TD 1. Congruences

Exercice 1 (Puissances)

1. a) Soit $n \in \mathbb{Z}$ et $\varepsilon \in \{0,1\}$. Développer $(2n+\varepsilon)^2$; en déduire que le carré d'un entier est toujours congru à 0 ou 1 modulo 4.
   b) Faire un raisonnement analogue pour montrer que le cube d'un entier est toujours congru à -1, 0 ou 1 modulo 9.
2. Soit p un nombre premier, on considère l'équation en nombres entiers :

$$x^p + y^p = z^p \ ,$$

où x, y et z sont supposés premiers à p.

   a) On suppose que (x,y,z) est solution du problème pour $p=3$. Montrer qu'alors $x^3+y^3 \equiv -2$, 0 ou 2 $\mod 9$; en déduire qu'il n'y a pas de solution pour $p=3$.
   b) On suppose $p=5$, peut-on faire de même ?

   Pour $p=7$, on pourra "vérifier" la relation : $1^7 + 30^7 \equiv 31^7 \mod 49$.

Exercice 2 (Fermat pour $n=2$)

On considère l'équation :

$$x^2 + y^2 = z^2 \ . \tag{1}$$

1. Soit $(x,y,z) \in \mathbb{Z}^3$ une solution de (1) avec x et y strictement positifs premiers entre eux.
   a) En considérant l'équation modulo 4, montrer que x ou y est pair. *On suppose désormais que x est pair.*
   b) Montrer que $\frac{z-y}{2}$ et $\frac{z+y}{2}$ sont entiers et premiers entre eux.
   c) En déduire qu'il existe $a,b \in \mathbb{N}$ tels que $\frac{z+y}{2} = a^2$ et $\frac{z-y}{2} = b^2$ et qu'on a alors :

$$x = 2ab \ , \quad y = a^2 - b^2 \ , \quad z = a^2 + b^2 \ .$$

   d) Montrer qu'on a de plus :

$$a \not\equiv b \mod 2 \ , \quad (a,b) = 1 \ , \quad a > b > 0 \ . \tag{2}$$

2. Soient $a,b \in \mathbb{Z}$ satisfaisant les conditions (2). Montrer que $x = 2ab$, $y = a^2 - b^2$, $z = a^2 + b^2$ sont strictement positifs, solutions de l'équation (1), et que x et y sont premiers entre eux.

Exercice 3 (Les inversibles de $\mathbb{Z}/n\mathbb{Z}$)

Soit n un entier ≥ 2. Pour $s \in \mathbb{Z}$, on note $\bar{s}$ l'image de s dans $\mathbb{Z}/n\mathbb{Z}$.

1. Montrer l'équivalence des trois assertions suivantes *[penser à Bézout]* :
   (i) s est un entier premier à n ;
   (ii) $\bar{s}$ est un générateur de $\mathbb{Z}/n\mathbb{Z}$;
   (iii) $\bar{s} \in (\mathbb{Z}/n\mathbb{Z})^*$.
2. Soit p un nombre premier.
   a) Montrer que le cardinal de $(\mathbb{Z}/p\mathbb{Z})^*$ est $p-1$.
   b) Soit $x \in (\mathbb{Z}/p\mathbb{Z})^*$, qu'en déduit-on pour x^{p-1} ?
   c) Montrer que pour tout entier s, on a $s^p \equiv s \mod p$.
   d) Vérifier de deux manières que, pour tous $s,t \in \mathbb{Z}$, on a $(s+t)^p \equiv s^p + t^p \mod p$.

3. a) Montrer qu'on a : $X^{p-1} - 1 = \prod_{k=1}^{p-1} (X - \bar{k})$ en tant que polynômes à cœfficients dans $\mathbb{Z}/p\mathbb{Z}$.

   b) En déduire que, pour tout $s \in \mathbb{Z}$, on a : $(s+1)(s+2)\cdots(s+p-1) \equiv s^{p-1} - 1 \mod p$,

   c) puis que : $(p-1)! \equiv -1 \mod p$.

   d) Montrer que pour n entier on a l'implication *[on pourra raisonner par l'absurde ; le cas $n = 4$ est à traiter à part]* :

$$(n-1)! \equiv -1 \mod n \implies n \text{ est premier.}$$

Exercice 4 (Indicatrice d'Euler)

Pour $n \in \mathbb{N}$, on rappelle que $\varphi(n)$ est le cardinal de $(\mathbb{Z}/n\mathbb{Z})^*$. On a vu ci-dessus que $\varphi(p) = p - 1$ pour p premier.

1. a) Soit s un entier ≥ 1, vérifier à l'aide de la question 1. de l'exercice précédent que $\varphi(p^s) = p^{s-1}(p-1)$.

   b) À l'aide du théorème chinois des restes, montrer que, si n et m sont deux entiers premiers entre eux, alors $\varphi(nm) = \varphi(n)\varphi(m)$.

   c) Soit n un entier ≥ 1, dont la décomposition en produit de premiers s'écrit $n = p_1^{e_1} \cdots p_r^{e_r}$. Déduire de ce qui précède que :

$$\varphi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) \ .$$

2. Soit $x \in \mathbb{Z}$.

   a) Montrer que $\bar{x}$ est d'ordre n dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si x est premier à n ;

   b) Soit d un diviseur de n, montrer que $\bar{x}$ est d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $\frac{n}{d}$ divise x et $\frac{xd}{n}$ est d'ordre d dans $\mathbb{Z}/d\mathbb{Z}$.

   c) En déduire une bijection entre l'ensemble U_d des éléments d'ordre d de $\mathbb{Z}/n\mathbb{Z}$ et $(\mathbb{Z}/d\mathbb{Z})^*$), puis l'égalité :

$$n = \sum_{d \,|\, n} \varphi(d) \ .$$

   d) On suppose que la décomposition en produit de premiers de n est $n = p_1^{e_1} \cdots p_r^{e_r}$. Établir la formule :

$$n = \prod_{i=1}^{r} \left(1 + \varphi(p_i) + \cdots + \varphi(p_i^{e_i})\right) \ .$$

3. Calculer $\varphi(13\,625)$ et $\varphi(d)$ pour tout $d \,|\, 13\,625$.

Exercice 5 (Loi de réciprocité quadratique)

Soit p un nombre premier impair et soit $n = p_1^{e_1} \cdots p_r^{e_r}$ un entier naturel impair. On rappelle qu'on définit, pour $a \in \mathbb{Z}$, les *symboles de Legendre* et *de Jacobi* par :

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \text{ est un carré non nul mod } p \\ 0 & \text{si } p \,|\, a \\ -1 & \text{si } a \text{ n'est pas un carré mod } p \end{cases} \quad , \qquad \left(\frac{a}{n}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)^{e_i} \ .$$

Pour m, n entiers naturels impairs premiers entre eux, on a la loi de réciprocité quadratique et les identités :

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}} \ , \quad \left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}} \ , \quad \left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}} \ .$$

Enfin, pour m, n entiers naturels impairs et $a, b \in \mathbb{Z}$:

$$\left(\frac{a}{m}\right) = \left(\frac{b}{m}\right) \text{ si } a \equiv b \mod m \ , \qquad \left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right) \ , \qquad \left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right) \ .$$

a) Montrer que, pour tous m, n entiers naturels impairs, on a $\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}} \left(\frac{n}{m}\right)$.

b) Calculer $\left(\frac{17}{41}\right)$ et $\left(\frac{1999}{65537}\right)$.