Université de Bordeaux L3 Math, Info, Math-Info
Collège Sciences et Technologies

Année Universitaire 2014-2015
Examen
Parcours : IN601, MA601, MA603 **UE :** N1MA6W31
Épreuve : Cryptographie et Arithmétique
Date : 5 Mai 2015 **Heure :** 14h00 **Durée :** 3h
Documents : Aucun document autorisé
Épreuve de M. Cerri

Corrigé

Exercice 1 [Algorithme de Dixon]

1. Si $x^2 \equiv y^2 \bmod N$, alors

$$N \mid (x+y)(x-y). \tag{1}$$

Si $\text{pgcd}(x+y, N) = N$, alors $N \mid x+y$ et $x \equiv -y \bmod N$, ce qui est faux. Si $\text{pgcd}(x+y, N) = 1$, alors (1) et le lemme de Gauss impliquent $N \mid x-y$ ou encore $x \equiv y \bmod N$, ce qui est encore faux. Par suite $\text{pgcd}(x+y, N)$ qui est un diviseur de N, est un diviseur non trivial de N. Le même raisonnement s'applique à $\text{pgcd}(x-y, N)$.

2. Si on multiplie entre elles les congruences (1) et (8) on obtient

$$(78865 \times 95323)^2 \equiv (2 \times 3 \times 7^3)^2 \bmod N,$$

ou encore

$$2747966^2 \equiv 2058^2 \bmod N.$$

En posant $x = 2747966$ et $y = 2058$, on constate que les hypothèses de la question 1 sont vérifiées. On calcule alors par exemple $\text{pgcd}(x+y, N)$ à l'aide de l'algorithme d'Euclide et on trouve 907. Un second diviseur non trivial de N est $N/907 = 3671$, que l'on peut aussi obtenir en calculant $\text{pgcd}(x-y, N)$.
On pouvait aussi multiplier entre elles les congruences (4) et (9), ou encore (2) et (7). On obtenait alors dans les deux cas $\text{pgcd}(x+y, N) = 3671$. Il y avait encore d'autres possibilités plus compliquées qui donnaient le même résultat.

Exercice 2 [Système de Rabin]

1. Comme p est premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps (en particulier il est intègre). Par conséquent

$$x^2 = y^2 \Leftrightarrow (x+y)(x-y) = 0 \Leftrightarrow x+y = 0 \text{ ou } x-y = 0 \Leftrightarrow x = \pm y.$$

On associe les $p-1$ éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$ deux par deux : x et $-x$. Notons ici que l'on a toujours $x \neq -x$ car p est impair, 2 est donc inversible modulo p et $2x = 0 \Rightarrow x = 0$. On obtient donc $\frac{p-1}{2}$ paires $\{1, p-1\}$, $\{2, p-2\}$,..., $\{\frac{p-1}{2}, \frac{p+1}{2}\}$. Par ce qui précède, les éléments d'une même paire ont le même carré (non nul car $\mathbb{Z}/p\mathbb{Z}$ est un corps) et deux éléments de deux paires distinctes ont des carrés distincts. Il y a donc $\frac{p-1}{2}$ carrés non nuls dans $\mathbb{Z}/p\mathbb{Z}$: $1^2 = (p-1)^2$, $2^2 = (p-2)^2$,..., $(\frac{p-1}{2})^2 = (\frac{p+1}{2})^2$.

2. Soit a un carré non nul de $\mathbb{Z}/p\mathbb{Z}$: $a = x^2$ avec $x \neq 0$. On a alors $a^{\frac{p-1}{2}} = x^{p-1} = 1$ par le petit théorème de Fermat. On en déduit que a est racine de $X^{\frac{p-1}{2}} - 1$. Par conséquent les $\frac{p-1}{2}$ carrés non nuls de $\mathbb{Z}/p\mathbb{Z}$ sont racines de $X^{\frac{p-1}{2}}$, et comme ce polynôme de degré $\frac{p-1}{2}$ a au plus $\frac{p-1}{2}$ racines dans le corps $\mathbb{Z}/p\mathbb{Z}$, on obtient la conclusion.

3. Par ce qui précède, -1 est un carré si et seulement si -1 est racine de $X^{\frac{p-1}{2}} - 1$. Ceci équivaut à $(-1)^{\frac{p-1}{2}} = 1$ dans $\mathbb{Z}/p\mathbb{Z}$. Comme $p > 2$ ceci équivaut à $\frac{p-1}{2}$ pair ou encore $p \equiv 1 \bmod 4$.

4. Si $x = 0$, $y = 0$ et on a bien $y^2 = x$. Si $x \neq 0$, on a $y^2 = x^{\frac{p+1}{2}} = x^{\frac{p-1}{2}} x$. Or on a vu dans la question 2 que $x^{\frac{p-1}{2}} = 1$. On a donc $y^2 = x$.
L'algorithme est le suivant :

- Si $x = 0$ retourner 0
- Si $x \neq 0$ retourner $y = x^{\frac{p+1}{4}}$ et $-y$.

Notons que l'on a bien toutes les racines carrées à chaque fois. Si $z^2 = 0$, nécessairement $z = 0$ car on travaille dans le corps $\mathbb{Z}/p\mathbb{Z}$. Si $z^2 = x \neq 0$, x a deux racines carrées opposées par la question 1, nécessairement y et $-y$.
Pour le calcul de y, on utilise bien sûr l'exponentiation binaire modulo p.

5. La complexité arithmétique est en $O(\log \frac{p+1}{4}) = O(\log p)$ multiplications dans $\mathbb{Z}/p\mathbb{Z}$. Si on utilise la multiplication naïve et la réduction naïve modulo p, la complexité binaire est en $O((\log p)^3)$.

6. Cas (i) : $x = 0$. Soit $y \in \mathbb{Z}/N\mathbb{Z}$ tel que $y^2 = 0$. Posons $y = a \bmod N$ (où $a \in \mathbb{Z}$). Alors $a^2 = 0 \bmod N$ donc $a^2 = 0 \bmod p$ et $a^2 = 0 \bmod q$. On en déduit $a = 0 \bmod p$ et $a = 0 \bmod q$. Le théorème chinois implique alors $a = 0 \bmod N$ et $y = 0$.
Cas (ii) $x \neq 0$ et $x \notin (\mathbb{Z}/N\mathbb{Z})^\times$. Posons $x = b \bmod N$. Alors $\text{pgcd}(b, N) \neq 1$ et par symétrie on peut supposer : $p \mid b$ et $q \nmid b$ ou encore $b \bmod p = 0$ et $b \bmod q \neq 0$. Soit $y \in \mathbb{Z}/N\mathbb{Z}$ tel que $y^2 = x$. Posons $y = a \bmod N$ (où $a \in \mathbb{Z}$). Alors $a^2 \bmod p = b \bmod p = 0$ et $a^2 \bmod p = b \bmod p \neq 0$. On en déduit que $a = 0 \bmod p$ et qu'il y a deux solutions (non nulles et opposées) pour a modulo q. Le théorème chinois implique alors que l'on a deux solutions (non nulles et opposées) modulo N.
Cas (iii) : $x \in (\mathbb{Z}/N\mathbb{Z})^\times$. Avec les mêmes notations on trouve $a^2 \bmod p \neq 0$ et $a^2 \bmod q \neq 0$. On obtient deux solutions (non nulles et opposées a_p et $-a_p$)) modulo p et deux solutions (non nulles et opposées a_q et $-a_q$) modulo q. Le théorème chinois implique alors qu'il y a quatre solutions modulo N (correspondant aux quatre couples (a_p, a_q), $(-a_p, a_q)$, $(a_p, -a_q)$ et $(-a_p, -a_q)$).

7. Posons $c = x \bmod N$. Bob regarde si p ou q divise x.
- Si p et q divisent x, autrement dit si $c = 0$, alors $m = 0$.
- Si p divise x et si q ne divise pas x, alors Bob calcule a tel que $a^2 = x \bmod q$ par l'algorithme de la question 4. Puis à l'aide du théorème chinois il calcule y tel que $y = 0 \bmod p$ et $y = \pm a \bmod q$, c'est à dire $\pm ap(p^{-1} \bmod q)$. Alors $m = y \bmod N$ et Bob a deux candidats pour m.
- Même chose par symétrie si p ne divise pas x et q divise x.
- Si ni p ni q ne divisent x, alors Bob calcule a tel que $a^2 = x \bmod p$ et b tel que $b^2 = x \bmod q$ par l'algorithme de la question 4. Puis à l'aide du théorème chinois il calcule y tel que $y = \pm a \bmod p$ et $y = \pm b \bmod q$. Alors $m = y \bmod N$ et Bob a quatre candidats pour m.

8. On a $537 \bmod p = 5 \neq 0$ et $537 \bmod q = 10 \neq 0$. On est donc dans le dernier cas. On calcule $5^{\frac{p+1}{4}} \bmod p = 5^5 \bmod 19$ et $10^{\frac{q+1}{4}} \bmod q = 10^8 \bmod 31$. On a $5^2 = 6 \bmod 19$ d'où $5^4 = 17 \bmod 19$ et $5^5 = 9 \bmod 19$. On a $10^2 = 7 \bmod 31$ d'où $10^4 = 18 \bmod 31$ et $10^8 = 14 \bmod 31$. On a donc deux racines carrées modulo p (± 9) et deux racines carrées modulo q (± 14). Pour utiliser le théorème chinois, on a besoin d'une relation de Bézout entre 19 et 31. L'algorithme d'Euclide étendu fournit : $8 \times 31 - 13 \times 19 = 1$. On a donc comme solutions $m = 9 \times 8 \times 31 - 14 \times 13 \times 19 \bmod 589 = 541$, $m = 9 \times 8 \times 31 + 14 \times 13 \times 19 \bmod 589 = 389$. Les autres combinaisons donnent évidemment $-541 \bmod 589 = 48$ et $-389 \bmod 589 = 200$. Les candidats pour m sont donc 48, 200, 389, 541.

9. Posons $c = x \bmod N$. Si l'attaquant ne trouve que deux racines carrées, c'est que par exemple p divise x et q ne divise pas x. En calculant $\text{pgcd}(x, N)$ il obtiendra p et pourra factoriser N. Si l'attaquant trouve quatre racines carrées on est dans le dernier cas. Il a donc obtenu deux entiers a et b vérifiant $a^2 = b^2 \bmod N = c$ et $a \neq \pm b \bmod N$. On sait qu'en calculant $\text{pgcd}(a \pm b, N)$ (voir exercice 1), il obtiendra un diviseur non trivial de N et pourra donc factoriser N.

10. Si $c = 0$, il n'y a pas de problème : $m = 0$. Si $c \neq 0$ et $c \notin (\mathbb{Z}/N\mathbb{Z})^\times$ on a par exemple $y = 0 \bmod p$ et $y = \pm a \bmod q \neq 0$ (où l'on a posé $m = y \bmod N$). Mais si m est un carré, $y \bmod q$ est un carré. Parmi $a \bmod q$ et $-a \bmod q$ au plus un élément est un carré. En effet si $a \bmod q = r^2$ et $-a \bmod q = s^2$ avec $r, s \in \mathbb{Z}/q\mathbb{Z}$, $r, s \neq 0$, alors $-1 = (rs^{-1})^2$ est un carré de $\mathbb{Z}/q\mathbb{Z}$ et par la question 3 ceci implique $q \equiv 1 \bmod 4$, ce qui est faux par hypothèse. D'où au plus un candidat et la solution. Dans le dernier cas le raisonnement est le même. On a au plus un candidat modulo p et au plus un candidat modulo q, d'où au plus un candidat modulo N et la solution.

Exercice 3 [Log Discret]

1. Le système est

$$\begin{cases} 42 &= x_5 + x_7 + x_{13} \\ 55 &= x_5 + 2x_7 \\ 862 &= 2x_5 + x_{13} \end{cases}$$

2. Modulo 2 le système devient

$$\left\{\begin{array}{rcl} 0 & = & x_5 + x_7 + x_{13} \\ 1 & = & x_5 \\ 0 & = & x_{13} \end{array}\right.$$

On en déduit immédiatement que modulo 2 on a $x_5 = x_7 = 1$ et $x_{13} = 0$. Modulo 641 il devient

$$\left\{\begin{array}{rcl} 42 & = & x_5 + x_7 + x_{13} \\ 55 & = & x_5 + 2x_7 \\ 221 & = & 2x_5 + x_{13} \end{array}\right.$$

En faisant (3) − (1) on obtient $179 = x_5 - x_7$. En retranchant cette équation à (2) on obtient $-124 = 3x_7$ ou encore $3x_7 = 517$. Comme $3 \times 214 = 642 = 1 \bmod 641$ on sait que modulo 641 l'inverse de 3 est 214. En multipliant les deux membres de l'équation en x_7 précédente par 214, on trouve $x_7 = 517 \times 214 = 386 \bmod 641$. En reportant dans l'équation (2) on trouve : $x_5 = 55 - 2 \times 386 = 565 \bmod 641$.
3. Une relation de Bézout entre 2 et 641 est trivialement $641 - 2 \times 320 = 1$. On applique le théorème chinois et on obtient

$$\left\{\begin{array}{lll} x_5 = & 1 & \bmod\ 2 \\ x_5 = & 565 & \bmod\ 641 \end{array}\right. \Leftrightarrow x_5 = 1 \times 641 + 565 \times (-2 \times 320) \bmod 1282,$$

d'où $x_5 = 565$. Puis

$$\left\{\begin{array}{lll} x_7 = & 1 & \bmod\ 2 \\ x_7 = & 386 & \bmod\ 641 \end{array}\right. \Leftrightarrow x_7 = 1 \times 641 + 386 \times (-2 \times 320) \bmod 1282,$$

d'où $x_7 = 1027$. Notons que le recours à la formule du théorème chinois est ici artificielle. On pouvait trouver directement les solutions (uniques modulo 1282) car pour x_5, 565 convient évidemment, et pour x_7, si 386 ne convient pas, $386 + 641 = 1027$ le fait.
D'ailleurs le système était directement résoluble modulo 1282.
4. On a $x = 222 + 2x_5 + x_7 \bmod 1282 = 1097$.

Exercice 4 [Corps finis]

1. On vérifie facilement que $P(X)$ n'a pas de racine dans $\mathbb{F}_2$ et n'est pas divisible par le seul polynôme irréductible de degré 2 de $\mathbb{F}_2[X]$, à savoir $X^2 + X + 1$. Comme il est de degré 4, on en déduit que $P(X)$ est irréductible.
2. Le corps $\mathcal{C}$ a pour cardinal $2^{\deg P(X)} = 16$. Ses éléments sont les $a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3$ où les a_i parcourent $\mathbb{F}_2$.
3. Comme $\mathcal{C}$ est un corps, le cardinal de $\mathcal{C}^\times$ est $16 - 1 = 15$. Il y a $16^4 \times 15^4 = 3317760000$ clés secrètes possibles.
4. Il sufit de vérifier que $c_i \in \mathcal{C}^\times$ pour $i = 1, 2, 7, 8$. Or comme $m_1, K_1 \in \mathcal{C}^\times$, $m_1K_1 \in \mathcal{C}^\times$ (qui est un groupe multiplicatif). De même comme $m_2, K_2 \in \mathcal{C}^\times$ on a $m_2^{-1} \in \mathcal{C}^\times$ et $m_2^{-1}K_2 \in \mathcal{C}^\times$. Même chose pour c_7 et c_8.
5. On a $c_1 = 1 \times \alpha^2 = \alpha^2$ et $c_2 = \alpha^{-1}\alpha^3 = \alpha^2$. Inutile ici de chercher à déterminer l'inverse de α. On a $c_3 = (\alpha^3 + 1) \times 0 + (\alpha^3 + \alpha^2)\alpha^2 = \alpha^5 + \alpha^4$. Or $P(\alpha) = 0 \Rightarrow \alpha^4 = \alpha^3 + 1$ et $\alpha^4 = \alpha^3 + 1 \Rightarrow \alpha^5 = \alpha^4 + \alpha = \alpha^3 + \alpha + 1$. On en déduit que $c_3 = \alpha^3 + \alpha + 1 + \alpha^3 + 1 = \alpha$. On a $c_4 = (\alpha^2 + \alpha + 1) \times 0 + (\alpha^3 + 1)\alpha^2 + 1 = \alpha^5 + \alpha^2 + 1 = \alpha^3 + \alpha^2 + \alpha$ par ce qui précède. De même, on a $c_5 = (\alpha^2 + \alpha) \times 1 + (\alpha^2 + 1) \times 0 + 0 = \alpha^2 + \alpha$. On a $c_6 = (\alpha^3 + \alpha + 1) \times 1 + (\alpha^2 + \alpha) \times 0 + \alpha = \alpha^3 + 1$. On a $c_7 = (\alpha^3 + 1)^{-1}\alpha$. Pour déterminer $(\alpha^3 + 1)^{-1}$ on cherche une relation de Bézout entre $P(X) = X^4 + X^3 + 1$ et $X^3 + 1$ à l'aide de l'algorithme d'Euclide étendu. On trouve

$$X^2(X^4 + X^3 + 1) + (X^3 + X^2 + 1)(X^3 + 1) = 1,$$

d'où l'on déduit que $(\alpha^3 + 1)^{-1} = \alpha^3 + \alpha^2 + 1$. On en tire $c_7 = \alpha^4 + \alpha^3 + \alpha = \alpha + 1$. Enfin $c_8 = (\alpha^2 + \alpha)(\alpha^3 + \alpha) = \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 = \alpha^3 + \alpha^2 + \alpha$ par ce qui précède. Le message chiffré est donc

$$c = (\alpha^2, \alpha^2, \alpha, \alpha^3 + \alpha^2 + \alpha, \alpha^2 + \alpha, \alpha^3 + 1, \alpha + 1, \alpha^3 + \alpha^2 + \alpha).$$

6. On observe que $c_1 = m_1K_1 \Rightarrow m_1 = c_1K_1^{-1}$, puis que $c_2 = m_2^{-1}K_2 \Rightarrow m_2 = c_2^{-1}K_2$. De même $m_8 = c_8K_8^{-1}$ et $m_7 = c_7^{-1}K_7$. Maintenant notons A la matrice qui intervient dans le calcul de c_3 et c_4. Alors,

$$\begin{pmatrix} c_3 \\ c_4 \end{pmatrix} = A \begin{pmatrix} m_3 \\ m_4 \end{pmatrix} + \begin{pmatrix} K_3 \\ K_4 \end{pmatrix} \Rightarrow \begin{pmatrix} m_3 \\ m_4 \end{pmatrix} = A^{-1}\left[\begin{pmatrix} c_3 \\ c_4 \end{pmatrix} - \begin{pmatrix} K_3 \\ K_4 \end{pmatrix} \right].$$

Comme l'énoncé le suggère ("l'algorithme est le même") on soupçonne que $A^{-1} = A$ ce qui se vérifie en calculant A^2 et en trouvant Id_2. Le lecteur est invité à la faire. On a donc

$$\begin{pmatrix} m_3 \\ m_4 \end{pmatrix} = A\left[\begin{pmatrix} c_3 \\ c_4 \end{pmatrix} - \begin{pmatrix} K_3 \\ K_4 \end{pmatrix} \right] = A \begin{pmatrix} c_3 \\ c_4 \end{pmatrix} - A \begin{pmatrix} K_3 \\ K_4 \end{pmatrix}.$$

Notons que comme on est en caractéristique 2 on peut aussi écrire

$$\begin{pmatrix} m_3 \\ m_4 \end{pmatrix} = A \begin{pmatrix} c_3 \\ c_4 \end{pmatrix} + A \begin{pmatrix} K_3 \\ K_4 \end{pmatrix}.$$

De même si on note B la matrice intervenant dans le calcul de c_5 et c_6, on obtient

$$\begin{pmatrix} m_5 \\ m_6 \end{pmatrix} = B \begin{pmatrix} c_5 \\ c_6 \end{pmatrix} + B \begin{pmatrix} K_5 \\ K_6 \end{pmatrix}.$$

On constate que l'algorithme de déchiffrement est le même que l'algorithme de chiffrement à la nuance près que la clé est

$$K' = (K_1^{-1}, K_2, K_3', K_4', K_5', K_6', K_7, K_8^{-1})$$

où

$$\begin{pmatrix} K_3' \\ K_4' \end{pmatrix} = A \begin{pmatrix} K_3 \\ K_4 \end{pmatrix} \text{ et } \begin{pmatrix} K_5' \\ K_6' \end{pmatrix} = B \begin{pmatrix} K_5 \\ K_6 \end{pmatrix}.$$

7. On commence par calculer K'. On connaît déjà K_2' et K_7'. Calculons d'abord K_1' et K_8'. On a $K_1' = \alpha^{-2}$. Comme $1 = \alpha^4 + \alpha^3$ on a $\alpha^{-2} = \alpha^2 + \alpha$ et $K_1' = \alpha^2 + \alpha$. Pour K_8' c'est moins direct. On a $K_8' = (\alpha^3 + \alpha)^{-1}$. On cherche une relation de Bézout entre $P(X) = X^4 + X^3 + 1$ et $X^3 + X$ à l'aide de l'algorithme d'Euclide étendu. On trouve

$$(X^2 + X + 1)(X^4 + X^3 + 1) + (X^3 + X + 1)(X^3 + X) = 1,$$

d'où l'on tire $K_8' = \alpha^3 + \alpha + 1$. Finalement

$$\begin{pmatrix} K_3' \\ K_4' \end{pmatrix} = \begin{pmatrix} \alpha^3 + 1 & \alpha^3 + \alpha^2 \\ \alpha^2 + \alpha + 1 & \alpha^3 + 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha^3 + \alpha^2 \\ \alpha^3 + 1 \end{pmatrix}$$

et

$$\begin{pmatrix} K_5' \\ K_6' \end{pmatrix} = \begin{pmatrix} \alpha^2 + \alpha & \alpha^2 + 1 \\ \alpha^3 + \alpha + 1 & \alpha^2 + \alpha \end{pmatrix} \begin{pmatrix} 0 \\ \alpha \end{pmatrix} = \begin{pmatrix} \alpha^3 + \alpha \\ \alpha^3 + \alpha^2 \end{pmatrix}.$$

Passons au calcul de m. On obtient $m_1 = \alpha(\alpha^2 + \alpha) = \alpha^3 + \alpha^2$. On a $m_2 = (\alpha^2 + \alpha)^{-1}\alpha^3$. Facilement $\alpha^2(\alpha^2 + \alpha) = \alpha^4 + \alpha^3 = 1 \Rightarrow (\alpha^2 + \alpha)^{-1} = \alpha^2$, d'où $m_2 = \alpha^5 = \alpha^3 + \alpha + 1$ (calcul déjà effectué plus haut). On a $m_4 = (\alpha^3 + 1) \times 0 + (\alpha^3 + \alpha^2) \times 1 + \alpha^3 + \alpha^2 = 0$ et $m_5 = (\alpha^2 + \alpha + 1) \times 0 + (\alpha^3 + 1) \times 1 + \alpha^3 + 1 = 0$. Puis $m_5 = (\alpha^2 + \alpha)\alpha + (\alpha^2 + 1)(\alpha^2 + 1) + \alpha^3 + \alpha = \alpha^4 + \alpha^2 + \alpha + 1 = \alpha^3 + \alpha^2 + \alpha$ et $m_6 = (\alpha^3 + \alpha + 1)\alpha + (\alpha^2 + \alpha)(\alpha^2 + 1) + \alpha^3 + \alpha^2 = \alpha^2$. Enfin $m_7 = (\alpha^3 + \alpha)^{-1}\alpha$. On a déjà vu en début de question que $(\alpha^3 + \alpha)^{-1} = \alpha^3 + \alpha + 1$ d'où l'on tire $m_7 = \alpha^4 + \alpha^2 + \alpha = \alpha^3 + \alpha^2 + \alpha + 1$. Finalement, $m_8 = (\alpha^3 + \alpha^2)(\alpha^3 + \alpha + 1) = \alpha^6 + \alpha^5 + \alpha^4 + \alpha^2$. Comme $\alpha^5 = \alpha^3 + \alpha + 1$ on a $\alpha^6 = \alpha^4 + \alpha 2 + \alpha = \alpha^3 + \alpha^2 + \alpha + 1$ et après simplification, $m_8 = \alpha^3 + 1$. Le message clair est donc

$$m = (\alpha^3 + \alpha^2, \alpha^3 + \alpha + 1, 0, 0, \alpha^3 + \alpha^2 + \alpha, \alpha^2, \alpha^3 + \alpha^2 + \alpha + 1, \alpha^3 + 1).$$