2 \pmod 3$
n が奇数のとき，
$(-1)^n+1\equiv -1+1\equiv 0 \pmod 3$
よって，2^n+1 が3で割り切れるための条件は，n が奇数であることである．

合同式って便利やな
マスターしといた方がよさそうです　スゲ～

■

1.2　二項定理の利用

二項定理キ～イ

整数問題でも二項定理を利用することがよくあります．

▷Point◁(二項定理)

$$(a+b)^n=\sum_{k=0}^{n}{}_nC_k a^{n-k}b^k$$

整数問題なのに…　なんで～？

注　二項定理より，

$$\begin{aligned}(a+b)^n&={}_nC_0a^nb^0+{}_nC_1a^{n-1}b^1+\cdots\\&\qquad\cdots+{}_nC_{n-1}a^1b^{n-1}+{}_nC_na^0b^n\\&=(a\text{ の倍数})+b^n\end{aligned}$$

となるので，$(a+b)^n$ を a で割った余りは，b^n を a で割った余りに等しいことがわかります．つまり，合同式で書けば

$$(a+b)^n\equiv b^n \pmod a$$

解 (1) 二項定理より，

落ち着いて公式にあてはめるだけ…

$$\begin{aligned}4^n&=(3+1)^n\\&=\sum_{k=0}^{n}{}_nC_k3^{n-k}1^k\\&={}_nC_03^n1^0+{}_nC_13^{n-1}1^1+\cdots\\&\qquad\cdots+{}_nC_{n-1}3^11^{n-1}+{}_nC_n3^01^n\\&=(3\text{ の倍数})+1\end{aligned}$$

よく見ると　ジ～ッ

ほとんど3の倍数なのね…

よって，4^n-1 は3の倍数である．

(2) 二項定理より，

$$\begin{aligned}2^n+1&=(3-1)^n+1\\&=\sum_{k=0}^{n}{}_nC_k3^{n-k}(-1)^k\\&={}_nC_03^n(-1)^0+{}_nC_13^{n-1}(-1)^1+\cdots\\&\cdots+{}_nC_{n-1}3^1(-1)^{n-1}+{}_nC_n3^0(-1)^n+1\\&=(3\text{ の倍数})+(-1)^n+1\end{aligned}$$

符号に注意しよう

これが3の倍数になるためには，$(-1)^n+1=0$ でなければならないので，n は奇数である．

こんなふうに使うのか～　ナットク

■

注　うすうす気づいているかもしれませんが，上の解法において，二項定理で展開して出てきた項のうちで，3の倍数の項を除外し，3の倍数以外の項だけに注目して考えるのが最初に紹介した「合同式を用いた解法」に他なりません．つまり，合同式とは二項定理による解法を簡略化しただけのことです．

それだけのことか…

1.3　因数分解の利用

次の因数分解は整数問題に限らず重要な公式でいろんなところで登場します．

▷Point◁（因数分解の公式）

公式①　n を自然数とするとき，

$$a^n-b^n$$
$$=(a-b)(a^{n-1}+a^{n-2}b+a^{n-3}b^2+\cdots+a^2b^{n-3}+ab^{n-2}+b^{n-1})$$

公式②　n が奇数のとき，

$$a^n+b^n$$
$$=(a+b)(a^{n-1}-a^{n-2}b+a^{n-3}b^2-\cdots+a^2b^{n-3}-ab^{n-2}+b^{n-1})$$

この因数分解は指数の形の式を「積の形に変形する」ことができるという点でとても重要です．

a^n-b^n は全ての自然数 n で $a-b$ を因数にもち，a^n+b^n は n が奇数のときだけ $a+b$ を因数にもつことに注意しよう．

解

(1)　$4^n-1=4^n-1^n$ となるので，前問と同様に，公式①で $a=4$，$b=1$ とすれば，

$$4^n-1^n=(4-1)(4^{n-1}+\cdots+1^{n-1})$$
$$=3(4^{n-1}+\cdots+1^{n-1})$$

となり，3の倍数になることがわかる．

(2)　$n=2m$ のとき，

$$2^n+1=2^{2m}+1=4^m+1=(4^m-1)+2$$

となり，(1)より，4^m-1 は3の倍数だから，2^n+1 は3で割ると2余る．

$n=2m+1$ のとき，

$$2^n+1=2^{2m+1}+1=4^m\times2+1=2(4^m-1)+3$$

となり，(1)より，4^m-1 は3の倍数だから，2^n+1 は3で割り切れる．

よって，2^n+1 が3で割り切れるような自然数 n は n が奇数であることである．

■

⇨注　(2)で，なぜいきなり n が偶数か奇数かで場合分けしたのでしょう．それは公式②が背景にあります．「いつ 2^n+1 が3で割り切れるか」と問われたとき，公式②をイメージして，「n が奇数なら $2^n+1=(2+1)(\cdots\cdots)$ と因数分解できるので3で割り切れるはずだ」と考えたからです．

解答では，(2)は(1)の結果を利用しているので，因数分解の公式を直接的に使っていませんが，場合分けを考える際に（間接的に）因数分解の公式を考えているのです．

以上，3通りの解法を紹介しましたが，圧倒的に合同式を利用した解法が簡単なのがわかります．しかし，二項定理や因数分解も重要な解法なので，今回だけは3通り全てマスターしておきましょう．

例題 2.
2^n を7で割ったときの余りが1であることの必要十分条件は，n が3の倍数であることを証明せよ．

考え方　必要十分条件なので，双方向の証明が必要です．もちろん合同式を利用しましょう．

解

「n が3の倍数
$\Longrightarrow$ 2^n を7で割ったときの余りが1」の証明

$n=3k$ とおく．

$$2^n\equiv2^{3k}\equiv8^k\equiv1^k\equiv1 \pmod 7$$

よって，2^n を7で割ると余り1である．

「2^n を7で割ったときの余りが1
$\Longrightarrow$ n が3の倍数」の証明

n が3の倍数ではないと仮定する．

$n=3k+1$ のとき，

$$2^n\equiv2^{3k+1}\equiv2\cdot8^k\equiv2\cdot1^k\equiv2 \pmod 7$$

$n=3k+2$ のとき，

$$2^n\equiv2^{3k+2}\equiv4\cdot8^k\equiv4\cdot1^k\equiv4 \pmod 7$$

いずれの場合も 2^n を7で割ると余り1ではない．

よって，対偶命題が証明されたのでもとの命題は正しい．