25

Savoir-faire et thèmes classiques – Algèbre modulaire

Savoir-faire

- ☐ Définir la relation de congruence modulo n, traduire que deux nombres sont congrus modulo n par un argument de divisibilité
- ☐ Connaître les critères de divisibilité par $2, 3, 4, 5, 8, 9, 10, 11$
- ☐ Obtenir une divisibilité par calcul modulaire
- ☐ Définir l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ des entiers modulo n, déterminer ses éléments inversibles, les générateur du groupe cyclique additif correspondant, connaître une CNS pour que ce soit un corps (noté alors $\mathbb{F}_p$)
- ☐ Calculer effectivement l'inverse d'un élément inversible de $\mathbb{Z}/n\mathbb{Z}$
- ☐ Résoudre un système linéaire, une équation du second degré dans $\mathbb{F}_p$
- ☐ Connaître les deux versions (pratique et théorique) du théorème chinois
- ☐ Résoudre un système de congruence par théorème chinois ou par résolution d'équations diophantienne, être capable en particulier de trouver une solution particulière rapidement
- ☐ Définir l'indicatrice d'Euler, connaître les images des puissances des nombres premiers, son caractère multiplicatif, en déduire l'expression de $\varphi(n)$ à l'aide des diviseurs premiers de n
- ☐ Connaître le théorème d'Euler et son corollaire, le petit théorème de Fermat
- ☐ Calculer les puissances d'un entier modulo n : soit en trouver une cyclicité à la main, soit en utilisant le théorème d'Euler ou le petit théorème de Fermat

Thèmes Classiques

- ☐ Carrés dans $\mathbb{F}_p$
- ☐ Théorème de Wilson
- ☐ Chiffrement RSA
- ☐ Expression de $\varphi(n)$ obtenue avec des arguments probabilistes
- ☐ Identité $n = \sum_{k|n} \varphi(k)$