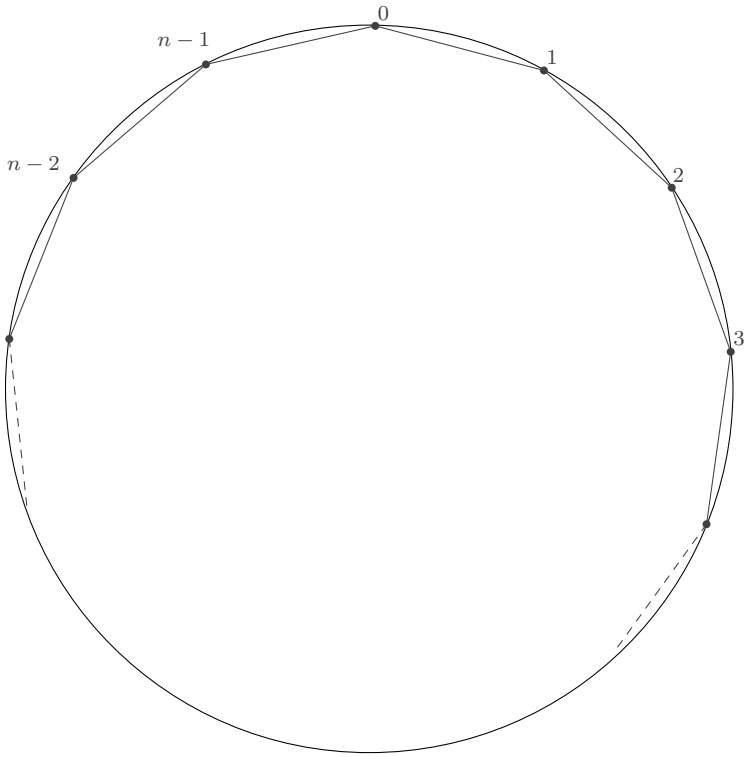
Activité 3 : arithmétique

Nombre de sommets parcourus

Soit n un entier naturel, on considère un polygone (régulier) à n sommets, que l'on numérote de 0 à $n-1$ (avec un choix arbitraire du sommet « origine » et du sens de rotation) :



Si p est un entier naturel, « aller de p en p » sur les sommets du polygone (ou faire un **pas** de p) consiste à parcourir les sommets en allant du sommet numéroté x à celui dont le numéro est

$$x + p \bmod n$$

c'est-à-dire le reste de $x + p$ dans la division euclidienne par n.

Si l'on part du sommet origine (numéroté 0), on parcourt donc les sommets dont les numéros sont les multiples de p modulo n :

$$0,\ p \bmod n,\ 2p \bmod n,\ 3p \bmod n,\ \ldots$$

jusqu'à revenir à l'origine. Supposons qu'on revient à l'origine après avoir parcouru k sommets (sans compter l'origine), où k est un entier, on a alors :

$$kp \equiv 0 \bmod n$$

autrement dit n divise kp (au sens de l'arithmétique, c'est-à-dire kp est un multiple entier de n).

Le premier retour à l'origine se produit donc lorsque kp est le plus petit multiple commun à p et à n. Or on sait que

$$\text{ppcm}(p,n) = \frac{pn}{\text{pgcd}(p,n)}$$

donc il se produit lorsque $kp = pn/\text{pgcd}(p,n)$, autrement dit lorsque le nombre de sommets parcourus (sans compter l'origine) est égal à

$$\frac{n}{\text{pgcd}(p,n)}$$

Remarquons qu'une fois de retour à l'origine, on repasse ensuite par les mêmes sommets. Notons $N_n(p)$ le nombre de sommets parcourus dans le polygone à n sommets lorsqu'on le parcourt de p en p, on a montré la propriété suivante.

Proposition 1. *Soient n et p des entiers alors $N_n(p) = \dfrac{n}{\text{pgcd}(p,n)}$.*

Enfin, si l'on itère n fois l'opération « aller d'un sommet au suivant quand on va de p en p », puisqu'on revient au sommet de départ après avoir parcouru $N_n(p)$ sommets, chacun de ses sommets sera parcouru

$$\frac{n}{N_n(p)} = \text{pgcd}(p,n)$$

fois.

Critères de (co-)primalité

On déduit immédiatement de la Proposition 1 un critère de co-primalité de deux entiers.

Corollaire 2. *Soient n et p des entiers, alors n et p sont premiers entre eux si et seulement si $N_n(p) = n$.*

On peut énoncer ce critère en termes purement géométriques : n et p sont premiers entre eux si et seulement si, lorsqu'on joint de p en p les sommets d'un polygone régulier à n côtés, on passe par tous ces points avant de revenir au premier.

Exercice 1. Adapter le script de l'Activité 2 (avec les listes de variables) pour tester la co-primalité de deux entiers.

Puisqu'un entier n est premier si et seulement si il est premier à tous les entiers qui lui sont strictement inférieurs et qu'on a, pour tout entier p compris entre 1 et $n-1$:

$$N_n(n-p) = N_n(p)$$

on en déduit le critère de primalité suivant.

Corollaire 3. *Soient n un entier, alors n est premier si et seulement si $N_n(p) = 1$ pour tout entier p compris entre 2 et $n/2$.*

On sait par un autre argument élémentaire qu'il suffit de vérifier que $N_n(p) = 1$ pour p compris entre 2 et $\sqrt{n}$.

Exercice 2. Adapter le script de l'exercice précédent (boucle sur p) pour tester la primalité d'un entier.

La théorie de l'ordre de Poinsot

Le contenu de cette partie et les citations sont tirées de l'article de Jenny Boucard — «Une géométrie de l'ordre et de la situation au XIX^{e} siècle. Polygones et théorie des nombres chez Louis Poinsot» — Images des Mathématiques, CNRS, 2016, en ligne sur

`http://images.math.cnrs.fr/`

Louis Poinsot (1777-1859) est un mathématicien français reconnu de la première moitié du XIX^{e} siècle, notamment pour ses travaux sur l'utilisation des polygones étoilés pour les démonstrations de propriétés arithmétiques. Il appelle ce mode de raisonnement la *théorie de l'ordre*, et il voit cette théorie comme le principe fondamental dont découlent les propriétés des nombres.

Dans son mémoire de 1841, il démontre notamment la propriété suivante.

Proposition 4. *Soient a, b, n des entiers avec a premier à n et b premier à n, alors ab est premier à n.*

Cette propriété sert dans de nombreux autres raisonnements, il l'établit à l'aide du critère de co-primalité que nous avons appelé ci-dessus Corollaire 2, en raisonnant comme suit.

> « Il suffit de considérer un sommet de départ, puis de parcourir le polygone de n sommets de a en a. Comme, par hypothèse, a et n sont premiers entre eux, on forme ainsi un nouveau polygone à n côtés. Sur ce polygone à n côtés, on va de b sommets en b sommets : comme b et n sont premiers entre eux, on obtient à nouveau un autre polygone de n côtés, en étant passé une unique fois sur chaque sommet. Or, considérer des intervalles de a sommets, puis, à partir de ces intervalles, considérer des intervalles de b sommets, revient à considérer des intervalles de ab sommets. Comme on obtient un polygone de n côtés, en passant une seule fois par chaque sommet, le produit ab est bien premier à n. »

Autre application de la théorie de l'ordre, la recherche de solution d'équation en nombres entiers du type

$$Lx + My = 1$$

où L et M sont premiers entre eux (autrement dit recherche d'une *relation de Bézout* entre L et M). Voici comment Poinsot raisonne.

> « Pour déterminer une valeur de x, il suffit de considérer M points a, b, c,..., m rangés en cercle et de les joindre de L en L : puisque L et M sont premiers entre eux, on obtient un polygone étoilé. Une valeur de x est alors donnée par l'écart λ séparant a et b dans ce nouveau polygone. En effet, prendre les points de L en L, puis de λ en λ, revient à les joindre de $L\lambda$ en $L\lambda$, c'est-à-dire de 1 en 1. Donc $L\lambda = 1 + kM$, où k est un nombre entier. On peut en déduire la valeur de y, ou bien la déterminer directement en utilisant le même procédé. Poinsot propose un exemple, avec l'équation $12x - 7y = 1$. »

Exercice 3. Appliquer la méthode de Poinsot pour déterminer une solution (x, y) de l'équation $12x - 7y = 1$.

Preuve géométrique du théorème de Fermat

Dans le chapitre *Image de combinatoires en France au XIX^{e} siècle : à la recherche des combinaisons dans les Nouvelles annales de mathématiques (1842-1914)* du livre *Les travaux combinatoires en France (1870-1914) et leur actualité : un hommage à Henri Delannoy* (Limoges, PULIM, 2017), Jenny Boucard présente une preuve originale et élémentaire du théorème de Fermat par Raoul Bricard (1870-1943), mathématicien français qui la publie en esperanto en 1903 dans les *Nouvelles*

Annales de Mathématiques, une revue destinée « aux candidats aux concours d'admission aux Écoles polytechnique et normale, puis également aux aspirants à la licence et l'agrégation à partir de 1888 ».

Il s'agit bien sûr ici du "petit" théorème de Fermat, celui qui stipule que si p est un nombre premier et m un entier quelconque, alors $m^p - m$ est un multiple de p. Bricard se place dans le système de numération en base m ; on peut y écrire exactement m^p nombres à p chiffres, dont m nombres ont tous leurs chiffres identiques. Étant donné l'un des $m^p - m$ nombres à p chiffres non tous identiques, disons $A_0 = a_0 a_1 \dots a_{p-1}$, on considère les nombres obtenus par permutation circulaire des chiffres de A_0 :

$$A_1 = a_1 a_2 \dots a_{p-1} a_0,\ A_2 = a_2 \dots a_{p-1} a_0 a_1,\ \dots,\ A_{p-1} = a_{p-1} a_0 \dots a_{p-2},\ A_p = A_0$$

Il suffit de voir que ces nombres sont tous distincts pour en déduire que les $m^p - m$ nombres à p chiffres non tous identiques se répartissent en classes à p éléments, toutes disjointes, ce qui entraîne que $m^p - m$ est un multiple de p.

Raisonnons par l'absurde en supposant que $A_0 = A_h$ pour un entier h compris entre 1 et $p-1$ (donc h premier à p). On a

$$A_h = a_h \dots a_{p-1} a_0 \dots a_{h-1}$$

et, pour $0 \leq i \leq p-1$, le i-ième chiffre de A_h est $a_{i+h \bmod p}$ donc notre hypothèse entraîne

$$a_0 = a_h = a_{2h \bmod p} = a_{3h \bmod p} = \dots$$

Si l'on trace un polygone (régulier) à p sommets, indicés par les chiffres a_0, a_1,..., a_{p-1} de A_0, aller de h en h dans ce polygone (en partant de a_0) fait donc passer par des sommets dont les indices sont tous égaux. Or h est premier à p donc on passe par tous les sommets du polygone lorsqu'on va de h en h et on obtient, par ce qui précède, que tous les chiffres de A_0 sont identiques, ce qui est une contradiction.

L'originalité de cette preuve vient surtout de l'interprétation combinatoire de la quantité $m^p - m$, dont on veut prouver qu'elle est un multiple de p, comme le nombre de nombres à p chiffres non tous identiques en base m. Le critère géométrique de co-primalité de deux entiers (h et p dans le raisonnement par l'absurde), qui a l'avantage de s'exprimer de façon élémentaire, pourrait être remplacé par la propriété suivante.

Proposition 5. *Soient n et m des entiers, alors m est premier à n si et seulement la classe de m modulo n engendre le groupe additif $\mathbb{Z}/n\mathbb{Z}$ des classes d'entiers modulo n.*

Il faut reconnaître que cette formulation (dont la preuve peut se faire en passant par le critère de Bézout), équivalente à notre critère géométrique, est moins parlante pour le non initié !