1 Mathématiques discrètes – M1201

Prérequis :

- Algorithme d'Euclide étendu + Théorème de Bachet-Bézout
- Résolution d'équations diophantiennes

Cours :

Lemme de Gauss : $a, b, c \in \mathbb{N}^*$

Si $a|bc$ et $\text{pgcd}(a, b) = 1$ alors $a|c$

Petit théorème de Fermat : $a \in \mathbb{N}^*$ et p un nombre premier

Si p ne divise pas a alors : $a^{p-1} \equiv_p 1$

Théorème d'Euler : $n \in \mathbb{N}^*$ et $a \in \mathbb{N}$ tel que $\text{pgcd}(a, n) = 1$

$$a^{\varphi(n)} \equiv_n 1$$

Fonction $\varphi(n)$: p est premier

$$\varphi(p^\alpha) = p^{\alpha-1}(p-1) \quad \text{et} \quad \varphi(p^\alpha * q^\beta) = \varphi(p^\alpha) * \varphi(q^\beta)$$

Théorème des reste chinois : $(a, b) \in \mathbb{Z}^2$ et n_1 et n_2 sont premiers entre eux $\rightarrow \exists(u, v) \in \mathbb{Z}^2, n_1u + n_2v = 1$

Les solutions de $\begin{cases} x \equiv_{n_1} a \\ x \equiv_{n_2} b \end{cases}$ sont :

$$x \equiv_{n_1 * n_2} n_1u * b + n_2v * a$$

<u>Exemples méthodes :</u>

- **Calculer $a \equiv_p$**
  - Si p est premier : $7^{126} \equiv_{11}$?
    - Appliquer le petit théorème de Fermat : $7^{10} \equiv_{11} 1$
    - Élever les nombres des deux côtés pour se rapprocher du nombre de base : $(7^{10})^{12} \equiv_{11} (1)^{12} \quad \leftrightarrow \quad 7^{120} \equiv_{11} 1$
    - Multiplier par des puissances de *a* des deux côtés pour retrouver le nombre de base : $7^{120} * 7^6 \equiv_{11} 1 * 7^6 \quad \leftrightarrow \quad 7^{126} \equiv_{11} 7^6$

  - Si *a* et p sont premiers entre eux : $2^{50} \equiv_{45}$?
    - Appliquer le théorème d'Euler : $2^{\varphi(45)} \equiv_{45} 1$
    - Calculer $\varphi(p)$:
      $\varphi(45) = \varphi(3^2 * 5) = \varphi(3^2) * \varphi(5) = 3^{2-1}(3-1) * (5-1) = 6 * 4 = 24$
    - Élever les nombres des deux côtés pour se rapprocher du nombre de base : $(2^{24})^2 \equiv_{45} (1)^2 \quad \leftrightarrow \quad 2^{48} \equiv_{45} 1$
    - Multiplier par des puissances de *a* des deux côtés pour retrouver le nombre de base : $2^{48} * 2^2 \equiv_{45} 1 * 2^2 \quad \leftrightarrow \quad 2^{50} \equiv_{45} 2^2$

  - En appliquant le théorème des restes chinois : $63^{241} \equiv_{175}$?
    - On cherche à décomposer *p* en produit de deux facteurs premiers entre eux: $175 = 25 * 7$
    - On calcule *a* modulo ces deux facteurs (si nécessaire appliquer les méthodes précédentes) : $63^{241} \equiv_{25}$? et $63^{241} \equiv_7$?
    - On fait l'algorithme de Bachet-Bézout avec les deux facteurs : $2 * 25 - 7 * 7 = 1$
    - On trouve $\begin{cases} a \equiv_{f1} b \\ a \equiv_{f2} c \end{cases}$ puis on applique donc le théorème des restes chinois :

      On a $\begin{cases} 63^{241} \equiv_{25} 13 \\ 63^{241} \equiv_7 0 \end{cases} \rightarrow \quad 63^{241} \equiv_{25*7} 2 * 25 * 0 + 7 * 7 * 13 \quad \leftrightarrow$

      $63^{241} \equiv_{175} -49 * 13$

- **Résoudre des équations dans un anneau ($\bar{a}x = \bar{b}$ dans $\mathbb{Z}$/n$\mathbb{Z}$)**
  - $\bar{a}$ est inversible dans $\mathbb{Z}$/n$\mathbb{Z}$ ($\mathrm{pgcd}(a, n) = 1$) : $\overline{143}x = \bar{2}$ dans $\mathbb{Z}$/3072$\mathbb{Z}$
    - Trouver l'inverse de $\bar{a}$
      - Théorème de Bachet-Bézout : $3072 * (-29) + 143 * 623 = 1$
      - Passer l'équation dans l'anneau : $\overline{3072} * \overline{(-29)} + \overline{143} * \overline{623} = \bar{1} \quad \leftrightarrow$

        $\bar{0} * \overline{(-29)} + \overline{143} * \overline{623} = \bar{1} \quad \leftrightarrow \quad \overline{143} * \overline{623} = \bar{1}$
    - Multiplier par l'inverse des deux côtés de l'équation : $\overline{623} * \overline{143}x = \bar{2} * \overline{623}$

      $\leftrightarrow \quad x = \bar{2} * \overline{623} \quad \leftrightarrow \quad x = \overline{1246}$