Université Paris 7
IUP 2
Analyse de Performance et Simulation
Année 2003-2004

Résumé de Cours pour le TD no 3
Carrés et Equations du Second Degré dans F_p.

Dans tout ce paragraphe, p désigne un nombre premier différent de 2. L'équation du second degré dans $F_p = \mathbb{Z}/p\mathbb{Z}$ se discute comme dans le cas classique (i.e. réel).

Proposition 1 *L'équation du second degré $ax^2 + bx + c = 0, a \neq 0$ se discute et se résoud selon le discriminant $\Delta = b^2 - 4ac$.*
i) Si $\Delta = \delta^2$ est un carré dans F_p, alors l'équation admet les racines :

$$\frac{-b-\delta}{2a} \quad \frac{-b+\delta}{2a}$$

ii) Si Δ n'est pas un carré, l'équation n'a pas de solution.

Remarque 1 *Si $\Delta = 0$, les deux racines du cas i) se confondent en une racine dite double $\frac{-b}{2a}$.*

Proposition 2 (Les carrés se calculent sur la "première moitié" de F_p) *L'application donnée par $x \to x^2$ définit une bijection entre $[0..\frac{p-1}{2}]$ et l'ensemble des carrés de F_p.*