Factorisation des polynômes à coefficients entiers

Exercice 1.

1. Écrire une procédure `hensel` prenant en entrée un polynôme $f \in \mathbb{Z}[x]$, 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 $m \geq 1$, et renvoyant un entier y tel que $x \equiv y \,(\mathrm{mod}\, p)$ et $f(y) \equiv 0 \,(\mathrm{mod}\, p^{2^m})$.
2. En utilisant cette fonction, déterminer les racines carrées de 2 dans $\mathbb{Z}/7^{32}\mathbb{Z}$.

Exercice 2. Soit $f = x^3 + 2x + 16$.

1. La réduction $\bar{f}$ de f modulo 11 est-elle sans facteur carré ?
2. Montrer que $\bar{f}$ admet une racine dans $\mathbb{Z}/11\mathbb{Z}$.
3. En utilisant la fonction `hensel`, déterminer l'unique racine de f modulo 11^2.
4. En utilisant les bornes de Mignotte, déduire que f est irréductible dans $\mathbb{Z}[x]$.

Exercice 3.

1. Soit $f = \Phi_7(x) \in \mathbb{Z}[x]$ le 7-ième polynôme cyclotomique.
   Rappel : le n-ième polynôme cyclotomique Φ_n est le polynôme dont les racines (toutes simples) sont les racines primitives n-ièmes de l'unité, on a alors $x^n - 1 = \prod_{d/n} \Phi_d$.
   (a) Factoriser f modulo 2 et modulo 13.
   (b) Déduire que f est irréductible dans $\mathbb{Z}[x]$.
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 4.

1. Écrire une procédure `hensel_polynomes` prenant en entrée un polynôme $f \in \mathbb{Z}[x]$, un nombre premier p, deux polynômes $g_0, h_0 \in \mathbb{Z}[x]$ tels que $f \equiv g_0 h_0 \,(\mathrm{mod}\, p)$ et $\mathrm{Res}(g_0, h_0) \not\equiv 0 \,(\mathrm{mod}\, p)$, et un entier $m \geq 1$, et renvoyant deux polynômes $g, h \in \mathbb{Z}[x]$ tel que $g \equiv g_0 \,(\mathrm{mod}\, p)$, $h \equiv h_0 \,(\mathrm{mod}\, p)$ et $f(y) \equiv gh \,(\mathrm{mod}\, p^{2^m})$.
2. En déduire une procédure qui permet de relever modulo p^{2^m} une factorisation d'un polynôme f modulo p contenant un nombre arbitraire de facteurs.

Exercice 5. 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 $\mathbb{Z}[x]$, alors il admet un facteur de degré 3.
3. Factoriser f modulo 8419 et conclure quant à l'irréductibilité de f.
4. On fixe $p = 97$.
   (a) Factoriser f modulo p.
   (b) Relever la factorisation modulo p^2.
   (c) Conclure.

Exercice 6. Soit

$$f = \prod_{\varepsilon=\pm1,\eta=\pm1,\kappa=\pm1} \left(x + \varepsilon\sqrt{2} + \eta\sqrt{3} + \kappa\sqrt{5}\right) .$$

1. Utiliser `Sage` pour donner la forme développée de f.
2. Factoriser f modulo 2, 3, 5, 7 .... Que peut-on conjecturer quant à la forme de la factorisation de f modulo p ? Essayer de prouver cette conjecture.
3. Vérifier que f est irréductible dans $\mathbb{Z}[x]$.