Capítol 4

Arrels cúbiques a $\mathbb{Z}_m$

L'existència i el càlcul d'arrels quadrades mòdul un nombre compost m està a l'arrel de molts problemes teòrics i pràctics en Teoria de Nombres. El problema de com calcular arrels quadrades és computacionalment equivalent al de la factorització del nombre m, del qual se suposa que és un problema computacionalment difícil. És per això que aquest problema s'utilitza en alguns criptosistemes.

Diversos algorismes s'han descrit per calcular arrels quadrades mòdul un nombre primer p, però cap algorisme específic ha estat publicat per calcular d'arrels cúbiques mòdul p. Els principals algorismes per treure arrels quadrades són: algorismes generals per a factoritzar polinomis, l'algorisme de Adleman-Manders-Miller, l'algorisme de Tonelli-Shanks, l'algorisme de Peralta, algorisme de Schoof i l'algorisme de Lehmer.

Farem una breu introducció al problema de l'existència i nombre d'arrels cúbiques en un $\mathbb{Z}_p$. Tot seguit generalitzarem els algorismes de Peralta i el de Tonelli-Shanks pel càlcul d'arrels quadrades al càlcul d'arrels cúbiques mòdul un nombre primer p molt gran. Tot això ens permetrà calcular arrels cúbiques mòdul un nombre m, gran, de descomposició factorial coneguda (fent ús del teorema xinès dels residus i passant les arrels cúbiques de un $\mathbb{Z}_p$ a un $\mathbb{Z}_{p^r}$). Cal remarcar que aquestes qüestions han estat objecte d'estudi del Projecte Final de Carrera de l'*Escola Tècnica Superior d'Enginyeria de Telecomunicacions de Barcelona* [4].

Trobar l'*arrel cúbica* d'un nombre a mòdul un nombre primer p, és resoldre l'equació

$$x^3 \equiv a \mod p$$

El cas $a \equiv 0 \mod p$ té una solució única $x \equiv 0 \mod p$. També són trivials el

casos $p = 3$ i $p = 2$ ja que $x^3 \equiv x \mod p$ i per tant l'equació

$$x^3 \equiv a \mod 3 \text{ si i només si } x \equiv a \mod 3$$

Per tant descartarem tots aquests casos del nostre estudi.

4.1 Existència i nombre de solucions

Les solucions de la congruència són les antiimatges de a per l'aplicació:

$$\begin{array}{rccc} \varphi & : & \mathbb{Z}_p^* & \longrightarrow & \mathbb{Z}_p^* \\ & & x & \longmapsto & \varphi(x) = x^3 \end{array}$$

Aquesta aplicació és un endomorfisme de grups:

$$\varphi(x \cdot y) = (x \cdot y)^3 = x^3 y^3 = \varphi(x)\varphi(y)$$

El conjunt imatge és el conjunt dels cubs: $\operatorname{Im}\varphi = \mathbb{Z}_p^{*3}$. El nucli de φ són les solucions de $x^3 \equiv 1$ o sigui:

$$(x-1)(x^2+x+1) \equiv 0$$

que té per solució $x = 1$ i :

$$x \equiv \frac{-1 \pm \sqrt{-3}}{2}$$

Fent ús del símbol de Legendre podem saber quan existeix l'arrel quadrada de -3:

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1 \pmod 3 \\ -1 & \text{si } p \equiv -1 \pmod 3 \end{cases}$$

Per tant si $p \equiv -1 \mod 3$ només hi ha una arrel cúbica de la unitat i

$$|\operatorname{Ker}\varphi| = 1 \text{ llavors } |\mathbb{Z}_p^{*3}| = \frac{p-1}{1} = p-1$$

Així coneguda una arrel cúbica de a, només té aquesta ja que

$$\varphi^{-1}(a) = \{x \in \mathbb{Z}_p^* \mid x^3 \equiv a\} = x_0 \operatorname{Ker}\varphi = \{x_0\}$$

Com a conseqüència:

Proposició 4.1.1 *Si $p \equiv -1 \pmod 3$ tots els elements de $\mathbb{Z}_p^*$ són cubs i cada element només té una arrel cúbica*

En el cas que $p \equiv 1 \pmod 3$ tenim tres arrels cúbiques de la unitat, és a dir, $|\operatorname{Ker}\varphi| = 3$ i pel primer teorema d'isomorfia:

$$\mathbb{Z}_p^*/\operatorname{Ker}\varphi \simeq \mathbb{Z}_p^{*3}$$

i per tant $|\mathbb{Z}_p^{*3}| = (p-1)/3$. Llavors,

Proposició 4.1.2 *La tercera part dels elements de $\mathbb{Z}_p^*$ amb $p \equiv 1 \pmod 3$ són cubs i les dues terceres parts no.*

□

Si anomenem ϵ a una de les arrels cúbiques de la unitat diferent de 1 l'altre arrel és ϵ^2. Coneixent una solució particular x_0 les solucions de la congruència venen donades per:

$$\varphi^{-1}(a) = \{x \in \mathbb{Z}_p^* \mid x^3 \equiv a\} = x_0 \cdot \operatorname{Ker}\varphi = \{x_0, x_0\epsilon, x_0\epsilon^2\}$$

Per tant:

Proposició 4.1.3 *Per $p \equiv 1 \bmod 3$ si un nombre no nul té arrel cúbica, en té tres. A partir d'una de les arrels es troben les altres multiplicant per les arrels cúbiques de la unitat. La suma de les tres arrels cúbiques val 0.*

Però com saber si existeix arrel cúbica? Sabem que es verifica $a^{p-1} \equiv 1 \bmod p$ i d'aquí $(a^{(p-1)/3})^3 \equiv 1 \bmod p$, per tant

$$a^{\frac{p-1}{3}} \equiv \begin{cases} 1 \\ \epsilon \\ \epsilon^2 \end{cases}$$

Ara bé, si $a \in \mathbb{Z}_p^{*3}$ aleshores existeix un x_0 tal que $a \equiv x_0^3$ per tant $a^{\frac{p-1}{3}} = (x_0^3)^{\frac{p-1}{3}} = x_0^{p-1} \equiv 1$.

És a dir, que si $a \in \mathbb{Z}_p^{*3}$ aleshores $a^{\frac{p-1}{3}} \equiv 1$. I a l'inrevés? Sigui ψ:

$$\begin{array}{rccc} \psi & : & \mathbb{Z}_p^* & \longrightarrow & \mathbb{Z}_p^* \\ & & x & \longmapsto & \psi(x) = x^{\frac{p-1}{3}} \end{array}$$

morfisme de grups perquè:

$$\psi(x \cdot y) = (x \cdot y)^{\frac{p-1}{3}} = x^{\frac{p-1}{3}} y^{\frac{p-1}{3}} = \psi(x)\psi(y)$$

Raonem que $\operatorname{Im}\psi = \{1, \epsilon, \epsilon^2\}$. Sabem que $Im\psi$ és subgrup de $\{1, \epsilon, \epsilon^2\}$, per tant ha de ser $\{1\}$ o bé $\{1, \epsilon, \epsilon^2\}$. Si fos $\operatorname{Im}\psi = \{1\}$ voldria dir que per a tot

$x \in \mathbb{Z}_p^*$ tindríem $x^{(p-1)/3} \equiv 1$, però en el grup multiplicatiu d'un cos sempre hi ha un generador (és cíclic) que no verificarà això. Per tant $\operatorname{Im}\psi = \{1, \epsilon, \epsilon^2\}$. A més $\operatorname{Ker}\psi = \{x \mid x^{(p-1)/3} \equiv 1 \bmod p\}$ aleshores pel primer teorema d'isomorfia:

$$\frac{p-1}{|\operatorname{Ker}\psi|} = 3 \text{ llavors } |\operatorname{Ker}\psi| = \frac{p-1}{3} = |\mathbb{Z}_p^{*3}|$$

i com $\mathbb{Z}_p^{*3} \subset \operatorname{Ker}\psi$ es dedueix $\mathbb{Z}_p^{*3} = \operatorname{Ker}\psi$. Aleshores queda provat que

Proposició 4.1.4 *Per* $p \equiv 1 \pmod 3$

$$a \in \mathbb{Z}_p^{*3} \quad \textit{si i només si} \quad a^{\frac{p-1}{3}} \equiv 1 mod p$$

Aquest criteri ens permet esbrinar si un nombre té arrel cúbica o no (idèntic al criteri de Euler que tenim amb les arrels quadrades i el símbol de Legendre).

Veiem un parell d'exemples: a $\mathbb{Z}_{11}$ tenim:

x	x^3	$\sqrt[3]{x}$
± 1	± 1	± 1
± 2	∓ 3	∓ 4
± 3	± 5	∓ 2
± 4	∓ 2	± 5
± 5	± 4	± 3

A $\mathbb{Z}_{13}$ tenim que $x^{\frac{p-1}{3}} = x^4$ i els valors corresponents:

x	x^3	x^4	$\sqrt[3]{x}$
± 1	± 1	1	$\pm 1, \pm 3, \mp 4$
± 2	∓ 5	3	no en té
± 3	± 1	3	no en té
± 4	∓ 1	-4	no en té
± 5	∓ 5	1	$\mp 2, \mp 6, \mp 5$
± 6	∓ 5	-4	no en té

De fet això ens porta a definir un símbol cúbic que actuarà com el símbol de Legendre per a l'arrel cúbica:

$$\left[\frac{a}{p}\right] = \begin{cases} 0 & \text{si} \quad p \mid a \\ 1 & \text{si} \quad p \equiv -1 \pmod 3 \text{ i } p \nmid a \\ a^{\frac{p-1}{3}} & \text{si} \quad p \equiv 1 \pmod 3 \text{ i } p \nmid a \end{cases}$$

Que verifica:

Proposició 4.1.5 *Es verifica*

1. *Si* $p \not| a$ *llavors,* $\left[\frac{a}{p}\right] = 1$ *si i només si* a *és un residu cúbic mòdul* p
2. $\left[\frac{a \cdot b}{p}\right] = \left[\frac{a}{p}\right] \cdot \left[\frac{b}{p}\right]$
3. $a \equiv b (mòd.p)$ *aleshores* $\left[\frac{a}{p}\right] = \left[\frac{b}{p}\right]$
4. $p \not| a$ *aleshores* $\left[\frac{a^3}{p}\right] = 1$

Una vegada feta la discusió del problema de l'existència de l'arrel cúbica en un $\mathbb{Z}_p$, ens podem preguntar pel càlcul efectiu d'aquesta. Com en el cas de l'arrel quadrada hi ha molts casos pels quals és fàcil d'expressar l'arrel cúbica de a com a potència del propi nombre a. Per exemple, si $p \equiv 2 \bmod 3$ tenim que $p = 2 + 3k$ per cert enter k. A partir d'aquí sabem que

$$a^{1+3k} \equiv 1 \bmod p$$

elevant al quadrat $a^{2+6k} \equiv 1 \bmod p$ i llavors $a^{3+6k} \equiv a \bmod p$, conseqüentment l'arrel cúbica de a és a^{1+2k}, per la qual cosa:

$$\sqrt[3]{a} = a^{\frac{2p-1}{3}} \text{ si } p \equiv 2 \bmod p$$

Ens podem preguntar sota quines condicions l'arrel cúbica d'un nombre és una potència del mateix nombre. La resposta és la següent:

Proposició 4.1.6 *Sigui* $a \not\equiv 0, 1 \bmod p$ *i* α_0 *el seu ordre. L'arrel cúbica de* a *és una potència de* a *si i només si* $\text{mcd}(3, \alpha_0) = 1$ *i en aquest cas val* $\sqrt[3]{a} = a^{3^{-1}}$ *amb* 3^{-1} *l'invers de* 3 *a* $\mathbb{Z}_{\alpha_0}$.

Demostració: Anomenem $\langle a \rangle = \{a^\alpha \mid \alpha \in \mathbb{Z}\}$. Diem $\text{ord}(a) = \alpha_0 \mid p - 1$ a l'ordre de a. Si $\sqrt[3]{a} \in \langle a \rangle$ llavors $\sqrt[3]{a} = a^\beta$ amb $0 < \beta < \alpha_0$ i $(a^\beta)^3 \equiv a$. Per tant $a^{3\beta - 1} \equiv 1$ o sigui $3\beta - 1 = k\alpha_0$ o equivalentment $3\beta - k\alpha_0 = 1$. El recíproc també és cert. Per tant si l'arrel cúbica de a existeix, serà una potència del mateix a si i només si $mcd(3, \alpha_0) = 1$ i l'exponent serà el que hem avançat. □

Quan $p \equiv 2 \bmod 3$ s'observa que l'invers de 3 a $\mathbb{Z}_{\alpha_0}$ és $(2p - 1)/3$ (amb $\alpha_0 = \text{ord}(a)$) ja que $3 \cdot (2p - 1)/3 = 2p - 1 = 2(p - 1) + 1$, i $p - 1$ és un múltiple de α_0.

4.2 Modificació del mètode de Peralta

El *mètode de Peralta* [72] és un mètode ràpid per a calcular arrels quadrades en un $\mathbb{Z}_p$ per un nombre primer de la forma $p = 2^e q + 1$ ($q \not\equiv 0 \bmod 2$) amb e gran. Nosaltres construirem dos algorismes per a calcular arrels cúbiques per un nombre primer de la forma $p = 3^e q + 1$ ($q \not\equiv 0 \bmod 3$) amb e gran.

Considerem un nombre $a \in \mathbb{Z}_p$ tal que $\left[\frac{a}{p}\right] = 1$, això és, existeix l'arrel cúbica de a. Considerem l'anell

$$R = \mathbb{Z}_p[x]/(x^3 - a) = \{\alpha + \beta Y + \gamma Y^2 \,|\, \alpha, \beta, \gamma \in \mathbb{Z}_p\}$$

amb les operacions usuals i $Y^3 = a$. Sigui $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$ l'anell producte directe de $\mathbb{Z}_p$ tres vegades. Aleshores,

Proposició 4.2.1 *$R \simeq \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$ com a isomorfisme d'anells considerant l'adició i producte directes.*

Demostració: Considerem $x_0 \in \mathbb{Z}_p$ una arrel cúbica de a, això és, $x_0^3 \equiv a \bmod p$ i la funció $\varphi : R \longrightarrow \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$ definida per

$$\varphi(\alpha + \beta Y + \gamma Y^2) = (\alpha + \beta x_0 + \gamma x_0^2, \alpha + \beta\epsilon x_0 + \gamma\epsilon^2 x_0^2, \alpha + \beta\epsilon^2 x_0 + \gamma\epsilon x_0^2)$$

El sistema d'equacions lineals

$$\left.\begin{array}{llll} \alpha+ & \beta x_0+ & \gamma x_0^2 & \equiv x \bmod p \\ \alpha+ & \beta\epsilon x_0+ & \gamma\epsilon^2 x_0^2 & \equiv y \bmod p \\ \alpha+ & \beta\epsilon^2 x_0+ & \gamma\epsilon x_0^2 & \equiv z \bmod p \end{array}\right\}$$

té una solució única perquè el determinant del sistema $a(\epsilon - 1)^3(\epsilon + 1)\epsilon$ no és nul ($a \not\equiv 0 \bmod p$, $p \neq 2$ i $p \neq 3$). Llavors φ és una bijecció. Aquest és un isomorfisme d'anells, perquè verifica $\varphi(z_1 + z_2) = \varphi(z_1) + \varphi(z_2)$, $\varphi(z_1 z_2) = \varphi(z_1)\varphi(z_2)$, $\varphi(1) = (1, 1, 1)$ per a cada $z_1, z_2 \in R$. □

Com a conseqüència de la isomorfia el *petit teorema de Fermat* es verifica a R,

Corol·lari 4.2.2 *Per a cada $z \in R^*$, $z^{p-1} = 1$*

Demostració: Si $\varphi(z) = (r, s, t)$ aleshores $\varphi(z^{p-1}) = (r^{p-1}, s^{p-1}, t^{p-1}) = (1, 1, 1) = \varphi(1)$ i és per això que $z^{p-1} = 1$. □

El primer algorisme que proposem utilitza el darrer Corol·lari. Si coneixem $z \in R^*$ de tal manera que $z^{\frac{p-1}{3}} = \beta Y$ per cert $\beta \in \mathbb{Z}_p$ llavors

$$\sqrt[3]{a} = \beta^{-1}$$

perquè si $z^{\frac{p-1}{3}} = \beta Y$ aleshores $1 \equiv \beta^3 a \bmod p$ i $(\beta^{-1})^3 \equiv a \bmod p$.

L'algorisme següent troba una arrel cúbica d'un residu cúbic $a \in \mathbb{Z}_p$,

Algorisme 4.2.3 *Per un primer* $p \equiv 1 \bmod 3$
Entrada: *un residu cúbic a mòdul* p
Sortida: $x \in \mathbb{Z}_p$ *tal que* $x^3 \equiv a \bmod p$
1)Escull $z \in R^*$ *aleatòriament.*
2)Calcula $z^{\frac{p-1}{3}} = \alpha + \beta Y + \gamma Y^2$.
3)Si $\alpha = \gamma = 0$, *aleshores treu* $x = \beta^{-1} \bmod p$ *si no anar a 1.*

És natural preguntar-se per la probabilitat que un $z \in R^*$ escollit aleatòriament verifiqui que $z^{\frac{p-1}{3}} = \beta Y$ per cert $\beta \in \mathbb{Z}_p$.

Proposició 4.2.4 $\Pr(z^{\frac{p-1}{3}} = \beta Y$ *per cert* $\beta \in \mathbb{Z}_p | z \in R^*) = \frac{1}{9}$

Demostració: Si $z \in R^*$ és tal que $z^{\frac{p-1}{3}} = \beta Y$ per cert $\beta \in \mathbb{Z}_p$ i $\varphi(z) = (r, s, t)$ llavors $(r^{\frac{p-1}{3}}, s^{\frac{p-1}{3}}, t^{\frac{p-1}{3}}) = (\beta x_0, \beta\epsilon x_0, \beta\epsilon^2 x_0)$. Com que $r^{\frac{p-1}{3}}, s^{\frac{p-1}{3}}, t^{\frac{p-1}{3}} \in \{1, \epsilon, \epsilon^2\}$ el nombre β ha de ser $\beta \equiv x_0^{-1}\epsilon^i \bmod p$ per cert $i = 0, 1, 2$, a més $\left[\frac{r}{p}\right] = \epsilon^i$, $\left[\frac{s}{p}\right] = \epsilon^{i+1}$, $\left[\frac{t}{p}\right] = \epsilon^{i+2}$. Aleshores tenim $3(\frac{p-1}{3})^3$ valors possibles per (r, s, t) d'entre $(p-1)^3$ valors possibles d'elements invertibles. □

Com a màxim en 19 iteracions l'algorisme troba una arrel cúbica amb una probabilitat de 99%.

Podem observar a la demostració de la Proposició 5.2.4 que per $i = 0$ trobem una de les arrels cúbiques, per $i = 1$ la segona i per $i = 2$ la darrera. És per això que utilitzant aquest Algorisme 5.2.3 trobem cada arrel cúbica amb un 1/3 de probabilitat. Per tal de trobar totes les arrels cúbiques iterarem l'algorisme fins que trobem x_0, x_1 dues arrels cúbiques diferents, calculant la tercera com $x_3 = -x_0 - x_1$.

Per tal de distingir quan un element és invertible utilitzem el *conjugat* d'un nombre $\alpha + \beta Y + \gamma Y^2$ amb $\alpha, \beta, \gamma \in \mathbb{Z}_p$ definit com

$$\overline{\alpha + \beta Y + \gamma Y^2} = \alpha + \beta\epsilon Y + \gamma\epsilon^2 Y^2$$

Amb aquest isomorfisme d'anells podem definir la *norma* de un nombre de R com l'element de $\mathbb{Z}_p$

$$N(z) = z \cdot \overline{z} \cdot \overline{\overline{z}}$$

Aquesta aplicació verifica que $N(z_1 z_2) = N(z_1)N(z_2)$ i podem comprovar si un element és invertible amb la seva norma de la manera següent: $z \in R^* \Leftrightarrow N(z) \neq 0$. Ara som capaços de traduir el pas 1) de l'algorisme,

1')Escull $z \in R$ aleatòriament tal que $N(z) \neq 0$.

S'observa que n'hi ha prou en escollir z en el pas 1) de la forma $z = 1 + xY + yY^2$.

Veurem un algorisme més ràpid utilitzant la proposició següent.

Proposició 4.2.5 *Sigui $z = \alpha + \beta Y + \gamma Y^2$ un element de R amb almenys dos coeficients no nuls*

1)Si $z^3 = \alpha'$ amb $\alpha' \in \mathbb{Z}_p^*$ llavors

1.a)si $\beta, \gamma \not\equiv 0 \bmod p$ llavors $\sqrt[3]{a} = \frac{\alpha}{\beta}$

1.b)si $\beta \equiv 0 \bmod p, \alpha, \gamma \not\equiv 0 \bmod p$ llavors $\sqrt[3]{a} = \frac{1}{a}(\frac{\alpha}{\gamma})^2$

1.c)si $\gamma \equiv 0 \bmod p, \alpha, \beta \not\equiv 0 \bmod p$ llavors $\sqrt[3]{a} = -\frac{\alpha}{\beta}$

2)Si $z^3 = \beta' Y$ amb $\beta' \in \mathbb{Z}_p^*$ llavors $\sqrt[3]{a} = \frac{N(z)}{\beta'}$

3)Si $z^3 = \gamma' Y^2$ amb $\gamma' \in \mathbb{Z}_p^*$ llavors $\sqrt[3]{a} = \frac{(N(z))^2}{(\gamma')^2 a}$

Demostració: 1.a)Com que $z^3 = (\alpha + \beta Y + \gamma Y^2)^3 =$

$= \alpha^3 + \gamma^3 a^2 + a(6\alpha\beta\gamma + \beta^3) + 3((\alpha\gamma^2 + \beta^2\gamma)a + \alpha^2\beta)Y + 3(\alpha^2\gamma + \alpha\beta^2 + \beta\gamma^2 a)Y^2$

és un element de $\mathbb{Z}_p^*$,

$$\left.\begin{array}{rcl} (\alpha\gamma^2 + \beta^2\gamma)a + \alpha^2\beta & \equiv & 0 \bmod p \\ \alpha^2\gamma + \alpha\beta^2 + \beta\gamma^2 a & \equiv & 0 \bmod p \end{array}\right\}$$

multiplicant la primera equació per β i restant-li la segona multiplicada per α tenim $\beta^3\gamma a - \alpha^3\gamma \equiv 0 \bmod p$ i llavors $a \equiv (\frac{\alpha}{\beta})^3 \bmod p$ si $\beta, \gamma \neq 0 \bmod p$.

1.b)Si $z^3 = (\alpha + \gamma Y^2)^3 \in \mathbb{Z}_p^*$, conjugant $\overline{z}^3 = (\alpha + \gamma\epsilon^2 Y^2)^3 \in \mathbb{Z}_p^*$, aleshores el producte $z^3\overline{z}^3 = (\alpha^2 + \epsilon^2\gamma^2 aY + \alpha\gamma(1+\epsilon^2)Y^2)^3 \in \mathbb{Z}_p^*$ i utilitzant 1.a) obtenim el resultat.

1.c)Si $z^3 = (\alpha + \beta Y)^3 \in \mathbb{Z}_p^*$, conjugant $\overline{z}^3 = (\alpha + \beta\epsilon Y)^3 \in \mathbb{Z}_p^*$, llavors el producte $z^3\overline{z}^3 = (\alpha^2 + (1+\epsilon)\alpha\beta Y + \beta^2\epsilon Y^2)^3 \in \mathbb{Z}_p^*$ i utilitzant 1.a) obtenim el resultat, perquè $1 + \epsilon \not\equiv 0 \bmod p$ $(p \neq 2)$ i l'invers de $1 + \epsilon$ is $-\epsilon$.

2)Tenim $z^3 = \beta' Y$, aleshores $N(z^3) \equiv \beta'^3 a \bmod p$ i $a \equiv (\frac{N(z)}{\beta'})^3 \bmod p$.

3)Tenim $z^3 = \gamma' Y^2$, llavors $(z^2)^3 = \gamma'^2 aY$. Utilitzant 2) $\sqrt[3]{a} = \frac{N(z^2)}{\gamma'^2 a} = \frac{(N(z))^2}{\gamma'^2 a}$. □

Sigui $z \in R^*$ un element amb almenys dos coeficients no nuls i tal que el seu cub té dos coeficients iguals a zero. Com a conseqüència de la Proposició 5.2.5, una arrel cúbica de a pot ser calculada en funció de z i z^3. Una opció per trobar un $z \in R^*$ en aquestes condicions és utilitzant que $(z^q)^{3^e} = 1$ segons es desprén del Corol·lari 5.2.2 per $z \in R^*$. El procediment és calcular z^q i després d'això, elevant al cub tantes vegades com calgui fins que trobem un cub amb dos zeros i llavors utilitzar la Proposició 5.2.5. Només quan z^q tingui dos zeros no podrem aplicar aquest mètode. L'algorisme que proposem és

Algorisme 4.2.6 *Per un primer $p = 3^e q + 1$ tal que $q \not\equiv 0 \bmod 3$ amb $e > 1$*

Entrada: *un residu cúbic a mòdul p*

Sortida: *$x \in \mathbb{Z}_p$ tal que $x^3 \equiv a \bmod p$*

1)Escull $z \in R$ aleatòriament tal que $N(z) \neq 0$ amb dos coeficients no iguals a zero.

2)Calcula $z_1 = z^q$.

3)Si z_1 té dos coeficients igual a zero, llavors anar a 1.

4)Calcula $z_1^{3^i}$ per $i = 1, 2, \ldots$ per cubs repetits fins que $z_1^{3^i}$ tingui dos coeficients iguals a zero, aleshores treu una arrel cúbica aplicant les fórmules de la Proposició 5.2.5 a $z_1^{3^{i-1}}$ i $z_1^{3^i}$.

Quina és la probabilitat que un $z \in R^*$ escollit aleatòriament verifiqui que z^q tingui dos zeros?

Proposició 4.2.7 *Sigui p un primer tal que $p = 3^e q + 1$ ($q \not\equiv 0 \bmod 3$), llavors*

$$\Pr(z^q \text{ té almenys dos coeficients no nuls } | z \in R^*) = 1 - \frac{1}{3^{2e-1}}$$

Demostració: Sigui $z \in R^*$ un element tal que z^q té dos zeros. El corresponent element de $\mathbb{Z}_p^* \times \mathbb{Z}_p^* \times \mathbb{Z}_p^*$ és $(r, s, t) = \varphi(z)$ amb (r^q, s^q, t^q) igual a (α, α, α) o bé $(\beta x_0, \beta x_0 \epsilon, \beta x_0 \epsilon^2)$ o bé $(\gamma x_0^2, \gamma x_0^2 \epsilon, ^2, \gamma x_0^2 \epsilon)$.

En el primer cas $(r/t)^q \equiv 1, (s/t)^q \equiv 1 \bmod p$. Utilitzant el fet que $(\mathbb{Z}_p^*, \cdot)$ és isomorf a $(\mathbb{Z}_{p-1}, +)$ coneixem que l'equació $x^q \equiv 1 \bmod p$ té $\mathrm{mcd}(q, 3^e q) = q$ solucions $a_1, \ldots, a_q$. Aleshores $(r, s, t) = (a_i t, a_j t, t)$ per $i, j = 1, \ldots, q$ i $t = 1, \ldots, p-1$ representen cada element de R^* tal que $z^q \in \mathbb{Z}_p$. Tenim $q^2(p-1) = 3^e q^3$ elements diferents.

És fàcil de comprovar que el mateix càlcul és cert en el segon cas quan $(r/t)^q \equiv \epsilon, (s/t)^q \equiv \epsilon^2 \bmod p$ i en el tercer cas quan $(r/t)^q \equiv \epsilon^2, (s/t)^q \equiv \epsilon \bmod p$.

Resumint, tenim $3^{e+1} q^3$ elements diferents, i la probabilitat és $1 - 3^{e+1} q^3 / (3^e q)^3 = 1 - 1/3^{2e-1}$. □

La complexitat de la part no probabilística d'ambdós algorismes és $log^3 p$, però el segon és, en general, computacionalment més eficient.

4.3 Modificació del mètode de Tonelli-Shanks

Trobarem un algorisme probabilístic per treure arrels cúbiques d'un nombre anàleg al de *Tonelli-Shanks* [87, 35] per arrels quadrades.

Sigui p un primer tal que $p = 3^e q + 1$ ($q \not\equiv 0 \bmod 3$). Sabem que $(\mathbb{Z}_p^*, \cdot)$ és isomorf a $(\mathbb{Z}_{p-1}, +)$. Com que $|\mathbb{Z}_{p-1}| = 3^e q$, existeix G l'únic subgrup 3-*Sylow* [56], això és, un subgrup G de 3^e elements que conté tot subgrup de d'ordre divisor de 3^e. Podem expressar aquest amb un generador g com a $G = \{g^i | 0 \leq i < 3^e\}$ perquè és cíclic. Trobarem les arrels cúbiques en funció de g de la manera següent,

Proposició 4.3.1 *Sigui p un primer tal que $p = 3^e q + 1$ ($q \not\equiv 0 \bmod 3$) i $G = \langle g \rangle$ l'únic subgrup 3-Sylow de $\mathbb{Z}_p^*$. Existeix $0 \leq k < 3^e$ tal que si $q \equiv 1 \bmod 3$ llavors $\sqrt[3]{a} = a^{\frac{2q+1}{3}} g^k$ i si $q \equiv 2 \bmod 3$ aleshores $\sqrt[3]{a} = a^{\frac{q+1}{3}} g^k$*

Demostració: Podem observar que un element és un cub en G si i només si l'odre de l'element és un divisor de 3^{e-1}. Tenint en compte que $a^{\frac{p-1}{3}} \equiv 1 \bmod p$ llavors $(a^q)^{3^{e-1}} \equiv 1 \bmod p$ i l'ordre de a^q és un divisor de 3^{e-1}, això és un nombre de la forma 3^i per cert $i = 1, \ldots, e-1$. Com a conseqüència a^q és un cub en G i el 3-subgrup $\langle a^q \rangle$ generat per a^q és un subgrup de G, aleshores $a^q \in G$. Per tant existeix un nombre $0 \leq i < 3^e$ tal que $a^q \equiv g^{3i} \bmod p$.

Si $q \equiv 2 \bmod 3$ llavors $q+1$ és un multiple de 3 i $a^{q+1} g^{-3i} \equiv a \bmod p$ pot ser reescrit com $(a^{\frac{q+1}{3}} g^{-i})^3 \equiv a \bmod p$ i aleshores $\sqrt[3]{a} = a^{\frac{q+1}{3}} g^k$ per cert k.

Si $q \equiv 1 \bmod 3$ llavors $2q \equiv 2 \bmod 3$. Com que $2q+1$ és un multiple de 3 i $a^{2q} g^{-6i} \equiv 1 \bmod p$, aleshores $a^{2q+1} g^{-6i} \equiv a \bmod p$ i $(a^{\frac{2q+1}{3}} g^{-2i})^3 \equiv a \bmod p$, per tant $\sqrt[3]{a} = a^{\frac{2q+1}{3}} g^k$ per cert k. □

Per tal de trobar un generador del grup G busquem un no residu cúbic $n \in \mathbb{Z}_p^*$, això és $\left[\frac{n}{p}\right] \neq 1$. D'aquesta manera $g = n^q$ és un generador de G ja que $g^{3^e} = n^{3^e q} = n^{p-1} \equiv 1 \bmod p$, però $g^{3^{e-1}} = n^{3^{e-1} q} = n^{\frac{p-1}{3}} = \left[\frac{n}{p}\right] \not\equiv 1 \bmod p$.

Proposem l'algorisme següent,

Algorisme 4.3.2 *Per un primer $p = 3^e q + 1$ tal que $q \not\equiv 0 \bmod 3$ amb $e \geq 1$*

Entrada: $a \in \mathbb{Z}_p$

Sortida: *tots els $x \in \mathbb{Z}_p$ tal que $x^3 \equiv a \bmod p$ si x és un residu cúbic, altrament treu un missatge de no existència d'arrel cúbica.*

1)Troba $n \in \mathbb{Z}_p$ aleatòriament tal que $\left[\frac{n}{p}\right] \neq 1 \bmod p$

2)Inicialitza:

$g := n^q$; simbol $:= \left[\frac{n}{p}\right]$; $y := g$; $r := e$;

Si $q \equiv 2 \bmod 3$ llavors $x := a^{\frac{q-2}{3}}$; si no $x := a^{\frac{2q-2}{3}}$.

$b := a^2 x^3$; $x := ax$

3)Troba exponent o acaba:
Si $b \equiv 1 \bmod p$ *aleshores escriu(*$x, x \cdot simbol, x \cdot simbol^2$*) i acaba. Altrament troba* $m := \min\{i | b^{3^i} \equiv 1 \bmod p\}$.
Si $m = r$ *llavors escriu('no hi ha arrel cúbica') i acaba.*

4)Redueix exponent:
Si $simbol = b^{3^{m-1}}$ *aleshores* $t := y^2$, $simbol := simbol^2$. *Altrament* $t := y$.
$t := t^{3^{r-m-1}}$; $y := t^3$; $r := m$; $x := xt$; $b := by$; *anar al pas 3*

És fàcil comprovar que aquest algorisme calcula sis successions definides per

$$r_{n+1} = \min\{i | b_n^{3^i} \equiv 1 \bmod p\},\ t_{n+1} = y_n^{k_n 3^{r_n - r_{n+1} - 1}},$$

$$y_{n+1} = t_{n+1}^3,\ x_{n+1} = x_n t_{n+1},\ b_{n+1} = b_n y_{n+1}$$

amb $k_n = 2$ si $y_n^{3^{r_n-1}} \equiv b_n^{3^{r_{n+1}-1}} \bmod p$ i $k_n = 1$ altrament; $x_1 = a^{\frac{2q+1}{3}}, b_1 = a^{2q}$ si $q \equiv 1 \bmod 3$ i $x_1 = a^{\frac{q+1}{3}}, b_1 = a^q$ si $q \equiv 2 \bmod 3$; $r_1 = e$, $y_1 = g$. Verifiquen

$$ab_n \equiv x_n^3,\ y_n^{3^{r_n-1}} \equiv \epsilon \text{ or } \epsilon^2,\ b_n^{3^{r_n-1}} \equiv 1 \bmod p$$

i la successió de nombres r_n és estrictament decreixent, és per això que quan r_n arriba a $r_n = 1$, b_n és 1 i x_n és tal que $a \equiv x_n^3 \bmod p$. De fet, amb aquest algorisme podem calcular el valor de l'exponent k de la Proposició 5.3.1 com a $k = \sum_{i=2}^{n} k_1 \cdot \ldots \cdot k_{i-1} 3^{e-r_i-1}$.

Si diem G_r al subgrup dels elements amb ordre divisor de 3^r, tenim $G_r = \langle y \rangle$ i $b \in G_{r-1}$. La successió de subgrups G_r és estrictament decreixent, $G_r \subset G_{r-1}$ amb longitud menor que e i quan $r = 1$ el corresponent subgrup és $G_r = \{1\}$.

L'única part probabilística de l'algorisme és el pas 1). La probabilitat de trobar un no residu cúbic a $\mathbb{Z}_p^*$ és $2/3$, una probabilitat molt alta. Per exemple, la probabilitat de no trobar un no residu cúbic després 13 intents és menor que 10^{-6}. El nombre de bucles dels pasos 3) i 4) és com a màxim e vegades. Aquest algorisme és d'ordre $\log^4 p$ perquè una multiplicació amb una reducció modular és d'ordre $\log^2 p$.

4.4 Algunes aplicacions criptogràfiques

Podem estendre alguns criptosistemes basats en la intractabilitat de la factorització dels nombres enters que fan servir quadrats i arrels quadrades canviant-los per cubs i arrels cúbiques. Aquest és el cas de *l'esquema d'identificació i de signatura digital de Fiat- Shamir* [39] o el *criptosistema de Rabin* [73]. Ambdós

són probablement segurs contra a un adversari passiu perquè el problema de trobar arrels quadrades mòdul un nombre compost n és computacionalment equivalent al problema de la factorització entera.

El fet que poguem canviar quadrats i arrels quadrades en aquests criptosistemes per cubs i arrels cúbiques és degut al resultat següent,

Proposició 4.4.1 *Sigui n un producte de dos nombres primers almenys un d'ells congruent amb 1 mòdul 3. El problema de trobar les arrels cúbiques mòdul un nombre compost n és computacionalment equivalent al problema de factoritzar l'enter n.*

Demostració: Hem provat que coneixent la factorització entera de n podem trobar eficientment arrels cúbiques d'un residu cúbic donat.

Suposem $n = p_1p_2$ amb $p_1 \equiv 1 \bmod 3$ i $a \not\equiv 0 \bmod n$ residu cúbic. Si $\mathrm{mcd}(a, n) \neq 1$ llavors tenim la factorització entera de n. Si no, per a cada x_i, x_j tal que $x_i^3 \equiv a \bmod n$, $x_j^3 \equiv a \bmod n$ tenim $(x_i - x_j)(x_i^2 + x_ix_j + x_j^2) \equiv 0 \bmod n$. Si $p_2 \equiv -1 \bmod 3$, $x_i \equiv x_j \bmod p_2$ i aleshores $x_i^2 + x_ix_j + x_j^2 \equiv 3x_i^2 \not\equiv 0 \bmod p_2$ i la factorització entera de n és $\mathrm{mcd}(x_i - x_j, n)$, $n/\mathrm{mcd}(x_i - x_j, n)$. Quan $p_2 \equiv 1 \bmod 3$ fent les quatre arrels cúbiques, almenys dues d'elles han de ser congruents mòdul p_2 i llavors utilitzant el càlcul anterior podem trobar la factorització entera de n. □

Un dels problemes de la encriptació de clau pública de Rabin és l'ús de redundància per tal de seleccionar el missatge correcte entre les quatre posibilitats (quatre arrels quadrades). En el cas de fer servir cubs i arrels cúbiques no es necesita redundància quan s'utilitza $n = p_1p_2$ amb $p_1 \equiv p_2 \equiv -1 \bmod 3$ perquè l'arrel cúbica és única. De fet aquest cas coincideix amb l'encriptació de RSA per exponent $e = 3$. Però en aquest cas l'equivalència computacional amb la factorització entera no ha estat provada fins ara.