110 – Nombres premiers. A.

« Quand vous étiez petits, vous connaissiez $\mathbb{N}$. Puis après, vous avez appris que le mal existait : $\mathbb{Z}$, les négatifs ! »

Le plan :

I) Résultats fondamentaux.
Résultats dus à Euclide. Infinité de nombres premiers. $\mathbb{Z}$ est factoriel. Valuation p-adique. Propriétés de congruence. Fermat, Wilson, Fermat-Euler. Application au système de cryptage RSA.

II) Localisation.
Dirichlet faible. $\sum 1/p=+\infty$. Tchebychev. Théorème des nombres premiers. Nombres remarquables : Fermat, Mersenne. Tests de primalité : cribles d'Eratosthène et Matiiasevitch, test de Fermat, Lucas-Lehner.

III) Arithmétique.
Indicatrice d'Euler. Propriétés générales. Symbole de Legendre : critère d'Euler, loi de réciprocité quadratique. Théorème de Frobenius-Zolotarev. Somme de deux carrés : $\mathbb{Z}[i]$, théorème des deux carrés.

IV) Applications.
Théorie des groupes : groupes cycliques, théorèmes de Sylow. Corps finis : construction, existence, caractéristique. Réduction des polynômes : Eisenstein, réduction modulo p.

Les développements :

A16 : Frobenius-Zolotarev
A20 : Théorème des deux carrés
A21 : Théorème de Tchebychev

La bibliographie :

[CaA]-[Zem]-[Per]-[HaW]-[Cmb]-[BMP]-[Duv]-[Del]