Exercice 6
Dans tout l'exercice $x, y, z \in z$ vérifient l'équation $x^2 + y^2 = z^2$.

1) On suppose que x, y, z sont premiers entre eux (c'est-à-dire qu'il n'existe pas de $d \in \mathbb{Z}, d > 1$ tel que $d|x$, $d|y$ et $d|z$). On veut montrer qu'ils sont deux à deux premiers entre eux. Supposons que $d|x$ et $d|y$; alors on a aussi $d|(x^2+y^2)$ donc $d|z^2$. Ceci n'implique pas en général que $d|z$, par contre c'est le cas si d est premier par le lemme de Gauss que l'on rappelle ici :

Si p est premier et $p|nm$ alors $p|n$ ou $p|m$

et qui est une conséquence immédiate de la décomposition en facteurs premiers. Il suit qu'aucun nombre premier ne peut diviser à la fois x et y, c'est-à-dire que $\text{pgcd}(x, y) = 1$. De même on montre que $\text{pgcd}(x, z) = 1$ en utilisant que $y^2 = z^2 - x^2$ et que $\text{pgcd}(y, z) = 1$ à partir de $x^2 = z^2 - y^2$.

On veut maintenant voir que x et y ne peuvent pas avoir même parité. Comme ils sont premiers entre eux ils ne peuvent pas tous deux être pairs. Montrons qu'ils ne peuvent pas non plus tous deux être impairs. Pour ceci on suppose le contraire : les deux sont alors congrus à 1 ou 3 modulo 4. Comme

$$3^2 = 9 \equiv 1 \pmod 4$$

il suit que l'on a forcément $x^2, y^2 \equiv 1 \pmod 4$ et donc que

$$z^2 = x^2 + y^2 \equiv 2 \pmod 4$$

ce qui n'est pas possible car les carrés modulo 4 ne sont que 0 et 1.

Enfin z ne peut pas être pair car si c'était le cas on aurait

$$x^2 = z^2 - y^2 \equiv y^2 \pmod 2$$

qui implique que x et y ont même parité, ce qui n'est pas le cas par le point précédent.

2) On a vu que z est impair, donc si x est aussi impair alors $z - x$ et $z + x$ sont tous deux pairs. Donc 2 divise $d = \text{pgcd}(x, z)$. Il rest à montrer que :

(1) Si $p > 2$ est premier alors p ne divise pas d.

(2) 4 ne divise pas d ;

On commence par démontrer (1) : si p divise $z - x$ et $z + x$ alors p divise $2z = (z + x) + (z - x)$ et par le lemme de Gauss p divise z. de même p divise $2x = (z + x) - (z - x)$ donc p divise x, ce qui contredit 1).

L'énoncé (2) se démontre de la même manière : si 4 divise $x + y, x - y$ alors $4|(2z)$ donc $2|z$ (en effet si $2z = 4k$ il vient $z = 2k$) et de même on obtient que $2|x$, ce qui contredit encore 1).

Soit $r = (z + x)/2$ et $s = (z - x)/2$. D'après ce qui précède $\text{pgcd}(r, s) = 1$. De plus on a

$$rs = \frac{(z+x)(z-x)}{4} = \frac{z^2 - x^2}{4} = \frac{y^2}{4} = \left(\frac{y}{2}\right)^2$$

donc rs est un carré. Il suit que $r/s = (rs)/s^2$ est un carré dans $\mathbb{Q}$, c'est-à-dire qu'il existe $u, v \in \mathbb{Z}$ premiers entre eux tels que

$$\frac{r}{s} = \frac{u^2}{v^2}$$

et les deux côtés de l'inégalité sont des expréssions réduites pour une fraction, donc $r = u^2$ et $s = v^2$ sont des carrés.

On a alors

$$z = r + s = u^2 + v^2,\ x = r - s = u^2 - v^2 \text{ et } y^2 = (u^2 + v^2)^2 - (u^2 - v^2)^2 = 4u^2v^2$$

et il suit de la dernière égalité que $y = 2uv$.

3) D'après ce qui précède les solutions sont paramétrées de la manière suivante :

$$\{(x,y,z) = (d(u^2-v^2), 2duv, d(u^2+v^2)) : (u,v) \in \mathbb{Z}^2 : \text{pgcd}(u,v) = 1, d \in \mathbb{Z}\}$$

(Exercice supplémentaire : démontrer directement ce résultat à l'aide des formules donnant $\sin(\theta), \cos(\theta)$ en fonction de $\tan(\theta/2)$).

4) **(Plus dur)** On va montrer par récurrence sur $t \in \mathbb{Z}, t > 0$ que l'équation

$$x^4 + y^4 = t^2$$

n'a pas de solution entière non-évidente (ici ceci veut dire que $xy \neq 0$). Le cas où $t = 1$ est clair : si $x^4 + y^4 = 1$ alors $x^4 = 0$ ou $y^4 = 0$ et toute solution est donc évidente.

Sinon, en raisonnant comme à la question 1) on se ramène au cas où x, y, z sont deux à deux premiers entre eux, x et z sont impairs. On peut écrire

$$x^4 + y^4 = z^4 \Leftrightarrow (x^2)^2 + (y^2)^2 = t^2$$

et par le résultat de la question 2) il existe alors $m, n \in \mathbb{Z}$ avec $\text{pgcd}(m,n) = 1$ tels que

$$x^2 = m^2 - n^2, y^2 = 2mn \text{ et } t = m^2 + n^2.$$

On a $x^2 + n^2 = m^2$ et $\text{pgcd}(x,n) = 1 = \text{pgcd}(x,m)$ et en utilisant une fois de plus le résultat de 2) on peut donc écrire

$$x = r^2 - s^2, n = 2rs \text{ et } m = r^2 + s^2$$

pour des $r, s \in \mathbb{Z}$ avec $\text{pgcd}(r,s) = 1$. Il vient :

$$y^2 = 2mn = 4rs(r^2+s^2).$$

Comme $\text{pgcd}(r,s) = 1 = \text{pgcd}(r, r+s^2) = \text{pgcd}(s^2, r^2+s^2)$ il suit de cette égalité que r, s et r^2+s^2 doivent tout trois être des carrés. On écrite alors que

$$r = u^2, s = v^2, r^2 + s^2 = w^2$$

et il vient $u^4 + v^4 = w^2$. D'autre part on a $w = \sqrt{r^2+s^2} = \sqrt{m}$. Il y a alors deux possibilités :

- Soit $n = 0$, auquel cas $y = 2mn = 0$ et la solution (x,y) est donc évidente ;
- Soit $n \neq 0$, et alors $\sqrt{m} \leq m \leq m^2 < m^2 + n^2 = t$ de sorte que $w < t$. Par l'hypothèse de récurrence la solution (u,v) est évidente, c'est-à-dire que $uv = 0$. Il vient alors $rs = 0$ et donc $n = 0$, ce qui est une contradiction.

Exercice 9

1. Soit n un entier dont la représentation décimale est $a_l a_{l-1} \cdots a_0$, où $l = \lfloor \log_{10}(n) \rfloor$. Ceci signifie que

$$n = a_0 + 10a_1 + \cdots + 10^l a_l.$$

Comme $10 \equiv 1 \pmod 9$ on voit que

$$n \equiv a_0 + \cdots + a_l \pmod 9$$

et ceci démontre que le critère de divisibilité par 9 donné dans l'énoncé est correct.

2. On a :

$$10 \equiv 3 \pmod 7, \quad 10^2 \equiv 2 \pmod 7, \quad 10^3 \equiv -1 \pmod 7,$$
$$10^4 = -3 \pmod 7, \quad 10^5 \equiv -2 \pmod 7 \text{ et } 10^6 \equiv 1 \pmod 7.$$

On note que ce calcul montre que $\overline{10}$ engendre le groupe multiplicatif de $\mathbb{Z}/7\mathbb{Z}$ (montrer que ce n'est pas le cas de $\overline{2}$).

Il suit de la dernière égalité ci-dessus (ou du petit théorème de Fermat, que l'on a vérifié dans ce cas particulier) que si $a \equiv b \pmod 6$ alors $10^a \equiv 10^b \pmod 7$. On constate donc que si $a_l a_{l-1} \cdots a_0$

est la représentation décimale de n (pour simplifier la notation on suppose que $l = 6k$, quitte à ce que $a_l = 0$) alors

$$n \equiv \sum_{i=0}^{k} (a_{6i} + 3a_{6i+1} + 2a_{6i+2} - a_{6i+3} - 3a_{6i+4} - 2a_{6i+5})$$

ce qui donne un critère de divisibilité par 7. Pour un nombre à trois chiffres $a_2a_1a_0$ il revient à ce que 7 divise $2a_2 + 3a_1 + a_0$, par exemple 7 divise 301 (on vérifie $301 = 7 \times 43$).

Pour la divisibilité par 11 c'est plus simple vu que $10 \equiv -1 \pmod 1$1, et $a_{2k}a_{2k-1}\cdots a_1a_0$ est donc divisible par 11 si et seulement si

$$(a_0 + a_2 + \cdots + a_{2k}) - (a_1 + a_3 + \cdots + a_{2k-1})$$

l'est. Par exemple 2134 est divisible par 11 (on vérifie $2134 = 11 \times 194$).

Exercice 13

d) On veut montrer que :

$$(*) \qquad \forall n \in \mathbb{N} : 1 + \sum_{\substack{d|n \\ d>1}} \varphi(d) = n.$$

On va procéder par récurrence sur le nombre de facteurs premiers de n. Si $n = 1$ l'énoncé est trivial vu que la somme est vide. Si $n = p$ est premier alors $\varphi(n) = p - 1$ et p est le seul diviseur > 1 de n et on a bien $p = 1 + (p - 1)$. Plus généralement, si $n = p^a$ on a par la question b) que :

$$\begin{aligned}\sum_{p|n,p>1} \varphi(d) &= \varphi(p^a) + \varphi(p^{a-1}) + \cdots + \varphi(p) \\ &= (p^a - p^{a-1}) + (p^{a-1} - p^{a-2}) + \cdots + (p - 1) = p^a - 1\end{aligned}$$

et l'égalité $(*)$ est bien vérifiée dans ce cas encore.

Supposons maintenant que n a au moins deux facteurs premiers distincts. On peut alors écrire $n = p^a m$ où $m > 1$ n'est pas divisible par p. On a alors $\varphi(de) = \varphi(d)\varphi(e)$ pour touts e, d divisant respectivement p^a, m. Par l'hypothèse de récurrence appliquée aux nombres p^a, m qui ont tout deux strictement moins de facteurs premiers que n on a

$$m = 1 + \sum_{d|m,d>1} \varphi(d), \quad p^a = 1 + \sum_{e|p^a,e>1} \varphi(e)$$

et il suit que

$$\begin{aligned}n = p^a m &= \left(1 + \sum_{d|m,d>1} \varphi(d)\right)\left(1 + \sum_{e|p^a,e>1} \varphi(e)\right) \\ &= 1 + \sum_{d|m,e|p^a,de>1} \varphi(d)\varphi(e) = 1 + \sum_{d|m,e|p^a,de>1} \varphi(de) \\ &= 1 + \sum_{f|n,f>1} \varphi(f)\end{aligned}$$

où l'avant-dernière égalité suit de ce que l'application

$$\begin{cases} \{\text{diviseurs de } m\} \times \{\text{diviseurs de } p^a\} & \to \{\text{diviseurs de } n\} \\ (d, e) & \mapsto d \cdot e \end{cases}$$

est une bijection.