例題 5.　今日は金曜日です．
(1)　10^6 日後は何曜日ですか．
(2)　10^{100} 日後は何曜日ですか．
(3)　3^{100} 日後は何曜日ですか．

おもしろい
問題や

考え方　実際に某大学入試で出題された問題です．曜日は7日周期なので，7で割った余りに注目します．(1) だけやってみます．(2)(3) は各自で．

解　$10^6 \equiv 3^6 \equiv 9^3 \equiv 2^3 \equiv 1 \pmod 7$

よって，土曜日．

合同式って
おもしろいネ

■

例題 6.　n を自然数とするとき，
$3^{n+2}+4^{2n+1}$ は13で割り切れることを示せ．

解

$$
\begin{aligned}
3^{n+2}+4^{2n+1} &\equiv 3^n\cdot 3^2+4^{2n}\cdot 4^1 && \pmod{13}\\
&\equiv 9\cdot 3^n+4\cdot 16^n && \pmod{13}\\
&\equiv 9\cdot 3^n+4\cdot 3^n && \pmod{13}\\
&\equiv 13\cdot 3^n && \pmod{13}\\
&\equiv 0 && \pmod{13}
\end{aligned}
$$

実にうまい
変形!!

よって，$3^{n+2}+4^{2n+1}$ は13で割り切れる．

■

$16\equiv 3 \pmod{13}$ であることを用いて実にうまく変形しています．合同式を用いないならば数学的帰納法で証明するしかありません（勉強になるので念のため各自でやっといてください）．

はーい

応用問題
ですよ

ムムム

例題 7.
(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．

解

(1)　$4\equiv 1 \pmod 3$ なので，
$4^n\equiv 1^n\equiv 1 \pmod 3$
よって，$4^n-1\equiv 0 \pmod 3$．

エッ
これで
終わり？

(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．

あまりに
シンプルすぎて
言葉が
出ません

■

注　合同式を使わないなら，二項定理より，

$$
\begin{aligned}
4^n &= (3+1)^n\\
&= \sum_{k=0}^{n} {}_nC_k 3^{n-k}1^k\\
&= {}_nC_0 3^n 1^0 + {}_nC_1 3^{n-1}1^1+\cdots\\
&\qquad \cdots + {}_nC_{n-1}3^1 1^{n-1} + {}_nC_n 3^0 1^n\\
&= (3\text{の倍数})+1
\end{aligned}
$$

二項定理
キラ〜イ

よって，4^n-1 は3の倍数であることがわかります．また，(2) も，

$$
\begin{aligned}
2^n+1 &= (3-1)^n+1\\
&= \sum_{k=0}^{n} {}_nC_k 3^{n-k}(-1)^k\\
&= {}_nC_0 3^n(-1)^0 + {}_nC_1 3^{n-1}(-1)^1+\cdots\\
&\qquad \cdots + {}_nC_{n-1}3^1(-1)^{n-1} + {}_nC_n 3^0(-1)^n+1\\
&= (3\text{の倍数})+(-1)^n+1
\end{aligned}
$$

よって，これが3の倍数になるには，$(-1)^n+1=0$ でなければならないので，n は奇数であることがわかります．

■

注　うすうす気づいているかもしれませんが，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．

そうやったんか

知らんかったー
やってることは
同じなのね

注　二項定理の他にも因数分解を利用する解法もありますが，今回は省略します．

2　アタリマエでないこと

合同記号（≡）は等号（＝）とほとんど同じように処理することができますが，全く同じというわけ

にはいきません．「普通の等式ならば成立すること」として次の2つを考えてみます．はたして，合同記号でもそのまま成立するのでしょうか．ますは自分で考えてみてください．　はーい

疑惑その①

普通の等式なら

$$ab=0 \Longrightarrow a=0 \text{ または } b=0$$

が成立するが，合同式でも

$$ab\equiv 0 \Longrightarrow a\equiv 0 \text{ または } b\equiv 0 \pmod{m}$$

が成立するか？　うーん どうかなあ…　?

要するに

$$ab \text{ が } m \text{ の倍数} \Longrightarrow a \text{ または } b \text{ が } m \text{ の倍数}$$

が成立するかどうかですが，これは，常には成立しないことは明らかです．例えば $4\times 9=36$ は6の倍数ですが，4も9も6の倍数ではありませんね．

そりゃ そうや

しかし，m が特別な数の場合は成立します．次の素数に関する重要性質を思い出そう．

▷Point◁（素数の基本性質）

p を素数とするとき，ab が p の倍数ならば，a または b が p の倍数である．

したがって，合同式の世界では

▷Point◁（合同式の性質 Ⅱ）

p が <u>素数</u> のときに限り，

$$ab\equiv 0 \Longrightarrow a\equiv 0 \text{ または } b\equiv 0 \pmod{p}$$

ナットク!!　OK

つまり，素数を法とする場合にのみ，等式と同じことが成立するのです．

疑惑その②

普通の等式なら，$c\neq 0$ のとき，両辺を c で割って

$$ca=cb \Longrightarrow a=b$$

が成立するが，合同式でも，$c\neq 0$ のとき

$$ca\equiv cb \Longrightarrow a\equiv b \pmod{m}$$

が成立するか？　うーん どうかなあ…　??

これも具体例で考えてみよう．

例えば，合同式 $35\equiv 5 \pmod{6}$ の両辺を5で割って

$$7\equiv 1 \pmod{6}$$

← 成り立つ

は成立しますが，合同式 $14\equiv 8 \pmod{6}$ の両辺を2で割って，

$$7\equiv 4 \pmod{6}$$

← 成り立たない!!

ホンマや　あかんわ

は成立しません．このことからも常には成立しないようです．

しかし，c と m がある条件をみたすならば，合同式の世界でも成立します．その根拠となるのが，次の重要性質です．

▷Point◁（整数の基本性質）

A と B が互いに素な整数のとき，AC が B で割り切れるならば，C は B で割り切れる．

AC が B で割り切れるとき，$\dfrac{AC}{B}$ は整数になるが，A と B が互いに素なので約分できないから，C が B で割り切れなければならないということです．

フムフム

したがって，

$$\begin{aligned} & ca\equiv cb \pmod{m} \\ \Longleftrightarrow\ & ca-cb \text{ が } m \text{ で割り切れる} \\ \Longleftrightarrow\ & c(a-b) \text{ が } m \text{ で割り切れる} \end{aligned}$$

より，ここで，c と m が互いに素であれば，整数の基本性質より，$a-b$ が m で割り切れることになり，$a-b\equiv 0 \pmod{m}$，つまり，$a\equiv b \pmod{m}$ が成立します．

したがって，合同式の世界では

▷Point◁（合同式の性質 Ⅲ）

c と m が <u>互いに素</u> のときに限り，

$$ca\equiv cb \Longrightarrow a\equiv b \pmod{m}$$

と，合同式の両辺を c で割ることができる．

ナットク!!　OK

となります．

先ほどの例で，合同式 $35\equiv 5 \pmod{6}$ の両辺を5で割っても成立したのは，5と6が互いに素であったからで，合同式 $14\equiv 8 \pmod{6}$ の両辺を2で割って成立しなかったのは，2と6が互いに素でなかったからです．　なるほど そういうことか!!

例題 5．の(2)(3)の答えはいずれも火曜日．