Méthodes Arithmétique

Calculer le reste a^n dans la division par k

Pour calculer le reste de a^n dans la division par k,

- on commence par rechercher un entier $m \geq 1$ tel que $a^m \equiv 1\ [k]$ (on pourra calculer les puissances successives, ou utiliser le petit théorème de Fermat);
- si $n \equiv r\ [m]$, alors $n = qm + r$ et $a^n \equiv (a^m)^q a^r\ [k] \equiv a^r\ [k]$;
- il reste à calculer le reste de a^r dans la division par k;

Calculer le pgcd de deux entiers a et b

- On peut utiliser l'algorithme d'Euclide
- On peut utiliser la décomposition en facteurs premiers des entiers concernés
- On peut utiliser la définition

Résoudre une équation de Bézout $ax+by=c$

- On commence par calculer $d=a\wedge b$.
- Si dd ne divise pas cc, alors puisque $d|ax+by$, l'équation ne peut pas avoir de solutions. Sinon, on peut tout diviser par dd. Cela revient à supposer que a et b sont premiers entre eux, ce que nous supposerons désormais.
- On cherche un couple d'entiers (u,v) tel que $au+bv=1$. On sait qu'un tel couple existe par le théorème de Bézout, et on le détermine par l'algorithme d'Euclide étendu.
- On pose $x_0=cu$ et $y_0=cv$. Alors (x_0,y_0) est une solution particulière de $ax+by=c$.
- Soit (x,y) une solution. Alors on retranche $ax_0+by_0=c$ à $ax+by=c$, et on trouv e$a(x-x_0)=-b(y-y_0)$.Puisque $a\wedge b=1$, ceci entraîne $a|y-y_0$ et donc $y=y_0+a$, $k\in Z$. On reporte alors ceci dans l'équation $a(x-x_0)=-b(y-y0)$ pour exprimer x en fonction de x_0 et k.
- Réciproquement, on doit prouver que les solutions trouvées conviennent.