DM 8 - Loi de réciprocité quadratique

1 Symbole de Legendre

1. RAS

2. Souvent confus. L'image de θ_p n'est pas clairement identifiée comme l'ensemble des entiers de $[\![1, p-1]\!]$, qui sont des carrés modulo p. Maintenant qu'on a le recul de la manipulation de $\mathbb{Z}/p\mathbb{Z}$, on pourrait travailler plutôt dans $\mathbb{Z}/p\mathbb{Z}$ à la place.
   Pour montrer que chaque élément de l'image a deux antécédents, il n'y a pas besoin de procéder en deux temps : il suffit de montrer que pour tout x, l'équation $\theta_p(x) = \theta_p(x')$ (d'inconnue x') a exactement deux solutions : en l'occurrence x et $p-x$.

3. Normalement, conséquence immédiate de la question précédente. Comme souvent les choses n'ont pas été proprement dites à la question d'avant, elles sont redites ici... Bien lire l'énoncé et montrer ce qui est demandé.

4. L'implication $a^{p-1} \equiv 1\,[p] \implies a^{\frac{p-1}{2}} \equiv \pm 1\,[p]$ doit être un minimum justifiée (par exemple en revenant à la définition, en factorisant et en utilisant le lemme d'Euclide ; ou en utilisant ce qui a été dit précédemment sur l'application θ_p).

5. **Critère d'Euler.**

   (a) L'implication $\left(\frac{a}{p}\right) = 1 \implies a^{\frac{p-1}{2}} \equiv 1\,[p]$ est assez immédiate. Beaucoup affirment sur leur copie qu'on s'en sort de même avec -1, de façon plus ou moins confuse. Cependant, il y a une vraie subtilité ici et il fallait utiliser l'indication pour conclure.

   (b) RAS

   (c) Il s'agissait de calculer 5^{11} modulo 23. Bien sûr, énumérer les carrés modulo 23 fonctionne aussi, mais n'était pas dans l'esprit de la question.

   (d) Dans quelques copies, on affirme que $(-1)^{\frac{p-1}{2}}$ vaut 1 car p est impair. Attention à ne pas confondre la parité de p et celle de $\dfrac{p-1}{2}$!

6. **Un (autre) lemme de Gauss.** Soit $a \in \mathbb{Z}$, non divisible par p.

   (a) Rédaction souvent confuse. Bien distinguer la partie Existence de la partie Unicité.

   (b) Le plus simple est de montrer le caractère injectif et de conclure par égalité des cardinaux au départ et à l'arrivée. Pour l'injectivité, il ne suffit pas de dire qu'elle résulte de l'unicité à la question précédente (ce n'est pas la *même* unicité dont il s'agit).

   (c) Le point crucial sur l'égalité de deux produits par changement de variable bijectif est le plus souvent bien compris.

   (d) Bien distinguer quand l'énoncé parle de congruence et quand il parle d'égalité, comme ici.

7. (a) Il est sous-entendu que la condition demandée doit être nécessaire et suffisante. Trop souvent, la rédaction est celle d'une implication, dans un sens ou dans l'autre.
   (b) Dans ce genre de questions, il est agréable de faire un bilan rapide, pour résumer les calculs.
   (c) RAS
   (d) RAS
   (e) Il n'y a pas vraiment besoin de traiter à part le cas où $\frac{N}{2}$ serait lui-même premier (déjà dans la preuve de l'infinité des nombres premiers, cette distinction n'apparait pas).

8. On cherche $\left(\frac{3}{p}\right)$ et il y a deux choses à savoir sur p pour conclure : s'il est congru à 1 ou 3 modulo 4 (pour calculer $(-1)^{\frac{(3-1)(p-1)}{4}}$) et $\left(\frac{p}{3}\right)$ (ce qui revient à savoir si p est congru à 1 ou à 2 modulo 3 (seul 1 est un carré modulo 3).
   On obtient ainsi 4 cas possibles avec les congruences de p modulo 3 et 4 ; par le théorème des restes chinois, on se ramène à des congruences modulo 12.

9. cf. corrigé pour une rédaction rapide du calcul.

2 Une démonstration de la loi de réciprocité quadratique

10. (a) Ce calcul est une nouvelle variante sur un thème vu depuis le début de l'année. Il ne doit plus poser aucune difficulté.
    (b) Les arguments pour montrer que les racines trouvées sont distinctes sont beaucoup trop longs. Utiliser la propriété de stricte croissance de $\sin^2$, sur le bon intervalle.
    (c) RAS
    (d) RAS

    Les calculs de la fin ont en général été bien traités par les personnes qui s'y sont essayés. Il n'y a pas besoin de grande technique et on conseille à celles et ceux qui ne les auraient pas fait de s'y replonger.