Mathématiques discrètes – M1201

Cours :

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

Si $a|bc$ et $\mathrm{pgcd}(a,b) = 1$ 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 $\mathrm{pgcd}(a,n) = 1$

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

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 → $\exists(u,v) \in \mathbb{Z}^2, n_1u + n_2v = 1$

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

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

Exemples méthodes :

- **Résoudre $a \equiv_p b$**
  - 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 : $2^{48} * 2^2 \equiv_{45} 1 * 2^2 \quad \leftrightarrow \quad 2^{50} \equiv_{45} 2^2$

-