Cours : **Théorie algébrique des nombres (AL420)**

Enseignant : **Pr. Francesco Pappalardi**

Etudiant : **Fouotsa Tako Boris** Cycle : **XXXIV** MATRICULE : **48123**

Rapport sur le corps des nombres défini par le polynôme $X^8+93X^7+62X^6+61X^5+5X^4+99X^3-20X^2-77X-76$

Un corps des nombres est une extension de degré fini du corps des nombres rationnels $\mathbb{Q}$. Tout corps de nombres admet un élément primitif; ainsi, il est entièrement déterminé par la donnée d'un de ses éléments primitifs, du polynôme minimal d'un de ses élément primitifs ou d'une de ses bases sur $\mathbb{Q}$. Dans cet essai, nous nous intéressons au corps de nombre F défini par le polynôme

$$f(X) = X^8+93X^7+62X^6+61X^5+5X^4+99X^3-20X^2-77X-76.$$

Nous déterminons tour à tour son discriminant, ses unités, son groupe de Galois, une base d'entiers algébriques, la décomposition des nombres premiers à 2 chiffres dans l'anneau d'entiers de F, le groupe des classes et le nombre de classe de F. Nous donnons un bref aperçu de chacun des concepts précédents. Tous les résultats et toutes les définitions que nous mentionnons dans ce document proviennent des notes de cours de René Schoof intitulés *Algebraic number theory*, disponibles à l'adresse http://www.mat.uniroma2.it/~eal/moonen.pdf. Nous effectuons les calculs dans Pari/GP version 2.11.2 qui peut être téléchargé à l'adresse : https://pari.math.u-bordeaux.fr/download.html. A cet adresse, vous trouverez aussi des tutoriels très détaillés et accompagnés d'exemples.

1 Discriminant, groupe de Galois et unités de F

Pour la mise en place des concepts, f est un polynôme irréductible de degré n (dans ce contexte $n=8$), $F=\mathbb{Q}[X]/\left(f(X)\right)$ est le corps des nombres défini par $f(X)$.

Un élément $\alpha \in F$ est dit **entier (algébrique)** si son polynôme minimal $f^{\alpha}_{min} \in \mathbb{Z}[X]$. Un **réseau** sur un espace vectoriel V de dimension finie est un sous-groupe additif et discret de V contenant une base de V. L'ensemble de tous les éléments algébriques de F, noté $\mathcal{O}_F$, est appelé **l'anneau des entiers de** F et il a une structure de réseau sur F (F vu comme un $\mathbb{Q}-$espace vectoriel de dimension finie $n=[F:\mathbb{Q}]=deg(f)$). Toute base du réseau $\mathcal{O}_F$ est aussi une base de F et est appelée **base intégrale de** F. Attention il existe des bases de F, constituées d'entiers algébriques, mais qui ne sont pas des bases intégrales de F. Par exemple

$$F=\mathbb{Q}(i) \text{ où } i^2=-1, \quad \mathcal{O}_F=\mathbb{Z}[i].$$

$\{7, 5i\}$ est une base de F constituée d'entiers algébriques, mais ce n'est pas une base intégrale de F, car $1 \in \mathcal{O}_F$ mais $\quad 1 \notin \mathbb{Z}[7, 5i]$.

Un automorphisme φ de F est dit de **Galois** si $\quad \varphi_{|\mathbb{Q}} = Id_{\mathbb{Q}}$; $\quad$ c'est-à-dire φ est invariant point par point sur $\mathbb{Q}$. L'ensemble de tous les automorphismes de Galois de F est un groupe appelé **groupe de Galois de** F et noté $Gal_{F/\mathbb{Q}}$. En appliquant φ à $f(X)$, on voit directement que si φ est un automorphisme de Galois alors φ est une permutation des racines de $f(X)$. Considérant le fait que les extensions de $\mathbb{Q}$ soient séparables, il vient que le polynôme irréductible $f(X)$ a n racines distinctes. Donc $Gal_{F/\mathbb{Q}} \subset S_n$, et en ce qui nous concerne, $Gal_{F/\mathbb{Q}} \subset S_8$.

On appelle **discriminant** d'un n-uplet $\{\omega_1, \cdots, \omega_n\}$ d'éléments de F le nombre rationnel

$$\Delta(\omega_1, \cdots, \omega_n) = det\left(Tr\left(\omega_i \omega_j\right)_{1 \leqslant i,j \leqslant n}\right)$$

Un $n-$uplet $\{\omega_1, \cdots, \omega_n\}$ est une base de F si et seulement si son determinant est non nul. On montre que toutes les bases intégrales de F ont le même discriminant Δ_F qui ne dépend que du corps F et ce discriminant est appelé **le discriminant du corps** F.
Pour tout polynôme g de degré m et dont les racines sont $\alpha_1, \cdots, \alpha_m$, on appelle **discriminant de** g la quantité

$$\Delta(g) = \prod_{1 \leqslant i < j \leqslant m} (\alpha_j - \alpha_i)$$

Ce discriminant est nul si et seulement si g a des racines multiples. Si f est monique et α est une racine de f, alors $\{1, \alpha, \cdots, \alpha^{n-1}\}$ est une base de f et

$$\Delta(1, \alpha, \cdots, \alpha^{n-1}) = \Delta(f)$$

On montre que, si α est un élément primitif de F qui est aussi entier algébrique, alors

$$\Delta(1, \alpha, \cdots, \alpha^{n-1}) = [\mathcal{O}_F : \mathbb{Z}[\alpha]]^2 \Delta_F,$$

donc $\Delta_F | \Delta(f)$. IL y a égalité seulement lorsque $\{1, \alpha, \cdots, \alpha^{n-1}\}$ est une base intégrale de F; ceci est équivalent à $\mathcal{O}_F = \mathbb{Z}[\alpha]$.

On appelle **unité de** F tout élément inversible de l'anneau des entiers de F. L'ensemble des unités de F n'est rien d'autre que $\mathcal{O}_F^\times$. On appelle signature de F le couple $[r_1, r_2]$ où r_1 est le nombre de racines réelles de f et $2r_2$ est le nombre de racines complexes de f (lorsqu'on décompose f dans $\mathbb{C}$). On remarque directement que $r_1 + 2r_2 = n$. La structure $\mathcal{O}_F^\times$ est bien connue et est donnée par

$$\mathcal{O}_F^\times \simeq (\mathbb{Z}/\omega_F\mathbb{Z}) \times \mathbb{Z}^{r_1+r_2-1}$$

où ω_F est le nombre de racines de l'unité dans F. Les générateurs de la partie libre $\mathbb{Z}^{r_1+r_2-1}$ de ω_F sont appelés **les unités fondamentales de** F.

A présent nous passons à la phase de calcul des invariants que nous venons de décrire. Nous présentons des résultats obtenus dans Pari/GP.

Nous stockons le polynôme $f(X)$ en mémoire à l'aide de la commande :

`f = x^8 + 93 * x^7 + 62 * x^6 + 61 * x^5 + 5 * x^4 + 99 * x^3 - 20 * x^2 - 77 * x - 76;`.

La commande `polisirreducible(f)` (qui revoie `%2 = 1`) nous rassure que le polynôme est bel et bien irréductible. Nous initialisons le corps des nombre F a l'aide de la commande `F=nfinit(f);`.

La commande `polgalois(f)` donne le groupe de Galois de f : $Gal_{F/\mathbb{Q}} = S_8$.

Pour calculer $\Delta(f)$ et Δ_F, on utilise les commandes `poldisc(f)` et `F.disc` respectivement. En plus de calculer, les commandes `factor(poldisc(f))` et `factor(F.disc)` factorisent les résultats obtenus et nous avons :

$$\Delta(f) = -2^{17} * 3 * 17 * 313 * 92899904916133992165557$$

$$\Delta_F = -2^{9} * 3 * 17 * 313 * 92899904916133992165557$$

Donc $\Delta(f) = (2^4)^2 \Delta_F$.

La commande `F.zk` nous renvoie une base intégrale de F. Soit α une racine de f, alors une base intégrale de F est :

$$\left\{1;\quad \alpha+12;\quad \frac{1}{4}\alpha^7+\frac{93}{4}\alpha^6+\frac{61}{4}\alpha^5-8\alpha^4-14\alpha^3+\frac{131}{4}\alpha^2+9\alpha-30;\quad \frac{1}{4}\alpha^6+\frac{93}{4}\alpha^5+\frac{61}{4}\alpha^4-8\alpha^3-14\alpha^2+\frac{131}{4}\alpha-1;\right.$$
$$-\frac{1}{2}\alpha^6-\frac{91}{2}\alpha^5+\frac{123}{2}\alpha^4-15\alpha^3+28\alpha^2-\frac{59}{2}\alpha+64;\quad -\alpha^7-\frac{185}{2}\alpha^6-\frac{31}{2}\alpha^5-\frac{61}{2}\alpha^4-20\alpha^3-35\alpha^2+\frac{109}{2}\alpha+74;$$
$$-\frac{1}{2}\alpha^7-\frac{187}{4}\alpha^6-\frac{215}{4}\alpha^5-\frac{1}{4}\alpha^4-56\alpha^3-\frac{41}{2}\alpha^2-\frac{203}{4}\alpha+68;$$
$$\left.\frac{3}{4}\alpha^7+\frac{139}{2}\alpha^6+\frac{47}{2}\alpha^5+\frac{215}{4}\alpha^4+27*\alpha^3+\frac{321}{4}\alpha^2-\frac{247}{4}\alpha-37\right\}$$

Pour le calcul des unités, nous avons besoin des calculs un peu plus avancés, pour cela nous réinitialisons le corps avec la commande `F1=bnfinit(F);`. La commande `nfrootsof1(F1)` calcule les racines de l'unité de F et `F1.sign` calcule la signature de F. F a pour signature $[2,3]$ et les racines de l'unité de F sont $\mu_F = \{-1,1\}$. Ainsi, F a exactement $r = r_1 + r_2 - 1 = 2+3-1 = 4$ unités fondamentales et

$$\mathcal{O}_F^\times \simeq (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}^4$$

Il peut arriver que la commande `F1=bnfinit(F);` n'inclut pas le calcul des unités fondamentales, alors pour qu'elle puisse les inclure, on la modifie comme suit : `F2=bnfinit(F1,1);`. Pour afficher les unités fondamentales on utilise la commande `lift(F2.fu)`. Vous constaterez que ceux ci sont d'une taille énorme, nous n'affichons que le premier :

$$\begin{aligned}
&67750620466262703486477098898438387825587476231464118773635767050446961853306796838974436729771998621616529790765484305310447679918571912161448026277577965338599 * \alpha^7 + \\
&11925025882767001207849168971653201371498974629475799946266158081234769232227709642293116861708522554355031161328523064510979847794952687180202495166014890176718629/2 * \alpha^6 - \\
&53732332545628625336037295394630595887303500507627121021029326683894267221781221674191040064129575761781817615306850608340105986814796935473966847700236438106592561/2 * \alpha^5 + \\
&39446033430372829018442835033808337502828413426091292732247225364054301988527656105510033386929723371071994089776743821486519117586163416140891421519427919535024725/2 * \alpha^4 - \\
&94375208430088698838255599129120153992189657077124074316379186202004732985547386926760457874835623683367737091870757220936921696403679767665683400551013710711913242 * \alpha^3 - \\
&53125393138214798997122074127976599627352971249318630515553362217006942147805565745113356301061887076439590866957645694834930822554445500339977970913279262723723 66 * \alpha^2 - \\
&12660698824393273905012028131578214263865404164477142679749786829276207828659953946219643146084021865336129210504274675468145517779491782036641296459828126119299041/2 * \alpha + \\
&15072872045738617375907201203944405643687696496599790091925319269555637994911834815486332023147070110069517170608823109079383805586656592187164290117667019246763387
\end{aligned}$$

Il y a aussi un déterminant appelé le régulateur de F et noté R_F. Nous n'allons pas le définir explicitement mais néanmoins, il est, à facteur d'erreur près, égal au covolume de $\mathcal{O}_F^\times/\mu_F$ vu comme un réseau de dimension $r = r_1 + r_2 - 1$ sur $\mathbb{R}$ (en effet, on peut entièrement décomposer $f(X)$ dans $\mathbb{C}$ et plonger F dans $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, et ainsi parler de réseau sur $\mathbb{R}$). De ce fait, ce la nous donne une idée sur la taille des unités fondamentales de F. Pour afficher la régulateur de $\mathbb{F}$, nous utilisons la commande `F2.reg`. Le régulateur de F est :

$$R_F = 3031972080442.329183312399334$$

2 Décomposition d'idéaux et groupe des classes de F

Lorsqu'on s'intéresse à la décomposition d'éléments de $\mathcal{O}_F$ en produits d'éléments réductibles, on constate que $\mathcal{O}_F$ n'est pas toujours factoriel. Par exemple dans $\mathbb{Q}(\sqrt{-5})$; $6 = 2*3 = (1+\sqrt{-5})(1-\sqrt{-5})$ a deux décompositions en produit de facteurs irréductibles distinctes. On s'est retourné vers les idéaux de $\mathcal{O}_F$ et on a constaté que cet obstacle n'y existe pas.

On appelle idéal fractionnaire de $\mathcal{O}_F$ (ou de F) tout sous groupe additif $I \subset F$ pour lequel il existe $\alpha \in F$ tel que αI soit un idéal non nul de $\mathcal{O}_F$. En particulier les idéaux non nuls de $\mathcal{O}_F$ sont tous des idéaux fractionnaires de $\mathcal{O}_F$. L'ensemble des idéaux fractionnaires de $\mathcal{O}_F$ est un groupe (multiplicatif) noté $Id(\mathcal{O}_F)$, d'élément neutre $\mathcal{O}_F$ et où le produit est défini par

$$IJ = \left\{ \sum_i^{<\infty} x_i y_i ;\ x_i \in I,\ y_i \in J \right\}$$

Tout idéal factionnaire de $\mathcal{O}_F$ se décompose de façon unique comme produit d'idéaux premiers.

Comment se décomposent les idéaux principaux engendrés par des nombres entiers premiers ? Soit p un nombre premier ; p est dit **inerte** si l'idéal $(p) = p\mathcal{O}_F$ est premier, **scindé** si la décomposition de l'idéal $(p) = p\mathcal{O}_F$ est sans facteur carré, **ramifié** si la décomposition de l'idéal $(p) = p\mathcal{O}_F$ comporte des facteurs carrés. Un théorème de Dedekind nous dit qu'un nombre premier p est ramifié dans $\mathcal{O}_F$ si et seulement si p divise le discriminant Δ_F ; par conséquent, pour un corps de nombre F fixé, il existe un nombre fini de nombres premiers ramifies dans $Id(\mathcal{O}_F)$. Pour les nombres premiers restants, une moitié est scindée et l'autre est inerte.

On note $PId(\mathcal{O}_F)$ le sous groupe des idéaux fractionnaires principaux de $\mathcal{O}_F$. On appelle **groupe des classes** $\mathcal{O}_F$ le groupe $Cl(\mathcal{O}_F)$ des classes de $Id(\mathcal{O}_F)$ modulo $PId(\mathcal{O}_F)$; c'est-à-dire

$$Cl(\mathcal{O}_F) = Id(\mathcal{O}_F)/PId(\mathcal{O}_F)$$

On montre que le groupe des classes de l'anneau d'entiers d'un corps de nombres est fini. Le cardinal de $Cl(\mathcal{O}_F)$ est appelé le **nombre de classes de** $\mathcal{O}_F$ et on le note $h(\mathcal{O}_F)$. Lorsque $h(\mathcal{O}_F) = 1$, tous les idéaux fractionnaires de $\mathcal{O}_F$ sont principaux.

Lorsque nous passons aux calculs, la commande `F2.no` qui calcule $h(\mathcal{O}_F)$ renvoie 1. Donc tous les idéaux fractionnaires de $\mathcal{O}_F$ sont principaux.

Au paragraphe précédent, nous avons vu que :

$$\Delta_F = -2^9 * 3 * 17 * 313 * 92899904916133992165557 = -2^9 * 3 * 17 * 313 * q$$

Donc les nombres premiers ramifiés dans F sont 2, 3, 17, 313 et q. A l'aide de la commande `idealprimedec(F2,p);`, nous calculons la décomposition d'un nombre premier p (plus précisément de l'idéal $p\mathcal{O}_F$) en produit d'idéaux premiers. Nous présentons ici la décomposition des nombres premiers ramifiés dans F et celle des nombres premiers inférieurs à 100.

Nombres premiers ramifiés			
p	décomp.	facteurs	norme des facteurs
2	$\mathfrak{p}_1\mathfrak{p}_2^3\mathfrak{p}_3$	$\mathfrak{p}_1 = (2,\alpha)$; $\mathfrak{p}_2 = (2,\alpha+1)$; $\mathfrak{p}_3 = (2,\alpha^3+\alpha^2+1)$	$N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = 2$; $N(\mathfrak{p}_3) = 2^3$
3	$\mathfrak{p}_1^2\mathfrak{p}_2$	$\mathfrak{p}_1 = (3,\alpha+1)$; $\mathfrak{p}_2 = (3,\alpha^6+\alpha^5+2\alpha^4+2\alpha^3+2\alpha^2+2)$	$N(\mathfrak{p}_1) = 3$; $N(\mathfrak{p}_3) = 3^6$
17	$\mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{p}_3$	$\mathfrak{p}_1 = (17,\alpha+1)$; $\mathfrak{p}_2 = (17,\alpha^2+\alpha+6)$ $\mathfrak{p}_3 = (17,\alpha^4+5\alpha^3+4\alpha^2+8\alpha+10)$	$N(\mathfrak{p}_1) = 17$; $N(\mathfrak{p}_2) = 17^2$; $N(\mathfrak{p}_3) = 17^4$
313	$\mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{p}_3$	$\mathfrak{p}_1 = (313,\alpha+153)$; $\mathfrak{p}_2 = (313,\alpha+274)$; $\mathfrak{p}_3 = (313,\alpha^5+139\alpha^4+302\alpha^3+134\alpha^2+281\alpha+142)$	$N(\mathfrak{p}_1) = 313$; $N(\mathfrak{p}_2) = 313$; $N(\mathfrak{p}_3) = 313^5$
q	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3^2\mathfrak{p}_4\mathfrak{p}_5$	$\mathfrak{p}_1 = (q,\alpha+2078787256805518474347)$; $\mathfrak{p}_2 = (q,\alpha+22571330117563818136364)$; $\mathfrak{p}_3 = (q,\alpha+27760659838793388611630)$; $\mathfrak{p}_4 = (q,\alpha+92469187071143534661595)$; $\mathfrak{p}_5 = (q,\alpha^3+13159185709168335835641\alpha^2$ $+30237008569302467179358\alpha$ $+21984004422269968851233)$	$N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = q$; $N(\mathfrak{p}_3) = N(\mathfrak{p}_4) = q$; $N(\mathfrak{p}_5) = q^3$

Nombres premiers inférieurs à 100			
p	décomp.	facteurs	norme des facteurs
5	$\mathfrak{p}_1$	$\mathfrak{p}_1 = (5, f(\alpha) \ mod\ 5)$;	$N(\mathfrak{p}_1) = 5^8$
7	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	$\mathfrak{p}_1 = (7, \alpha+2)$;$\mathfrak{p}_2 = (7, \alpha^3+6\alpha+5)$;$\mathfrak{p}_3 = (7, \alpha^4+2\alpha+5)$	$N(\mathfrak{p}_1) = 7$; $N(\mathfrak{p}_2) = 7^3$; $N(\mathfrak{p}_3) = 7^4$
11	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{p}_1 = (11, \alpha^3+8\alpha^2+6\alpha+5)$; $\mathfrak{p}_2 = (11, \alpha^5+8\alpha^4+3\alpha^3+6\alpha^2+9\alpha+9)$	$N(\mathfrak{p}_1) = 11^3$; $N(\mathfrak{p}_2) = 11^5$
13	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	$\mathfrak{p}_1 = (13, \alpha+11)$; $\mathfrak{p}_2 = (13, \alpha^3+12\alpha^2+9\alpha+5)$; $\mathfrak{p}_3 = (13, \alpha^4+5\alpha^3+\alpha^2+9\alpha+5)$	$N(\mathfrak{p}_1) = 13$; $N(\mathfrak{p}_2) = 13^3$; $N(\mathfrak{p}_3) = 13^4$
19	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	$\mathfrak{p}_1 = (19, \alpha)$ $\mathfrak{p}_2 = (19, \alpha^3+7\alpha^2+15\alpha+18)$ $\mathfrak{p}_3 = (19, \alpha^4+10\alpha^3+15\alpha^2+16\alpha+1)$	$N(\mathfrak{p}_1) = 19$; $N(\mathfrak{p}_2) = 19^3$; $N(\mathfrak{p}_3) = 19^4$
23	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$	$\mathfrak{p}_1 = (23, \alpha+5)$ $\mathfrak{p}_2 = (23, \alpha^2+6\alpha+13)$ $\mathfrak{p}_3 = (23, \alpha^2+6\alpha+22)$ $\mathfrak{p}_4 = (23, \alpha^3+7\alpha^2+19\alpha+4)$	$N(\mathfrak{p}_1) = 23$; $N(\mathfrak{p}_2) = 23^2$; $N(\mathfrak{p}_3) = 23^2$; $N(\mathfrak{p}_4) = 23^2$
29	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	$\mathfrak{p}_1 = (29, \alpha+8)$ $\mathfrak{p}_2 = (29, \alpha^3+23\alpha^2+25\alpha+15)$ $\mathfrak{p}_3 = (29, \alpha^4+4\alpha^3+19\alpha^2+16\alpha+10)$	$N(\mathfrak{p}_1) = 29$; $N(\mathfrak{p}_2) = 23^3$; $N(\mathfrak{p}_3) = 23^4$
31	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4\mathfrak{p}_5$	$\mathfrak{p}_1 = (31, \alpha+26)$; $\mathfrak{p}_2 = (31, \alpha+27)$; $\mathfrak{p}_3 = (31, \alpha^2+2)$; $\mathfrak{p}_4 = (31, \alpha^2+10\alpha+14)$; $\mathfrak{p}_5 = (31, \alpha^2+30\alpha+24)$	$N(\mathfrak{p}_1) = 31$; $N(\mathfrak{p}_2) = 31$; $N(\mathfrak{p}_3) = 31^2$; $N(\mathfrak{p}_4) = 31^2$; $N(\mathfrak{p}_5) = 31^2$
37	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	$\mathfrak{p}_1 = (37, \alpha+19)$; $\mathfrak{p}_2 = (37, \alpha+36)$; $\mathfrak{p}_3 = (37, \alpha^6+\alpha^5+26\alpha^4+19\alpha^3+9\alpha^2+2\alpha+4)$	$N(\mathfrak{p}_1) = 37$; $N(\mathfrak{p}_2) = 37$; $N(\mathfrak{p}_3) = 37^6$
41	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$	$\mathfrak{p}_1 = (41, \alpha+15)$; $\mathfrak{p}_2 = (41, \alpha+19)$; $\mathfrak{p}_3 = (41, \alpha^2+30\alpha+1)$; $\mathfrak{p}_4 = (41, \alpha^4+29\alpha^3+16\alpha^2+16\alpha+38)$	$N(\mathfrak{p}_1) = 41$; $N(\mathfrak{p}_2) = 41$; $N(\mathfrak{p}_3) = 41^2$; $N(\mathfrak{p}_4) = 41^4$
43	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	$\mathfrak{p}_1 = (43, \alpha+36)$; $\mathfrak{p}_2 = (43, \alpha^3+23\alpha^2+19\alpha+25)$; $\mathfrak{p}_3 = (43, \alpha^4+34\alpha^3+4\alpha^2+31\alpha+11)$	$N(\mathfrak{p}_1) = 43$; $N(\mathfrak{p}_2) = 43^3$; $N(\mathfrak{p}_3) = 43^4$
47	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{p}_1 = (47; \alpha^4+22\alpha^3+6\alpha^2+18\alpha+10)$; $\mathfrak{p}_2 = (47; \alpha^4+24\alpha^3+45\alpha^2+37\alpha+30)$	$N(\mathfrak{p}_1) = 47^4$; $N(\mathfrak{p}_2) = 47^4$
53	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$	$\mathfrak{p}_1 = (53, \alpha+8)$; $\mathfrak{p}_2 = (53, \alpha+14)$; $\mathfrak{p}_3 = (53, \alpha^2+34\alpha+43)$; $\mathfrak{p}_4 = (53, \alpha^4+37\alpha^3+2\alpha^2+50\alpha+26)$	$N(\mathfrak{p}_1) = 53$; $N(\mathfrak{p}_2) = 53$; $N(\mathfrak{p}_3) = 53^2$; $N(\mathfrak{p}_4) = 53^4$;
59	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$	$\mathfrak{p}_1 = (59, \alpha+44)$; $\mathfrak{p}_2 = (59, \alpha+53)$; $\mathfrak{p}_3 = (59, \alpha^2+23\alpha+55)$; $\mathfrak{p}_4 = (59, \alpha^4+32\alpha^3+41\alpha^2+27\alpha+52)$	$N(\mathfrak{p}_1) = 59$; $N(\mathfrak{p}_2) = 59$; $N(\mathfrak{p}_3) = 59^2$; $N(\mathfrak{p}_4) = 59^4$
61	$\mathfrak{p}_1$	$\mathfrak{p}_1 = (61, f(\alpha) \ mod\ 61)$;	$N(\mathfrak{p}_1) = 61^8$
67	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{p}_1 = (67, \alpha^4+46\alpha^3+27\alpha^2+2\alpha+29)$; $\mathfrak{p}_2 = (67, \alpha^4+47\alpha^3+17\alpha^2+18\alpha+2)$	$N(\mathfrak{p}_1) = 67^4$; $N(\mathfrak{p}_2) = 67^4$
71	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	$\mathfrak{p}_1 = (71, \alpha^2+18\alpha+39)$; $\mathfrak{p}_2 = (71, \alpha^3+14\alpha^2+20\alpha+33)$; $\mathfrak{p}_3 = (71, \alpha^3+61\alpha^2+31)$	$N(\mathfrak{p}_1) = 71^2$; $N(\mathfrak{p}_2) = 71^3$; $N(\mathfrak{p}_3) = 71^3$
73	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{p}_1 = (73, \alpha^3+58\alpha^2+3\alpha+63)$; $\mathfrak{p}_2 = (73, \alpha^5+35\alpha^4+39\alpha^2+64\alpha+66)$	$N(\mathfrak{p}_1) = 73^3$; $N(\mathfrak{p}_2) = 73^5$
79	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{p}_1 = (79, \alpha^4+40\alpha^3+9\alpha^2+23\alpha+35)$; $\mathfrak{p}_2 = (79, \alpha^4+53\alpha^3+66\alpha^2+2\alpha+52)$	$N(\mathfrak{p}_1) = 79^4$; $N(\mathfrak{p}_2) = 79^4$
83	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{p}_1 = (83, \alpha+35)$; $\mathfrak{p}_2 = (83, \alpha^7+58\alpha^6+24\alpha^5+51\alpha^4+46\alpha^3+66\alpha^2+77\alpha+50)$	$N(\mathfrak{p}_1) = 83$; $N(\mathfrak{p}_2) = 83^7$
89	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	$\mathfrak{p}_1 = (89, \alpha+65)$; $\mathfrak{p}_2 = (89, \alpha^3+31\alpha^2+66\alpha+74)$; $\mathfrak{p}_3 = (89, \alpha^4+86\alpha^3+49\alpha^2+84\alpha+70)$	$N(\mathfrak{p}_1) = 89$; $N(\mathfrak{p}_2) = 89^3$; $N(\mathfrak{p}_3) = 89^4$
97	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{p}_1 = (97, \alpha^2+67\alpha+45)$; $\mathfrak{p}_2 = (97, \alpha^6+26\alpha^5+21\alpha^4+6\alpha^3+16\alpha^2+18\alpha+91)$	$N(\mathfrak{p}_1) = 97^2$; $N(\mathfrak{p}_2) = 97^6$