Resolution d'equations de petit degre modulo de grands nombres premiers

F. Morain

INRIA

UNITÉ DE RECHERCHE
INRIA-ROCQUENCOURT

Institut National
de Recherche
en Informatique
et en Automatique

Domaine de Voluceau
Rocquencourt
B.P.105
78153 Le Chesnay Cedex
France
Tél. (1) 39 63 55 11

Rapports de Recherche

N° 1085

Programme 1
Programmation, Calcul Symbolique
et Intelligence Artificielle

RESOLUTION D'EQUATIONS DE PETIT DEGRE MODULO DE GRANDS NOMBRES PREMIERS

François MORAIN

Septembre 1989

RR_1085

SOLVING EQUATIONS OF SMALL DEGREE MODULO LARGE PRIMES

Francois MORAIN * †

morain@inria.inria.fr

Abstract. Solving equations modulo p is ordinarily done by means of Berlekamp's algorithm. We show how to find roots of polynomials of degree less than five using Lucas sequences. We also compare the time required by both algorithms.

RESOLUTION D'EQUATIONS DE PETIT DEGRE MODULO DE GRANDS NOMBRES PREMIERS

Résumé. La résolution d'équations polynomiales dans $\mathbf{Z}/p\mathbf{Z}$ se fait ordinairement avec l'algorithme de Berlekamp. Nous montrons comment il est possible d'utiliser les suites de Lucas pour résoudre les équations de degré 3 et 4 modulo p. Des comparaisons de temps d'execution entre les deux algorithmes sont également donnés.

*Institut National de Recherche en Informatique et en Automatique, Domaine de Voluceau, B. P. 105, 78153 LE CHESNAY CEDEX (France) & Département de Mathématiques, Université Claude Bernard, 69622 Villeurbanne CEDEX (France).

† On leave from the French Department of Defense, Délégation Générale pour l'Armement.

1 Introduction

L'algorithme d'Atkin ([10]) nécessite la résolution d'équations polynomiales de degré pouvant aller jusqu'à 10, modulo de grands nombres premiers (plusieurs centaines de chiffres). Les polynômes qui nous interessent ont la particularité d'avoir toutes leurs racines dans le corps $\mathbf{Z}/p\mathbf{Z}$ dans lequel on travaille.

L'algorithme le mieux adapté est l'algorithme de Berlekamp sous sa forme probabiliste ("folk method" de [7]). Cette méthode sert en fait à effectuer une séparation des facteurs des polynômes dans le cas général. On pourra consulter l'article récent de Shoup [14] pour des compléments sur les algorithmes de factorisation.

Il s'avère toutefois que l'on a souvent des équations particulières à résoudre. Par exemple, l'extraction de racines q-ièmes (q premier) dans $\mathbf{Z}/p\mathbf{Z}$ a été étudiée dans [13] pour le cas du degré 2 et [18] pour le cas q impair. On peut se demander aussi s'il n'est pas possible de transcrire la résolution classique des équations de degré 3 ou 4 dans $\mathbf{C}$ dans le cas où on travaille modulo p. Après des recherches poussées dans la littérature (notamment grâce aux bibliographies contenues dans [6] et [17]), la réponse à ce problème est affirmative. Non seulement on peut utiliser les mêmes méthodes, mais les algorithmes qui en découlent sont beaucoup plus rapides que l'algorithme de Berlekamp.

Après un bref rappel de l'algorithme de Berlekamp, nous présenterons un théorème qui nous permet de dresser un cadre de travail agréable pour traiter les cas des équations de degré 3 et 4. Enfin, on donnera des temps de comparaison entre les différentes méthodes pour le cas du degré 3.

2 Algorithme de Berlekamp

Soit f un polynôme de degré n, à coefficients entiers, et p un nombre premier. On cherche UNE racine de f modulo p. L'algorithme de Berlekamp, sous forme probabiliste est (Cf. [1, 7]) :

fonction BERLEKAMP($f(X)$, p);

(* retourne une racine de $f(X) \equiv 0 \bmod p$ *)

1. $F := f$, $x_0 := 0$;
2. **tant que** degré(f)$\neq 1$
   1. $x_0 := x_0 + 1$;
   2. $F := \mathrm{pgcd}((X + x_0)^{\frac{p-1}{2}} - 1, f(X)) \bmod p$;
   3. **si** degré(F)> 1 **alors si** degré(F)$\leq$ degré(f)$/2$ **alors** $f := F$ **sinon** $f := f/F$;
3. f est de degré 1 : $f = X - X_0$; X_0 est la racine cherchée;
4. **fin.**

On montre que la probabilité de succès pour chaque valeur de x_0 est $\frac{1}{2}$ (on conjecture même que cette probabilité est $\geq 1 - 1/2^n$ Cf. [12]). Si l'on emploie des algorithmes de calcul classiques sur les polynômes, le coût de cet algorithme est :

$$O((n^3 + n^2(\log p))(\log n)(\log p)^2).$$

Dans le cas qui nous interesse, n est beaucoup plus petit que $\log p$, et donc la complexité "pratique" est

$$O(n^2 \log n(\log p)^3).$$

3 Un théorème interessant

Le but de cette section est de démontrer le théorème suivant, dû originellement à Pellet ([11]).

Théorème 3.1 *Soit $f(X)$ un polynôme de degré n à coefficients dans $\mathbf{Z}/p\mathbf{Z}$ (p nombre premier plus grand que n). Soit $\mathcal{D}$ le discriminant de f et ω le nombre de facteurs irréductibles de f dans $\mathbf{Z}/p\mathbf{Z}$. On suppose que $p \not| \mathcal{D}$. Alors :*

$$\left(\frac{\mathcal{D}}{p}\right) = (-1)^{n-\omega}, \tag{1}$$

où $(./p)$ désigne le symbole de Jacobi (Cf. [5]).

Nous suivons la démonstration donnée dans [16]. On commence par démontrer le cas particulier suivant.

Lemme 3.1 *Avec les mêmes hypothèses, si f est irréductible, alors :*

$$\left(\frac{\mathcal{D}}{p}\right) = (-1)^{n-1}. \tag{2}$$

Démonstration.
Comme f est irréductible modulo p, f est irréductible sur $\mathbf{Q}$. Alors :

$$F = \mathbf{F}(p^n) \simeq (\mathbf{Z}/p\mathbf{Z}[X])/(f).$$

La *trace* d'un élément α de F est :

$$\mathrm{Tr}(\alpha) = \alpha + \alpha^p + \ldots + \alpha^{p^{n-1}}, \tag{3}$$

qui est un élément de $\mathbf{Z}/p\mathbf{Z}$.

Soit θ une racine de f dans F. On a :

$$f(x) = (x-\theta)(x-\theta^p)\ldots(x-\theta^{p^{n-1}}) \tag{4}$$

et

$$\mathcal{D} = g(\theta)^2, \tag{5}$$

avec :

$$g(\theta) = \begin{matrix} (\theta-\theta^p) & (\theta-\theta^{p^2}) & \ldots & (\theta-\theta^{p^{n-1}}) \\ & (\theta^p-\theta^{p^2}) & \ldots & (\theta^p-\theta^{p^{n-1}}) \\ & & \ldots & \\ & & & (\theta^{p^{n-2}}-\theta^{p^{n-1}}) \end{matrix} \tag{6}$$

Il n'est pas difficile de voir que :

$$g(\theta^p) = (-1)^{n-1} g(\theta). \tag{7}$$

On doit distinguer deux cas, suivant la parité de n. Supposons n impair. Alors :

$$g(\theta^p) = g(\theta) \tag{8}$$

et plus généralement

$$g(\theta^{p^i}) = g(\theta), \text{ pour } 2 \leq i \leq n. \tag{9}$$

On en déduit :

$$ng(\theta) = g(\theta) + g(\theta^p) + \ldots + g(\theta^{p^{n-1}}) = \mathrm{Tr}(g(\theta)), \tag{10}$$

qui est un élément de $\mathbf{Z}/p\mathbf{Z}$. Comme $p > n$, n est premier avec p et donc $g(\theta)$ est dans $\mathbf{Z}/p\mathbf{Z}$. On a donc réussi à écrire : $\mathcal{D} \equiv g^2$ dans $\mathbf{Z}/p\mathbf{Z}$ et donc $\mathcal{D}$ est un carré modulo p.

Si n est pair, on a :

$$g(\theta^p) = g(\theta)^p = -g(\theta) \tag{11}$$

dans F. Si $g(\theta)$ était dans $\mathbf{Z}/p\mathbf{Z}$, on aurait $g(\theta)^p \equiv g(\theta) \bmod p$ et cela impliquerait $g(\theta) \equiv 0 \bmod p$, contredisant l'hypothèse faite sur $\mathcal{D}$. Donc $g(\theta)$ n'est pas dans $\mathbf{Z}/p\mathbf{Z}$. Si $\mathcal{D}$ était un carré modulo p, $\mathcal{D} \equiv g^2$, on aurait $g(\theta) \equiv \pm g \bmod p$, ce qui est impossible. ■

Démonstration du théorème.

On raisonne par récurrence sur n. Ce théorème est trivial quand $n = 1$ ou $n = 2$. Nous faisons maintenant l'hypothèse que la propriété est vraie pour tous les degrés plus petits que n ($n > 2$). Soit maintenant f un polynôme de degré n ($n > 2$) satisfaisant aux hypothèses du théorème. Si f est irréductible, on applique le lemme précédent. Supposons maintenant que f est le produit de deux polynômes f_1 et f_2 de degrés respectifs m et $n - m$ avec $n > m$, de discriminants $\mathcal{D}_1$ et $\mathcal{D}_2$ et ayant respectivement ω_1 et ω_2 facteurs irréductibles modulo p. On écrit :

$$f_1(X) = \prod_{r=1}^{m} (X - X_r), \tag{12}$$

$$f_2(X) = \prod_{s=m+1}^{n} (X - X_s). \tag{13}$$

Alors :

$$\mathcal{D}(f) = \mathcal{D}(f_1 f_2) = \prod_{1 \le i < j \le n} (X_i - X_j)^2, \tag{14}$$

ce que l'on récrit :

$$\begin{aligned} \mathcal{D}(f) &= \mathcal{D}_1\, \mathcal{D}_2 \prod_{i=1}^{m} \prod_{j=m+1}^{n} (X_i - X_j)^2 \\ &= \mathcal{D}_1\, \mathcal{D}_2\, \mathrm{Res}(f_1, f_2)^2, \end{aligned} \tag{15}$$

où $\mathrm{Res}(f_1, f_2)$ est le résultant de f_1 et f_2 qui est un élément de $\mathbf{Z}/p\mathbf{Z}$. D'où :

$$\mathcal{D} \equiv \mathcal{D}_1\, \mathcal{D}_2\, A^2 \bmod p \tag{16}$$

c'est-à-dire :

$$\left(\frac{\mathcal{D}}{p}\right) \equiv \left(\frac{\mathcal{D}_1}{p}\right)\left(\frac{\mathcal{D}_2}{p}\right) \bmod p. \tag{17}$$

Appliquant l'hypothèse de récurrence, on a :

$$\left(\frac{\mathcal{D}}{p}\right) \equiv (-1)^{m-\omega_1}(-1)^{n-m-\omega_2} \equiv (-1)^{n-\omega} \tag{18}$$

ce qui démontre le résultat pour n. ■

Nous terminons par quelques remarques sur l'utilisation de ce théorème. Soit $f(x)$ un polynôme à coefficients dans $\mathbf{Z}[X]$. Soit p un nombre premier. Supposons que l'on cherche le type de

factorisation possible de f dans $\mathbf{Z}/p\mathbf{Z}$. On dira que f est *du type* $(r_1, \ldots, r_k)$ *modulo* p si et seulement si

$$f(x) \equiv f_1(x) \ldots f_k(x) \bmod p \tag{19}$$

avec :

$$\forall\, i, \deg(f_i) = r_i.$$

Il y a autant de types possibles que de partitions de l'entier n en somme d'entiers strictement positifs. Le théorème démontré ci-dessus donne des renseignements sur la parité de k.

4 Rappels sur les suites de Lucas

Nous nous contentons de donner un bref aperçu des propriétés qui nous interessent. On pourra consulter [3, 8, 19] pour plus d'informations.

4.1 Définition

Soient P et Q deux entiers. On considère la récurrence d'ordre deux

$$X_n = PX_{n-1} - QX_{n-2}, \tag{20}$$

définie pour $n \geq 2$. Son équation caractéristique est :

$$y^2 - Py + Q = 0, \tag{21}$$

dont le discriminant est $\Delta = P^2 - 4Q$. On introduit les solutions particulières U_n et V_n de la récurrence (20) définies par :

$$U_0 = 0, U_1 = 1; V_0 = 2, V_1 = P. \tag{22}$$

Si α et β sont les deux racines de l'équation (21), on montre facilement que :

$$\forall\, n, U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, V_n = \alpha^n + \beta^n. \tag{23}$$

On pose aussi $A = \alpha/\beta$ et on a le résultat trivial suivant :

Lemme 4.1

$$\forall\, m,\ U_m = 0 \Leftrightarrow A^m = 1.$$

Ces suites vérifient de nombreuses identités. Parmi celles-ci, on a

Proposition 4.1 *Pour tout n :*

$$V_n^2 - \Delta U_n^2 = 4Q^n; \tag{24}$$

$$V_{2n} = V_n^2 - 2Q^n, U_{2n} = U_n V_n; \tag{25}$$

$$V_{3n} = V_n(V_n^2 - 3Q^n), U_{3n} = U_n(V_n^2 - Q^n); \tag{26}$$

$$U_{m+n} = V_n U_m - Q^n U_{m-n}, V_{m+n} = V_n V_m - Q^n V_{m-n}; \tag{27}$$

$$2V_{n+m} = V_n V_m + \Delta U_n U_m, 2U_{m+n} = U_n V_m + U_m V_n. \tag{28}$$

Nous suivons maintenant l'approche de [17] (voir aussi [4]).

Définition 4.1 *On définit les* polynômes de Sylvester *par :*

$$G_{-1}(x) = -1, G_0(x) = 1$$
$$G_{k+1}(x) = xG_k(x) - G_{k-1}(x) \text{ pour } k \geq 0.$$

Proposition 4.2 *Pour tout $s \geq 0$, on a :*

$$x^s G_s\left(x + \frac{1}{x}\right) = \frac{x^{2s+1} - 1}{x - 1}. \tag{29}$$

La démonstration de cette proposition se fait aisément par récurrence. Notons que $G_s(-2) = (-1)^s$.

Corollaire 4.1 *On a :*

$$V_{(2s+1)n} = (-1)^s Q^{ns} G_s(-V_{2n}/Q^n) V_n; \tag{30}$$
$$U_{(2s+1)n} = Q^{ns} G_s(V_{2n}/Q^n) U_n. \tag{31}$$

Démonstration. On applique la proposition précédente avec $x = \pm(\alpha/\beta)^n$. ■

Des propriétés (25) et (4.1) on déduit aisément :

$$U_k = 0 \Rightarrow \forall\, m,\ U_{km} = 0. \tag{32}$$

4.2 Propriétés

Soit p un nombre premier. On définit les suites de Lucas U_n et V_n comme précédemment, les opérations étant considérées modulo p. On démontre :

Théorème 4.1 *On suppose que $p \not| \Delta$. Si $\epsilon = \left(\frac{\Delta}{p}\right)$ et $\eta = \left(\frac{Q}{p}\right)$, alors :*

$$\begin{array}{rcll} U_{p-\epsilon} & \equiv & 0 & \mod p \\ V_{p-\epsilon} & \equiv & 2Q^{(1-\epsilon)/2} & \mod p \end{array} \tag{33}$$

et

$$U_{(p-\epsilon)/2} \equiv 0 \Leftrightarrow \eta = -1. \tag{34}$$

Proposition 4.3 *Soit p un nombre premier impair ne divisant pas ΔQ. Soit $c \in \{1, 2\}$ et r un diviseur impair de $p - \epsilon$. On pose $t = (p - \epsilon)/r$. Alors :*

$$U_{ct} \equiv 0 \bmod p \Leftrightarrow V_{ct} \equiv 2\,\eta^c\, Q^{ct/2} \bmod p. \tag{35}$$

Démonstration. La réciproque est claire avec (24). Dans le sens direct, on a soit $U_t \equiv 0 \bmod p$, soit $V_t \equiv 0$ et $c = 2$ (avec (25)).

Supposons que $U_t \equiv 0$. Alors (24) implique :

$$V_t \equiv 2\,\zeta\, Q^{t/2}, \text{ avec } \zeta \in \{\pm 1\}.$$

Avec (25), on déduit : $V_{2t} \equiv 2Q^t$. On applique le corollaire (4.1) pour trouver :

$$V_{rt} \equiv (-1)^k Q^{kt} G_k(-2) V_t \bmod p,$$

avec $r = 2k+1$. On en déduit :

$$V_{rt} \equiv Q^{kt}\, V_t \equiv 2\,\zeta\, Q^{kt+t/2} \equiv 2\,\zeta Q^{(p-\epsilon)/2} \equiv 2\,\zeta\,\eta\, Q^{(1-\epsilon)/2}.$$

Comme d'autre part, $V_{rt} \equiv V_{p-\epsilon} \equiv 2\,Q^{(1-\epsilon)/2}$, on trouve donc $\zeta = \eta$.

Supposons maintenant que $c = 2$ et que $V_t \equiv 0$. Alors :

$$0 \equiv U_{p-\epsilon} \equiv U_{rt} \equiv Q^{kt}\, G_s(-2)\, U_t,$$

c'est-à-dire $U_t \equiv 0$. Mais à cause de (24), on ne peut avoir simultanément U_t et V_t nuls. Donc ce cas est impossible. ■

4.3 La suite W_n

On suppose que p est un nombre premier. Suivant [4] et [17] on introduit la suite W_n définie par :

$$W_n \equiv V_{2n} Q^{-n} \bmod p, W_1 \equiv \frac{P^2}{Q} - 2 \bmod p.$$

Cette suite satisfait les relations :

$$\begin{cases} W_{2n} \equiv & W_n^2 - 2 \\ W_{2n+1} \equiv & W_n W_{n+1} - W_1. \end{cases} \tag{36}$$

Il existe un algorithme rapide pour évaluer W_n pour n grand. Ecrivons n en base 2 : $n = (b_0 b_1 \ldots b_t)_2$. On pose $\mathcal{P}_0 = \{W_1, W_2\}$. Si $\mathcal{P}_i = \{A, B\}$, on a

$$\mathcal{P}_{i+1} = \begin{cases} \{A^2 - 2, AB - W_1\} \text{ si } b_{i+1} = 0, \\ \{AB - W_1, B^2 - 2\} \text{ sinon,} \end{cases} \tag{37}$$

et : $\mathcal{P}_t = \{W_n, W_{n+1}\}$. Enfin, il est possible d'exprimer U_n et V_n en fonction de W_n par :

$$PV_{2n+1} Q^{-n} \equiv Q(W_{n+1} + W_n), \tag{38}$$

$$\Delta (U_{2n} Q^{-n})^2 \equiv W_n^2 - 4 \bmod p, \tag{39}$$

$$\Delta U_{2n+1} Q^{-n} \equiv Q(W_{n+1} - W_n) \bmod p. \tag{40}$$

On en déduit le lemme suivant :

Lemme 4.2

$$U_{2k+1} \equiv 0 \bmod p \Leftrightarrow W_{k+1} \equiv W_k \bmod p; \tag{41}$$

$$U_{2k} \equiv 0 \bmod p \Leftrightarrow W_k \equiv \pm 2 \bmod p. \tag{42}$$

5 Equations du troisième degré dans $\mathbf{Z}/p\mathbf{Z}$

Nous suivons [2] et [17].

5.1 Préliminaires

On cherche à résoudre l'équation :

$$f(x) = x^3 + ux + v \equiv 0 \bmod p. \tag{43}$$

Le discriminant de cette équation est $\mathcal{D} = -4u^3 - 27v^2$. On pose $\nu = \left(\frac{\mathcal{D}}{p}\right)$. On suppose que $u \not\equiv 0 \bmod p$ (le cas des extractions de racine cubique est traité dans [18]).

Il y a trois partitions possibles de l'entier 3 en somme d'entiers strictement positifs, à savoir : $3 = 1+1+1 = 1+2$. A l'aide du théorème (3.1), on voit que f est du type **(1 2)** si $\nu = -1$ et du type **(1 1 1)** ou **(3)** si $\nu = +1$.

On écrit $p = 3m + \xi$, avec $\xi \in \{\pm 1\}$. On récrit (43) sous la forme :

$$x^3 - 3\alpha\beta x + \alpha\beta(\alpha + \beta) \equiv 0. \tag{44}$$

Les coefficients α et β sont les solutions de :

$$y^2 + \frac{3v}{u}y - \frac{u}{3} = 0, \tag{45}$$

dont le discriminant est :

$$\Delta = \frac{9v^2}{u^2} + \frac{4u}{3} = \frac{-3\mathcal{D}}{(3u)^2}. \tag{46}$$

Lemme 5.1 *Soit x_0 une racine de (43). Soit $z = (x_0 - \alpha)/(x_0 - \beta)$. Alors :*

$$z^3 = A = \frac{\alpha}{\beta}. \tag{47}$$

Démonstration. On écrit :

$$x = \frac{\beta z - \alpha}{z - 1}.$$

On en déduit :

$$x^3 + ux + v = \frac{(\beta z - \alpha)^3 + u(\beta z - \alpha)(z-1)^2 + v(z-1)^3}{(z-1)^3}.$$

Le numérateur s'écrit :

$$(\beta^3 + u\beta + v)z^3 - (3\alpha\beta^2 + 2u\beta + u\alpha + 3v)z^2 + (3\alpha^2\beta + 2u\alpha + u\beta + 3v)z - (\alpha^3 + u\alpha + v).$$

Or :

$$\begin{aligned} 3\alpha\beta^2 + 2u\beta + u\alpha + 3v &= 3\alpha(-\frac{3v}{u}\beta + \frac{u}{3}) + 2u\beta + u\alpha + 3v & (48)\\ &= -\frac{9v}{u}\alpha\beta + 2u(\alpha + \beta) + 3v & (49)\\ &= 0. & (50) \end{aligned}$$

Par symétrie, le coefficient de z est nul. On montre de la même façon que :

$$\beta^3 + u\beta + v = \Delta\beta, \alpha^3 + u\alpha + v = \Delta\alpha,$$

et finalement, on a le résultat annoncé. ■

On introduit les suites de Lucas associées à l'équation (45), c'est-à-dire avec pour valeurs de P et Q respectivement $-3v/u$ et $-u/3$. On pose comme précédemment :

$$\epsilon = \left(\frac{\Delta}{p}\right) = \left(\frac{-3}{p}\right)\left(\frac{\mathcal{D}}{p}\right) = \xi\,\nu, \tag{51}$$

et

$$\eta = \left(\frac{Q}{p}\right). \tag{52}$$

5.2 Résolution

Tout tourne autour de l'exploitation de l'équation (47). Quand des racines existent dans le corps contenant A (i.e. dans $\mathbf{Z}/p\mathbf{Z}$ si $\epsilon = +1$ et dans $\mathbf{Z}/p\mathbf{Z}[\sqrt{\Delta}]$ si $\epsilon = -1$), nous allons expliquer comment extraire une racine cubique de A et comment en déduire une solution pour (43).

Introduisons des notations supplémentaires. On écrit comme précédemment $p = 3m + \xi$, avec $\xi \in \{\pm 1\}$. On pose $m = 3^\lambda n$, avec $\lambda \geq 0$, $n = 3\mu + \theta$, où $\theta \in \{\pm 1\}$. Notons que ces définitions entrainent que m est pair.

Passons maintenant aux conditions sur les résidus cubiques. Si $p \not\equiv 1 \bmod 3$, alors tout élément de $\mathbf{Z}/p\mathbf{Z}$ ou $\mathbf{Z}/p\mathbf{Z}[\sqrt{\Delta}]$ est un cube.

Si $p \equiv 1 \bmod 3$, et si A est dans $\mathbf{Z}/p\mathbf{Z}$, la condition pour que A soit résidu cubique est :

$$A^{\frac{p-1}{3}} \equiv 1 \bmod p \Leftrightarrow U_{(p-1)/3} \equiv 0 \bmod p, \tag{53}$$

et quand A est dans $\mathbf{Z}/p\mathbf{Z}[\sqrt{\Delta}] \cong \mathbf{F}(p^2)$, on a :

$$A^{\frac{p^2-1}{3}} = 1 \text{ dans } \mathbf{Z}/p\mathbf{Z}[\sqrt{\Delta}] \Leftrightarrow U_{(p^2-1)/3} \equiv 0 \bmod p. \tag{54}$$

Nous allons maintenant appliquer les résultats de la section 1 et étudier séparément les deux cas $\nu = +1$ et $\nu = -1$.

5.2.1 Le cas $\nu = -1$

Dans ce cas, on sait que f est du type **(2 1)**. Autrement dit, f n'a qu'une racine dans $\mathbf{Z}/p\mathbf{Z}$. Deux cas se présentent, selon la valeur de ξ. Si $\xi = -1$, alors $\epsilon = 1$ et A est dans $\mathbf{Z}/p\mathbf{Z}$. Comme $p = 3m - 1$, l'unique solution de l'équation $z^3 \equiv A \bmod p$ est

$$\left(\frac{\beta}{\alpha}\right)^{m-1} \bmod p. \tag{55}$$

Revenant à x, on trouve :

$$x \equiv \frac{\beta(\beta/\alpha)^{m-1} - \alpha}{(\beta/\alpha)^{m-1} - 1} \equiv \frac{\beta^m - \alpha^m}{\beta^{m-1} - \alpha^{m-1}} \equiv \frac{U_m}{U_{m-1}} \bmod p. \tag{56}$$

Si $\xi = 1$, alors $\epsilon = -1$ et α et β sont dans $\mathbf{Z}/p\mathbf{Z}[\sqrt{\Delta}]$. Il en est de même pour A. D'après (33), on a :

$$U_{p+1} \equiv 0 \bmod p, \tag{57}$$

et comme $(p^2-1)/3 = (p+1)(p-1)/3$ et que $(p-1)/3$ est un entier, on en déduit, avec (32), que :

$$U_{(p^2-1)/3} \equiv 0 \bmod p,$$

et donc A est un résidu cubique. De plus, on a :

$$\left(\frac{\alpha}{\beta}\right)^{3m+3} = \frac{\alpha}{\beta} \tag{58}$$

(dans $\mathbf{Z}/p\mathbf{Z}[\sqrt{\Delta}]$). On peut alors prendre pour z la valeur :

$$\left(\frac{\alpha}{\beta}\right)^{m+1} \tag{59}$$

et revenant à x, on trouve :

$$x \equiv \alpha\beta\frac{U_m}{U_{m+1}} \equiv Q\frac{U_m}{U_{m+1}} \tag{60}$$

qui est un élément de $\mathbf{Z}/p\mathbf{Z}$.

5.2.2 Le cas $\nu = +1$

Le type de f est du type **(1 1 1)** ou **(3)**. Si A n'est pas résidu cubique (dans $\mathbf{Z}/p\mathbf{Z}$ ou $\mathbf{Z}/p\mathbf{Z}[\sqrt{\Delta}]$), alors f est du type **(3)**, sinon il est du type **(1 1 1)**.

Dans le cas où $p \equiv 1 \bmod 3$, la condition sur A est équivalente à $U_m \equiv 0$. En effet, on a $(p^2-1)/3 = 3m^2 - 2m$ et :

$$A^{(p^2-1)/3} = 1 \Leftrightarrow A^{3m^2-2m} = 1 \Leftrightarrow A^m = A^{-3m^2+3m} = 1,$$

car $U_{p-1} \equiv 0 \equiv U_{3m}$ (d'après (33)).

Supposons donc que A est résidu cubique. Soit t le plus petit diviseur pair de m tel que $U_t \equiv 0$. Ce nombre existe car $U_{p-\epsilon} \equiv 0 \bmod p$, d'après (33). Nous allons démontrer le théorème suivant.

Théorème 5.1 ([17]) *Supposons que t n'est pas multiple de 3. Une solution de (43) est donnée par :*

$$x \equiv -\eta^c P^{-1} Q(W_{k+1} + W_k),$$

où c est choisi dans $\{1,2\}$ de façon que $3 \mid c\,t+1$; k est alors défini par $ct+1 = 3\,r = 3\,(2k+1)$.

Démonstration. Comme $U_t \equiv 0$, on a aussi $U_{2t} \equiv 0$ et donc, d'après (35) :

$$U_{ct} \equiv 0, V_{ct} \equiv 2\,\eta^c\,Q^{ct/2}, \tag{61}$$

pour tout c dans $\{1,2\}$. Avec (27), on écrit :

$$2V_{ct+1} \equiv V_{ct}V_1 + \Delta U_{ct}U_1 \equiv 2\,P\,\eta^c\,Q^{ct/2}.$$

Or (Cf. (26)):

$$V_{ct+1} = V_{3r} = V_r\,(V_r^2 - 3Q^r).$$

On en déduit :

$$V_r^3 - 3Q^rV_r \equiv P\,\eta^c\,Q^{ct/2}. \tag{62}$$

Comme $ct = 2(3k+1)$, on multiplie (62) par Q^{-3k} pour trouver :

$$(V_r Q^{-k})^3 - 3Q(V_r Q^{-k}) \equiv \eta^c PQ. \tag{63}$$

Mais $-3Q \equiv u$ et $PQ \equiv v$. On en déduit :

$$(-\eta^c V_r Q^{-k})^3 + u(-\eta^c V_r Q^{-k}) + v \equiv 0. \tag{64}$$

Remarquant pour finir que :

$$V_r Q^{-k} = V_{2k+1} Q^{-k} \equiv P^{-1} Q(W_{k+1} + W_k),$$

on voit qu'une solution de (43) est :

$$x \equiv -\eta^c P^{-1} Q(W_{k+1} + W_k). \blacksquare$$

Si maintenant t est divisible par 3, on désigne par A_0 une racine cubique de $A^{3\mu+\theta}$. Alors une racine de (47) est

$$z \equiv (A_0 A^{-\mu})^\theta \bmod p. \tag{65}$$

Dans ce cas, on ne peut exprimer x avec les suites de Lucas. Dans le cas où A est dans $\mathbf{Z}/p\mathbf{Z}[\sqrt{\Delta}]$, l'extraction de racine cubique est assez pénible et dans ce cas, l'algorithme de Berlkamp est plus efficace.

Pour terminer, on trouve les autres racines de f en divisant f par le monôme $x - x_0$ et en résolvant une équation du second degré.

6 Equations du quatrième degré

L'exposé de la méthode se trouve dans [15]. Nous ne donnons que quelques détails, en insistant sur le cas où $f(x) = x^4 + a_1x^3 + a_2x^2 + a_3x + a_4$ est du type **(1 1 1 1)**. On suppose que a_1 et a_3 ne sont pas simultanément nuls.

Soient $(x_i)_{1\le i\le 4}$ les racines de f dans un corps convenable. On pose :

$$\begin{cases} z_1 &= x_1 + x_2 - x_3 - x_4 \\ z_2 &= x_1 - x_2 + x_3 - x_4 \\ z_3 &= x_1 - x_2 - x_3 + x_4, \end{cases} \tag{66}$$

et $y_i = z_i^2$. Alors les y_i sont racines de

$$g(y) = y^3 + b_1y^2 + b_2y + b_3 \equiv 0 \bmod p, \tag{67}$$

où :

$$\begin{aligned} b_1 &= 8a_2 - 3a_1^2 \\ b_2 &= 3a_1^4 - 16a_1^2a_2 + 16a_1a_3 + 16a_2^2 - 64a_4 \\ b_3 &= -(a_1^3 - 4a_1a_2 + 8a_3)^2. \end{aligned} \tag{68}$$

Le discriminant de g est précisément celui de f.

Réciproquement, si les y_i sont les racines de g et si les z_i sont choisis de sorte que :

$$-z_1z_2z_3 \equiv a_1^3 - 4a_1a_2 + 8a_3, \tag{69}$$

alors les x_i définis par (66) (et $x_1 + x_2 + x_3 + x_4 \equiv a_1$) sont les racines de f.

Comme 4 admet 5 types de partitions, on voit que f est du type **(1 1 1 1)**, **(2 2)** ou **(3 1)** si $\mathcal{D}$ est résidu quadratique modulo p et du type **(2 1 1)** ou **(4)** sinon.

Le cas **(1 1 1 1)** correspond au cas où g est du type **(1 1 1)** et où les trois racines sont résidus quadratiques modulo p. Dans ce cas, les z_i correspondant sont dans $\mathbf{Z}/p\mathbf{Z}$ et on a facilement les racines de f.

7 Application au test d'Atkin

Dans ce cas, nous avons à trouver une racine d'un polynôme, de degré 3 ou 4 et nous savons que ce polynôme a toutes ses racines dans $\mathbf{Z}/p\mathbf{Z}$. Cela simplifie considérablement le travail d'implémentation. On voit que le cas du degré 4 nécessite trois extractions de racines carrées en plus du calcul d'une racine d'une équation d'ordre 3, qui elle aussi a trois racines dans $\mathbf{Z}/p\mathbf{Z}$.

J'ai comparé les deux algorithmes (Berlekamp et Williams) sur le polynôme $P_{23}(X) = X^3 + 3491750X^2 - 5151296875X + 23375^3$. Ce polynôme a trois racines dans $\mathbf{Z}/p\mathbf{Z}$, pour tous les p qui sont représentés par la forme quadratique principale de discriminant -23, i.e. $Q(x,y) = x^2+xy+6y^2$ (Cf. [10]). Parmis 200 nombres premiers de 100 chiffres choisis "au hasard", 34 vérifiaient cette propriété, 29 permettaient l'application de la méthode de Williams (sans les racines cubiques). C'est la proportion attendue car la probabilité qu'un nombre premier au hasard vérifie la propriété est 1/6. Les programmes sont écrits en `Le_Lisp 15.21`, avec une arithmétique 32-bits, sur un SUN 3/60. Les temps sont donnés ci-dessous.

Berlekamp	Williams	rapport
33.50	13.24	2.53
33.56	9.76	3.44
32.30	9.22	3.50
34.38	9.16	3.75
33.32	8.86	3.76
32.48	8.36	3.89
66.56	13.84	4.81
68.84	13.98	4.92
67.84	9.72	6.98
72.22	10.26	7.04
65.40	9.26	7.06
74.52	10.42	7.15
65.54	8.84	7.41
65.64	8.84	7.43
67.14	8.94	7.51
80.58	9.12	8.84
93.74	10.08	9.30
88.98	9.42	9.45
99.98	9.60	10.42
100.00	8.94	11.19
98.60	8.32	11.85
129.86	9.84	13.20
117.80	8.88	13.27
146.26	9.80	14.92
135.18	9.00	15.02
165.72	10.28	16.12
231.44	13.74	16.84
200.82	10.18	19.73
318.82	9.46	33.70

8 Conclusions

L'algorithme de recherche de racine préconisé est donc le suivant :

procédure SEARCHROOT($f(X)$, p);

1. $F := f$, $x_0 := 0$;
2. **tant que** degré(f)$\neq 1$
    1. **si** degré(f)$= 2$ **alors** appliquer SHANKS, aller à 4;
    2. **si** degré(f)$= 3$ **alors** appliquer WILLIAMS, aller à 4;
    3. **si** degré(f)$= 4$ **alors** appliquer SKOLEM, aller à 4;
    4. 1. $x_0 := x_0 + 1$;
       2. $F := \text{pgcd}((X + x_0)^{\frac{p-1}{2}} - 1, f(X)) \bmod p$;
       3. **si** degré(F)> 1 **alors si** degré(F)$\leq$ degré(f)$/2$ **alors** $f := F$ **sinon** $f := f/F$;
3. $f = X - X_0$;
4. **fin.**

Dans un prochain article, je me propose d'expliquer comment on peut résoudre une équation modulo p quand son groupe de Galois (sur **C**) est résoluble.

References

[1] E. R. Berlekamp. Factoring polynomials over large finite fields. *Math. of Comp.*, **24**, 111, 1970, pp. 713-735.

[2] C. Cailler. Sur les congruences du troisième degré. *Enseign. Math.*, volume 10, 1908, pp. 474-487.

[3] L. E. Dickson. *History of the Theory of Numbers.* Volume 1, Chelsea, New York, 1952.

[4] H. Dubner, H. C. Williams. The primality of $R1031$. *Math. of Comp.*, volume 47, number 176, October 1986, pp. 703-711.

[5] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*, Clarendon Press, 1985, Oxford, 5th edition.

[6] J. W. P. Hirschfeld. *Projective Geometries over Finite Fields.* Clarendon Press, Oxford, 1979.

[7] D. E. Knuth. *The Art of Computer Programming*, volume II: *Seminumerical algorithms*, Addison-Wesley.

[8] D. H. Lehmer. An extended theory of Lucas' functions. *Ann. of Math.*, (2), volume 31, 1930, pp. 419-448.

[9] P. A. Leonard. On factoring quartics mod$p$. *J. Number Theory*, 1, 1969, pp. 113-115.

[10] F. MORAIN. Implementation of the Atkin-Goldwasser-Kilian primality testing algorithm. Rapport de Recherche INRIA, 911, 1988.

[11] A. E. PELLET. Comptes rendus, Paris, 86, 1878, pp. 1071-2.

[12] M. O. RABIN. Probabilistic algorithms in finite fields. *SIAM J. Comput.*, **9**, 2, 1980, pp. 273-280.

[13] D. SHANKS. Five number theoretic algorithms. *Proc. 2nd Manitoba Conference on Numerical Mathematics*, 1972, pp. 51-70.

[14] V. SHOUP. On the deterministic complexity of factoring polynomials over finite fields. *Submitted to Information Processing Letters*, February 21, 1989.

[15] TH. SKOLEM. The general congruence of 4th degree modulo p, p prime. *Norsk. Mat. Tidsskr*, 34, 1952, pp. 73-80.

[16] TH. SKOLEM. On a certain connection between the discriminant of a polynomial and the number of its irreducible factors mod p. *Norsk. Mat. Tidsskr*, 34, 1952, pp. 81-85.

[17] H. C. WILLIAMS. Effective primality tests for some integers of the forms $A5^n - 1$ and $A7^n - 1$. *Math. of Comp.*, volume 48, number 177, January 1987, pp. 385-403.

[18] H. C. WILLIAMS. Some algorithms for solving $x^q \equiv N \bmod p$. *Proc. 3rd S-E Conf. Combinatorics, Graph Theory, and Computing*, pp. 451-462.

[19] H. C. WILLIAMS. A $p+1$ method of factoring. *Math. of Comp.*, volume 39, number 159, July 1982, pp. 225-234.

Imprimé en France
par
l'Institut National de Recherche en Informatique et en Automatique