PGCD, Nombres premiers entre eux

Objectifs :

- Connaître et savoir utiliser la notion de PGCD, le théorème de Bézout, le théorème de Gauss
- Aborder les applications de ces théorèmes dans des contextes variés (cryptographie par exemple)

Aperçu historique :

La cryptographie est l'ensemble des techniques qui permettent de coder et décoder des messages. Ses usages sont variés, mais souvent militaires. cependant le premier document "chiffré" connu remonte à l'antiquité et décrit la recette secrète d'un potier. Les Grecs ont utilisé les messages chiffrés principalement militaires, en enroulant une bande de cuir autour d'un bâton (*scytale*). Nabuchodonosor, roi de Babylone, écrivait sur le crâne rasé de ses esclaves et attendait que leurs cheveux repoussent.
Les Hébreux chiffraient des textes religieux en utilisant une méthode de substitution, l'*Atbash*.
C'est vers -200 qu'apparaissent les premiers véritables systèmes de chiffrement, en général des chiffrements par substitution : le *chiffre de César* (simple chiffrement affine), le *carré de Polybe* (homophonique).
Qui dit chiffrement dit déchiffrement, et au IXème siècle, le savant arabe *Al-Kindi* écrit le *manuscrit sur le déchiffrement de messages cryptographiques*. Il y présente la méthode de l'analyse des fréquences, qui est très efficace pour décoder les chiffres de substitution.
En 1379, *Gabriele de Lavinde*, secrétaire du Pape, écrit un recueil de codes appelé *Nomenclateur*.
Puis apparaissent, pour déjouer la méthode d'analyse des fréquences, les chiffres *polyalphabétiques*, le *chiffre de Vigenère*, le *Grand Chiffre du Roi Louis XIV* ...
En 1883, le Hollandais *Auguste Kerckhoffs* publie *La cryptographie militaire*, où il expose les règles pour concevoir un bon système cryptographique, toujours valables aujourd'hui.
Pendant la première guerre mondiale, les Français mettent en place le "*cabinet noir*", chargé de décrypter les messages allemands ; *le télégramme Zimmermann*, intercepté en 1917 par le Royaume-Uni qui cryptanalysa son contenu, a accéléré l'entrée en guerre des États-Unis.
Lors de la seconde guerre mondiale, la mise au point par les Allemands de *la machine Enigma* leur donne un avantage certain jusqu'à ce que l'équipe qui travaillait avec *Alan Turing à Bletchley Park* mette au point une machine appelée "*La bombe*" qui permettait de décoder les messages encodés avec Enigma.
D'autres codes furent utilisés, le *chiffre de Lorenz*, le *code Navajo*...
De nos jours, le *chiffrement RSA* et le développement grâce à la puissance de calcul des ordinateurs modernes des *fonctions de hachage* (dont la réciproque est impossible à déterminer) permettent de chiffrer efficacement les données sensibles qui circulent sur internet, par exemple.
Pour plus de renseignements sur le cryptographie, se référer à l'excellent et très accessible livre de *Simon Singh*, "**Histoire des codes secrets**".

Scytale

Enigma

1. PGCD de deux entiers

Définition 7.1 Soient $a, b \in \mathbb{Z}$ dont l'un au moins est non nul. L'ensemble des des diviseurs communs à a et b admet un plus grand élément , appelé **plus grand commun diviseur** à a et b, et noté $PGCD(a, b)$.
Lorsque $PGCD(a, b) = 1$, on dit que a et b sont **premiers entre eux**.

Démonstration L'ensemble des diviseurs communs à a et b est non vide (il contient 1) et fini ; or tout sous-ensemble de $\mathbb{Z}$ fini non vide admet un plus petit élément, d'où l'existence du PGCD.
Son unicité se démontre par l'absurde (on en suppose deux distincts et on aboutit à une contradiction).

Propriété 7.1 Soient $a, b \in \mathbb{Z}$, avec $a \neq 0$. On a :

- $PGCD(a, 0) = a$; $PGCD(a, 1) = 1$
- $PGCD(a, b) = PGCD(|a|, |b|)$
- Si $b|a$, alors $PGCD(a, b) = |b|$
- Si b est premier et $b \nmid a$, $PGCD(a, b) = 1$

Compte tenu du deuxième point, on peut se limiter à l'étude du PGCD de deux entiers naturels.

Propriété 7.2 Lemme d'Euclide Soient $a, b \in \mathbb{N}^*$, avec $b < a$. Soit r le reste de la division euclidienne de a par b.
L'ensemble des diviseurs communs à a et b est confondu avec celui des diviseurs communs à b et r.
Par suite, $PGCD(a, b) = PGCD(b, r)$.

Cette propriété a pour conséquence la recherche du PGCD par l'algorithme d'Euclide.

Démonstration On a $a = bq + r$ avec les notations habituelles. Il vient :
$d|a$ et $d|b \Rightarrow d|r$
$d|b$ et $d|r \Rightarrow d|a$

Propriété 7.3 Soient $a, b \in \mathbb{N}^*$, avec $D = PGCD(a, b)$. L'ensemble des diviseurs communs à a et b est l'ensemble des diviseurs de D.

Propriété 7.4 Homogénéité Soient $a, b, k \in \mathbb{N}^*$. Alors :

$$PGCD(ka, kb) = k \times PGCD(a, b)$$

Démonstration Soient $D = PGCD(a, b)$ et $D' = PGCD(ka, kb)$.
$D|a$ et $D|b$, donc $kD|ka$ et $kD|kb$; ainsi, $kD \leqslant D'$ (car D' est "le plus grand" diviseur commun).
Par ailleurs, $k|ka$ et $k|kb$, donc $k|D'$, i.e. $\exists n \in \mathbb{N}$ t.q. $D' = kn$.
Or $D'|ka$ et $D'|kb$ donc $n|a$ et $n|b$; donc $n \leqslant D$ (car D est "le plus grand" diviseur commun).
En multipliant membre à membre par $k > 0$, il vient $kn \leqslant kD$, i.e. $D' \leqslant kD$.
Finalement, $D' = kD$. (car la relation d'ordre $\leqslant$ est antisymétrique).

Propriété 7.5 caractérisation Soient $a, b \in \mathbb{N}^*$.
$D = PGCD(a, b)$ ssi $\frac{a}{D}$ et $\frac{b}{D}$ sont des entiers premiers entre eux.

Démonstration faite en exercice.

2. Théorème de Bézout, Théorème de Gauss.

Propriété 7.6 Soient $a, b \in \mathbb{Z}^*$, et soit $D = PGCD(a, b)$.
Alors il existe $u, v \in \mathbb{Z}$ tels que $au + bv = D$.

Démonstration

- Soit E l'ensemble des **entiers naturels non nuls** de la forme $ax + by$, où x et y sont des entiers relatifs.
  E est une partie non vide de $\mathbb{N}$ (elle contient $|a|$), elle admet un plus petit élément. Notons-le n.
  Par définition de E, il existe $u, v \in \mathbb{Z}$ t.q. $n = au + bv$.
  Or $D|a$ et $D|b$, donc $D|n$. Donc $D \leqslant n$.
- Écrivons la division euclidienne de a par n :
  $a = nq + r$, avec $0 \leqslant r < n$, et $q \in \mathbb{Z}$.
  Il vient $r = a - nq = a - q(au + bv) = a(1 - qu) + b(1 - qv)$; ainsi r est de la forme $ax + by$, avec $x = 1 - qu \in \mathbb{Z}$ et $y = 1 - qv \in \mathbb{Z}$.
  Mais $r < n$, et par définition de n, $r \notin E$.
  On a donc $r = 0$, et par suite $n|a$.
- On montre de la même manière que $n|b$.
- Donc n est un diviseur commun à a et b, et par définition de D, $n \leqslant D$.
- Finalement, $D \leqslant n$ et $n \leqslant D$, donc $n = D$, et par suite $D = au + bv$.

Théorème 7.1 de Bézout, *initialement énoncé par Bachet*.
Deux entiers relatifs a et b sont premiers entre eux si et seulement si il existe des entiers relatifs u et v tels que

$$au + bv = 1$$

Démonstration $(\Rightarrow)$. Supposons $PGCD(a; b) = 1$. Alors, d'après la propriété qui précède, il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$.
$(\Leftarrow)$. Supposons qu'il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$. Soit $D = PGCD(a, b)$. Alors $D|a$ et $D|b$, donc $D|(au + bv)$, i.e. $D|1$. Donc $D = 1$.

Théorème 7.2 de Gauss.
Soient $a, b, c \in \mathbb{Z}^*$.
Si $a|bc$ et si a et b sont premiers entre eux, alors $a|c$.

Démonstration Soient $a, b, c \in \mathbb{Z}^*$ tels que $a|bc$ et a et b sont premiers entre eux.
$a|bc \Rightarrow \exists k \in \mathbb{Z}^*$ t.q. $bc = ka$.
Or a et b sont premiers entre eux, donc d'après le théorème de Bézout, $\exists u, v \in \mathbb{Z}$ t.q. $au + bv = 1$.
On multiplie par c cette égalité, il vient $c = acu + bcv = acu + kav = a(cu + kv)$.
Or $(cu + kv) \in \mathbb{Z}$, donc $a|c$.