SF 1 Montrer que b divise a

- *Option 1.* On parvient à écrire $a = kb$ avec $k \in \mathbb{Z}$.
- *Option 2.* On utilise les congruence pour montrer que : $a \equiv 0\ [b]$.
- *Option 3.* On utilise le lemme de Gauss en montrant que $b \mid aa'$ où $b \wedge a' = 1$.
- *Option 4.* On utilise les décompositions en facteurs premiers de a et b en comparant les exposants des facteurs premiers dans les deux décompositions

SF 2 Utiliser les congruences pour obtenir le reste d'une division

Pour obtenir le reste de la division euclidienne de a par b on utilise le calcul avec les congruences afin d'obtenir $a \equiv r\ [b]$ pour un $r \in [\![0, b-1]\!]$.

SF 3 Utiliser les congruences pour simplifier a^n modulo b

- On cherche une puissance de a congrue à 1 modulo b : $a^q \equiv 1\ [b]$.
- Notant r le reste de la D.E. de n par l'exposant q trouvé on a alors : $a^n \equiv a^r\ [b]$

SF 4 Résoudre l'équation $ax \equiv b\ [n]$ lorsque $a \wedge n = 1$

- On détermine[a] un inverse u de a modulo n *i.e.* u tel que $au \equiv 1\ [n]$
- En multipliant l'équation par u on se ramène à $x \equiv ub\ [n]$.

a. Eventuellement via une relation de Bézout entre a et n qui fournit u et v tels que $au + nv = 1$

SF 5 Calculer le PGCD de a et b et une relation de Bézout entre a et b

- Pour le calcul du PGCD, on effectue une suite de division euclidiennes : $a \wedge b$ est le dernier reste non-nul fourni par l'algorithme d'Euclide.
- Pour la relation de Bézout, on « remonte » l'algorithme d'Euclide en « renversant » les divisions euclidiennes.

SF 6 Etablir une égalité du type : $a \wedge b = c \wedge d$

- *Option 1.* A l'aide de la propriété de conservation du PGCD : $a \wedge b = b \wedge (a - bq)$ on parvient, par une succession d'égalités, à transformer $a \wedge b$ en $c \wedge d$
- *Option 2.* On montre que $d = a \wedge b$ et $\delta = c \wedge d$ vérifient : $d \mid \delta$ et $\delta \mid d$

SF 7 Résoudre dans $\mathbb{Z}^2$ l'équation diophantienne $ax + by = c$ où $a \wedge b = 1$

- On trouve une solution particulière (éventuellement via une relation de Bézout)
- *Analyse.* Si (x, y) est solution :
  - on obtient : $(\star) \quad a(x - x_0) = b(y_0 - y) \qquad$ où $a \wedge b = 1$
  - on détermine la forme de y à l'aide du lemme de Gauss
  - on en déduit la forme de x en reportant l'expression de y dans $(\star)$.
- *Synthèse.* On vérifie que les couples candidats obtenus sont solutions.

SF 8 Résoudre dans $\mathbb{N}^2$ une équation faisant intervenir $x \wedge y$ ou $x \vee y$

- *Analyse.* Si (x, y) est solution on peut :
- Factoriser par le PGCD *i.e.* écrire $x = dx'$ et $y = dy'$ où $x' \wedge y' = 1$ et $x' \vee y' = x'y'$.
- Essayer d'obtenir une relation simple sur x' et y' comme :
  - Essayer de déterminer la valeur de la somme $x' + y'$.
  - Essayer de déterminer les valeurs de $x' + y'$ et $x'y'$.
  - Essayer de factoriser l'égalité obtenue sur x' et y' pour se ramener à un produit égal à un entier a et raisonner sur les diviseurs de a.
- *Synthèse.* On vérifie si les couples candidats obtenus sont solutions.

SF 9 Montrer que a et b sont premiers entre eux

- *Option 1* A l'aide de la propriété de conservation : « $a \wedge b = b \wedge a - bq$ » on parvient à transformer $a \wedge b$ en un PGCD du type $c \wedge 1$.
- *Option 2* Grâce au théorème de Bézout : on trouve $u, v \in \mathbb{Z}$ tels que $au + bv = 1$
- *Option 3* On pose $d = a \wedge b$ et on montre que $d \mid 1$.

SF 10 Savoir quand utiliser la décomposition en facteur premier

Pour traiter des exercices abstraits mêlant divisibilité et puissances il peut être efficace d'utiliser au choix :

- les propriétés des valuations p-adiques (l'additivité et lien avec la divisibilité)
- ou la décomposition en facteur premier

SF 11 Calculer une valuation p-adique : $v_p(a)$

On peut exploiter :

- la propriété d'additivité : v_p transforme les produits en somme
- le fait que $v_p(a) = k$ ssi $a = p^k q$ où p ne divise pas q