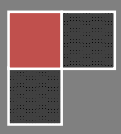
2012

La joia de l'aritmètica

Aritmètica Modular i Llei de la Reciprocitat Quadràtica

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Leibniz



$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Índex

1 Introducció

1.1 L'aritmètica modular

L'aritmètica modular és una branca de les matemàtiques, concretament de la teoria de nombres. Tracta sobre els residus i les diferents operacions aritmètiques que es poden fer amb conjunts reduïts d'enters. Té diferents aplicacions i moltes d'elles més importants del que poguem pensar. Un exemple clàssic i quotidià de l'aritmètica modular és en el rellotge: per a nosaltres les 15h són les 3 de la tarda, i les 21h són les 9 de la nit. És a dir, busquem sempre el seu "residu"al dividir entre 12 o, de forma més entenedora, un cop s'arriba a les 12 es torna a començar des de 0. Així que, per exemple, les 25h serien la 1.

1.2 Motivacions

Inicialment, quan vaig haver d'escollir un tema per al Treball de Recerca vaig dubtar molt i ja havia escollit un altre tema abans no em vaig decidir per aquest. Però el fet de trobar un treball de matemàtiques del qual no havia sentit mai a parlar i que tenia un contingut algebraic em va motivar. Potser el que menys m'agradava era que el tema és principalment teòric, però no em va fer enrere.

També em va motivar el fet que era un treball proposat per la Facultat de Matemàtiques de la Universitat Politècnica de Catalunya (UPC), que és on havia fet classes de preparació pel Cangur i Olimpíada.

I, el que finalment em va fer decidir per aquest tema, va ser el repte que suposava, perquè el que sabia sobre el tema era zero i, tot i que sabia que no seria fàcil, em va motivar més a intentar-ho.

1.3 Objectius

Els objectiu principals del treball són:

- Mostrar la Llei de la Reciprocitat Quadràtica i explicar d'una forma clara i entenedora una de les seves múltiples demostracions.
- Trobar un mètode eficaç, sitemàtic i mecànic per a calcular Símbols de Jacobi i

Legendre, fent servir les seves propietats i la Llei de la Reciprocitat Quadràtica.

Com a objectiu secundari vull analitzar com seria el procés informàtic de definició i elaboració d'un programari que calculi Símbols de Legendre.

El treball és introductori a l'aritmètica modular (o superior, com l'anomenava Gauss) i per tant, vull que aquest sigui el més entenedor possible, ja que el tema en si no és senzill. A més, també tinc la intenció d'aprendre més sobre l'aritmètica modular i les eines d'escriptura en matèmatiques, que sé que en un futur em pot ser molt beneficiós.

1.4 Estructura

En el treball trobarem diferents parts amb un contingut bastant diferent. Primerament una part introductòria a la història i a un dels matemàtics més importants d'aquest camp de les matemàtiques: **Carl Friedrich Gauss**. També trobarem una part d'ambientació històrica.

També trobem un petit apartat amb aplicacions i la situació de l'aritmètica modular a l'actualitat.

A continuació trobem el cos, la base matemàtica del treball. La part més bibliogràfica i potser la més important, sense la qual el treball mancaria d'un important objectiu. Segueix l'estructura d'escriptura matemàtica i intenta ser el màxim fidel als documents de divulgació pedagògica matemàtica, dividint els conceptes en proposicions, teoremes, aprofitant i posant exemples per millorar la comprensió, adjuntant taules...

Trobem després la part de la Llei de la Reciprocitat quadràtica, amb totes les versions trobades escrites i una de les més de dues-centes demostracions que s'han trobat.

Tot seguit trobem l'apartat referent al càlcul de símbols de Jacobi i Legendre, la part més pràctica i d'aplicació dels coneixements del punt anterior, tot comparant el mètode manual amb l'escriptura informàtica. En aquest punt en concret he rebut l'ajut d'un programador i la meva feina és, bàsicament, de comparació dels dos mètodes i aprenentatge i comprensió d'un llenguatge informàtic.

I finalment, un apartat amb les conclusions i valoracions del treball, tot allò que he après i el que pretenia aprendre abans d'acabar-lo.

1.5 Metodologia

A l'hora de buscar informació he buscat documents de text i audiovisuals via internet i d'altres que m'han recomanat alguns experts en el camp. També he consultat el llibre d'aritmètica modular més conegut de **Carl Friedrich Gauss**, les *Disquisitiones arithmeticae* traduïdes al català per una antiga professora del meu centre, **Griselda Pascual Xufré**.

Per acabar, dir que tot el treball ha estat editat per un programa anomenat "Winedt"el qual compila el llenguatge Tex (Annex1). Per tant, hi ha també una part d'aprenentatge del codi i comprensió de les comandes. El motiu pel qual escric el treball amb aquest programa és perquè la majoria de texts matemàtics són escrits en aquest codi i permet una millor escriptura de les diferents fòrmules i símbols que he necessitat per fer el treball.

Us deixo doncs, amb el meu treball i espero que l'explicació del qual sigui entenedora, planera i que no es faci massa feixuga la lectura de les diferents parts.

2 El pare de l'aritmètica modular: Carl Friederich Gauss

2.1 Biografia

Carl Friedrich Gauss (1777-1855)"El príncep dels matemàtics"

No és exagerat el títol pòstum de "Príncep"del matemàtics, encunyat en una moneda, amb la que el rei Jorge V de Hannover honorà a Gauss després de la seva mort. Segons E.T.Bell , i és una opinió compartida per la majoria dels historiadors de la ciència, Arquímedes, Newton i Gauss son tres homes que constitueixen una classe especial entre els grans matemàtics (...). Gauss va elevar l'aritmètica superior a la categoria de reina de les matemàtiques.

Carl Friedrich Gauss, va néixer a Brunswick, actual Alemanya, l'any 1777 i va morir a Gotinga, l'any 1855. Matemàtic, físic i astrònom alemany, encara avui, dos segles després del seu naixement, les seves idees i els seus innovadors mètodes segueixen sent actuals. Es va interessar i va fer descobriments en gairebé totes les branques de les matemàtiques, tant pures -Teoria dels nombres, Anàlisi, Geometria- com aplicades - astronomia, Geodèsia, Teoria d'errors- i en Física -Magnetisme, Òptica, Teoria del potencial...-.

Va néixer en el si d'una família humil. Des de molt petit, va donar mostres d'una prodigiosa capacitat per a les matemàtiques. Hi ha moltes anècdotes sobre la seva precoç genialitat. Una de les més famoses és que quan tenia vuit anys el seu professor d'aritmètica va proposar el problema de sumar els cent primers nombres naturals : 1+2+3...+100.

Gauss va escriure un sol nombre en la seva pissarra, mentre que tots els altres alumnes l'omplien de interminables sumes. Gauss va ser l'únic que va donar la resposta correcta.

El matemàtic Martin Bartels era ajudant del professor Buttner, a l'escola de Brunswick on estudiava Gauss. Des que Gauss va conèixer a Bartels, es van accelerar els seus progressos an matemàtiques. Els dos estudiaven junts, es recolzaven i desxifraven manuals sobre àlgebra i anàlisi elemental. Durant aquests anys, es van començar a gestar algunes de les idees i formes de veure les matemàtiques que van caracteritzar posteriorment a Gauss. Es va adonar, per exemple, del poc rigor en moltes demostracions de grans matemàtics que el van precedir com Newton, Euler i altres més.

Als 14 anys va conèixer al Duc de Brunswick, Ferdinand. El duc va quedar fascinat pel que havia sentit del noi i es va fer càrrec de totes les seves despeses perquè la seva educació fos completa.
Als 16 anys va tenir les primeres idees intuïtives sobre la possibilitat d'altre tipus de geometria. El seu gust per l'aritmètica va perdurar tota la seva vida.

Gauss va estudiar al Collegium Carolinum on, sorprenentment, adquirí també coneixements en llengües com el llati i el grec amb facilitat. En aquesta època ja havia descobert la llei dels mínims quadrats.

L'any 1801 va publicar el llibre *Disquisitiones Arithmeticae*, amb sis seccions dedicades a la Teoria de nombres, donant a aquesta branca de les matemàtiques una estructura sistematitzada. En la última secció del llibre, exposa la seva tesi doctoral. Aquest mateix any, va predir l'òrbita de Ceres aproximant paràmetres per mínims quadrats.

En 1809 va ser nombrat director de l' Observatorio de Gotinga. En aquest mateix any, va publicar *Theoria motus corporum coelestium in sectionibus conicis Solem ambientium* descrivint com calcular l'òrbita d'un planeta i com refinar-la posteriorment.També va profunditzar sobre equacions diferencials i seccions còniques.

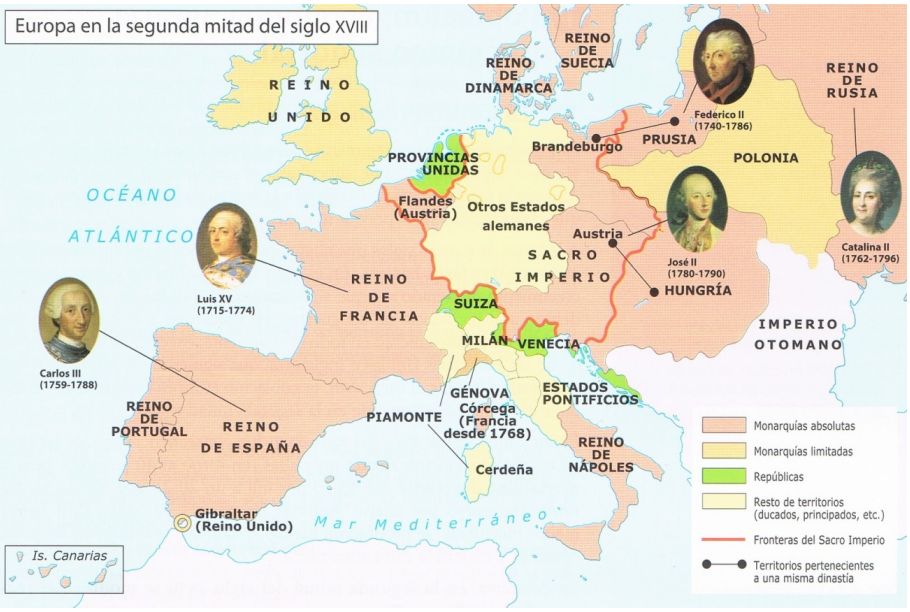
L'any 1809 va ser nombrat director de l' Observatorio de Gotinga càrrec en el que va estar tota la vida. En aquest mateix any, va publicar *Theoria motus corporum coelestium in sectionibus conicis Solem ambientium* descrivint com calcular l'òrbita d'un planeta i com refinar-la posteriorment. Va morir la seva primera dona al donar a llum el seu tercer fill. Es va tornar a casar i va tenir tres fills més. Cap el 1820 va desenvolupar eines per a tractar les dades observacionals, entre la que destaca la corba de distribució d'errors de Gauss (Campana de Gauss) que és un pilar de l'estadística.

Interessat en molts camps de les matemàtiques i la física, va inventar l'heliotrop pel seu interès en la geodèsia, i va investigar el magnetisme, investigació que va culminar amb la instal·lació del primer telègraf electric (1833). Relacionats amb aquesta matèria, van

ser el principis de la teòria elèctrica del potencial publicats l'any 1840. El seu interés per a la física el va orientar també cap a la mecànica, l'acústica, la capil·laritat i sobretot l'òptica, disciplina sobre la que va publicar el tractat d'investigacions diòptriques (1841) que demostra que qualsevol sistema de lents es pot reduir sempre a una sola lent amb les característiques adequades. Aquesta potser va ser la darrera aportació fonamental de Gauss.
Gauss va morir a Göttingen, Hannover (ara part de la Baixa Saxònia, Alemanya) el 1855 i fou enterrat al cementeri d'Albanifriedhof .

2.2 Context Històric

Per a la història occidental, el S XVIII és el darrer dels segles de la Edat Moderna, i el primer de l'Edad Contemporània. En el S. XVIII, la il·lustració domina l'Europa de Gauss. Aquesta manera de pensar, en la que la raó s'imposa a les supersticions i "il·lumina per a regenerar el món", influeix en tots els aspectes de la vida de la societat del S.XVIII. En els diferents aspectes, es pot destacar:



- Religió: entre el cristianisme reformista i l'ateisme.
- Racionalització de l'estat i la societat.
- Reconciliar la burgesia i la noblesa.
- Millores econòmiques, millores agràries i inici de la industrialització.
- Increment important de població
- Pèrdua de poder de les monarquies absolutes. L'any 1793 el rei Lluís XVI de França mor a la guillotina.
- Desenvolupament científic.

En relació amb l'important desenvolupament científic, hi ha diferents fets importants a remarcar:

* Llei de conservació de la materia de Lavosier (1743-1795): La massa dels productes d'una reacció química és igual a la massa dels reactius de la reacció.

* Llei de les proporcions recíproques o Llei de Richter (1762- 1807): Les masses d'elements diferents que es combinen amb una mateixa massa d'un element donat són les masses relatives d'aquells elements quan es combinen entre sí, o bé múltiples o submúltiples d'aquestes masses.

* Llei de Coulomb (1736-1806): La llei diu que la força electrostàtica que hi ha entre dues càrregues elèctriques puntuals és directament proporcional a la magnitud de les càrregues i inversament proporcional al quadrat de la distància que les separa.

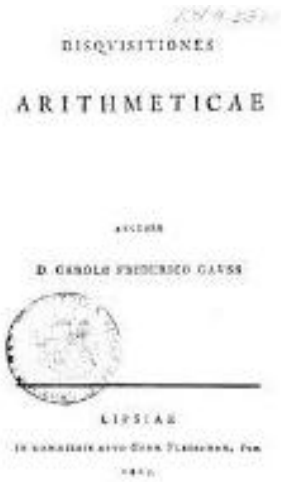
Altres fets importants del S.XVIII:

- Celsius idea l'escala termomètrica que porta el seu nom.
- S'inocula la primera vacuna, contra la verola.
- S'inicia el coneixement de les galaxies.

La matemàtica il·lustrada:

Les matemàtiques d'aquest període, continuen explorant els camps oberts durant el S XVII i basant-se principalment en el sentit comú. Tot i ser un periode productiu, a finals de segle, apareix cert pesimisme que es reflexa en una carta que Lagrange envia al seu amic D'Alambert l'any 1781

2.3 Disquisitiones arithmeticae


DISQVISITIONES

ARITHMETICAE

LIPSIAE

Gauss inicia les seves investigacions sobre teoria de nombres, durant la seva estància al Collegium Carolinum, l'any 1795. El llibre el comença a escriure al llarg de la seva estancia a la Universitat de Göttingen.

L'any 1801 es publica la seva primera obra mestre, les *Disquisitiones arithmeticae*. Aquestes disquisicions cobreixen la Teoria elemental dels nombres com a parts de l'àrea que actualmente coneixem com a Teoria algebraica de nombres. Amb les disquisicions, Gauss converteix la Teoria de nombres en una branca de les matemàtiques tant important com l'anàlisi o la geometria.

Gauss va dedicar el llibre al seu mentor, el Duc de Brunswick:
"Penso que ningú no ignora que és habitual en Tu una tan insigne liberalitat vers tots els que sembla que es dediquen a cultivar les millors disciplines, i que no són excloses del Teu patrocini aquelles ciències que són considerades per la gent més abstruses i més allunyades de la utilitat de la vida comuna, perquè Tu mateix t'adones fins a l'arrel de l'íntim i necessari vincle de totes les ciències entre elles, amb una ment molt sàvia i molt coneixedora de totes les coses que interessen per tal d'augmentar la prosperitat de la societat humana".

En el prefaci del llibre descriu com va enfocar l'estudi: "Les investigacions contingudes en aquest volum, pertanyen a aquella part de les Màtemàtiques que tracta particularment sobre els enters, a vegades les fraccions, però sempre s'exclouen els irracionals".

Les disquisicions están organitzades en 7 seccions:

1. Sobre els nombres congruents en general.
2. Sobre les congruencies de primer grau.
3. Sobre els residus de potències.
4. Sobre les congruencies de segon grau.
5. Sobre les formes i equacions indeterminades de segon grau.
6. Aplicacions vàries de les questions precedents.
7. Sobre les equacions que defineixen seccions de cercles.

Hi ha una vuitena secció que s'hauria d'haver publicat posteriorment, però mai no es va fer. Es va editar després de la seva mort, en les seves obres completes.

3 Aplicacions de l'aritmètica modular i la llei de la reciprocitat quadràtica

Al llarg de la història, l'aritmètica que tracta els residus i les congruències no s'ha anomenat aritmètica modular. Primerament se la coneixia com a "matemàtica superior", títol donat per *Gauss*, i l'objectiu d'aquesta era merament intel·lectual. Però a partir del S.XX se li trobaren aplicacions en camps com la criptografia, la teoria de codificació i la informàtica. A partir de llavors, i sempre parlant en aquests camps d'aplicació, se l'anomena "aritmètica modular". En matemàtiques pures no s'utilitza aquest terme, se l'anomena com a "Teoria algebraica de nombres"que designa un marc més ampli que tracta també, per exemple, les nocions d'enters algebraics i la Teoria de Galois.

Particularment, des que se li trobà una aplicació a aquest àmbit de les matemàtiques el seu desenvolupament no ha parat. Cada cop s'avança més en aquest camp, sobretot en l'àmbit de la criptografia i la informàtica, ja que en la època en que vivim aquestes dues disciplines són molt presents en la nostra vida.

Un exemple d'aplicació és el test de primalitat *Solovay-Strassen*, que utilitza el criteri d'Euler (Teorema 12.). El que fa és calcular diferents $\left(\frac{a}{n}\right)$ a partir de dos mètodes: el criteri d'Euler i una variació de l'algoritme d'Euclides. Si el resultat dels dos difereix, llavors n no és primer, i si és el mateix, llavors n pot ser primer o no. Com que la meitat dels $1, 2..., n-1$ coincidiran (amb n no-primer), el que fa és repetir el procés amb diferents a de forma que s'arriba a un "primer probable".

4 Part Teòrica

4.1 Aritmètica modular

4.1.1 L'anell $\mathbb{Z}/m\mathbb{Z}$

- Dos nombres a i $b \in \mathbb{Z}$ s'anomenen congruents entre si mòdul m si la seva diferència és divisible entre m (és a dir, tenen el mateix residu al dividir-los entre m), o dit d'altra forma : $a - b = km$. Es denota així : $a \equiv b \pmod{m}$
- Tot enter a és congruent a un únic r, amb $0 \leq r < m$, que correspon al residu de dividir a entre m. A més, si $a \equiv b$ i $c \equiv d$, llavors $a + c \equiv b + d$ i $ac \equiv bd$. Per tant el conjunt d'aquests r té estructura d'anell i l'anomenarem $\mathbb{Z}/m\mathbb{Z}$.

4.1.2 Element invers

- Un element $a \in \mathbb{Z}/m\mathbb{Z}$ s'anomena invertible si existeix un b tal que $ab \equiv 1 \pmod{m}$, cosa que només és possible si i només si $\text{mcd}(a, m) = 1$.
- El fet de que a sigui coprimer amb el mòdul es demostra a partir de l'identitat de Bézout (veure Annex2), que diu que si $\text{mcd}(a, m) = d$, llavors existeixen x, y tals que compleixen $ax + ym = d$.
  Aquesta expressió es pot traduir a $ax \equiv d \pmod{m}$ i, per tal de que x sigui l'invers d'a, $\text{mcd}(a, m) = 1$ i es compleix la condició.
- Una forma fàcil de trobar l'element invers d'un nombre és fent servir l'algorisme d'Euclides a l'equació diofàntica $ax + ym = 1$ (veure Annex2), on a és el nombre en qüestió, x és l'element invers d'aquest i m és el mòdul.
- El conjunt d'elements invertibles en $\mathbb{Z}/m\mathbb{Z}$ l'anomenarem per $U(\mathbb{Z}/m\mathbb{Z})$.

Proposició 1. *Si un element té invers, aquest és únic.*

Demostració. Ens disposem a demostrar-ho per reducció a l'absur.Posem per cas que existeixen 2 elements, b i c, inversos d'a. Tindríem que:

$$ab \equiv 1 \pmod{m} \quad ac \equiv 1 \pmod{m}$$

per tant

$$ab \equiv ac \pmod{m}$$

i multiplicant els dos membres per b

$$b \equiv c \pmod{m}$$

I arribem a contradicció. Per tant, existeixen tants elements en $U(\mathbb{Z}/m\mathbb{Z})$ com a entre 0 i m tals que $\text{mcd}(a, m) = 1$ □

Corol.lari: Si m és un primer senar p, llavors $U(\mathbb{Z}/p\mathbb{Z}) = \mathbb{Z}/p\mathbb{Z} - \{0\}$

Exemples: En la taula següent podem veure tots els inversos dels nombres de $\mathbb{Z}/11\mathbb{Z}$ i les congruències en fer el producte. Fixem-nos que al ser 11 un nombre primer, tots els elements tenen invers.

mod(11)	1	2	3	4	5	6	7	8	9	10
1	**1**	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	**1**	3	5	7	9
3	3	6	9	**1**	4	7	10	2	5	8
4	4	8	**1**	5	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	**1**	6
6	6	**1**	7	2	8	3	9	4	10	5
7	7	3	10	6	2	9	5	**1**	8	4
8	8	5	2	10	7	4	**1**	9	6	3
9	9	7	5	3	**1**	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	**1**
Inversos:	1	6	4	3	9	2	8	7	5	10

Observació: fixem-nos que els únics que són els seus propis elements inversos són 1 i $p - 1$, ja que un nombre és el seu propi invers si

$$x^2 \equiv 1 \pmod{p}$$

$$x^2 - 1 \equiv 0 \pmod{p}$$

$$(x + 1)(x - 1) \equiv 0 \pmod{p}$$

$$x = \pm 1$$

Teorema 2 (de Wilson)**.** *Un nombre enter p és primer si, i només si:*

$$(p - 1)! \equiv -1 \pmod{p}$$

Demostració. Utilitzarem els elements invertibles a l'hora de demostrar el teorema.

Posem per cas que p no és primer. Llavors, el producte $(p-1)!$ tindrà tots els factors de p. Per tant,

$$(p-1)! \equiv 0 \pmod{p}$$

Però, si p és primer, tots els elements $2, ..., (p-2)$ tindran invers dins de $2, ..., (p-2)$ i multiplicats donaran 1. Per tant, podrem transformar l'expressió:

$$(p-1)! \equiv (1 \cdot 2 \cdot 3 \cdot ... \cdot (p-2))(p-1) \equiv (1 \cdot 1 \cdot 1...)(p-1) \equiv (p-1) \equiv -1 \pmod{p}$$

□

4.2 La funció φ de Euler

Sigui n un enter. Definim $\varphi(n)$ com la quantitat de nombres naturals més petits que n i primers amb n. Per la proposició anterior, $\varphi(n) = |U(\mathbb{Z}/m\mathbb{Z})|$.

Exemples: $\varphi(1) = 1, \varphi(2) = 1, \varphi(15) = 8$....

Si p és primer:

$\varphi(p) = p - 1$

$\varphi(p^k) = p^k - p^{k-1} = (p-1)p^{k-1} = (1 - \frac{1}{p})p^k$

Demostració. Volem demostrar que $(p^k) = p^k - p^{k-1}$. En el conjunt $\{1, 2, 3, ..., p^k\}$ hi ha exactament p^{k-1} múltiples de p, que serien $\{1p, 2p, 3p, ..., (p^{k-1})p\}$, i aquests són els únics no primers amb p. □

Proposició 3. *La funció d'Euler és multiplicativa, és a dir, $\varphi(nm) = \varphi(n)\varphi(m)$ sempre que $mcd(m, n) = 1$.*

Demostració. Sigui $z \in \mathbb{Z}$. Denotem per $\mathbb{Z}_k$ a $\mathbb{Z}/k\mathbb{Z}$ i $[z]_k$ al valor de z dins de $\mathbb{Z}_k$. A partir d'aquí, anomenem $[z]_{mn}$, $[z]_m$ i $[z]_n$, amb m i n coprimers. Llavors, definim la correspondència:

$$\mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$$

$$[z]_{mn} \to (a, b)$$

On $a = [z]_m$ i $b = [z]_n$. Aquesta correspondència és injectiva, és a dir, a elements diferents de $\mathbb{Z}_{mn}$ corresponen parelles diferents de $\mathbb{Z}_m \times \mathbb{Z}_n$. Per a demostrar-ho, imaginem que de $[z_1]_{mn} \neq [z_2]_{mn}$ obtenim $a_1 = a_2$ i $b_1 = b_2$. Tindríem que:

$$\left.\begin{array}{l} a_1 = z_1 + kn \\ a_2 = z_2 + pn \end{array}\right\} \Rightarrow z_1 - z_2 = \dot{n}$$

Igualment, per a b_1 i b_2 arribem a que $z_1 - z_2 = \dot{m}$. Per tant:

$\left.\begin{array}{l} z_1 - z_2 = \dot{n} \\ z_1 - z_2 = \dot{m} \end{array}\right\}$ i tenint en compte que m i n són coprimers $\Rightarrow z_1 - z_2 = \dot{nm} \Rightarrow [z_1]_{mn} = [z_2]_{mn}$

i arribem a contradicció.

A més, la quantitat d'elements dins de $\mathbb{Z}_{mn}$ i de $\mathbb{Z}_n \times \mathbb{Z}_m$ és la mateixa (mn elements), per tant, la correspondència és també bijectiva.

Seguint aquesta mateixa norma i notació, volem demostrar que, si $U(\mathbb{Z}_{mn})$ és el conjunt d'elements invertibles en $\mathbb{Z}_{mn}$ la correspondència següent:

$$U(\mathbb{Z}_{mn}) \to U(\mathbb{Z}_m) \times U(\mathbb{Z}_n)$$

és també bijectiva.

És a dir, que z és invertible a $\mathbb{Z}_{mn}$ quan a i b ho són a $\mathbb{Z}_m$ i $\mathbb{Z}_n$ i viceversa.

Primer demostrarem que si $z \in U(\mathbb{Z}_{mn})$, llavors $z \in U(\mathbb{Z}_m)$ i $z \in U(\mathbb{Z}_n)$.

Sabem que $\text{mcd}(z, mn) = 1$. Llavors, si

$$d = \text{mcd}(z, n) \Rightarrow d|n \Rightarrow d|mn \text{ i } d|z \Rightarrow d = 1$$

Si $\text{mcd}(z, n) = 1$, llavors $z \in U(\mathbb{Z}_n)$. De la mateixa manera, $z \in U(\mathbb{Z}_m)$.

Ara, demostrarem que si $a \in U(\mathbb{Z}_n)$ i $b \in U(\mathbb{Z}_m)$, existirà un z, amb $[z]_n = a$ i $[z]_m = b$, que complirà $z \in U(\mathbb{Z}_{mn})$.

Sabem que

$$z = a + kn = b + pm$$

i que

$$\begin{array}{c} \text{mcd}(a, n) = 1 \\ \text{mcd}(b, m) = 1 \end{array}$$

Si $d|z, n \Rightarrow d|a = z - np$. És a dir, $d|a, z, n$ i com que $\text{mcd}(a, n) = 1$, $d = 1$. De la mateixa manera, ho fem per b i per m. Llavors:

$$\text{mcd}(z, n) = 1$$
$$\text{mcd}(z, m) = 1$$

Si tenim un $d|z, mn$, llavors o bé $d|m$ o $d|n$, ja que m i n són coprimers. Però, com que $\text{mcd}(z, n) = 1$ i $\text{mcd}(z, m) = 1$, llavors $\text{mcd}(z, mn) = 1$ i $z \in U(\mathbb{Z}_{mn})$. □

Proposició 4. *Per a qualsevol $n < 1$ es compleix que:*

$$\varphi(n) = n \prod_{p_i|n} \left(1 - \frac{1}{p_i}\right)$$

on p_i són tots els primers divisors de n.

Demostració. Partim de $n = p_1^{k_1} \cdot ... \cdot p_r^{k_r}$. Sabent que $\varphi(nm) = \varphi(n)\varphi(m)$ si $\text{mcd}(m, n) = 1$ i el valor de $\varphi(p^k)$, podem dir que:

$$\varphi(n) = (1 - \frac{1}{p_1})p_1^{k_1} \cdot ... \cdot (1 - \frac{1}{p_r})p_r^{k_r}$$

Per definició, $n = p_1^{k_1} \cdot ... \cdot p_r^{k_r}$ per tant queda demostrat. □

Proposició 5. *Si p és un nombre primer i senar, llavors el grup d'elements d'$U(\mathbb{Z}/p^k\mathbb{Z})$ és cíclic d'ordre $p^k - p^{k-1}$. És a dir, existeix un g tal que:*

$$U(\mathbb{Z}/p^k\mathbb{Z}) = \{g^r : r = 1, ..., p^k - p^{k-1}\}.$$

Dit d'altra manera, existeix un g del qual podrem obtenir tots els elements de $U(\mathbb{Z}/p^k\mathbb{Z})$ si l'elevem a potències d'exponent desde 1 fins a $p^k - p^{k-1}$.

Dada útil: en el cas de $k = 1$ (un primer qualsevol) és interessant observar que l'ordre és de $p - 1 = \varphi(p)$.

Exemple: Sigui $p = 3$ i $k = 2$. Llavors agafem el conjunt $U(\mathbb{Z}/9\mathbb{Z})$, els elements del qual són $\{1, 2, 4, 5, 7, 8\}$ i provem què obtenim amb diferents elements.

Agafant el 4 obtenim: $4^1 \equiv 4$, $4^2 \equiv 7$, $4^3 \equiv 1$. És a dir, no obtenim tots els elements del conjunt $U(\mathbb{Z}/\mathbb{Z}_9)$.

Provem ara amb el 2: $2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 8, 2^4 \equiv 7, 2^5 \equiv 5, 2^6 \equiv 1$. Fixem-nos en que l'últim exponent és $6 = 3^2 - 3^{2-1}$, i que hem generat el conjunt d'elements $U(\mathbb{Z}/9\mathbb{Z})$. Llavors, direm que el 2 és un generador d'$U(\mathbb{Z}/9\mathbb{Z})$.

És essencial veure que cal que p sigui senar. Per exemple, $U(\mathbb{Z}/8\mathbb{Z})$ no és cíclic. De fet, té 4 elements pero tots són d'ordre 2 (és a dir, satisfan $g^2 = 1$)

4.2.1 Equacions lineals i sistemes d'equacions

Anomenarem equació lineal a aquella de la forma $ax \equiv b \pmod{m}$.

Proposició 6. *Si mcd$(m, a) = 1$, l'equació tindrà una única solució.*

Demostració. Procedirem a fer la demostració per reducció a l'absurd. Com que mcd(a, m)=1 sabem que a tindrà un element invers. Llavors, una solució a l'equació seria $x_0 = a^{-1}b$ ja que

$$ax_0 \equiv aa^{-1}b \equiv b \pmod{m}$$

Imaginem que existeixen dues solucions, x_0, x_1. Sabriem que

$$ax_1 \equiv b \pmod{m}$$

$$x_1 \equiv a^{-1}b \equiv x_0 \pmod{m}$$

Per tant, $x_0 \equiv x_1$ i arribem a contradicció. □

Proposició 7. *Si mcd$(m, a) = d$, existiran exactament d solucions de l'equació $ax \equiv b \pmod{m}$.*

Demostració. La congruència $ax \equiv b \pmod{m}$ equival a que existeixi algun enter y tal que $ax - ym = b$.
Tenint en compte que mcd$(a, m) = d$, d divideix b. Per tant, podem dir que $a = a'd, b = b'd, m = m'd$, i transformar la primera equació en una reduïda: $a'x \equiv b' \pmod{m'}$.

Aquesta equació reduïda sí que tindra una única solució $t \in \mathbb{Z}/m\mathbb{Z}$, ja que mcd$(a', m') = 1$. Per tant, un element $x_0 \in \mathbb{Z}/m'\mathbb{Z}$ és solució de l'equació no reduïda exactament quan $x_0 \equiv t \pmod{m'}$, és a dir, $x_0 = t + zm'$ per algun enter z.

Per tant, hi ha exactament d solucions, que corresponen a $0 \leq z < d$. □

Teorema 8 (Petit de Fermat)**.** *Sigui p un primer i a un enter, llavors $a^p \equiv a \pmod{p} \forall a$.*

En particular, si mcd$(p, a) = 1$, llavors $a^{p-1} \equiv 1 \pmod{p}$.

Demostració. Seguirem el mètode d'inducció. En el cas $a = 1$ és obvi. Suposem que val per $a = n$. Comprovem que es compleix per $a = n + 1$. Cal que comprovem que

$$(n + 1)^p \equiv n + 1$$

Si desenvolupem $(n+1)^p$ ens dóna que

$$(n+1)^p \equiv n^p + 1 \pmod{p}$$

ja que tots els factors $\binom{p}{k}$ amb $0 < k < p$ seran múltiples de p. I finalment, com que $n^p \equiv n \pmod{m}$ per hipòtesi inductiva,

$$(n+1)^p \equiv n^p + 1 \equiv n + 1 \pmod{p}$$

□

Teorema 9 (d'Euler)**.** *Si mcd$(a, m) = 1$, llavors $a^{\varphi(m)} \equiv 1 \pmod{p}$ per a qualsevol a enter. Per tant, $a^{\varphi(m)-1}$ és l'element invers de a.*

Demostració. Siguin $\{r_1, ..., r_{\varphi(m)}\}$ tots els naturals primers amb m menors que aquest. Ara multipliquem cada r_i per a, i cadascun d'aquest $r_i a$ serà congruent a un únic altre r_j. De forma que tindrem:

$$ar_1 \cdot ... \cdot ar_{\varphi(m)} \equiv r_1 \cdot ... \cdot r_{\varphi(m)} \pmod{m}$$

Llavors:

$$a^{\varphi(m)}(r_1 \cdot ... \cdot r_{\varphi(m)}) \equiv r_1 \cdot ... \cdot r_{\varphi(m)} \pmod{m}$$

I això és només possible si $a^{\varphi(m)} \equiv 1 \pmod{m}$ (es pot simplificar als dos membres ja que $\text{mcd}(a, r_i) = 1$). □

Teorema 10 (Teorema xinès del residu)**.** *Siguin $m_1, ..., m_r$ enters positius coprimers dos a dos. El sistema d'equacions*

$$x \equiv a_1 \pmod{m_1} \quad ;...; \quad x \equiv a_r \pmod{m_r}$$

té solució per a qualssevol $a_1, ..., a_r$. Aquesta solució és única mòdul el producte de tots els $m_1, ..., m_r$.

Demostració. Sigui $M = m_1 \cdot ... \cdot m_r$. Llavors, qualsevol m_j $(1 \leq j \leq r)$ divideix a M i $\text{mcd}(M/m_j, m_j) = 1$. Com que $\text{mcd}(M/m_j, m_j) = 1$, sabem que existiran b_j tals que:

$$\frac{M}{m_j} b_j \equiv 1 \pmod{m_j}$$

A més, per a tot $m_i \neq m_j$ tindrem:

$$\frac{M}{m_j} b_j \equiv 0 \pmod{m_i}$$

A partir d'aquests b_j construirem la suma

$$w = \sum_{i=0}^{r} \frac{M}{m_j} b_j a_j$$

Per a $1 \leq i \leq r$:

$$w = \sum_{j=0}^{r} \frac{M}{m_j} b_j a_j \equiv \frac{M}{m_i} b_i a_i \equiv a_i \pmod{m_i}$$

Per acabar, suposem que existeixen dues solucions x i y diferents, que

$$x \equiv a_i \equiv y \pmod{m_i}$$

Per tant, $x - y$ és divisible per m_i, i com que tots els m_i són coprimers entre si, $x - y$ serà tambe divisible per M, per tant:

$$x \equiv y \pmod{M}$$

i arribem a contradicció. Per tant, w és l'única solució del sistema. □

4.3 Residus Quadràtics

4.3.1 Definició

Sigui p un primer imparell. Un enter a, coprimer amb p, és un residu quadràtic mòdul p si existeix un x tal que:

$$x^2 \equiv a \pmod{p}$$

En el cas contrari, a és un no-residu quadràtic mòdul p.

Exemples: Les dues taules següents mostren els diferents residus quadràtics mòdul 11 i mòdul 7 respectivament.

x	1	2	3	4	5	6	7	8	9	10
x^2	1	4	9	5	3	3	5	9	4	1
residus mod(11)	1,4,9,5,3									

x	1	2	3	4	5	6
x^2	1	4	2	2	4	1
residus mod(6)	1,4,2					

4.3.2 Propietats

Proposició 11. *Exactament la meitat dels enters a, amb $1 \leq a \leq p-1$ seran residus quadràtics mòdul p.*

Demostració. En el conjunt $S = \{1^2, 2^2, ..., \left(\frac{p-1}{2}\right)^2\}$ no existeixen dos nombres congruents entre si, ja que, imaginem el cas de dos nombres enters $1 \leq a < b \leq \frac{p-1}{2}$ tals que $b^2 \equiv a^2$. Això significaria que $(b+a)(b-a) \equiv 0 \pmod{p}$ cosa que és impossible ja que $1 \leq b-a < \frac{p-1}{2}$ i $1 < b+a < p-1$ (cap dels dos pot ser 0 o un múltiple de p).
Ara només cal comprovar que S conté tots els residus quadràtics.

Suposem que a és residu quadràtic mòdul p és a dir, que existeix un z tal que $z^2 \equiv a \pmod{p}$. Però com que $z^2 \equiv (p-z)^2$, podem suposar que $1 \leq z \leq \frac{p-1}{2}$(si cal, canviant z per $p-z$). Per tant, $a \in S$. □

4.3.3 El Símbol de Legendre

El símbol de Legendre ve donat pel següent:

- $\left(\frac{a}{p}\right) = 1$ si $\text{mcd}(a,p) = 1$ i a és un residu quadràtic mòdul p
- $\left(\frac{a}{p}\right) = 0$ si $\text{mcd}(a,p) \neq 1$
- $\left(\frac{a}{p}\right) = -1$ si $\text{mcd}(a,p) = 1$ i a és un no-residu quadràtic mòdul p

A més, si

$$a \equiv b \pmod{p}$$

llavors

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$$

Exemples:

- $\left(\frac{4}{7}\right) = 1$, ja que $4 \equiv 2^2 \pmod{7}$
- $\left(\frac{3}{7}\right) = -1$ ja que no existeix un x enter tal que $x^2 \equiv 3 \pmod{7}$.
- $\left(\frac{14}{7}\right) = 0$ ja que $\text{mcd}(14,7) \neq 1$

Hi ha 3 casos importants que cal saber i que ens permetran, posteriorment, calcular qualsevol símbol de Legendre aplicant la Llei de reciprocitat quadràtica. I són, per a qualsevol p primer:

- $\left(\frac{1}{p}\right) = 1$, que és obvi ja que $1^2 \equiv 1 \pmod{p}$
- $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \begin{cases} 1 \text{ si } p \equiv 1 \pmod{4} \\ -1 \text{ si } p \equiv 3 \pmod{4} \end{cases}$
- $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \begin{cases} 1 \text{ si } p \equiv 1,7 \pmod{8} \\ -1 \text{ si } p \equiv 3,5 \pmod{8} \end{cases}$

Teorema 12 (Criteri d'Euler)**.** *Sigui p un nombre primer imparell i a un enter qualsevol coprimer amb p. Llavors:*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

Demostració. Primer, observem que $(a^{\frac{p-1}{2}})^2 \equiv a^{p-1} \equiv 1 \pmod{p}$ i, per tant, $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$.
Així, només cal demostrar que quan $\left(\frac{a}{p}\right) = 1$ també $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ i viceversa, cosa que implicaria que si $\left(\frac{a}{p}\right) \equiv -1$ llavors $a^{\frac{p-1}{2}} \equiv -1$

Sigui g un generador de $U(\mathbb{Z}/p\mathbb{Z})$ i suposem que a és un residu quadràtic mòdul p, és a dir:

$$a \equiv x_0^2 \equiv (g^r)^2 \equiv g^{2r}$$

per a algun x_0 i algun r. Llavors,

$$a^{\frac{p-1}{2}} \equiv g^{2r\frac{p-1}{2}} \equiv (g^{p-1})^r \equiv 1$$

Suposem ara que $a^{\frac{p-q}{2}} \equiv 1$. També que $a \equiv g^r$, per a algun r. Llavors $g^{r\frac{p-1}{2}} \equiv 1$, i $p-1$ divideix a $\frac{r(p-1)}{2}$ i 2 divideix a r, per tant $a \equiv (g^{\frac{r}{2}})^2$, i a és un residu quadràtic mòdul p. □

Teorema 13. *Sigui p un primer imparell i sigui a i b enters coprimers amb p. Llavors:*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

Demostració. Immediata a partir del criteri d'Euler. □

4.3.4 El Símbol de Jacobi

Per a qualsevol enter a i qualsevol enter positiu imparell n, el símbol de Jacobi es defineix com el producte dels símbols de Legendre dels factors primers de n:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{k_1}\left(\frac{a}{p_2}\right)^{k_2} \cdot \ldots \cdot \left(\frac{a}{p_l}\right)^{k_l}$$

Fixem-nos, doncs, que en el símbol de Jacobi que el resultat sigui 1 no significa estrictament que a sigui un residu quadràtic de n. Posem un exemple:

$$\left(\frac{3}{7}\right) = -1 \qquad \left(\frac{3}{49}\right) = \left(\frac{3}{7}\right)^2 = 1$$

Com podem veure, el símbol de legendre (3|49) dóna 1, mentre que 3 no és un residu quadràtic mòdul 49, ja que no ho és mòdul 7. En canvi, si el resultat és -1, a si que és un no-residu quadràtic mòdul n.

El símbol de Jacobi comparteix moltes propietats amb el símbol de Legendre. Són:

- $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$ llavors $\left(\frac{a^2}{n}\right) = 1$ si mcd(a, n)=1.
- $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$ llavors $\left(\frac{a}{n^2}\right) = 1$ si mcd(a, mn)=1.
- $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$ $\begin{cases} 1 \text{ si } n \equiv 1 \pmod 4 \\ -1 \text{si } p \equiv 3 \pmod 4 \end{cases}$
- $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$ $\begin{cases} 1 \text{ si } n \equiv 1, 7 \pmod 8 \\ -1 \text{ si } p \equiv 3, 5 \pmod 8 \end{cases}$

Gràcies a totes aquestes propietats, podem fer servir els símbols de Jacobi en el càlcul de símbols de Legendre. Ja que, amb "denominador"primer, el símbol de Jacobi és un símbol de Legendre, però podem aplicar propietats directament a numeradors i denominadors no primers.

5 La Llei de la Reciprocitat Quadràtica

5.1 Versions

Cadascun dels diferents matemàtics que es van ocupar d'aquest fenòmen van formular-la de diferents maneres. La més difosa avui en dia és, però, la versió de Legendre, tot i que a vegades val més utilitzar alguna altra versió.

Versió de Legendre: Per a dos primers imparells p i q:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

On el símbol $\left(\frac{p}{q}\right)$ és el símbol de Legendre. En cas de parlar de símbols de Jacobi, p i q només han de ser imparells i coprimers.

Versió d'Euler: Si p i q són primers imparells diferents, llavors $\left(\frac{p}{q}\right) = 1$ si i només si $p \equiv \pm b^2 \pmod{4q}$ per a algun enter imparell b.

Versió de Gauss: Siguin p i q primers imparells. Llavors:

- Si p és de la forma $4n+1$, llavors q és un residu quadràtic mòdul p si i només si p és un residu quadràtic mòdul q.
- Si p és de la forma $4n+3$, llavors q és un residu quadràtic mòdul p si i només si $-p$ és un residu quadràtic mòdul q.

5.2 Demostració

Aquesta llei és de gran importància i té diverses aplicacions en les seves diferents expressions. És per això que després de la primera demostració publicada per *Carl Friedrich Gauss* en el seu llibre *Disquisitiones arithmeticae* se n'han trobades més de dues-centes! Totes utilitzen diferents propietats, algunes més i d'altres menys elementals. La majoria requerien d'un coneixement superior matèmatic a l'hora de comprendre-les, però la que he decidit donar és la que, personalment, considero més fàcil i gràfica a l'hora d'entendre i copsar.

La demostració que us donaré utilitza el *Lema d'Eisenstein* i pretèn explicar de forma molt gràfica la llei.

Teorema 14 (Lema d'Eisenstein)**.** *Siguin p i q dos primers imparells diferents. Llavors:*

$$\left(\frac{q}{p}\right) = (-1)^{\sum_u [qu/p]}$$

on $[x]$ designa la part entera i el sumatori recorre tots els $u \in \{2, 4...p-1\}$ naturals parells entre 1 i p.

Demostració. Donat un u denotem per $r(u)$ el menor residu positiu de qu mòdul p. Per exemple, amb $p = 13$ i $q = 11$, $u = 2, 4, 6, 8, 10, 12$ i els $r(u) = 9, 5, 1, 7, 6, 2$.

Amb aquesta definició, el menor residu positiu de $(-1)^{r(u)}r(u)$ mòdul p serà sempre parell, perquè si $r(u)$ és parell $(-1)^{r(u)}r(u) = r(u)$, que és parell.En canvi, si $r(u)$ és senar, $(-1)^{r(u)}r(u) = -r(u) \equiv p - r(u) \pmod p$ i $p - r(u)$ és parell.

A més tots ells són diferents, perque si $(-1)^{r(u)}r(u) \equiv (-1)^{r(t)}r(t)$, llavors:

$$(-1)^{r(u)}qu \equiv (-1)^{r(t)}qt \pmod p$$

$$(-1)^{r(u)}u \equiv (-1)^{r(t)}t$$

$$u \equiv \pm t$$

I forçosament $u \equiv t$ ja que els dos són parells i p és senar. Com que hi ha exactament $\frac{p-1}{2}$ d'aquests i tots són diferents, els podem reordenar de forma que:

$$(-1)^{r(2)}2q \cdot (-1)^{r(4)}4q \cdot ... \cdot (-1)^{r(\frac{p-1}{2})}\left(\frac{p-1}{2}\right)q \equiv 2 \cdot 4 \cdot ... \cdot \left(\frac{p-1}{2}\right) \pmod p)$$

Multiplicant pels inversos de $2, 4...$ $\left(\frac{p-1}{2}\right)$ successivament als dos membres (cosa que podem fer ja que són tots coprimers amb p) obtenim:

$$q^{\frac{(p-1)}{2}} \equiv (-1)^{r(2)+r(4)+...+r\left(\frac{p-1}{2}\right)} \pmod p$$

D'altra banda,

$$qu = p\left[\frac{qu}{p}\right] + r(u)$$

i com que p és imparell i u parell, sabem que $\left[\frac{qu}{p}\right]$ i $r(u)$ tenen la mateixa paritat. I com que al elevar (-1) a un nombre només importa la paritat, podrem dir que:

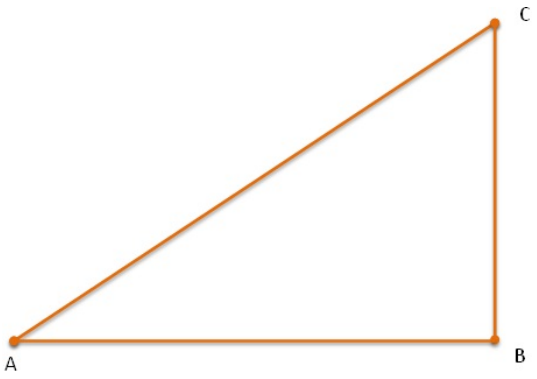
$$q^{\frac{p-1}{2}} \equiv (-1)^{\sum_u [qu/p]}$$

i pel criteri d'Euler, que diu que $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p$ queda demostrat. □

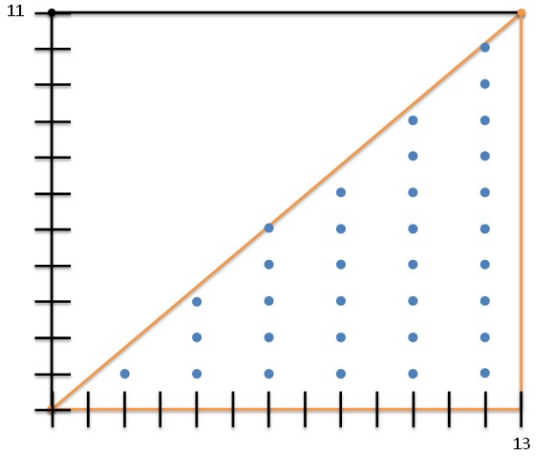
A partir de la versió de Legendre, el que pretenem demostrar és que:

$$(-1)^{\sum_u [qu/p]+\sum_u [pu/q]} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Demostració. Si representem q i p en dos eixos cartesians, ens adonem que la $\sum_u [qu/p]$ compta exactament la quantitat de punts de coordenades enteres amb abscissa parell i ordenada estrictament positiva dins del triangle ABC en el diagrama següent en color taronja, on $AB = p$ i $BC = q$:



Per a veure-ho més clar, posem l'exemple de $p = 13$ i $q = 11$.



Podem comprovar que la quantitat dels punts és la part entera de la fracció $\frac{qu}{p}$. Es pot comprovar fent semblança. Per exemple, en el punt d'abscissa 6, l'"altura"que li correspon es pot trobar fent:

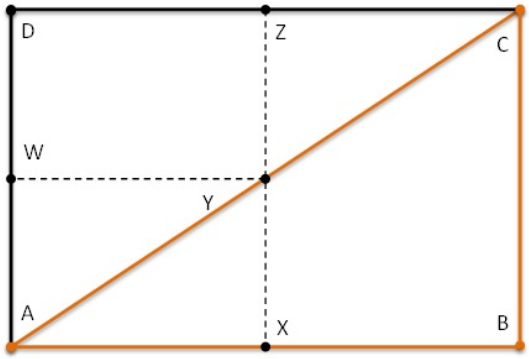
$$\frac{h}{11} = \frac{6}{13}$$

$$h = \frac{6 \cdot 11}{13}$$

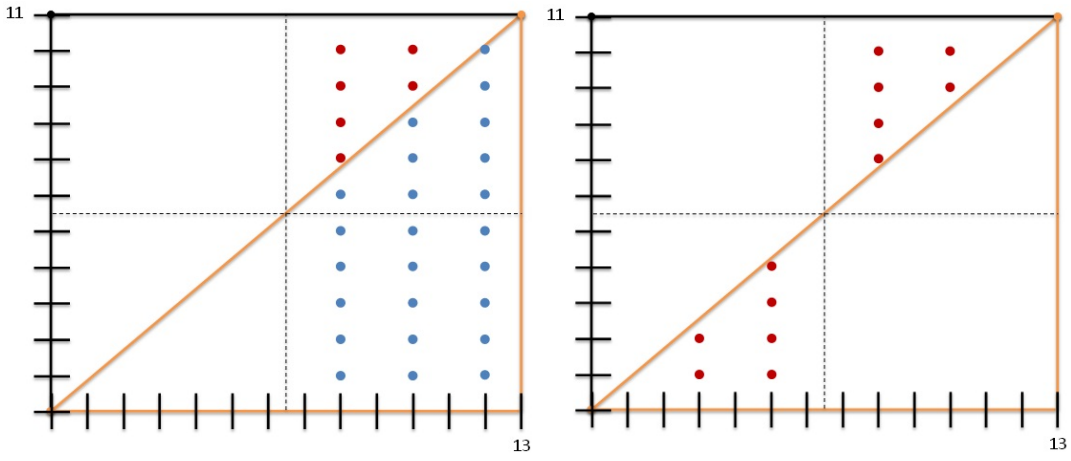
que equivaldria a $\frac{qu}{p}$. Per tant, la quantitat de tots aquests punts és $\sum_u [qu/p]$. Ara cal trobar un mètode eficient per contar aquests punts. Agafarem els punts següents marcats en la figura :

$A = (0,0), B = (p,0), C = (p,q), D = (0,q)$

$W = (0, \frac{q}{2}), X = (\frac{p}{2}, 0), Y = (\frac{p}{2}, \frac{q}{2}), Z = (\frac{p}{2}, q).$



Primer observem que el nombre de punts que formen les columnes de punts senceres és $q-1$ que és sempre parell. Per tant, podem dir que la paritat de la quantitat de punts dins la regió XYCB és la mateixa que la de ZCY (marcats en color vermell i blau en la següent figura), ja que un nombre parell és sempre la suma de dos parells o dos senars.



Fixem-nos ara que el triangle AXY és igual que el YZC i que els punts dins d'YZC corresponen als que trobariem dins del AXY en cordenades d'abscissa imparell. Per tant,

com que a l'hora d'elevar -1 a algun nombre el que compta és la paritat, podem dir que comptar tots els punts dins del triangle ABC amb cordenades d'abscissa parell és el mateix que comptar els que hi ha dins del triangle AXY amb abscissa parell i imparell. Anomenarem α aquesta quantitat. Per tant,

$$\left(\frac{q}{p}\right) = (-1)^{\alpha}$$

Ara, si invertim els eixos i fem el mateix per $\left(\frac{p}{q}\right)$ veiem que la quantitat de punts és la que hi ha dins del triangle AWY, i l'anomenarem β. Per tant,

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\alpha}(-1)^{\beta} = (-1)^{\alpha+\beta},$$

però $\alpha+\beta$ és la quantitat de punts de coordenades enteres estrictament positives dins del rectangle AWYX que és, exactament,

$$\frac{p-1}{2} \cdot \frac{q-1}{2}$$

i queda demostrat. □

6 Càlcul de símbols de Legendre i Jacobi

6.1 Mètodes per realitzar el càlcul

En l'apartat de residus quadràtics hem parlat del símbol de Legendre i com, a partir de saber tres casos concrets els podem calcular tots. El mètode a seguir consisteix en anar reduint el símbol en els seus factors primers (Teorema 13.) i anar invertint els símbols seguint la Llei de la Reciprocitat Quadràtica. Posem un exemple:

$$\left(\frac{98}{331}\right) = \left(\frac{7^2}{331}\right)\left(\frac{2}{331}\right)$$

- $\left(\frac{7}{331}\right) = \left(\frac{331}{7}\right) \cdot (-1)^{\frac{331-1}{2}\frac{7-1}{2}} = \left(\frac{2}{7}\right) \cdot (-1) = (-1)^{\frac{7^2-1}{8}} \cdot (-1) = -1$
- $\left(\frac{2}{331}\right) = (-1)^{\frac{331^2-1}{8}} = -1$
- $\left(\frac{98}{331}\right) = \left(\frac{7}{331}\right)^2 \left(\frac{2}{331}\right) = (-1)^2(-1)$

Aquest mètode pot semblar eficient, però aconseguir trobar els factors primers d'un nombre pot arribar a ser molt difícil. Llavors pensem, com podríem calcular-ho...?

Existeix un símbol el qual no requereix que els dos nombres siguin primers per fer servir la Llei de la Reciprocitat quadràtica, i és el de Jacobi. Així, com que només cal que els dos siguin imparells, el que cal fer és "factoritzar"els dosos que puguem trobar en el "numerador" i aplicar la llei de la Reciprocitat quadràtica. I dividir entre 2 si que és una tasca senzilla. Posem un exemple:

$$\left(\frac{35}{41}\right) = (-1)^{\frac{35-1}{2}\frac{41-1}{2}}\left(\frac{41}{35}\right) = \left(\frac{6}{35}\right) = \left(\frac{2}{35}\right)\left(\frac{3}{35}\right) = (-1)^{\frac{35^2-1}{8}}\left(\frac{3}{35}\right) =$$

$$= (-1)(-1)^{\frac{35-1}{2}\frac{3-1}{2}}\left(\frac{35}{3}\right) = \left(\frac{2}{3}\right) = (-1)^{\frac{3^2-1}{8}} = -1$$

Per tant, el procés consisteix en una sèrie de càlculs que són sistemàtics, programables. Els diferents càlculs que cal fer són:

- Factoritzar els dosos del denominador, i aplicar la fòrmula corresponent.
- Invertir els nombres aplicant la llei de la reciprocitat quadràtica.

- Buscar el mínim residu.

I així successivament. I l'únic que vas és multiplicant cert nombre de -1. I com que, és un símbol de Jacobi amb "denominador"primer, si que el fet que sigui 1 ó -1 ens diu si el primer nombre és unr esidu quadràtic mòdul el segon.

Però hi ha una altra manera de calcular símbols de Jacobi que evita que hi apareguin nombres parells, però llavors n'apareixen de negatius. Consisteix en canviar qualsevol nombre parell sempre per el seu corresponent negatiu. Per exemple: $6 \equiv -29 \pmod{35}$, i en aquest cas després es factoritzaria el -29 en 29 i -1, de forma que la fòrmula que aplicaríem seria la del $\left(\frac{-1}{n}\right)$. El mateix exemple d'abans seria:

$$\left(\frac{35}{41}\right) = (-1)^{\frac{35-1}{2}\frac{41-1}{2}} \left(\frac{41}{35}\right) = \left(\frac{6}{35}\right) = \left(\frac{-29}{35}\right) = \left(\frac{-1}{35}\right)\left(\frac{29}{35}\right) = (-1)^{\frac{35-1}{2}} \left(\frac{29}{35}\right) =$$

$$-\left(\frac{29}{35}\right) = (-1)(-1)^{\frac{35-1}{2}\frac{29-1}{2}} \left(\frac{35}{29}\right) = \left(\frac{6}{29}\right) = \left(\frac{-23}{29}\right) = \left(\frac{-1}{29}\right)\left(\frac{23}{29}\right) = (-1)^{\frac{29-1}{2}} \left(\frac{23}{29}\right) =$$

$$(-1)^{\frac{23-1}{2}\frac{29-1}{2}} \left(\frac{29}{23}\right) = \left(\frac{6}{23}\right) = \left(\frac{-1}{23}\right)\left(\frac{17}{23}\right) = (-1)^{\frac{23-1}{2}} \left(\frac{17}{23}\right) = (-1)^{\frac{17-1}{2}\frac{23-1}{2}} \left(\frac{23}{17}\right) =$$

$$\left(\frac{-1}{17}\right)\left(\frac{11}{17}\right) = (-1)^{\frac{17-1}{2}} \left(\frac{11}{17}\right) = (-1)^{\frac{11-1}{2}\frac{17-1}{2}} \left(\frac{17}{11}\right) = \left(\frac{-1}{11}\right)\left(\frac{5}{11}\right) =$$

$$(-1)^{\frac{11-1}{2}} \left(\frac{5}{11}\right) = (-1)(-1)^{\frac{5-1}{2}\frac{11-1}{2}} \left(\frac{11}{5}\right) = \left(\frac{1}{5}\right) = -1$$

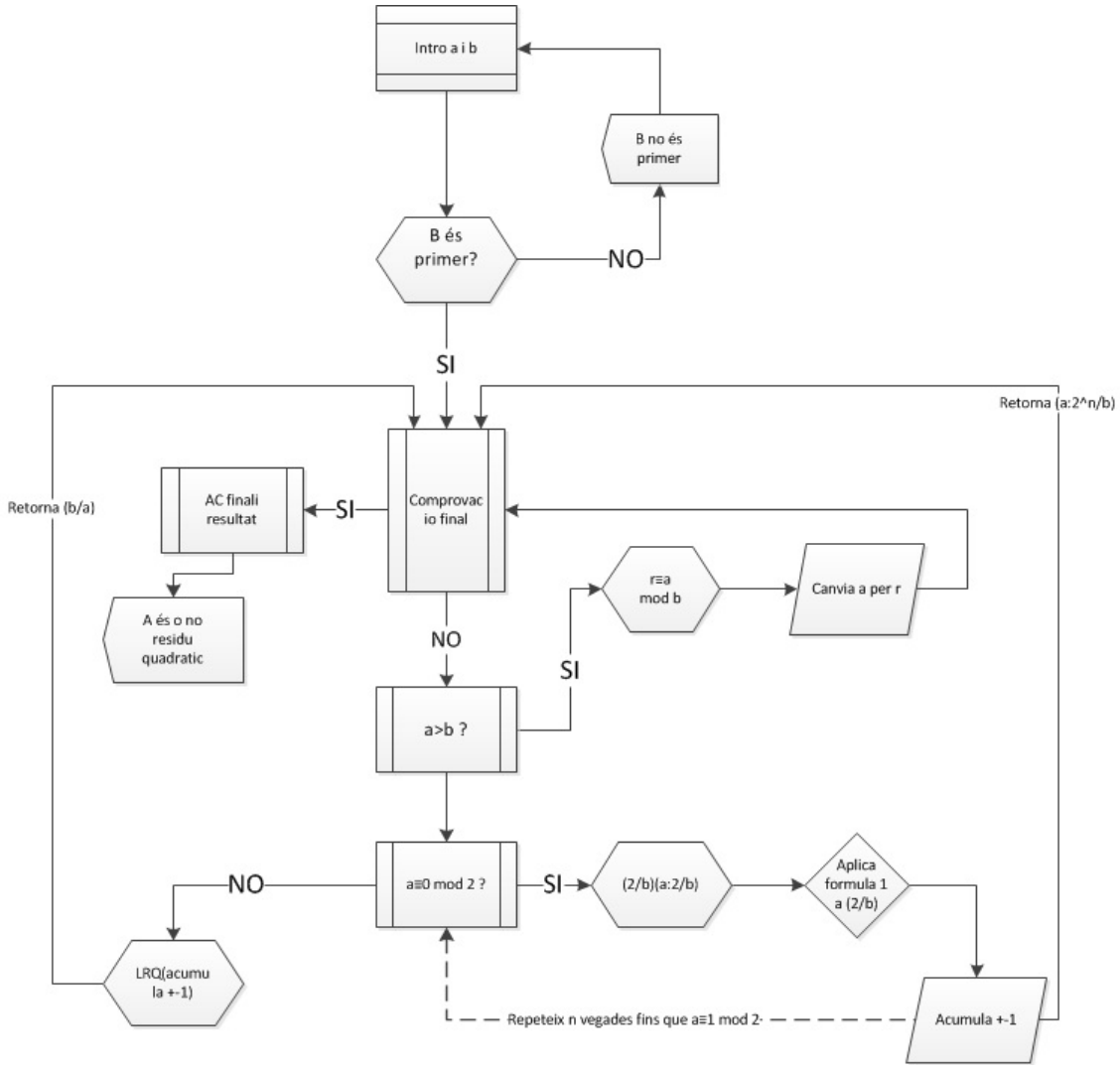
Com podem veure, el procés és molt feixuc quan el primer parell que agafes és molt petit, ja que llavors vas "reduint"molt poc a poc el denominador. Però provem ara amb un altre:

$$\left(\frac{34}{45}\right) = \left(\frac{-11}{45}\right) = \left(\frac{-1}{45}\right)\left(\frac{11}{45}\right) = (-1)^{\frac{45-1}{2}} \left(\frac{11}{45}\right) = (-1)^{\frac{11-1}{2}\frac{45-1}{2}} \left(\frac{45}{11}\right) = \left(\frac{1}{11}\right) = 1$$

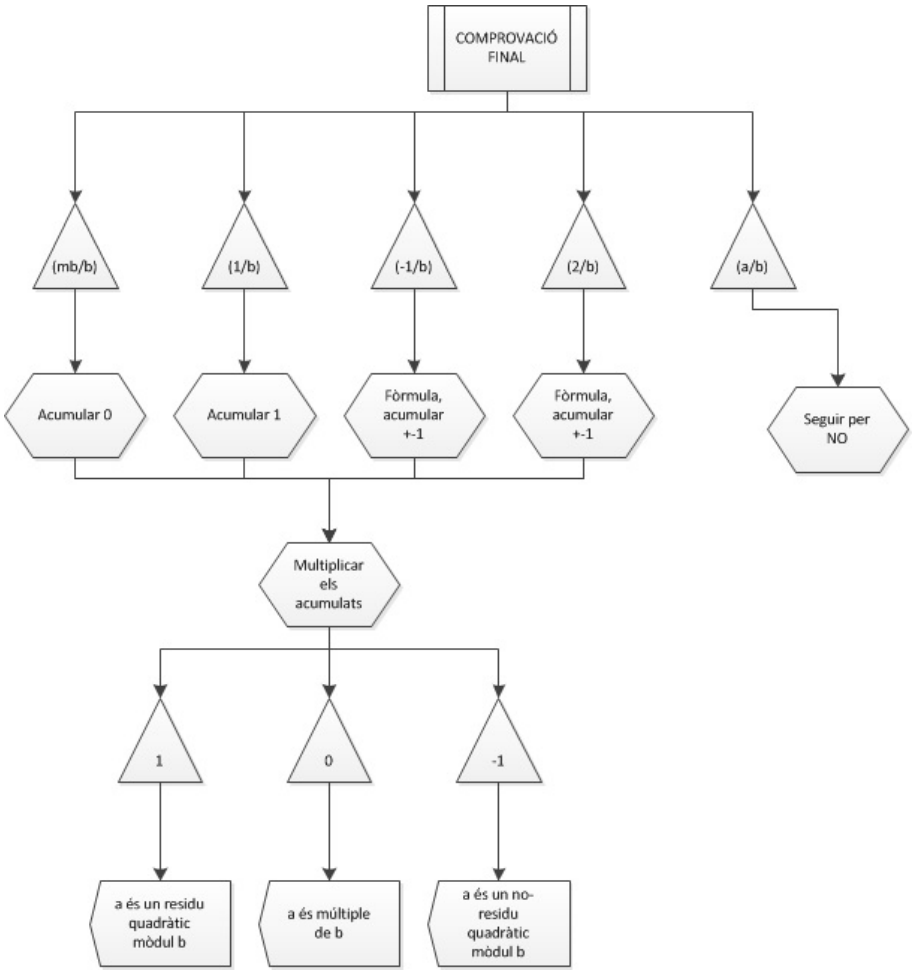
Quan la diferència entre els dos és menor que la meitat del denominador, el canvi del positiu pel negatiu és beneficiós. Per exemple, $14 \equiv -5 \pmod{19}$ i per això val més la pena fer el $(-1|19)$ i $(5|19)$ que no el $(2|19)$ i $(7|19)$ degut a la facilitat de les fòrmules i la major "reducció"del numerador.

6.2 Sistematització del procés

Com hem vist en l'apartat anterior, el càlcul es pot ordenar i organitzar de forma que podem trobar un cicle que ens permeti calcular els símbols informàticament. En l'esquema que he realitzat i que trobem a continuació, podem veure el procés i totes les seves parts i operacions.



L'apartat comprovació final és un procés que comprova si has arribat ja als casos en que ni numerador ni denominador poden ser reduïts, que son els casos de $\left(\frac{1}{n}\right)$, $\left(\frac{-1}{n}\right)$, $\left(\frac{2}{n}\right)$. Un cop s'arriba a aquests casos, cal multiplicar tots els 1 i -1 acumulats i donar el resultat final. La rutina que es mostra en l'esquema a continuació correspon aquesta comprovació:



Ara que ja hem mostrat l'esquema dels processos, en el següent apartat intentarem trobar una possible transcripció a llenguatge informàtic per al procés ja explicat anteriorment.

6.3 Programació i informatització del procés

El que pretenem aconseguir en aquest apartat és pensar i crear un codi informàtic que ens permeti realitzar el càlcul d'una forma eficaç. Per tant, cal aconseguir una transcripció del llenguatge matemàtic i estructurat que hem estat comentant en els apartats anteriors en un d'informàtic.

Per a fer la transcripció de llenguatge matemàtic a informàtic he hagut de contactar amb un programador, ja que el meu coneixement en informàtica no és suficient. El llenguatge usat és el de Visual Basic.NET Studio, creat per Microsoft. És un llenguatge estructurat de molta difusió en l'àmbit informàtic. Per això explicarem pas a pas el procés i què significa cada frase, per tal de comprendre la totalitat de les funcions i comandes.

Per a poder entendre millor el codi sencer (veure Annex3), cal tenir alguns coneixements previs sobre el llenguatge. Per entendre'ns, en la definició de les variables i funcions hem utilitzat la nomenclatura metodològica dels programadors de Microsoft Dynamics NAV, on a les variables se les anomena en funció del seu caràcter. Per exemple, una variable general s'escriuria sempre amb g , com *g_intA* on "int"vol dir *integer* (enter). De la mateixa forma, una variable local (que pertany només a la funció en concret, no al procés general) s'escriuria am loc davant, com *intALoc.* i, una variable que fa de paràmatre, se l'anomena per prm, com per exemple *intprmA*.

També cal que sapiguem diferenciar entre les funcions "booleanes"(el resultat de les quals només pot ser o veritable o fals) i les funcions corrents, el resultat de les quals depèn del que es faci.

A l'inici de qualsevol procés cal declarar primer totes les variables que utilitzaràs. En l'inici del codi trobem les variables de la següent forma:

```
private double g_intA = 0;
private double g_intB = 0;
private int g_intResultado = 0;
private string g_txtResultado1 = "";
private string g_txtResultado2 = "";
```

En la figura veiem com les variables `g_intA` i `g_intB` són declarades incialment com a 0. Aquestes dues variables són les dues variables a introduir, que, com veurem en el programa, les dues variables a l'inici són 0. El resultat de la operació, `g_intresultado` la declara inicialment també com a 0, i els dos textos que es mostren en la finestra com a buit, que es senyala per ""(variables `g_txtResultado1` i `g_txtResultado2`).

*Nota: en la declaració, la majoria de variables les trobem anomenades amb el prefix

`double`, que el que fa és declarar les variables com a decimals. Tot i que durant el nostre procés només treballem amb enters, determinar les variables com a decimals admet un rang més ampli de variables. També s'utilitza el prefixt `string` per determinar que una variable és de text.

Després de declarar les primeres variables, la funció primera i principal és la funció `Calcular`. En aquesta funció s'hi troben tots els processos que es farien al calcular el símbol. Les variables es tornen a declarar localment en aquesta funció, tal i com es mostra a continuació:

```
public void Calcular()
{
    g_intResultado = 1;
    g_txtResultado1 = "";
    g_txtResultado2 = "";
    TestParametres();

    double intALoc = g_intA;
    double intBLoc = g_intB;
```

Com podem veure, ara comença donant a la variable `g_intresultado` un 1, ja que, com que al llarg del procés "acumulem"$1, -1$ i 0, perque al final dongui $1, -1$ o 0 es multiplica la variable per tots els acumulats i dóna el resultat. El text segueix estant buit i a les dos variables de caràcter general les anomena ara per variables locals, anomenades `intALoc` i `intBLoc`. A l'inici del procés, cal comprovar que el segon nombre introduït és senar i primer, per això cal fer una comprovació prèvia als dos paràmetres. La funció que comprova els paràmetres és la funció `TestParàmetres`, que explicarem més endavant.

A partir d'aquí comença la funció de càlcul en si, on trobem dues parts: la primera, que és la part de càlcul amb els diferents passos i reduccions, i la segona, en què es dona els resultats numèrics i textuals del procés.

El codi de la part de càlcul és el següent:

```
bool blnFinal = TestComprobacioFinal(intALoc, intBLoc);
if (!blnFinal)
{
    do
    {
        bool blnTest = false;
        if (intALoc >= intBLoc)
        {
            intALoc = intALoc % intBLoc;
            blnTest = true;
        }

        //Treure factors 2 del numerador.
        if (!blnTest)
        {
            blnTest = QuitarFactores2(ref intALoc, intBLoc);
        }

        //Llei reciprocidad quadràtica.
        if (!blnTest)
        {
            PermutarParametros(ref intALoc, ref intBLoc);
            blnTest = true;
        }

        blnFinal = TestComprobacioFinal(intALoc, intBLoc);

    } while (!blnFinal);
```

És important veure que totes les funcions internes que hi ha dins de la `Calcular` agafen com a referència de variable les `intALoc` i `intBLoc`.

En aquesta funció trobem a l'inici la comprovació que s'ha arribat al final amb les dues variables locals, que seria el text que diu

`bool blnFinal = TestComprovacióFinal(intALoc, IntBLoc)`. Just a continuació diu que, mentre el resultat de la comprovació sigui fals (no s'hagi arribat al final) faci certs processos amb certes ordres. Aquesta part de la funció correspon a l'escrit `if(!blnFinal) do` i `while (!blnFinal)`. Els que farà és un bucle d'operacions , que és `bool blnTest=false` i que només s'inicia un cop comprovat que no ha arribat al final, i, a més, només comença un cop la comprovació final és falsa.

La seqüència d'operacions que cal fer a les dues variables correspon als passos dels que hem parlat amb el càlcul a mà i, un cop un és cert un dels passos, torna "cert"a la funció blnTest, i per tant, torna a comprovar si està al final i torna a fer el procés sempre que no hagi arribat al final (`(!blnFinal)`). Les operacions que busca i comprova, són, per ordre:

- Si $a \geq b$, es canvia a pel corresponent $r \equiv a \pmod{b}$ més petit, que és la comanda $a\%b$. Si això no és cert, segueix i comprova el següent.
- Si la operació anterior és falsa (`if (!blnTest)`) busca si el nombre és parell, amb al funció `QuitarFactores2` amb les variables `intALoc` i `intBLoc`. La funció `QuitarFactores2` la definirem més endavant.

- Si segueix sent falsa l'anterior, ara permuta els paràmetres fent servir la llei de la reciprocitat quadràtica.

Com podem veure, el procés queda tancat.

Després d'anar acumulant $1, -1$ i 0, arribem a un punt en que ens trobem un símbol del tipus $(1|n)$, $(-1|n)$ o $(2|n)$. Llavors, la comprovació final ens donaria cert, i per tant hem de donar el resultat en forma numèrica i text. Això segueix de la part que hem comentat anteriorment, i el codi que li correspon és el següent:

```
g_txtResultado1 = g_intResultado.ToString();
switch (g_intResultado)
{
    case 1:
        g_txtResultado2 = "<" + g_intA.ToString() + "> és residu quadràtic módul <" + g_intB.ToString() + ">";
        break;
    case -1:
        g_txtResultado2 = "<" + g_intA.ToString() + "> és un NO residu quadràtic módul <" + g_intB.ToString() + ">";
        break;
    case 0:
        g_txtResultado2 = "<" + g_intA.ToString() + "> és múltiple de <" + g_intB.ToString() + ">";
        break;
}
```

El que primer trobem és que ens transforma la variable de text 1 (`g_txtResultado1`) en una imatge textual de la variable númerica del resultat (`g_intResultado`). És a dir, transforma un nombre en text. A partir d'aquí, ens obre un conjunt de casos en els quals caldrà prendre certes decisions en funció de la variable resultat. Aquesta part correspon al text on diu `switch (g_intResultado)`. Els diferents casos seran:

- Cas `g_intResultado`$= 1$: la segona variable de text (`g_txtResultado1`) dirà: "La variable introduïda a l'inici és un residu quadràtic mòdul la segona".
- Cas `g_intResultado`$= -1$: la segona variable de text (`g_txtResultado1`) dirà: "La variable introduïda a l'inici és un NO residu quadràtic mòdul la segona".
- Cas `g_intResultado`$= 0$: la segona variable de text (`g_txtResultado1`) dirà: "La variable introduïda a l'inici és un múltiple de la segona".

Fixem-nos que en els tres casos escriu el text entre cometes, en cas contrari no s'entendria com a text. Però hi ha una part que no està entre cometes, que correspon a l'escrit de `g_intA.ToString()` i `g_intB.ToString()`. Aquestes dues ja seran text pel fet de dur la funció ToString, que significa "canvia a text".

Un cop hem parlat de la funció principal, anotarem les función secundàries que trobem en el procés general de càlcul i d'altres que són prèvies i que comproven els paràmatres.

Començarem per la primera que ens trobem, la funció `TestComprovacioFinal`, el codi de la qual és:

```
private bool TestComprobacioFinal(double intprmA, double intprmB)
{
    bool blnFinal = true;

    int aux = 0;
    try
    {
        aux = Convert.ToInt32(intprmA);
    }
    catch(Exception ex)
    {
        return false;
    }

    switch (aux)
    {
        case 0:
            AcumulaSigno(0);
            break;
        case 1:
            AcumulaSigno(1);
            break;
        case 2:
            AcumulaSigno(ResultadoFormula2(intprmB));
            break;
        case -1:
            AcumulaSigno(ResultadoFormula_1(intprmB));
            break;
        default:
            blnFinal = false;
            break;
    }
    return blnFinal;
}
```

En aquesta funció, el que volem verificar és si hem arribat ja a un símbol irreductible, com seria el cas de $(1|n)$, $(-1|n)$, $(2|n)$ o $(0|n)$.

Es tracta d'una funció booleana, amb solució inicial "cert". Llavors, anomena una variable auxiliar `aux` que la determina com a 0 inicialment. A partir d'aquí, intenta transformar la variable auxiliar en la variable d'entrada `intprmA` però com a enter, no com a decimal (la variable estava declarada a l'inici de la funció com a `double`, decimal). Si hi ha un error (`catch(Exception ex)`) a la transformació (és a dir, si la variable d'entrada no és entera), cal que surti resultat "fals". En cas contrari, obre una funció de casos com abans. La transformació a variable entera és necessària precisament per aquest pas, ja que amb variables decimals no es pot realitzar la funció `switch`.

Hi ha 5 casos diferents de la variable `intprmA`, que són els següents:

- Si la variable és 0, s'acumula un 0 i es trenca el procés (es queda la variable resultat com estava: "cert")
- Si la variable és 1, s'acumula un 1 i es trenca el procés, com en l'anterior.

- Si la variable és 2, s'acumula un 1 o un -1 aplicant la funció `ResultadoFormula2`, que correspon a la fòrmula de $(2|n)$.
- Si la variable és -1, s'acumula un 1 o un -1 aplicant la funció `ResultadoFormula_1`, que correspon a la fòrmula de $(-1|n)$. Llavors, es trenca el procés.
- I si la variable és qualsevol altre (`default`), es canvia el resultat per "falsï es trenca el procés.

Veiem com, només si es tracta d'un símbol final, la funció de comprovació dóna "cert". Per això, en la funció calcular tots els processos per a calcular i reduir els símbols només es duen a terme mentre que el resultat de la comprovació sigui "fals".

La següent amb la que ens trobem és la funció `QuitarFactores2` que a la funció calcula veiem que agafa de referència `intALoc` i `intBLoc`. A dins del procés, les canvia i anomena per `intprmAEntrada` i `intprmBEntrada`. Veiem-ne el codi:

```
private bool QuitarFactores2(ref double intprmAEntrada, double intprmBEntrada)
{
    bool blnSalida = false;

    while (intprmAEntrada % 2 == 0)
    {
        intprmAEntrada = intprmAEntrada / 2;
        blnSalida = true;
        AcumulaSigno(ResultadoFormula2(intprmBEntrada));
    }

    return blnSalida;
}
```

Com podem veure, torna a ser una funció booleana, de veritable o fals. Comença amb la variable fent-la falsa, i llavors el procés dura mentre el nombre sigui parell, com diu a `while(intprmAEntrada\%2==0`. Mentre sigui parell, canvia la variable per la seva meitat: `intprmAEntrada = intprmAEntrada / 2;` i torna "cert". I, després d'això, acumula un signe amb la funció `AcumulaSigno` amb el resultat de la fòrmula de $(2|p)$.

La funció que trobem a continuació i que feia referència dins de la funció calcular és la funció `PermutarParametros`. En aquesta funció s'aplica la Llei de la Reciprocitat Quadràtica. El codi que li correspon és el següent:

```
private void PermutarParametros(ref double intprmAEntrada, ref double intprmBEntrada)
{
    double intprmAaux = intprmAEntrada;
    double intprmBaux = intprmBEntrada;

    AcumulaSigno(LleiReciporcitatQuadràtica(intprmAEntrada, intprmBEntrada));
    intprmAEntrada = intprmBaux;
    intprmBEntrada = intprmAaux;
}

private int LleiReciporcitatQuadràtica(double intprmA, double intprmB)
{
    double decNumerador = ((intprmA - 1) / 2) * ((intprmB - 1) / 2);
    if ((decNumerador % 2) == 0)
        return 1;
    else
        return -1;
}
```

Com a les anteriors, té de referència les primeres variables, les `intALoc` i `intBLoc`, però les reanomena com a `intprmAEntrada` i `intprmBEntrada`. En la primera part, senzillament anomena dues variables auxiliars, que seran igual a les variables d'entrada. És a dir, `intprmAaux=intprmAEntrada` i viceversa.

A partir de llavors, acumula un signe amb la funció `AcumulaSigno` a partir del resultat de la funció `LleiReciprocitatQuadràtica`. Un cop fet això, intercanvia els valors, tal com faríem amb la Llei (`intprmAEntrada=intprmBaux` i `intprmBEntrada=intprmAaux`).

Aprofitarem la mateixa imatge per parlar de la funció `LleiReciprocitatQuadràtica`. L'objectiu d'aquesta funció és donar-nos o bé un 1 o bé un -1, ja que el resultat d'aquesta "s'acumularà"amb la funció `AcumulSigno`.

Senzillament, el que fa és operar les variables seguint la Llei de Reciprocitat Quadràtica, anomenant el resultat del producte `decNumerador`. Llavors, si (`if`) `decNumerador` és parell, és a dir, si és congruent amb 0 mòdul 2, el resultat és 1. Recordem que, en la Llei de Reciprocitat Quadràtica, trobem un -1 amb un exponent d'un producte de dues fraccions. Per tant, si el resultat del producte és parell, llavors el resultat és 1. En canvi, si no és parell (`else`), el resultat és -1.

La funció de la que parlarem a continuació és una funció clau, ja que és la que ens dóna el resultat final. Aquesta funció és la funció `AcumulaSigno`. El codi és el següent:

```
private void AcumulaSigno(int intprmAcumular)
{
    if ((intprmAcumular != 1) && (intprmAcumular != -1) && (intprmAcumular != 0))
        throw new Exception("Control. Només poden acumularse 0,1 ó -1.");
    g_intResultado = g_intResultado * intprmAcumular;
}
```

La variable en aquesta funció ve sempre d'alguna altra funció, i per tant sempre arriba en forma d'1,0 ó -1. Llavors, la reanomena per `intprmAcumular`.
A partir d'aquí comprova que tot el que li arribi de variable siguin 1,-1 i 0, ja que en cas contrari el resultat del símbol no seria 1,-1 ó 0.
Aquesta part correspon a
`if ((intprmAcumular != 1) && (intprmAcumular != -1) && (intprmAcumular != 0))`

que, literalment vol dir "si la variables no és 1, no és -1 i no és 0 mostra un error dient que només es poden acumular 1,-1 i 0". Aquest procés és un suport, un procés que es pot estalviar però que assegura que no es donguin irregularitats.
Llavors, a continuació multiplica la variable del resultat, `g_intResultado`, pel nombre que acumula, que és `intprmAcumular`. Per tant, al final quan es dóna el resultat, ha canviat en funció dels "signes"que ha acumulat.

Dins del procés d'acumular signes, hi ha dues fòrmules, una de les quals no s'utilitza degut al procés que hem escollit per calcular. Una és la fòrmula per a $(2|n)$ i l'altre per a $(-1|n)$. Tot i això, parlarem de les dues perquè són importants.

La funció que utilitza la fòrmula de $(-1|n)$ l'anomenarem `ResultadoFormula_1`, el codi de la qual és el següent:

```
private int ResultadoFormula_1(double intprmB)
{
    double decNumerador = (intprmB - 1) / 2;
    if ((decNumerador % 2) == 0)
        return 1;
    else
        return -1;
}
```

La variable dins de la funció l'anomena per `intrprmB` i n'anomena una altra, `decNumerador` com a resultat de la multiplicació de l'exponent de (-1) en la fòrmula de $(-1|n)$, que és $(-1)^{\frac{n-1}{2}}$, que es veu escrit en `(intprmB - 1) / 2;`. Llavors, en funció de si és parell la `decNumerador` dóna com a resultat 1 o -1, com podem veure escrit en
`if ((decNumerador % 2) == 0)return 1; else return -1;`.

Tot i això, com hem vist en el primer mètode de càlcul de símbols, aquest pas no es fa servir.

Si ara ens fixem en la funció que calcula els símbols del tipus $(2|n)$ amb la seva corresponent fòrmula, podem veure que no és gaire diferent. El codi és el següent:

```
private int ResultadoFormula2(double intprmB)
{
    double decNumerador = ((intprmB * intprmB) - 1) / 8;
    if ((decNumerador % 2) == 0)
        return 1;
    else
        return -1;
}
```

Com podem veure, és exactament igual que la de $(-1|n)$ només que la fòrmula canvia, ja que la de $(2|n)$ és $(-1)^{\frac{n^2-1}{8}}$.

I, per acabar de parlar del procés, hi ha una funció el motiu de la qual és corroborar que el que tu introdueixes és un símbol de Legendre , i s'anomena `TestParametres`. El codi és el següent:

```
private void TestParametres()
{
    if (g_intA <= 0 || g_intB <= 0)
        throw new Exception("Han de donar-se paràmetres diferents de zero i positius.");
    //if (intA == intB)
    //    throw new Exception("El paràmetres no poden ser iguals.");
    if (EsPar(g_intB))
        throw new Exception("Paràmetre 2 no pot ser parell.");
    if (!EsPrimer(g_intB))
        throw new Exception("Paràmetre 2 ha de ser primer.");
}
```

És una funció de comprovació de casos, com podem veure pels `if`. Agafa com a variables els primers paramàtres que introduïm, `g_intA` i `g_intB`. Passa per 4 condicions, que són:

- Si la primera o la segona variables són ≤ 0, dóna un error, dient que s'han de donar paràmetres positius i diferents de zero.
- Si els dos paràmetres són iguals, llavors dóna un error, dient que és diferent. Aquesta possibilitat està cancelada amb doble barra (//) ja que, obviament, si els dos nombres són iguals, el resultat del símbol és 0.
- Si la comprovació de la funció `EsPar` amb la segona variable és certa (és a dir, si el nombre és parell), dóna un error, dient que la 2na variable ha de ser imparell.
- Si la comprovació de `EsPrimer` és falsa, és a dir, si no és primer, dóna un nou error, dient que el 2n paràmetre ha de ser primer.

Dins de la comprovació hem vist dues funcions que ens disposem a explicar ara. La primera és la funció `EsPar`, el codi de la qual és:

```
private bool EsPar(double intprmTestear)
{
    return (intprmTestear % 2 == 0);
}
```

És una funcio senzilla on l'únic que fa és comprovar si la la variables és parell, és a dir, si `intprmTestear\%2 == 0`. Al ser una funció booleana, com posa en `bool`, només retorna veritat o fals.

La 2a funció que veiem en el `TestParametres` és la funció `EsPrimer`. Aquesta funció és, senzillament, el que s'anomena per *test de primalitat*. Veiem com funciona aquest, tot llegint el seu codi:

```
private bool EsPrimer(double intprmTestear)
{
    if (intprmTestear == 3)
        return true;

    bool blnSalida = true;
    double max = Math.Sqrt(intprmTestear);
    if (intprmTestear > 3)
    {
        double intAux = 3;
        do
        {
            blnSalida = (intprmTestear % intAux) != 0;
            intAux = intAux + 2;
        } while ((blnSalida != false) && (intAux <= max));
    }
    //Nota: para el caso 1 y 2 devuelve verdadero y no puede ser negativo.
    return blnSalida;
}
```

És tambe una funció booleana, l'ojectiu de la qual és dir-te si el nombre introduït en forma de variable és o no nombre parell. Comença donant una condició: si el nombre és 3, llavors és primer. Correspon a la part on diu `if (intprmTestear == 3)  return true;`. Llavors obre una altre funció booleana, que comença amb el resultat "veritable". El que fa és comprovar si el nombre és divisible entre els nombres a partir de 3 i tots els següents sumant 2 (així t'evites comprovar els parells). Ho prova així fins arribar a comprovar l'arrel quadrada del nombre, ja que és el nombre més gran que podem trobar que forma part dels factors primers que composen la variable si ja hem descartat els anteriors que s'haurien de multiplicar amb els més grans que l'arrel.

La part en que dictamina que dividirà per nombres del tipus $3+2k \leq \sqrt{n}$ és la següent:

```
if (intprmTestear > 3)
{
    double intAux = 3;
    do
    {
        blnSalida = (intprmTestear % intAux) != 0;
        intAux = intAux + 2;
    } while ((blnSalida != false) && (intAux <= max));
}
```

La part escrita `blnSalida=(intprmTestear \% intAux) != 0`, on != vol dir $\neq$, ens diu que el test és cert sempre que la variable no sigui divisible entre la variable auxiliar, és a dir, els nombres del tipus $3k+2$. Per tant, la variable "cert/fals"de la funció booleana és certa sempre i quan la variable d'entrada `intprmTestear` no sigui divisible entre la variable `intAux` que, un cop no ho és , se li suma 2, com podem veure a `intAux = intAux+2`. Aquest procés s'ha de repetir mentre (`while`) la variable cert/fals `blnSalida` no sigui falsa (`(blnSalida != false)`) i la variable "divisora" `intAux` sigui més petita o igual a l'arrel quadrada de la variable: `intprmTestear` (`(intAux <= max)`).

7 Conclusions i valoració

7.1 Conclusions

Com a conclusions del treball, podem dir que l'aritmètica modular és una branca de les matemàtiques que ha sorgit molt tard a diferència d'altres branques com al geometria o l'àlgebra, però que el seu desenvolupament ha estat igual de ràpid o major que el d'aquestes. És, llavors, una de les parts de les matemàtiques més contemporànies i alhora de les més usades actualment.

També que és més fàcil en general calcular símbols de Jacobi i Legendre a partir d'un mètode sistemàtic i organitzat que utilitzi la simplificació de símbols del tipus $\left(\frac{2}{n}\right)$ que no el mètode de simplificar $\left(\frac{-1}{n}\right)$, ja que aquest últim és més o menys llarg en funció dels dos nombres inicials.

Finalment, puc dir que el llenguatge LaTeX et permet escriure textos matemàtics més fàcilment que altres editors de text com poden ser el Microsoft Office Word o l'Open Office, ja que treballa amb un sistema d'escriptura lineal i no d'inserció de fòrmules i gràfics.

7.2 Valoració

A l'inici d'aquest treball em vaig plantejar molts dubtes a l'hora de si m'agradaria el tema que havia escollit. Al principi em pensava que sobre el que es basaria el meu treball era sobre la Llei de la Reciprocitat Quadràtica i les seves demostracions. Però, al llarg del procés d'elaboració del treball vaig veure que el que més m'agradava i més interessant trobava era el càlcul de Símbols de Legendre, junt amb la part d'infomàtica.

Malgrat això, he après aritmètica modular, he estat capaç d'entendre i explicar d'una manera més o menys entenedora la demostració de la llei i he estructurat i esquematitzat un procés de càlcul de símbols de Legendre i Jacobi. Per tant, podem dir que he complert tots els objectius que em proposava a l'inici del treball i que la valoració general és satisfactòria.

A més, he après a escriure en codi LaTeX i he pogut escriure tot l'apartat de base matemàtica amb el mateix format majoritàriament utilitzat per la comunitat matemàtica. Considero que aquests coneixements em seran beneficiosos en el meu futur com a estudiant i sé que ja tindré una part de la feina feta a l'hora d'aprendre a escriure textos matemàtics més complexos.

8 Bibliografia

Nota: Per a citar les pàgines web consultades, he fet servir les pautes elaborades pel TERMCAT fonamentades en la norma ISO 690 : 1987 i la descripció bibliogràfica internacional normalitzada (ISBD), excepte en aquells casos en que la mateixa pàgina inclou la opció de citar que es fa servir la que proporcionen i en l'idioma en que està la cita. Les cites de material audiovisual es referencien al canal que les emet donat que son d'autoria compartida.

AUTOR. Títol [En línia/imprès]. Edició o versió. Lloc de publicació: editorial o distribuïdora, any de publicació. adreça web [Consulta:]

CARL FRIEDRICH GAUSS.Disquisicions Aritmètiques.[Imprès].Barcelona:Societat Catalana de Matemàtiques,1996.

PAULO TIRAO. La Ley de Reciprocidad Quadràtica. [En línia]. Vaquerías: Agost de 2004. http://www.famaf.unc.edu.ar/series/pdf/pdfCMat/CMat31-3.pdf. [Consulta:7 de setembre]

REAL ACADEMIA DE LA LENGUA ESPAÑOLA. Diccionario de la lengua española [En línia]. 22a ed. Madrid. Real Academia de la Lengua Española, 2003.
http://buscon.rae.es/draeI [Consulta: 10 d'agost de 2011]

ANTONIO PÉREZ SANZ. Carl Friedrich Gauss (1777-1855) [En línia]. Madrid: IES Salvador Dalí.
http://platea.pntic.mec.es/aperez4/html/sigloxix/Carl%20Friedrich%20Gauss.htm [Consulta: 15 de juliol de 2011]

ERIC TEMPLE BELL. Los grandes Matematicos. [En línia]. Argentina: Losada, 2010.
http://www.librosmaravillosos.com/grandesmatematicos/capitulo14.html [Consulta: 15 de juliol de 2011]

FRANCISCO JAVIER CILLERUELO MATEO, ANTONIO CORDOBA, La Teoría de los Números Adaptació curs UAM Llicenciatura Matemàtiques 2011 2012. [En línia].
http://www.uam.es/personal_pdi/ciencias/cillerue/Curso/capitulo%204.pdf [Consulta 30 d'agost de 2011]

BIOGRAFIAS Y VIDAS. Biografias y vides: Karl Friedrich Gauss. [En línia]. Barcelona: Biografias y vides.
http://www.biografiasyvidas.com/biografia/g/gauss.htm. [Consulta 18 de juliol de 2011]

COLABORADORES DE WIKIPEDIA. Carl Friedrich Gauss [en línea]. Wikipedia, La enciclopedia libre, 2011 [fecha de consulta: 17 de septiembre del 2011]. Disponible en http://es.wikipedia.org/w/index.php?title=Carl_Friedrich_Gauss&oldid=49845054. [Consulta:23 de novembre]

TELEVISION ESPANYOLA.Universo matematico. Gauss de lo real a lo imaginario. [En línia] .Espanya :Televisión española
http://www.youtube.com/watch?v=dqevwjJrywE [Consulta: 15 de juliol de 2011]

MANUEL PULIDO BOSCH. FRANCISCO ROMERO HINOJOSA.El siglo XVIII la física y la química en su contexto histórico [En línia]
http://thales.cica.es/rd/Recursos/rd99/ed99-0314-01/asp_eco.htm [Consulta: 20 de desembre de 2011]

BIOGRAFICA.INFO Biografía de Gauss, Carl Friedrich [En línia] València.
http://www.biografica.info/biografia-de-gauss-karl-friedrich-983 [Consulta: 20 de desembre de 2011]

BIOGRAFICA.INFO Biografía de Gauss, Carl Friedrich [En línia] València.
http://www.biografica.info/linea-de-tiempo.php?crono=447 [Consulta: 20 de desembre de 2011]

MONOGRAFIAS.COM. Biografía de Gauss, Carl Friedrich [En línia] Mèxic.
http://www.monografias.com/trabajos55/historias-de-matematicos/historias-de-matematicos4.shtml [Consulta: 20 de desembre de 2011]

SERGIO DÁVILA. Cálculo Diferencial e Integral [En línia] Colegio Champagnat.
http://www.angelfire.com/de/calculus65/gauss.html [Consulta: 12 de setembre de 2011]

RICARDO SANTIAGO NETTO.Fisicanet [En línia] Mèxic.
http://www.fisicanet.com.ar/biografias/cientificos/g/gauss.php [Consulta: 19 d'octubre de 2011]

ANTONIO PEREZ SANZ. Matemàticas [En línia] I.E.S. Salvador Dalí:. Madrid 2011.
http://platea.pntic.mec.es/aperez4/ [Consulta: 15 de novembre de 2011]

CARLOS GUMBAU i ANTONIO LUIS MARTINEZ.El Paraiso de las matematicas [En línia] Elda :2010
http://www.matematicas.net/paraiso/historia.php?id=sxvii_sxviii [Consulta: 15 de juliol de 2011]

ANTONIO PEREZ SANZ. Matemàticas [En línia] I.E.S. Salvador Dalí:. Madrid 2011
http://platea.pntic.mec.es/aperez4/html/sigloxix/Carl%20Friedrich%20Gauss.htm [Con-

sulta: 29 de setembre de 2011]

PATRICIO BARROS .Los grandes Matemáticos [En línia] E.T. Bell : 2002. http://www.ciudadjardin.org/attachments/026_Grandes_Matematicos.pdf [Consulta: 12 de setembre de 2011]

COL·LABORADORS DE LA VIQUIPÈDIA. Carl Friedrich Gauß [en línia]. Viquipèdia, l'Enciclopèdia Lliure, 2011]. //ca.wikipedia.org/w/index.php?title=Carl_Friedrich_Gau%C3%9F&oldid=8542724. [Consulta: 6 de desembre del 2011]

COLABORADORES DE WIKIPEDIA. Disquisitiones arithmeticae [en línea]. Wikipedia, La enciclopedia libre, 2012. http://es.wikipedia.org/w/index.php?title=Disquisitiones_arithmeticae&oldid=49977743. [Consulta: 7 de gener de 2012]

J.VELASCO OCAMPO, L. GONZALEZ RAMIREZ, i alt. [En línia]. Mèxic: Secretaria de Educación Pública. http://www.pps.k12.or.us/district/depts/edmedia/videoteca/curso2/htmlb/SEC_48.HTM [Consulta: 18 de desembre de 2011]

WIKIPEDIA CONTRIBUTORS, 'Quadratic residue', Wikipedia, The Free Encyclopedia, 15 December 2011, 03:44 UTC, http://en.wikipedia.org/w/index.php?title=Quadratic_residue&oldid=465940083 [accessed 18 December 2011]

DEPARTAMENTO DE MATEMÁTICA APLICADA. [En línia]. Madrid: Universidad Politécnica de Madrid. http://www.dma.fi.upm.es/java/matematicadiscreta/aritmeticamodular/congruencias.html [Consulta: 2 de novembre de 2011]

DEPARTAMENTO DE MATEMÁTICA APLICADA. [En línia]. Madrid: Universidad Politécnica de Madrid. http://www.dma.fi.upm.es/java/matematicadiscreta/aritmeticamodular/tablas4.html [Consulta: 2 de novembre de 2011]

DEPARTAMENTO DE MATEMÁTICA APLICADA. [En línia]. Madrid: Universidad Politécnica de Madrid. http://www.dma.fi.upm.es/java/matematicadiscreta/aritmeticamodular/divisibilidad.html#algoeuc [Consulta: 2 de novembre de 2011]

MANUAL DE LATEX. [En línia]. Computer Based Learning Unit, University of Leeds

http://www.fceia.unr.edu.ar/lcc/cdrom/Instalaciones/LaTex/latex.html

MARIO BUNGE,RICARDO MIRÓ. Sintaxis para la inclusión de fórmules matemáticas en los foros. [En línia].
http://rinconmatematico.com/instructivolatex/formulas.htm [Consulta: 25 de setembre de 2011]

WIKIPEDIA CONTRIBUTORS, 'Euler's totient function', Wikipedia, The Free Encyclopedia, 1 January 2012, ,
http://en.wikipedia.org/w/index.php?title=Euler%27s_totient_function&oldid=468937206[accessed 2 november 2011]

WIKIPEDIA CONTRIBUTORS, 'Quadratic residue', Wikipedia, The Free Encyclopedia, 15 December 2011, 03:44 UTC,
http://en.wikipedia.org/w/index.php?title=Quadratic_residue&oldid=465940083 [accessed 2 november 2011]

WIKIPEDIA CONTRIBUTORS, 'Modular arithmetic', Wikipedia, The Free Encyclopedia, 12 January 2012, 21:19 UTC,
http://en.wikipedia.org/w/index.php?title=Modular_arithmetic&oldid=471032096 [accessed 2 november 2011]

NICOLA L. C. TALBOT. LaTeX for Complete Novices. [En línia]. School of Computing Sciences. University of East Anglia.
http://theoval.cmp.uea.ac.uk/ nlct/latex/novices/babel.html [Consulta: 25 de setembre de 2011]

IMÁGENES EN LATEX. Blog Acubons. [En línia].
http://ocubom.wordpress.com/2008/05/27/imagenes-en-latex/ [Consulta: 25 de setembre de 2011]

ANDERS SJÖQVIST. LaTeX tips and tricks . [En línia]. Suecia: Kungliga Tekniska högskolan , 2005.
http://www.f.kth.se/ ante/latex.php#enumeration [Consulta: 25 de setembre de 2011]

9 Agraïments

Per començar, voldria agrair el suport i l'ajuda rebuda per part de la meva tutora del treball, Dolors Ametller, sobretot en el procés d'aprenentatge del codi LaTeX i sobre l'estructuració i correcció del treball.

També agrair tot el material i consell rebut d'en Bernat Plans, vicedegà del centre de documentació de la Universitat Politècnica de Barcelona, del qual vaig escollir una de les seves propostes de treball de recerca. Li agraeixo també el suport en l'apartat de base teòrica d'aritmètica modular.

Vull destacar l'ajut rebut a l'hora d'elaborar el codi per al programa informàtic d'en German Alhama (llicenciat en Matemàtiques) i en Eleuterio Daimiel, programadors informàtics d'una empresa de software de Barcelona.

Per acabar, agrair tot el suport incondicional rebut per part dels meus pares, que han estat allà sempre que ho necessitava.

10 Annexos

10.1 Exemple d'escriptura en Latex (fragment del treball)

A continuació adjunto una part del treball escrit en llenguatge LaTex. Cal remarcar que tot el treball (excepte la portada) ha estat escrit i editat utilitzant aquest llenguatge.

A l'inici trobem el "*head*", que és on es configuren les característiques que vols que tingui el teu document i els diferents paquets de continguts que vols que s'utilitzin en aquest.

A continuació trobem el "*body*", que correspon al document escrit. És tot allò que està entre *begin*{*document*} i *end*{*document*}.

*Nota: les pàgines que corresponen al codi no estan comptabilitzades dins de l'enumeració de pàgines general.

```
\documentclass[12pt]{article}

\usepackage{amsmath,amssymb}
\usepackage{amsfonts}
\usepackage{amsthm}
\usepackage{graphicx}
\newtheorem{prop}{Proposici\'o}
\newtheorem{teo}[prop]{Teorema}
\newcommand{\lp}{\left(}
\newcommand{\rp}{\right)}
\usepackage{eurosym}

\usepackage[catalan]{babel}
\selectlanguage{catalan}
\usepackage[latin1]{inputenc}

\parskip .3cm
\topmargin 0 cm
\oddsidemargin .2cm
\itemsep .2cm
\textwidth 16cm
\textheight 20cm
\begin{document}
\section{Part Teòrica}
\subsection{Aritmètica modular}
\subsubsection{L'anell $\mathbb{Z}/m\mathbb{Z}$}

\begin{itemize}

\item Dos nombres $a$ i $b$ $\in$ $\mathbb{Z}$ s'anomenen congruents entre si mòdul $m$ si la
    seva diferència és divisible entre $m$ (és a dir, tenen el mateix residu al dividir-los
    entre $m$), o dit d'altra forma : $a-b=km$.
Es denota així : $a\equiv b\pmod{m}$

\item Tot enter $a$ és congruent a un únic $r$, amb $0\leq r<m$, que correspon al residu de
    dividir $a$ entre $m$. A més, si $a\equiv b$ i $c\equiv d$ , llavors $a+c\equiv b+d$ i
    $ac\equiv bd$. Per tant el conjunt d'aquests $r$ té estructura d'anell i l'anomenarem
    $\mathbb{Z}/m\mathbb{Z}$.
\end{itemize}
\subsubsection{Element invers}
\begin{itemize}
\item Un element $a\in \mathbb{Z}/m\mathbb{Z}$ s'anomena invertible si existeix un $b$ tal que
    $ab\equiv 1\pmod{m}$, cosa que només és possible si i només si $\mbox{mcd}(a,m)=1$.
\item El fet de que $a$ sigui coprimer amb el mòdul es demostra a partir de l'identitat de
    Bézout (veure Annex2), que diu que si mcd$(a,m)=d$, llavors existeixen $x,y$ tals que
    compleixen $ax+ym=d$.\\Aquesta expressió es pot traduir a $ax\equiv d\pmod{m}$ i, per tal
    de que $x$ sigui l'invers d'$a$, mcd$(a,m)=1$ i es compleix la condició.
\item Una forma fàcil de trobar l'element invers d'un nombre és fent servir l'algorisme
    d'Euclides a l'equació diofàntica $ax+ym=1$ (veure Annex2), on $a$ és el nombre en qüestió,
    $x$ és l'element invers d'aquest i $m$ és el mòdul.
\item El conjunt d'elements invertibles en $\mathbb{Z}/m\mathbb{Z}$ l'anomenarem per
    $U(\mathbb{Z}/m\mathbb{Z})$.
\end{itemize}

\begin{prop}Si un element té invers, aquest és únic.\end{prop}

\begin{proof}\hspace{0.25cm}Ens disposem a demostrar-ho per reducció a l'absur.Posem per cas que
existeixen $2$ elements, $b$ i $c$, inversos d'$a$. Tindríem que:
$$ab\equiv1\pmod{m}\hspace{0.5cm}ac\equiv1\pmod{m}$$

per tant$$ab\equiv ac\pmod{m}$$

i multiplicant els dos membres per $b$ $$b\equiv c\pmod{m}$$

I arribem a contradicció. Per tant, existeixen tants elements en $U(\mathbb{Z}/m\mathbb{Z})$ com
$a$ entre 0 i $m$ tals que mcd($a,m)=1$\end{proof}

\underline{Corol.lari:} Si $m$ és un primer senar $p$, llavors
$U(\mathbb{Z}/p\mathbb{Z})=\mathbb{Z}/p\mathbb{Z}-\{0\}$

\underline{Exemples:} En la taula següent podem veure tots els inversos dels nombres de
$\mathbb{Z}/11\mathbb{Z}$ i les congruències en fer el producte. Fixem-nos que al ser 11 un
nombre primer, tots els elements tenen invers.

\begin{figure}[h]
```

```
   \centering
     \includegraphics[width=15cm]{Taula1}
     \end{figure}

\underline{Observació}: fixem-nos que els únics que són els seus propis elements inversos són 1 i
$p-1$, ja que un nombre és el seu propi invers si $$x^2\equiv1\pmod{p}$$
$$x^{2}-1\equiv0\pmod{p}$$ $$(x+1)(x-1)\equiv0\pmod{p}$$ $$x=\pm1$$
\begin{teo}[de Wilson] Un nombre enter $p$ és primer si, i només si: $$(p-1)!\equiv-1\pmod{p}$$
\end{teo}
\begin{proof}\hspace{0.25cm} Utilitzarem els elements invertibles a l'hora de demostrar el
teorema.

Posem per cas que $p$ no és primer. Llavors, el producte $(p-1)!$ tindrà tots els factors de $p$.
Per tant, $$(p-1)!\equiv0\pmod{p}$$Però, si $p$ és primer, tots els elements $2,...,(p-2)$
tindran invers dins de $2,...,(p-2)$ i multiplicats donaran 1. Per tant, podrem transformar
l
'
expressió
:
$$
(
p-
1
)
!
\
equiv
(1\cdot2\cdot3\cdot...\cdot(p-2))(p-1)\equiv(1\cdot1\cdot1...)(p-1)\equiv(p-1)\equiv-1\pmod{p}$$
\end{proof}
\subsection{La funció $\varphi$ de Euler}

Sigui $n$ un enter. Definim $\varphi(n)$ com la quantitat de nombres naturals més petits que $n$
i primers amb $n$. Per la proposició anterior, $\varphi(n)=|U(\mathbb{Z}/m\mathbb{Z})|$.\\

\underline{Exemples:} $\varphi(1)=1,\varphi(2)=1,\varphi(15)=8...$.

Si $p$ és primer:

$\varphi(p)=p-1$

$\varphi(p^{k})=p^{k}-p^{k-1}=(p-1)p^{k-1}=(1-\frac{1}{p})p^{k}$

\begin{proof}\hspace{0.25cm} Volem demostrar que $(p^{k})=p^{k}-p^{k-1}$. En el conjunt
$\{1,2,3,...,p^{k}\}$ hi ha exactament $p^{k-1}$ múltiples de $p$, que serien $\{1p, 2p,
3p,...,(p^{k-1})p\}$, i aquests són els únics no primers amb $p$.
\end{proof}

\begin{prop}La funció d'Euler és multiplicativa, és a dir, $\varphi(nm)=\varphi(n)\varphi(m)$
sempre que $\mbox{mcd}(m,n)=1$.\end{prop}

\begin{proof}\hspace{0.25cm}Sigui $z\in\mathbb{Z}$. Denotem per $\mathbb{Z}_k$ a
$\mathbb{Z}/k\mathbb{Z}$ i $[z]_{k}$ al valor de $z$ dins de $\mathbb{Z}_k$. A partir d'aquí,
anomenem $[z]_{mn}$, $[z]_m$ i $[z]_n$, amb $m$ i $n$ coprimers. Llavors, definim la
correspondència:
$$\mathbb{Z}_{mn}\rightarrow\mathbb{Z}_{m}\times\mathbb{Z}_n$$ $$[z]_{mn}\rightarrow(a,b)$$

On $a=[z]_m$ i $b=[z]_n$. Aquesta correspondència és injectiva, és a dir, a elements diferents de
$\mathbb{Z}_{mn}$ corresponen parelles diferents de $\mathbb{Z}_{m}\times\mathbb{Z}_n$. Per a
demostrar-ho, imaginem que de $[z_{1}]_{mn}\neq[z_{2}]_{mn}$ obtenim $a_{1}=a_{2}$ i $b_{1}=b_2$.
Tindríem que:
$$
\
left
.
\
begin
{
matrix
}a_1=z_1+kn\\a_2=z_2+pn\end{matrix}\right\}\Rightarrow\begin{matrix}z_1-z_2=\dot{n}\end{matrix}$$

Igualment, per a $b_1$ i $b_2$ arribem a que $z_1-z_2=\dot{m}$. Per tant:
$$\left.\begin{matrix}z_1-z_2=\dot{n}\\z_1-z_2=\dot{m}\end{matrix}\right\}\ \mbox{i tenint en
compte que \textit{m} i \textit{n} són coprimers}\Rightarrow z_1-z_2=\dot{\bar{nm}}\Rightarrow
[z_1]_{mn}=[z_2]_{mn}$$i arribem a contradicció.
```

A més, la quantitat d'elements dins de $\mathbb{Z}_{mn}$ i de $\mathbb{Z}_n\times\mathbb{Z}_m$ és la mateixa (mn elements), per tant, la correspondència és també bijectiva.

Seguint aquesta mateixa norma i notació, volem demostrar que, si $U(\mathbb{Z}_{mn})$ és el conjunt d'elements invertibles en $\mathbb{Z}_{mn}$ la correspondència següent:
$$U(\mathbb{Z}_{mn})\rightarrow U(\mathbb{Z}_{m})\times U(\mathbb{Z}_n)$$és també bijectiva.

És a dir, que z és invertible a $\mathbb{Z}_{mn}$ quan a i b ho són a $\mathbb{Z}_{m}$ i $\mathbb{Z}_{n}$ i viceversa.

Primer demostrarem que si $z\in U(\mathbb{Z}_{mn})$, llavors $z\in U(\mathbb{Z}_{m})$ i $z\in U(\mathbb{Z}_{n})$.

Sabem que mcd$(z,mn)=1$. Llavors, si $$d=\mbox{mcd}(z,n)\Rightarrow d|n\Rightarrow d|mn\ \mbox{i}\ d|z\Rightarrow d=1$$
Si mcd$(z,n)=1$, llavors $z\in U(\mathbb{Z}_{n})$. De la mateixa manera, $z\in U(\mathbb{Z}_{m})$.

Ara, demostrarem que si $a\in U(\mathbb{Z}_{n})$ i $b\in U(\mathbb{Z}_{m})$, existirà un z, amb $[z]_n=a$ i $[z]_m=b$, que complirà $z\in U(\mathbb{Z}_{mn})$.

Sabem que $$z=a+kn=b+pm$$ i que
$$\begin{matrix}\mbox{mcd}(a,n)=1\\\mbox{mcd}(b,m)=1\end{matrix}$$
Si $d|z,n\Rightarrow d|a=z-np$. És a dir, $d|a,z,n$ i com que mcd$(a,n)=1$, $d=1$. De la mateixa manera, ho fem per b i per m.
Llavors:$$\begin{matrix}\mbox{mcd}(z,n)=1\\\mbox{mcd}(z,m)=1\end{matrix}$$
Si tenim un $d|z,mn$, llavors o bé $d|m$ o $d|n$, ja que m i n són coprimers. Però, com que mcd$(z,n)=1$ i mcd$(z,m)=1$, llavors mcd$(z,mn)=1$ i $z\in U(\mathbb{Z}_{mn})$.\end{proof}

\begin{prop}Per a qualsevol $n<1$ es compleix que: $$\varphi(n)=n\prod_{p_{i}|n}^{} \lp 1-\frac{1}{p_{i}}\rp $$ on p_{i} són tots els primers divisors de n.\end{prop}

\begin{proof}\hspace{0.25cm}Partim de $n=p_{1}^{k_{1}}\cdot...\cdot p_{r}^{k_{r}}$. Sabent que $\varphi(nm)=\varphi(n)\varphi(m)$ si $\mbox{mcd}(m,n)=1$ i el valor de $\varphi(p^{k})$, podem dir
que
:$$\varphi(n)=(1-\frac{1}{p_{1}})p_{1}^{k_{1}}\cdot...\cdot(1-\frac{1}{p_{r}})p_{r}^{k_{r}}$$Per definició, $n=p_{1}^{k_{1}}\cdot...\cdot p_{r}^{k_{r}}$ per tant queda demostrat.\end{proof}

\begin{prop}Si p és un nombre primer i senar, llavors el grup d'elements d'$U(\mathbb{Z}/p^{k}\mathbb{Z})$ és cíclic d'ordre $p^{k}-p^{k-1}$. És a dir, existeix un g tal que: $$U(\mathbb{Z}/p^{k}\mathbb{Z})=\{g^{r}:r=1,...,p^{k}-p^{k-1}\}.$$Dit d'altra manera, existeix un g del qual podrem obtenir tots els elements de $U(\mathbb{Z}/p^{k}\mathbb{Z})$ si l'elevem a potències d'exponent desde 1 fins a $p^{k}-p^{k-1}$.\end{prop}

\underline{Dada útil:} en el cas de $k=1$ (un primer qualsevol) és interessant observar que l'ordre és de $p-1=\varphi(p)$.

\underline{Exemple:} Sigui $p=3$ i $k=2$. Llavors agafem el conjunt $U(\mathbb{Z}/9\mathbb{Z})$, els elements del qual són $\{1,2,4,5,7,8\}$ i provem què obtenim amb diferents elements.

Agafant el 4 obtenim: $4^{1}\equiv4$, $4^{2}\equiv7$, $4^{3}\equiv1$. És a dir, no obtenim tots els elements del conjunt $U(\mathbb{Z}/\mathbb{Z}_9)$.

Provem ara amb el 2:
$2^{1}\equiv2,2^{2}\equiv4,2^{3}\equiv8,2^{4}\equiv7,2^{5}\equiv5,2^{6}\equiv1$. Fixem-nos en que l'últim exponent és $6=3^{2}-3^{2-1}$, i que hem generat el conjunt d'elements $U(\mathbb{Z}/9\mathbb{Z})$. Llavors, direm que el 2 és un generador d'$U(\mathbb{Z}/9\mathbb{Z})$.

És essencial veure que cal que p sigui senar. Per exemple, $U(\mathbb{Z}/8\mathbb{Z})$ no és cíclic. De fet, té 4 elements pero tots són d'ordre 2 (és a dir, satisfan $g^2=1$)

\subsubsection{**Equacions lineals i sistemes d'equacions**}

Anomenarem equació lineal a aquella de la forma $ax\equiv b\pmod{m}$.

\begin{prop}Si $\mbox{mcd}(m,a)=1$, l'equació tindrà una única solució.\end{prop}

\begin{proof}\hspace{0.25cm}Procedirem a fer la demostració per reducció a l'absurd. Com que mcd(a,m)=1 sabem que a tindrà un element invers. Llavors, una solució a l'equació seria $x_0=a^{-1}b$ ja que $$ax_0\equiv aa^{-1}b\equiv b\pmod{m}$$

Imaginem que existeixen dues solucions, x_0,x_1. Sabriem que $$ax_1\equiv b\pmod{m}$$
$$x_1\equiv a^{-1}b\equiv x_0\pmod{m}$$

```
Per tant, $x_0\equiv x_1$ i arribem a contradicció.\end{proof}

\begin{prop}Si $\mbox{mcd}(m,a)=d$, existiran exactament $d$ solucions de l'equació $ax\equiv
b\pmod{m}$.\end{prop}

\begin{proof}\hspace{0.25cm}La congruència $ax\equiv b\pmod{m}$ equival a que existeixi algun
enter $y$ tal que $ax-ym=b$.\\
Tenint en compte que $\mbox{mcd}(a,m)=d$, $d$ divideix $b$. Per tant, podem dir que
$a=a'd,b=b'd,m=m'd$, i transformar la primera equació en una reduïda: $a'x\equiv b'\pmod{m'}$.

Aquesta equació reduïda sí que tindra una única solució $t\in\mathbb{Z}/m\mathbb{Z}$, ja que
$\mbox{mcd}(a',m')=1$. Per tant, un element $x_0\in\mathbb{Z}/m'\mathbb{Z}$ és solució de
l'equació no reduïda exactament quan $x_0\equiv t\pmod{m'}$, és a dir, $x_0=t+zm'$ per algun
enter $z$.

Per tant, hi ha exactament $d$ solucions, que corresponen a $0\leq z<d$.\end{proof}

\begin{teo}[Petit de Fermat]

Sigui $p$ un primer i $a$ un enter, llavors $a^{p}\equiv a\pmod{p}\forall a$.

En particular, si $\mbox{mcd}(p,a)=1$, llavors $a^{p-1}\equiv 1\pmod{p}$.\end{teo}

\begin{proof}\hspace{0.25cm}Seguirem el mètode d'inducció. En el cas $a=1$ és obvi. Suposem que
val per $a=n$. Comprovem que es compleix per $a=n+1$. Cal que comprovem que $$(n+1)^{p}\equiv
n+1$$
Si desenvolupem $(n+1)^{p}$ ens dóna que $$(n+1)^{p}\equiv n^{p}+1\pmod{p}$$  ja que tots els
factors $\displaystyle{p \choose k}$ amb $0<k<p$ seran múltiples de $p$. I finalment, com que
$n^{p}\equiv n\pmod{m}$ per hipòtesi inductiva, $$(n+1)^{p}\equiv n^{p}+1\equiv
n+1\pmod{p}$$\end{proof}

\begin{teo}[d'Euler]

Si $\mbox{mcd}(a,m)=1$, llavors $a^{\varphi(m)}\equiv1\pmod{p}$ per a qualsevol $a$ enter. Per
tant, $a^{\varphi(m)-1}$ és l'element invers de $a$.\end{teo}

\begin{proof}\hspace{0.25cm}Siguin $\{r_{1},...,r_{\varphi(m)}\}$ tots els naturals primers amb
$m$ menors que aquest. Ara multipliquem cada $r_{i}$ per $a$, i cadascun d'aquest $r_{i}a$ serà
congruent a un únic altre $r_{j}$. De forma que tindrem: $$ar_{1}\cdot...\cdot
ar_{\varphi(m)}\equiv r_{1}\cdot...\cdot r_{\varphi(m)}\pmod{m}$$ Llavors:
$$a^{\varphi(m)}(r_{1}\cdot...\cdot r_{\varphi(m)})\equiv r_{1}\cdot...\cdot
r_{\varphi(m)}\pmod{m}$$I això és només possible si $a^{\varphi(m)}\equiv 1\pmod{m}$ (es pot
simplificar als dos membres ja que $\mbox{mcd}(a,r_{i})=1$).\end{proof}

\begin{teo}[Teorema xinès del residu]

Siguin $m_{1},...,m_{r}$ enters positius coprimers dos a dos. El sistema d'equacions $$x\equiv
a_{1}\pmod{m_{1}}\ \ \ ;...;\ \ \ x\equiv a_{r}\pmod{m_{r}}$$ té solució per a qualssevol
$a_{1},...,a_{r}$. Aquesta solució és única mòdul el producte de tots els $m_{1},...,m_{r}$.
\end{teo}
\begin{proof}\hspace{0.25cm}Sigui $M=m_{1}\cdot...\cdot m_{r}$. Llavors, qualsevol $m_{j}$
($1\leq j\leq r$) divideix a $M$ i $\mbox{mcd}(M/m_{j},m_{j})=1$.
Com que $\mbox{mcd}(M/m_{j},m_{j})=1$, sabem que existiran $b_{j}$ tals que:
$$\frac{M}{m_{j}}b_{j}\equiv1\pmod{m_{j}}$$A més, per a tot $m_{i}\neq m_{j}$
tindrem:$$\frac{M}{m_{j}}b_{j}\equiv0\pmod{m_{i}}$$A partir d'aquests $b_{j}$ construirem la
suma$$w=\sum_{i=0}^{r}\frac{M}{m_{j}}b_{j}a_{j}$$Per a $1\leq i\leq
r$:$$w=\sum_{j=0}^{r}\frac{M}{m_{j}}b_{j}a_{j}\equiv \frac{M}{m_{i}}b_{i}a_{i}\equiv
a_{i}\pmod{m_{i}}$$
Per acabar, suposem que existeixen dues solucions $x$ i $y$ diferents, que $$x\equiv a_{i}\equiv
y\pmod{m_{i}}$$Per tant, $x-y$ és divisible per $m_{i}$, i com que tots els $m_{i}$ són coprimers
entre si, $x-y$ serà tambe divisible per $M$, per tant:$$x\equiv y\pmod{M}$$i arribem a
contradicció. Per tant, $w$ és l'única solució del sistema.\end{proof} \end{document}
```

10.2 L'algorisme d'Euclides

L'algorisme d'Euclides és un mètode útil i eficaç per a calcular el màxim comú divisor de dos nombres naturals qualssevol. El procés consiteix en una sèrie de divisions successives.

Utilitza els residus i es basa en què, si a i b, amb $a > b$, existeix un q_1 tal que:

$$a = q_1 b + r_1 \quad \text{i} \quad r_1 < b$$

De la mateixa manera, existirà un q_2 tal que:

$$b = q_2 r_1 + r_2 \quad \text{i} \quad r_2 < r_1$$

Aquest procés es repeteix fins que s'arriba a $r_k = 0$. Llavors, el màxim comú divisor d'a i b serà r_{k-1}. Per exemple, $a = 2346$ i $b = 456$:

- $2346 = 456 * 5 + 66$
- $456 = 66 * 6 + 60$
- $66 = 60 * 1 + 6$
- $60 = 6 * 10 + 0$

Per tant, el $\text{mcd}(2346, 456) = 6$.

Si arrosseguem càlculs:

$$6 = 66 - 60 = 66 - (456 - 66 * 6) = 7 * 66 - 456 = 7(2346 - 5 * 456) - 456 = 7 * 2346 - 5 * 456$$

Aquest mètode ens permet trobar els inversos d'elements quan estem en $\mathbb{Z}/m\mathbb{Z}$. Posem per exemple que volem trobar l'invers de 19 dins de $\mathbb{Z}/31\mathbb{Z}$. Aplicant l'algorisme:

- $31 = 19 * 1 + 12$
- $19 = 12 * 1 + 7$
- $12 = 7 * 1 + 5$
- $7 = 5 * 1 + 2$

- $5 = 2 * 2 + 1$
- $2 = 1 * 2 + 0$

Tornem a arrossegar els diferents passos:

$$1 = 5 - 2 * 2 = 5 - 2 * (7 - 5 * 1) = 3 * 5 - 2 * 7 = 3 * (12 - 7 * 1) - 2 * 7 =$$

$$= 3*12-5*7 = 3*12-5*(19-12*1) = 8*12-5*19 = 8*(31-19*1)-5*19 = 8*31-19*13$$

Per tant, l'element invers de 19 és $-13 \equiv 18 \pmod{31}$.

Sabem que aquest mètode sempre servirà per l'identitat de Bézout, que diu que, si a i b són naturals qualssevol, sempre existiran x i y enters tals que $ax + by = d$, on $d = \text{mcd}(a, b)$.

10.3 Codi del programa de Càlcul de Símbols de Legendre

```
using System;
using System.ComponentModel;
using System.Drawing;
using System.Windows.Forms;

namespace Cuadratic
{
    public partial class Form1 : Form
    {
        public Form1()
        {
            InitializeComponent();
        }


        private double g_intA = 0;
        private double g_intB = 0;
        private int g_intResultado = 0;
        private string g_txtResultado1 = "";
        private string g_txtResultado2 = "";

        public void Calcular()
        {
            g_intResultado = 1;
            g_txtResultado1 = "";
            g_txtResultado2 = "";
            TestParametres();

            double intALoc = g_intA;
            double intBLoc = g_intB;

            bool blnFinal = TestComprobacioFinal(intALoc, intBLoc);
            if (!blnFinal)
            {
                do
                {
                    bool blnTest = false;
                    if (intALoc >= intBLoc)
                    {
                        intALoc = intALoc % intBLoc;
                        blnTest = true;
                    }

                    //Treure factors 2 del numerador.
                    if (!blnTest)
                    {
                        blnTest = QuitarFactores2(ref intALoc, intBLoc);
                    }

                    //Llei reciprocidad quadràtica.
                    if (!blnTest)
                    {
                        PermutarParametros(ref intALoc, ref intBLoc);
                        blnTest = true;
```

```
            }

            blnFinal = TestComprobacioFinal(intALoc, intBLoc);

        } while (!blnFinal);
    }
    g_txtResultado1 = g_intResultado.ToString();
    switch (g_intResultado)
    {
        case 1:
            g_txtResultado2 = "<" + g_intA.ToString() + "> és residu quadràtic mòdul
            <" + g_intB.ToString() + ">";

            break;
        case -1:
            g_txtResultado2 = "<" + g_intA.ToString() + "> és un NO residu quadràtic mòdul
            <" + g_intB.ToString() + ">";

            break;
        case 0:
            g_txtResultado2 = "<" + g_intA.ToString() + "> és múltiple de
            <" + g_intB.ToString() + ">";

            break;
    }
}

private void TestParametres()
{
    if (g_intA <= 0 || g_intB <= 0)
        throw new Exception("Han de donar-se paràmetres diferents de zero i positius.");
    //if (intA == intB)
    //    throw new Exception("El paràmetres no poden ser iguals.");
    if (EsPar(g_intB))
        throw new Exception("Paràmetre 2 no pot ser parell.");
    if (!EsPrimer(g_intB))
        throw new Exception("Paràmetre 2 ha de ser primer.");
}

private bool EsPar(double intprmTestear)
{
    return (intprmTestear % 2 == 0);
}

private bool EsPrimer(double intprmTestear)
{
    if (intprmTestear == 3)
        return true;

    bool blnSalida = true;
    double max = Math.Sqrt(intprmTestear);
    if (intprmTestear > 3)
    {
        double intAux = 3;
```

```
        do
        {
            blnSalida = (intprmTestear % intAux) != 0;
            intAux = intAux + 2;
        } while ((blnSalida != false) && (intAux <= max));
    }
    //Nota: para el caso 1 y 2 devuelve verdadero y no puede ser negativo.
    return blnSalida;
}

private bool TestComprobacioFinal(double intprmA, double intprmB)
{
    bool blnFinal = true;

    int aux = 0;
    try
    {
        aux = Convert.ToInt32(intprmA);
    }
    catch(Exception ex)
    {
        return false;
    }

    switch (aux)
    {
        case 0:
            AcumulaSigno(0);
            break;
        case 1:
            AcumulaSigno(1);
            break;
        case 2:
            AcumulaSigno(ResultadoFormula2(intprmB));
            break;
        case -1:
            AcumulaSigno(ResultadoFormula_1(intprmB));
            break;
        default:
            blnFinal = false;
            break;
    }
    return blnFinal;
}

private bool QuitarFactores2(ref double intprmAEntrada, double intprmBEntrada)
{
    bool blnSalida = false;

    while (intprmAEntrada % 2 == 0)
    {
        intprmAEntrada = intprmAEntrada / 2;
        blnSalida = true;
        AcumulaSigno(ResultadoFormula2(intprmBEntrada));
```

```
    }

    return blnSalida;
}

private void AcumulaSigno(int intprmAcumular)
{
    if ((intprmAcumular != 1) && (intprmAcumular != -1) && (intprmAcumular != 0))
        throw new Exception("Control. Només poden acumularse 0,1 ó -1.");
    g_intResultado = g_intResultado * intprmAcumular;
}

private int ResultadoFormula2(double intprmB)
{
    double decNumerador = ((intprmB * intprmB) - 1) / 8;
    if ((decNumerador % 2) == 0)
        return 1;
    else
        return -1;
}

private int ResultadoFormula_1(double intprmB)
{
    double decNumerador = (intprmB - 1) / 2;
    if ((decNumerador % 2) == 0)
        return 1;
    else
        return -1;
}

private void PermutarParametros(ref double intprmAEntrada, ref double intprmBEntrada)
{
    double intprmAaux = intprmAEntrada;
    double intprmBaux = intprmBEntrada;

    AcumulaSigno(LleiReciporcitatQuadràtica(intprmAEntrada, intprmBEntrada));
    intprmAEntrada = intprmBaux;
    intprmBEntrada = intprmAaux;
}

private int LleiReciporcitatQuadràtica(double intprmA, double intprmB)
{
    double decNumerador = ((intprmA - 1) / 2) * ((intprmB - 1) / 2);
    if ((decNumerador % 2) == 0)
        return 1;
    else
        return -1;
}

private void button1_Click(object sender, EventArgs e)
{
    try
    {
        g_intA = (double)numericUpDown1.Value;
```

```
                g_intB = (double)numericUpDown2.Value;
                Calcular();
                label1.Text = g_txtResultado1;
                label2.Text = g_txtResultado2;
            }
            catch (Exception ex)
            {
                MessageBox.Show(ex.Message);
            }
        }

        private void numericUpDown1_ValueChanged(object sender, EventArgs e)
        {
            g_txtResultado1 = "";
            g_txtResultado2 = "";
            label1.Text = g_txtResultado1;
            label2.Text = g_txtResultado2;
        }

        private void numericUpDown2_ValueChanged(object sender, EventArgs e)
        {
            g_txtResultado1 = "";
            g_txtResultado2 = "";
            label1.Text = g_txtResultado1;
            label2.Text = g_txtResultado2;
        }
    }
}
```