
Exercice 1

Le nombre 585 est divisible par 5 qui est un diviseur de la base (10). Donc $x+z$ est divisible par 5 (critère de divisibilité par un diviseur de la base). on a donc soit $x+y=0$, soit $x+y=5$, soit $x+y=10$, soit $x+y=15$ puisque x et y sont compris entre 0 et 9. Mais le dernier chiffre de $x+z$ est 5, on a donc $x+y=5$ ou $x+y=15$. Mais si $x+y=15$, le nombre $xyz+zyx$ s'écrirait avec quatre chiffres ; donc, $x+y=5$.
On a aussi $585 = 9\times 65 = 9\times 5\times 13$. Le critère de divisibilité par 9 (labase moins un) nous dit que la somme de ses chiffres est divisible par 9. Le premier chiffre de $xyz+zyx$ est 5. Le second est le premier chiffre de $2y$, mais $2y<10$ car sinon le troisième chiffre serait 6 et pas 5. Donc $10+2y$ est divisible par 9 et $2y<10$. Il vient $y=4$ et $x+z=5$. On observe que $x\neq 0$ et $z\neq 0$ car sinon un des nombre xyz ou zyx n'aurait pas trois chiffres.
Réciproquement, tout triplet $(x,4,5-x)$ avec $x\in\{1,2,3,4$ est tel que

$$\overline{x}\overline{45-x}+\overline{5-x4}\overline{x}=585.$$

Exercice 2

1. Par hypothèse, $m^2=\alpha n$, donc $d^2m_1^2=\alpha dn_1$ soit $dm_1^2=\alpha n_1$. Puisque d est le pgcd de m_1 et de n_1, n_1 ne divise pas m_1 et, donc, par Gauss, n_1 divise d. On peut donc écrire $d=\delta n_1$. on obtient alors $n=dn_1=\delta n_1^2$ et, donc, n est divisible par un carré parfait.
   On suppose n divisible par un carré parfait. Soit n_1 le plus grand carré parfait qui divise n et μ le plus petit entier tel que $\mu<n$ et n divise μ^2. Soit p un diviseur premier de n d'ordre $2j+\epsilon$ (ϵ est 0 ou 1) ; alors, $p^{2j+\epsilon}$ divise μ^2 donc $p^{j+\epsilon}$ divise μ. Donc si n admet $p_1^{\alpha_1}\dots p_\ell^{\alpha_\ell}$ comme décomposition en facteurs premiers, celle de μ est $p_1^{\lceil\alpha_1\rceil}\dots p_\ell^{\lceil\alpha_\ell\rceil}$. Par ce qui précède, une autre valeur de m qui convient est telle que μ^2 divise m^2 et donc, par Gauss, telle que μ divise m.
   On a $108=2^2\times 3^3$. Donc $\mu=2\times 3^2=18$. Les autres valeurs de m convenant s'écrivent 18β avec $2\times 3^2\beta<2^2\times 3^3$, on a donc $\beta=2$ ou $\beta=3$ ou $\beta=2\times 3$. D'une façon générale, si la décomposition en facteurs premiers de n est de la forme $p_1^{2\alpha_1}\dots p_\ell^{2\alpha_\ell}p_{1^\star}\dots p_k^\star$ où les $p_1\dots p_\ell$ et les $p_1^\star\dots p_k^\star$ peuvent ne pas être disjoints, les valeurs de m convenant sont de la forme $p_1^{\beta 1}\dots p_\ell^{\beta\ell}\mu$ avec $\beta_i\in\{0,\dots,\alpha_i\}$. Il y en a donc $(\alpha_1+1)\times\dots\times(\alpha_\ell+1)$.
2. On a $p=\frac{d^2n_1^2-d^2m_1^2}{n}=\frac{d^2}{n}(n_1+m_1)(n_1-m_1)$. La question précédente donne $n=dn_1$ et $d=\delta n_1$; il vient

   $$p=\delta(n_1+m_1)(n_1-m_1).$$

   On a $n>m$ et, donc, $n_1>m_1\geq 1$, soit $(n_1-m_1)>1$ et $(n_1+m_1)>2$. Donc p n'est jamais égal à 1 ou à 2.
   Si p est un nombre premier supérieur à 2, deux des trois nombres δ, (n_1-m_1) et (n_1+m_1) sont 1 et le troisième est p. (n_1-m_1) est inférieur à (n_1+m_1) est sa valeur est, donc, 1 ; on a $n_1=m_1+1$.

(n_1+m_1) est supérieur à 2 et ne peut être 1 ; donc $\delta = 1$. On obtient alors une unique solution donnée par $\delta = 1$, $2m_1 + 1 = p$ et $n_1 = m_1+1$; soit puisqu'alors $d = m_1+1$, $m = m_1(m_1+1)$ et $n = (m_1+1)^2$. L'unique solution est $n = \left(\frac{p-1}{2}+1\right)^2$ et $m = \frac{p-1}{2}\left(\frac{p-1}{2}+1\right)$.

Si $p = qr$ (on suppose $2 < q < r$), en ce cas,
- *ou bien* un des trois nombres δ, $(n_1 - m_1)$ et $(n_1 + m_1)$ est 1 et les deux autres sont q et r. (n_1+m_1) étant plus grand que (n_1-m_1), il ne peut pas être 1.
- *ou bien* deux des trois nombres δ, $(n_1 - m_1)$ et $(n_1 + m_1)$ sont 1 et le troisième est qr. Comme dans le cas précédent, c'est $(n_1 + m_1)$ qui vaut qr.

La discussion se fait sur les valeurs possibles de ces trois nombres
- $\delta = 1$ et alors $(n_1 - m_1) = q$ et $(n_1 + m_1) = r$ car $(n_1 + m_1) > (n_1 - m_1)$.
  On en déduit alors les valeurs de n_1 et de m_1. On a $n_1 = \frac{q+r}{2}$ et $m_1 = \frac{r-q}{2}$. Comme $m = \delta n_1 m_1$ et $n = \delta n_1^2$, on obtient $m = \frac{r^2-q^2}{4}$ et $n = \frac{(q+r)^2}{4}$.
- $(n_1 - m_1) = 1$, $\delta = q$ et $(n_1 + m_1) = r$.
  Il vient $n_1 = \frac{r+1}{2}$ et $m_1 = \frac{r-1}{2}$; soit $m = q\frac{r^2-1}{4}$ et $n_1 = q\frac{(r+1)^2}{4}$.
- $(n_1 - m_1) = 1$, $\delta = r$ et $(n_1 + m_1) = q$.
  Il vient $n_1 = \frac{q+1}{2}$ et $m_1 = \frac{q-1}{2}$; soit $m = r\frac{q^2-1}{4}$ et $n_1 = r\frac{(q+1)^2}{4}$.
- $(n_1 - m_1) = 1$, $\delta = 1$ et $(n_1 + m_1) = qr$.
  L'étude est similaire au cas où $p = q$; on obtient $n = \left(\frac{qr-1}{2}+1\right)^2$ et $m = \frac{qr-1}{2}\left(\frac{qr-1}{2}+1\right)$.

Les cas où q ou r sont 2 et où $q = r$ relèvent de l'étude précédente mais sont particuliers car les nombres intervenant peuvent être nuls ou non entiers.
- $r = 2$, $q > 2$ (ou $q = 2$, $r > 2$). Alors des quatre solutions précédentes, seules deux existent.
- $r > 2$, $q = r$. Alors des quatre solutions précédentes, seules trois existent.
- $q = r = 2$. Alors des quatre solutions précédentes, seules une existe.

Exercice 3

1. Si une solution n'est pas primitive, posons $d = \operatorname{pgcd}(x, y, z)$; on a alors $x = dx'$, $y = dy'$ et $z = dz'$ et si (x', y', z') est solution de $X^2 + Y^2 = Z^2$ alors (x, y, z) aussi. Donc toutes les solutions sont obtenues à partir des solutions primitives par multiplication par une constante. En outre si (x, y, z) est solution, $(\pm x, \pm y, \pm z)$ aussi ; on peut donc supposer que x, y et z sont positifs.
   Si $\operatorname{pgcd}(x, y) = d > 1$, alors d divise $x^2 + y^2$ et dpnc z^2 et donc z (par Gauss). On observe que si $x \equiv 1 \pmod 2$ et $y \equiv 1 \pmod 2$,

alors $z^2 \equiv 2 \pmod 4$, ce qui est impossible. Donc x ou y est pair. Supposons que ce soit x, alors y est impair (car sinon $\operatorname{pgcd}(x, y) = 2 > 1$).

2. Puisque $2|x$ et que $\operatorname{pgcd}(x, y) = 1$, alors z est impair et $\operatorname{pgcd}(y, z) = 1$ (sinon, un diviseur commun à y et z diviserait x^2 et donc x par Gauss). Donc $z + y$ et $z - y$ sont pairs et on peut donc écrire avec $\frac{z+y}{2}$ et $\frac{z-y}{2}$ entiers

$$\operatorname{pgcd}\left(\frac{z+y}{2}, \frac{z-y}{2}\right) = 1. \tag{1}$$

Or $x^2 + y^2 = z^2$ s'écrit

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

Donc, en considérant la décomposition de $\frac{x}{2}$ en facteurs premiers et la relation 1, il existe deux entiers positifs u et v tels que

$$\frac{z+y}{2} = u^2 \text{ et } \frac{z-y}{2} = v^2,$$

avec $u > 0$, $v > 0$, $u > v$ et $\operatorname{pgcd}(u, v) = 1$.
En outre $u^2+v^2 = z$ et $z \equiv 1 \pmod 2$, donc $u^2+v^2 \equiv 1 \pmod 2$ et, donc, $u + v \equiv 1 \pmod 2$; ce qui entraîne que u et v sont de parités différentes. Le calcul de x, y et z en fonction de u et v donne

$$\begin{cases} x = u^2 - v^2 \\ y = 2uv \\ z = u^2 + v^2 \end{cases}$$

Réciproquement, supposons que u et v soient de parité différente et satisfassent $u > v > 0$ et $\operatorname{pgcd}(u, v) = 1$, les valeurs de x, y et z précédentes donnent

$$x^2 + y^2 = 4u^2v^2 + (u^2 - v^2)^2 = (u^2 + v^2)^2 = z^2.$$

3. Une solution générale de $X^2 + Y^2 = Z^2$ s'obtient ainsi :
   - on part de deux entiers u et v satisfaisant $u > v > 0$ et $\operatorname{pgcd}(u, v) = 1$,
   - tout triplet $\big(\pm d2uv, \pm d(u^2 - v^2), \pm d(u^2 + v^2)\big)$ est solution (avec $d \geq 1$.