Factorisation de polynômes à coefficients entiers

Exercice 1

1. Écrire une procédure `hensel` prenant en entrée un polynôme $f \in \mathbf{Z}[x]$, un nombre premier p, un entier x vérifiant $f(x) \equiv 0 \,(\mathrm{mod}\, p)$ et $f'(x) \not\equiv 0 \,(\mathrm{mod}\, p)$, et un entier $m \geqslant 1$, et renvoyant un entier $y \in \{0, \dots, p^m - 1\}$ tel que $x \equiv y \,(\mathrm{mod}\, p)$ et $f(y) \equiv 0 \,(\mathrm{mod}\, p^m)$.
2. En utilisant cette fonction, déterminer les racines carrées de 2 dans $\mathbf{Z}/7^{30}\mathbf{Z}$.
3. Soit $f = x^3 + 2x + 16$.
   (a) La réduction $\bar{f}$ de f modulo 11 est-elle sans facteur carré ?
   (b) Montrer que $\bar{f}$ admet une racine dans $\mathbf{Z}/11\mathbf{Z}$.
   (c) En utilisant la fonction `hensel`, déterminer l'unique racine de f modulo 11^2.
   (d) En utilisant les bornes de Mignotte, déduire que f est irréductible dans $\mathbf{Z}[x]$.

Exercice 2

1. Soit $f = \Phi_7(x) \in \mathbf{Z}[x]$ le 7-ième polynôme cyclotomique.
   (a) Factoriser f modulo 2 et modulo 13.
   (b) Déduire que f est irréductible dans $\mathbf{Z}[x]$.
2. Soit $g = x^6 + x^3 + x + 3$.
   (a) Factoriser g modulo 3 et modulo 31.
   (b) Déduire que g est irréductible dans $\mathbf{Z}[x]$.

Exercice 3

Soit $f = x^9 - 30x^7 + 18x^6 + 237x^5 - 234x^4 - 283x^3 + 288x^2 + 12x - 8$.

1. Montrer que f n'est pas irréductible modulo p si p parcourt les 30 premiers nombres premiers.
2. Montrer que si f n'est pas irréductible dans $\mathbf{Z}[x]$, alors il admet un facteur de degré 3.
3. Factoriser f modulo 8419 et conclure quant à l'irréductibilité de f.
4. On souhaite donner un argument n'utilisant pas un nombre premier si grand. On fixe $p = 97$.
   (a) Factoriser f modulo p.
   (b) Écrire une procédure `hensel2` prenant en argument un polynôme P unitaire à coefficients entiers, un nombre premier p et un polynôme unitaire Q à coefficients entiers vérifiant les hypothèses du lemme de Hensel (en particulier la réduction modulo p de Q divise la réduction modulo p de P), et renvoyant un relèvement modulo p^2 de Q divisant la réduction modulo p^2 de P.
   [Avant de se lancer dans le codage de la procédure, on réfléchira à la façon de construire explicitement un antécédent de l'élément Δ par la fonction Φ (dans les notations du cours).]

(c) En appliquant la fonction `hensel2`, relever la factorisation de la question (a) modulo p^2.

(d) Conclure.

Exercice 4 (bonus)
Soit

$$f = \prod_{\varepsilon=\pm1,\eta=\pm1,\kappa=\pm1} \left(x + \varepsilon\sqrt{-1} + \eta\sqrt{2} + \kappa\sqrt{3}\right) .$$

1. Montrer que f est à coefficients entiers. Utiliser `Sage` pour donner la forme développée de f.
2. Factoriser f modulo 2, 3, 5, ... Que conjecturer quant à la forme de la factorisation de f modulo p ? Essayer de prouver cette conjecture.
3. Montrer que f est irréductible dans $\mathbf{Z}[x]$ (étant entendu que taper la commande `f.is_irreducible()` ou toute autre chose approchant ne constitue pas une preuve).