
Corrigé du devoir n° 1

Exercice 1. Le but de l'exercice était de démontrer que

Tout nombre premier $p \equiv 1 \pmod{4}$ est somme de deux carrés.

La preuve proposée ici est due à Don Zagier, spécialiste de Théorie des Nombres, actuellement professeur au collège de France ¹. Elle a fait l'objet d'une note parue dans l'American Mathematical Monthly en 1990 ².

Cette démonstration a l'avantage, par rapport à d'autres preuves classiques de ce résultat, d'être extrêmement brève. Autre avantage : elle n'utilise aucun outil sophistiqué d'algèbre ou d'arithmétique.

1. On définit une relation d'équivalence \mathcal{R} sur E en décrétant que deux éléments x et y de E sont en relation s'ils sont égaux ou si $y = \sigma(x)$ (ou si $x = \sigma(y)$, ce qui revient au même puisque σ est involutive). Clairement, la classe d'équivalence modulo \mathcal{R} d'un élément x contient 1 ou 2 éléments, selon que x est fixe par σ ou non. En écrivant la partition associée à \mathcal{R} et en considérant les cardinaux, on obtient la congruence annoncée.

De façon équivalente (et plus brièvement...) : le groupe cyclique d'ordre 2 engendré par σ opère sur E , et on conclut en appliquant la formule des classes.

En particulier, la parité du nombre de points fixes d'une involution sur un ensemble fini E donné *ne dépend pas de l'involution considérée*.

2. (a) S est non vide : en effet p étant congru à 1 modulo 4, il existe $z \in \mathbb{N}$ tel que $p = 1 + 4z$ et le triplet $(1, 1, z)$ appartient donc à S . Par ailleurs, les deuxième et troisième composantes d'un triplet de S sont nécessairement non nulles, car p n'est pas un carré. Il suit que si (x, y, z) est un élément de S , alors x, y et z sont majorés par p , et que S est donc fini.
(b) On a toujours $y - z < 2y$ pour un triplet (x, y, z) dans S et par ailleurs x ne peut pas être égal à $y - z$ (sinon p serait un carré) ni à $2y$ (car p serait alors divisible par 2, ce qui est incompatible avec la congruence $p \equiv 1 \pmod{4}$). Par conséquent, on peut partitionner S en la réunion de $E_1 := \{(x, y, z) \in S \mid x < y - z\}$, $E_2 := \{(x, y, z) \in S \mid y - z < x < 2y\}$ et $E_3 := \{(x, y, z) \in S \mid 2y < x\}$. Un calcul élémentaire montre alors que σ échange E_1 et E_3 , qu'elle applique E_2 sur lui-même et que $\sigma^2 = \text{Id}_E$.
(c) D'après ce qui précède, les points fixes de σ , s'il en existe, sont nécessairement dans E_2 . Ce sont donc les triplets (x, y, z) dans S tels que $x = y$. Comme $p = x^2 + 4yz$ est premier, l'égalité $x = y$ entraîne que x divise p , ce qui n'est possible que si $x = 1$. Comme on l'a vu, il existe un unique entier naturel z tel que $p = 1 + 4z$, et le triplet $(1, 1, z)$ est finalement l'unique point fixe de σ .

¹voir http://www.college-de-france.fr/default/EN/all/the_nom/index.htm

²Don Zagier, A one-sentence proof that every prime $p \equiv 1 \pmod{4}$ is a sum of two squares. *Amer. Math. Monthly* 97 (1990), no. 2, 144

- (d) De ce qui précède on peut déduire que le nombre de points fixes de n'importe quelle involution sur S est impair, donc non nul. Ainsi, l'involution $(x, y, z) \mapsto (x, z, y)$ a au moins un point fixe dans S , ce qui revient à dire qu'il existe deux entiers naturels x et y tel que $p = x^2 + 4y^2$.
- (e) Avec les notations de la question précédente, on a donc $p = x^2 + (2y)^2$, d'où le théorème.

Exercice 2. En posant $\zeta = e^{i\frac{\pi}{n}}$ on obtient :

$$\begin{aligned} \prod_{k=1}^{n-1} \sin \frac{k\pi}{n} &= \prod_{k=1}^{n-1} \frac{\zeta^k - \zeta^{-k}}{2i} \\ &= \frac{1}{2^{n-1}} \frac{1}{i^{n-1}} \prod_{k=1}^{n-1} \zeta^k \prod_{k=1}^{n-1} (1 - \zeta^{-2k}) \\ &= \frac{1}{2^{n-1}} \frac{\zeta^{\frac{n(n-1)}{2}}}{i^{n-1}} \prod_{k=1}^{n-1} (1 - \zeta^{-2k}) \\ &= \frac{1}{2^{n-1}} \prod_{k=1}^{n-1} (1 - \zeta^{-2k}) \end{aligned}$$

la dernière égalité provenant du fait que $\zeta^{\frac{n(n-1)}{2}} = i^{n-1}$.

Les puissances paires de ζ sont les racines, dans \mathbb{C} , du polynôme $X^n - 1$. Autrement dit

$$X^n - 1 = \prod_{k=0}^{n-1} (X - \zeta^{-2k}) = (X - 1) \prod_{k=1}^{n-1} (X - \zeta^{-2k}). \quad (1)$$

On a par ailleurs, dans $\mathbb{C}[X]$, l'identité

$$X^{2n} - 1 = (X^n - 1)(X^n + 1) = (X - 1)(X^{2n-1} + X^{2n-2} + \dots + X + 1). \quad (2)$$

En combinant (1) et (2) on obtient

$$\prod_{k=1}^{n-1} (X - \zeta^{-2k}) = \frac{X^{2n-1} + X^{2n-2} + \dots + X + 1}{X^n + 1}$$

et en évaluant cette dernière expression en $X = 1$, on trouve le résultat attendu, à savoir

$$\prod_{k=1}^{n-1} (1 - \zeta^{-2k}) = n.$$