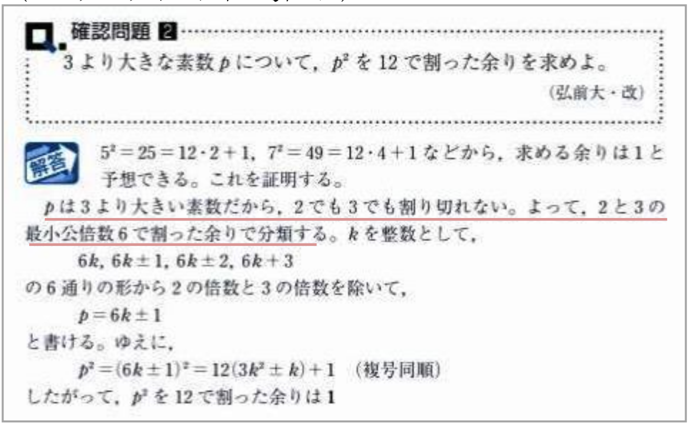
雑感　　他山の石

■　3 年生の受験勉強も佳境に入りつつあるためだろうか．昨年教えていた生徒が，放課後問題集などを抱えて質問にやってくることが多くなった．

■　「友だちから借りた本ですけど…」と言ってある生徒が参考書を持って来た．
　下の画像は，その参考書の「なか見！検索」のキャプチャ．（アンダーラインは私が引いた）



確認問題 2
3 より大きな素数 p について，p^2 を 12 で割った余りを求めよ。
（弘前大・改）

解答　$5^2=25=12\cdot 2+1$，$7^2=49=12\cdot 4+1$ などから，求める余りは 1 と予想できる。これを証明する。
　p は 3 より大きい素数だから，2 でも 3 でも割り切れない。よって，2 と 3 の最小公倍数 6 で割った余りで分類する。k を整数として，

$$6k,\ 6k\pm 1,\ 6k\pm 2,\ 6k+3$$

の 6 通りの形から 2 の倍数と 3 の倍数を除いて，

$$p=6k\pm 1$$

と書ける。ゆえに，

$$p^2=(6k\pm 1)^2=12(3k^2\pm k)+1 \quad (\text{複号同順})$$

したがって，p^2 を 12 で割った余りは 1

　なぜ 6 の剰余系を考えるのか，その理由が分からないという．

■　確かにこの問題では解答のように 6 の剰余系で調べ，素数の可能性がある $6k\pm 1$ の場合についてだけ調べればよいというということは正しいが，問題はその 6 の根拠である．

■　たとえば，「奇素数 p について，p^2 を 10 で割った余り」について考えると，この解答の流れでは，2 の剰余系で，要するに奇数か偶数かで調べればよいことになるし，p を 3 より大きい素数とすれば 6 の剰余系で調べればよいことになる．
　しかし，いずれの方法でも上手く行かないのは，自明である．
　p を奇素数とすれば，この場合は 10 による剰余系で考え，$p=10k+j$（$j=0, 1, 2, \cdots, 9; k\geqq 0$）の 10 パターンのうち，素数の可能性がある場合について考えればよい．
$k=0$ の場合は $p=3, 5, 7$；
$k\geqq 1$ の場合は，$p=10k+1, 10k+3, 10k+7, 10k+9$
の場合について調べ，
余りは $p=5$ のとき 5，$p=10k+1, 10k+9$ の形の素数のとき 1，
$p=10k+3, 10k+7$ の形の素数のとき 9
が答になる．
　したがって，参考書のような明快な答に近づけるためには「5 より大きい素数」と設定すれば，余りは 1 または 9 となる．

■　この参考書の問題では，本来 12 による剰余系で調べなければならないところ，$(6k+j)^2=36k^2+12kj+j^2$ で，$36k^2$, $12kj$ が共に 12 の倍数となるから，6 の剰余系でたまたま上手く行ったに過ぎない．
　もし，24 で割った余りという場合，6 による剰余系ではダメで，12 による剰余系ならばよい．
　結局，素数 p について p^2 をある自然数 m で割った余りというとき，$(nk+j)^2=n^2k^2+2nkj+j^2$ において，n^2k^2，$2nk$ が m の倍数になるような n を選ばなければならないということである．

■　このような間違った根拠を示してしまうようなことは，問題演習の授業などで私自身行ってしまっているかも知れないなあ．以て，他山の石とすべし．

2014 年 12 月 1 日