TD Arithmétique

LSI 1

1 Divisibilité dans $\mathbb{Z}$

Exercice 1. Montrer que :

1. Si un entier est de la forme $6k+5$, alors il est nécessairement de la forme $3k-1$, alors que la réciproque est fausse.
2. Le carré d'un entier de la forme $5k+1$ est aussi de cette forme.
3. Le carré d'un entier est de la forme $3k$ ou $3k+1$, mais jamais de la forme $3k+2$.

Exercice 2. Soit n un entier. Calculer le reste de la division euclidienne de n^2 par 4, suivant que cet entier est pair ou impair. Existe-t-il des entiers a et b tels que $a^2+b^2=8123$?

Exercice 3. Démontrer que, si a et b sont des entiers premiers entre eux, il en est de même des entiers $a+b$ et ab.

Exercice 4. Soient $a, b \in \mathbb{N}^*$ et m, n premiers entre eux tels que $a^n = b^m$. Montrer qu'il existe $c \in \mathbb{N}^*$ tel que $a = c^m$ et $b = c^n$.

2 Nombres premiers

Exercice 5. Soient a, b des entiers supérieurs ou égaux à 1. Montrer :

1. $(2^a-1)|(2^{ab}-1)$;
2. 2^p-1 premier $\Rightarrow$ p premier ;
3. $pgcd(2^a-1, 2^b-1) = 2^{pgcd(a,b)}-1$.

Exercice 6. On note $M_n = 2^n - 1$ (n-ième nombre de Mersenne).

1. Montrer que : M_n est premier $\Rightarrow n$ est premier.
2. Vérifier que M_{11} n'est pas premier.

3 Calculs de congruences

Exercice 7. Calculer 2000^{2000} modulo 7 et 2^{500} modulo 3.

Exercice 8.

1. Soit n un entier naturel, démontrer que pour tout $n \in \mathbb{N}$, $10^n - (-1)^n$ est divisible par 11.
2. Déterminer le reste dans la division par 7 de $2^{64}-1$.
3. Démontrer que pour tout entier n, $2n^2+n+1$ n'est pas divisible par 3.

Exercice 9. Soit n un entier naturel.

1. Démontrer que si $n \equiv 2 \mod 5$ ou si $n \equiv 3 \mod 5$, alors n^2+1 est un multiple de 5.
2. Démontrer que pour tout $n \in \mathbb{N}$, $n(n^4-1)$ est un multiple 5.

Exercice 10.

1. Démontrer que pour tout entier naturel n, $6^n + 13^{n+1} \equiv 0 \mod 7$
2. Démontrer que $n^3+3n-10$ est divisible par 13 équivaut à $n \equiv 3 \mod 13$ ou $n \equiv 5 \mod 13$.

Exercice 11.

1. Donner suivant les valeurs de l'entier naturel n les restes de la division euclidienne de 2^n par 7.

2. En déduire que si n n'est pas multiple de 3, $2^{2n} + 2^n + 1$ est divisible par 7.

Exercice 12. Soit a un entier relatif quelconque, démontrer que le nombre $a(a^2 - 1)$ et, plus généralement, $a(a^{2n} - 1)$ est divisible par 6.

Exercice 13.

1. Montrer que le reste de la division euclidienne par 8 du carré de tout nombre impair est 1.
2. Montrer de même que tout nombre pair vérifie $x^2 = 0 \pmod 8$ ou $x^2 = 4 \pmod 8$.
3. Soient a, b, c trois entiers impairs. Déterminer le reste modulo 8 de $a^2 + b^2 + c^2$ et celui de $2(ab + bc + ca)$.
4. En déduire que ces deux nombres ne sont pas des carrés puis que $ab + bc + ca$ non plus.

4 Équations aux congruences

Exercice 14. Résoudre les systèmes d'équations suivants :

1. $x + 2y \equiv 3 \mod 7$ et $y \equiv 5 \mod 7$;
2. $x + 2y \equiv 3 \mod 9$ et $x + y \equiv 5 \mod 9$;
3. $2x + 3y \equiv 3 \mod 9$ et $3x + 4y \equiv 5 \mod 9$;
4. $2x + 3y \equiv 1 \mod 15$ et $x + 4y = 2 \mod 15$;
5. $2x + 3y \equiv 1 \mod 15$ et $x + 4y = 3 \mod 15$.

Exercice 15. Soit ϕ l'application de $\{0, \ldots, 9\}$ dans lui-même définie par $\phi(x) = 2x$ si $x \leq 4$ et $\phi(x) = 1 + 2(x - 5)$ si $x \geq 5$. Un numéro de carte bancaire est un nombre décimal de la forme $a_n a_{n-1} \ldots a_1 a_0$, où les chiffres décimaux satisfont à la règle (dite de Luhn) : $a_0 + \phi(a_1) + a_2 + \phi(a_3) + \cdots \equiv 0 \mod 10$.

1. Montrer que cela permet de détecter la présence d'un chiffre décimal erroné.
2. Montrer que cela permet de détecter une permutation de deux chiffres consécutifs, à l'exception de la permutation $09 \to 90$. Avant l'introduction de l'Euro, les billets de banque allemands utilisaient paraît-il un code obtenu par l'adjonction d'un chiffre décimal à un nombre décimal de 9 chiffres qui détectait une erreur ou l'interversion de deux chiffres consécutifs.

5 Théorème Chinois

Exercice 16. Résoudre dans $\mathbb{Z}$ le système suivant :

$$\left\{ \begin{array}{lcll} x & \equiv & 4 & \mod 9 \\ x & \equiv & 2 & \mod 7 \end{array} \right. \tag{1}$$

Exercice 17. Trouver tous les entiers x tels que

$$\left\{ \begin{array}{lcll} 7x & \equiv & 5 & \mod 19 \\ 3x & \equiv & 1 & \mod 11 \end{array} \right. \tag{2}$$

Exercice 18.

1. Trouver le plus petit entier > 10000 qui divisé par 5, 12 et 14 ait pour reste 3.
2. Quel est le plus petit entier plus grand que 10000 qui divisé par 5, 12 et 17 ait pour reste 3 ?
3. Trouver tous les entiers compris entre 100 et 1000 qui divisés par 21 aient pour reste 8 et par 17 pour reste 5.

Exercice 19. La comète A passe tous les 5 ans et a été observée l'année dernière. La comète B passe tous les 8 ans et a été observée il y a 2 ans. La comète C passe tous les 11 ans et a été observée il y a 8 ans. Quelle est la prochaine fois où on pourra observer ces 3 comètes la même année ?

Exercice 20. Une vieille fermière s'en allant marché voit ses œufs écrasés par un cheval. Le cavalier vou- lant la rembourser lui demande combien d'œufs elle avait. Tout ce dont elle se souvient est qu'en les rangeant par 2, il en restait un, et de même en les rangeant par 3, 4, 5 ou 6 ; toute- fois, en les rangeant par 7, il n'en restait pas. Combien d'œufs, au moins, avait-elle ? (D'après Lauritzen, repris de Ore)