# OS – Théorie des nombres – Exercices

*5/10/2010 ⟶12/10/2010 – calcul « modulo $m$ »*

1. Démontrer les propriétés de compatiblité de la congruence modulo $m$ avec les opérations d'addition, de multiplication par un entier relatif et de multiplication interne :

$$\boxed{\begin{cases} a \equiv a'\,(m) \\ b \equiv b'\,(m) \end{cases} \implies \begin{cases} a+b \equiv a'+b'\,(m) \\ a\cdot b \equiv a'\cdot b'\,(m) \\ k\cdot a \equiv k\cdot a'\,(m) \end{cases}}$$

   [Pour simplifier, on n'a pas écrit les quantificateurs, et on a abrégé « $\equiv$(mod $m$) » en « $(\equiv (m)$ ».]

   Ce sont ces propriétés qui permettent de calculer « modulo $m$ », c'est-à-dire avec les classes de congruence modulo $m$.

2. Démontrer que $\boxed{a \equiv a'\,(m) \implies k\cdot a \equiv k\cdot a'\,(km)}$. (Ce n'est pas la même propriété que ci-dessus. Les deux implications sont valables).

3. Déterminez les inversibles modulo 24, (comme on l'a vu, le critère est d'être premier avec 24) et dresser la table de multiplication de ces nombres (pas de panique, ils ne sont pas si nombreux que ça !).

4. Calculer $2^2$; $2^3$; $2^4 \ldots 2^{12}$ modulo 7. Puis de même avec les puissances de 3. Que constatez-vous ? Si vous êtes futés, vous pouvez prendre les raccourcis et vous passer totalement de calculatrice...

5. Résolvez l'équation $95x + 14y = 1$ dans $\mathbb{Z}$.
   Une fois cette équation résolue, récrivez l'égalité trouvée modulo 95, puis modulo 14. Qu'est-ce que cela signifie pour les valeurs trouvées de $x$ et $y$ ? – La résolution de cette équation diophantienne permet de calculer l'..... de ..... modulo .....

6. Une démonstration plus difficile : nous avons trouvé de manière intuitive et expérimentale que la condition pour que $x$ soit inversible modulo $m$ est que $x$ et $m$ soient premiers entre eux. Démontrer cette condition.

***Exercices du livre*** : ex. 2.1 et 2.2 (rappel), 2.3 (on n'a pas encore vu de méthode de résolution, mais vous pouvez trouver quand même...), 2.7

# OS – Théorie des nombres – Exercices « modulo » ...

*5/10/2010 ⟶12/10/2010 – calcul « modulo $m$ »*

1. Démontrer les propriétés de compatiblité de la congruence modulo $m$ avec les opérations d'addition, de multiplication par un entier relatif et de multiplication interne :

$$\boxed{\begin{cases} a \equiv a'\,(m) \\ b \equiv b'\,(m) \end{cases} \implies \begin{cases} a+b \equiv a'+b'\,(m) \\ a\cdot b \equiv a'\cdot b'\,(m) \\ k\cdot a \equiv k\cdot a'\,(m) \end{cases}}$$

   [Pour simplifier, on n'a pas écrit les quantificateurs, et on a abrégé « $\equiv$(mod $m$) » en « $(\equiv (m)$ ».]

   Ce sont ces propriétés qui permettent de calculer « modulo $m$ », c'est-à-dire avec les classes de congruence modulo $m$.

2. Démontrer que $\boxed{a \equiv a'\,(m) \implies k\cdot a \equiv k\cdot a'\,(km)}$. (Ce n'est pas la même propriété que ci-dessus. Les deux implications sont valables).

3. Déterminez les inversibles modulo 24, (comme on l'a vu, le critère est d'être premier avec 24) et dresser la table de multiplication de ces nombres (pas de panique, ils ne sont pas si nombreux que ça !).

4. Calculer $2^2$; $2^3$; $2^4 \ldots 2^{12}$ modulo 7. Puis de même avec les puissances de 3. Que constatez-vous ? Si vous êtes futés, vous pouvez prendre les raccourcis et vous passer totalement de calculatrice...

5. Résolvez l'équation $95x + 14y = 1$ dans $\mathbb{Z}$.
   Une fois cette équation résolue, récrivez l'égalité trouvée modulo 95, puis modulo 14. Qu'est-ce que cela signifie pour les valeurs trouvées de $x$ et $y$ ? – La résolution de cette équation diophantienne permet de calculer l'..... de ..... modulo .....

6. Une démonstration plus difficile : nous avons trouvé de manière intuitive et expérimentale que la condition pour que $x$ soit inversible modulo $m$ est que $x$ et $m$ soient premiers entre eux. Démontrer cette condition.

***Exercices du livre*** : ex. 2.1 et 2.2 (rappel), 2.3 (on n'a pas encore vu de méthode de résolution, mais vous pouvez trouver quand même...), 2.7