Congruences, $\mathbb{Z}/n\mathbb{Z}$

1 Rappels d'arithmétique

Division euclidienne et formule de Bezout.
Description des idéaux de Z : tout idéal
- c'est à dire un sous-ensemble non vide S tel que si $x, \in S$ alors $x + y \in S$ et si $\lambda \in \mathbb{Z}$ et $x \in S$ alors $\lambda x \in S$-
est, si il contient un entier non nul, de la forme $(d) = \{\mu d | \mu \in \mathbb{Z}\}$, soit l'ensemble des multiples de d, d est le plus petit entier positif non nul contenu dans S.
Si p premier divise ab, p divise a où b,
Si a est premier à b et a divise bc, a divise b.
Il existe une infinité de nombres premiers, nombres premiers de la forme $4k + 1$.

2 Définition de $\mathbb{Z}/n\mathbb{Z}$

Soit n un entier. La classe de congruence $\bar{k}$ d'un entier k modulo n est l'ensemble des entiers ℓ tels que $k - \ell$ soit divisible par n.
Addition.

- associativité, commutativité
- élément neutre $\bar{0}$, opposé d'un élément.

Multiplication.

- associativité, commutativité
- élément neutre $\bar{1}$, inverse d'un élément.

3 Eléménts inversibles

Un élément $\bar{k}$ de $\mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement si k et sont premiers entre eux.
$(\mathbb{Z}/n\mathbb{Z})^*$
Indicatrice d'Euler φ, $\varphi(n)$ est le cardinal de $(\mathbb{Z}/n\mathbb{Z})^*$.
$\varphi(p^n) = p^n - p^{n-1}$ si p est premier.
$\varphi(mn) = \varphi(m)\varphi(n)$ si m et n sont premiers entre eux.
Formule

$$n = \sum_{d|n} \varphi(d)$$

4 Ordre d'un élément de $\mathbb{Z}/n\mathbb{Z}$

Définition : $ord(\bar{k})$ est le plus petit entier u strictement positif tel que $u\bar{k} = 0$.

$$ord(\bar{k}) = \frac{n}{pgcd(n,k)}$$

5 Lemme chinois

Si m et n sont premiers entre eux, alors les groupes additifs $\mathbb{Z}/mn\mathbb{Z}$ et à $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont isomorphes, *via* l'homomorphisme qui envoie la classe de congruence modulo mn sur les classes modulo m et modulo n.
De plus alors les groupes multiplicatifss $(\mathbb{Z}/mn\mathbb{Z})^*$ et à $(\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$ sont aussi isomorphes, *via* la même application.

6 Théorèmes de Fermat et d'Euler

Si p est premier et $x \in (\mathbb{Z}/p\mathbb{Z})^*$ alors $x^{p-1} = 1$. Soit $n > 1$, et $x \in (\mathbb{Z}/n\mathbb{Z})^*$ alors $x^{\varphi(n)} = 1$.