꩜ Devoir Maison 8 ꩜
Congruence - conjecture d'APW

Exercice 1. ♠♠

Lors du DM7, l'un d'entre vous a utilisé un résultat qui n'est pas présent dans le cours dont on va analyser la pertinence. J'ai nommé ce résultat conjecture d'APW.

Dans tous l'exercice $a \in \mathbb{Z}$, n est un entier naturel et r désigne le reste de la division euclidienne de a^2 par n, par conséquent on a :

$$a^2 \equiv r[n]$$

Conjecture d'APW : Si r est un carré parfait alors $a \equiv \sqrt{r}[n]$ ou $a \equiv -\sqrt{r}[n]$.

Partie A : Cas où $n = 9$.

1. Compléter le tableau suivant :

Reste possible de X par 9	0	1	2	3	4	5	6	7	8
Reste possible de X^2 par 9	0	1	4	0	7	7	0	4	1

2. Quels sont les restes possibles de la division euclidienne de a par 9 lorsque $a^2 \equiv 0[9]$?
   Les restes possibles de a par 9 lorsque $a^2 \equiv 0[9]$ sont d'après le tableau précédent 0, 3 ou 6.
3. La *conjecture d'APW* est-elle vérifiée lorsque $n = 9$? *On justifiera soigneusement.*
   La conjecture d'APW prévoit que si $a^2 \equiv 0[9]$ alors $a \equiv 0[9]$.
   Or, il suffit de choisir par exemple $a = 3 \equiv 3[9]$, dans ce cas $a^2 \equiv 0[9]$ ce qui est contradictoire avec la prédiction d'APW, en effet a n'est pas congru à 0 modulo 9 mais à 3 modulo 9.
4. Justifier que $a = 15$ est un contre-exemple qui invalide la *conjecture d'APW* ? En proposer un autre.
   $15^2 = 225$ est un multiple de 9 (2+2+5=9) donc $a^2 \equiv 0[9]$, si on applique la conjecture d'APW on obtient $a \equiv 0[9]$, or 15 n'est pas congru à 0 modulo 9.
   $a = 12$ est un autre contre exemple.

Partie B : Cas où $n = 5$.

1. Compléter le tableau suivant :

Reste possible de X par 5	0	1	2	3	4
Reste possible de X^2 par 5	0	1	4	4	1

2. Quels sont les restes possibles de la division euclidienne de a par 5 lorsque $a^2 \equiv 0[5]$? lorsque $a^2 \equiv 1[5]$? lorsque $a^2 \equiv 4[5]$?
   Si $a^2 \equiv 0[5]$ alors $a \equiv 0[5]$ d'après le tableau précédent.
   Si $a^2 \equiv 1[5]$ alors $a \equiv 1[5]$ ou $a \equiv 4[5] \iff a \equiv -1[5]$.
   Si $a^2 \equiv 4[5]$ alors $a \equiv 2[5]$ ou $a \equiv 3[5] \iff a \equiv -2[5]$
3. La *conjecture d'APW* est-elle vérifiée lorsque $n = 5$? *On justifiera soigneusement.*
   Soit a un entier relatif et r le reste de la division euclidienne de a^2 par 5, on a donc $a^2 \equiv r[5]$. Si $r = 0$ alors d'après la question précédente $a \equiv 0[5]$ ce qui est conforme à la conjecture d'APW. Si $r = 1$ alors $a \equiv 1[5]$ ou $a \equiv -1[5]$ ce qui est conforme à la conjecture d'APW. Enfin si $r^2 = 4$ alors $a \equiv \pm 2[5]$ ce qui est conforme aux prédictions d'APW.

Partie C : Cas où n est un nombre premier.

On rappelle ou on donne un résultat (que je démontrerai très prochainement) :

Lemme 1.

Lemme d'euclide

Si p, un nombre premier, divise le produit ab alors il divise a ou il divise b.

1. On suppose que $a^2 \equiv b^2[n]$, montrer en utilisant le lemme d'euclide, que $a \equiv b[n]$ ou que $a \equiv -b[n]$.
   Si $a^2 \equiv b^2[n]$ alors il existe un entier naturel k tel que :
   $$a^2 - b^2 = nk \Longleftrightarrow (a-b)(a+b) = nk$$
   Puisque $n|(a-b)(a+b)$ et que n est premier d'après le lemme d'euclide $n|a-b$ ou $n|a+b$ i.e $a \equiv b[n]$ ou $a \equiv -b[n]$.
2. En déduire que la *conjecture d'APW* est vraie lorsque n est premier.
   Le résultat de la question précédente équivaut au résultat prévu par APW donc cette conjecture est vraie dès lors que n est premier.