Demostración a la conjetura de Albert Girard

---

propiedades de los números primos

(y diferencias clave respecto de los elementos compuestos)

mediante ecuaciones cuadráticas específicas

Miguel Angel Rey Bonet

Índice

Introducción.

Se demostrará en la presente obra**...**:

1ro) La conjetura de Albert Girard /

Si $p \equiv 3 \pmod 4 \wedge p$ primo, $p > 2$

Entonces: $p = x^2 \pm 2y^2$ con: $x,y \in \mathbb{N}\backslash\{0\}$

2do) El teorema de Fermat (sobre suma de cuadrados) ó Lema de Thue, mediante procedimiento análogo al utilizado para la conjetura anterior. /

Si $p \equiv 1 \pmod 4 \wedge p$ primo, $p > 2$

Entonces: $p = x^2 + y^2$ con: $x,y \in \mathbb{N}\backslash\{0\}$

3ro) Finalmente, podrá demostrarse* si: para todo entero, impar y mayor que 2, dicho elemento es un número primo ó no. * Precisaremos que: podrá diferenciarse entre primo y no primo debido a que los primos cumplen ciertas características que los números compuestos no cumplen, es decir, conoceremos las diferencias clave entre números primos y números compuestos. (ver página 4 y siguientes para mayor comprensión)

Se utilizará para tales demostraciones el álgebra modular (anillos $\mathbb{Z}/p$), dando por demostrados los siguientes teoremas o proposiciones:

i) Teorema de Wilson / $(p-1)! \equiv -1 \pmod p$ si y sólo si p es primo

ii) Pequeño teorema de Fermat./ $(2)^{p-1} \equiv 1 \pmod p \ \forall$ p primo

iii) Si p es primo entonces $\exists \ \frac{p-1}{2}$ cuadrados perfectos comprendidos entre: [1,p-1] en $(\mathbb{Z}/p)$ anillo.

Si p no es primo entonces <u>no existen</u> $\frac{p-1}{2}$ cuadrados perfectos comprendidos entre [1,p-1] en el anillo $(\mathbb{Z}/p)$ (existen en menor cantidad).

iv) Si p es primo (cuadrado perfecto ≡ residuo cuadrático), entonces:

Si $p \equiv 1 \pmod 4$ ý m es un residuo cuadrático en $(\mathbb{Z}/p)$, entonces:

(-m) es también un residuo cuadrático en $(\mathbb{Z}/p)$.

Si $p \equiv 3 \pmod 4$ ý m es un residuo cuadrático en $(\mathbb{Z}/p)$, entonces:

(-m) <u>no es</u> un residuo cuadrático en $(\mathbb{Z}/p)$.

Durante la presente obra aparecerán símbolos como α, β, δ, λ, φ, ψ, σ**,...**, que nada tendrán que ver con otras matemáticas, y que aquí, simplemente, quedarán denotadas como elementos de $\mathbb{Z}$, $\mathbb{N}$,**...**, y que aparecerán como tales para diferenciarlos de otros más ordinarios. Y para destacarlos de los mismos de una forma más directa y visual, finalmente también, por resaltar de ellos diversas particularidades (las que correspondan), que otros elementos no posean.

La hipótesis central y las demostraciones oportunas de la misma se encuentran en la parte IIda. de este temario. La parte Ira. será necesaria para la hipótesis que se expondrá brevemente a continuación a modo de resumen. Se incluirá también un anexo, (págs. 88-99), que puede ser omitible, pues de él sólo se extraen ciertas particularidades no transcendentales.

Al inicio de cada parte se incluirá una breve introducción para mejor comprensión de la misma.

Expondremos a continuación algunos de los puntos más relevantes de la hipótesis propuesta en la proposición 21ra. págs. 39-43 (se omitirán ciertas particularidades aquí, por ser difícil definirlas brevemente).

Inciso Importante: De la parte Ira del temario se obtendrá un elemento denotado por el símbolo σ cuyo valor numérico dependerá de las siguientes condicionales tal que:

si $p \equiv 1 \pmod 4$ entonces $\sigma = -1$

si $p \equiv 3 \pmod 8$ entonces $\sigma = -2$

si $p \equiv 7 \pmod 8$ entonces $\sigma = +2$

además si p es primo entonces: $\exists\ \alpha \in \mathbb{Z}$, $\alpha \in (1,p-1)$ / (***importante*** ver: pág 39)

$$(\pm\alpha)^2 \equiv \sigma \pmod p \quad \wedge \quad \sigma \in \text{residuo cuadrático}$$

Tal que: $\forall\ k \in \mathbb{Z}$, $k \in (p,p-1) \wedge k \not\equiv \pm\alpha \pmod p$

entonces: $\{\pm k\}^2 \not\equiv \sigma \pmod p$

y en cambio si: p no es primo, entonces puede existir (ó no) un elemento $\beta \in \mathbb{Z}$,

con: $\beta \in (1,p-1) / (\pm\beta)^2 \equiv \sigma \pmod p$

- si $\exists\ \beta$ entonces existen** otros elementos:

β', β'', β''',…,β'^{w} pertenecientes al intervalo (1,p-1), distintos entre si, (no congruentes entre si) y que en cambio:

$(\pm\beta)^2 \equiv (\pm\beta')^2 \equiv (\pm\beta'')^2 \equiv \ldots \equiv (\pm\beta'^{w})^2 \equiv \sigma \pmod p$

** salvo ciertos números compuestos que serán tratados y claramente diferenciados de los números primos.

Nota 1ra: El valor α expresado en la página anterior, se obtiene mediante una ecuación, (omitimos expresarla aquí, por ser laboriosa la definición de la misma **ver: página 10**), y que sólo se cumple, si: p es primo, es decir, que para todo p no primo, dicho valor no existe, pero en cambio, pueden (ó no) existir otros valores enteros $\beta \in \mathbb{Z}$, $\beta \in (1, p-1) / (\pm\beta'^{i})^2 \equiv \sigma \pmod p$

Todo ello analizado y demostrado pertinentemente.

Hipótesis (ver proposición 21ra) págs. 39-43 $\forall$ p$\in \mathbb{N}$, p$\in$ **impar** entonces:

Iro) Si p es primo $\Rightarrow$ $\exists$ x,y$\in \mathbb{Z}\backslash\{0\}$

tal que: $p = x^2 - \sigma \bullet y^2$, siendo x$\in$ impar

con: $\sigma = -1$ si: $p = 4k+1$, $\sigma = -2$ si: $p = 8k+3$ $\wedge$ $\sigma = +2$ si: $p = 8k+7$ **

$\wedge$ y$\in$ par si: $p \equiv 1 \pmod 4$ é y$\in$ impar si: $p \equiv 3 \pmod 4$

además:

• si: $p = 4k+1$ ó $p = 8k+3$

Entonces: sean: $x', y' \in \mathbb{Z}\backslash\{0\} / \forall\ x' \neq \pm x \wedge y' \neq \pm y$

$\Rightarrow$ $p \neq x'^2 - \sigma \bullet y'^2$ $\wedge$ $\sigma \in$ residuo cuadrático en $\mathbb{Z}/p$ ($\pm\alpha$ raíces de σ *)

• si: $p = 8k+7$

entonces $\exists$ $x', y' \in \mathbb{Z}\backslash\{0\}$ / $x' \neq \pm x \wedge y' \neq \pm y$

/ $p = x'^2 - \sigma \bullet y'^2 = x''^2 - \sigma \bullet y''^2 = ... = (x'^w)^2 - \sigma \bullet (y'^w)^2$

• / $\exists\ \alpha \in \mathbb{Z}, \alpha \in (1,p-1) / (\pm\alpha)^2 \equiv \sigma \pmod p$ $\forall$p primo.

$\Rightarrow$ $\sigma \in$ residuo cuadrático en $\mathbb{Z}/p$ ($\pm\alpha$ raíces de σ *)

(*) Tal que: $\forall$ k$\in \mathbb{Z}$, k$\in$ $(p,p-1) \wedge k \not\equiv \pm\alpha \pmod p$

entonces: $\{\pm k\}^2 \not\equiv \sigma \pmod p$

(conjetura de Albert Girard ý lema de Thue)

** (***Nota 2da, muy importante***:) estamos afirmando claramente que: -1 es residuo cuadrático en $\mathbb{Z}/p$ para los números primos de la forma $p = 4k+1$, que -2 es residuo cuadrático en $\mathbb{Z}/p$ para los números primos de la forma $p=8k+3$, y que 2 es residuo cuadrático en $\mathbb{Z}/p$ para los números primos de la forma $p=8k+7$.

Debe quedar claro, que para los números primos de la forma $p = 8k+1$ los valores -2 y 2 también son residuo cuadrático en $\mathbb{Z}/p$ (esto no se demostrará). Pero que el valor σ para tales primos ($p=8k+1$ ó $p=8k+5$ es decir para: $p = 4k+1$) será $\sigma = -1$. (ver: punto VI pág 9 otros residuos cuadráticos en Z/p.)

IIdo) Algo más compleja y extensa: caso en que p no es primo.

i) si: $p \neq x^2 - \sigma \cdot y^2 \ \forall \ x,y \in \mathbb{Z}$, $x \in$ impar $\Rightarrow$

$$\forall \ \mu \in (1,p-1) \ \Rightarrow \ (\pm\mu)^2 \not\equiv \sigma \ (\text{mod } p)$$

ii) si: $p = x^2 - \sigma \cdot y^2 = x'^2 - \sigma \cdot y'^2 = x''^2 - \sigma \cdot y''^2 = \ldots = (x'^w)^2 - \sigma \cdot (y'^w)^2$

$\forall x'^i \neq \pm x'^j$, $i \neq j$($\Rightarrow \ y'^i \neq \pm y'^j$) con: $x'^m, y'^m \in \mathbb{Z} \backslash \{0\}$

Siendo: $f_0(p) = x^2 - \sigma \cdot y^2$, $f_1(p) = x'^2 - \sigma \cdot y'^2$, $f_2(p) = x''^2 - \sigma \cdot y''^2$,...,

,..., $f_w(p) = (x'^w)^2 - \sigma \cdot (y'^w)^2$ / $p = f_0(p) = f_1(p) = f_2(p) = \ldots = f_w(p)$

Y tal que: $\exists$ al menos $f_0(p)$ ý $f_1(p)$ que cumplen dicha igualdad con p

Entonces en $\mathbb{Z}/p$ ocurre que **si:** $\sigma \in$ residuo cuadrático en $\mathbb{Z}/p \Rightarrow$

$\exists \ f_i(p) = (x'^i)^2 - \sigma \cdot (y'^i)^2 \wedge f_j(p) = (x'^j)^2 - \sigma \cdot (y'^j)^2$

ecuaciones cuadráticas distintas

/ $p = (x'^i)^2 - \sigma \cdot (y'^i)^2 = (x'^j)^2 - \sigma \cdot (y'^j)^2$

$\wedge \ \text{mcd}(x'^i, y'^i) = \pm 1 \ \wedge \ \text{mcd}(x'^j, y'^j) = \pm 1$

es decir, existen (al menos**): $\beta \wedge \beta' \in (1,p-1)$ / $\beta \not\equiv \pm\beta' \ (\text{mod } p)$

y en cambio: $\{\pm \beta\}^2 \equiv \{\pm\beta'\}^2 \equiv \sigma \ (\text{mod } p)$

** (a diferencia de los números primos que sólo tienen dos raíces α ý (p-α) en el intervalo (1,p-1) ý de ciertos cuadrados perfectos, como se verá en el siguiente apartado iii.)

iii) si p no es primo ý $p \in$ cuadrado perfecto impar*, entonces:

ó: $p = x^2 - \sigma \cdot y^2 = f_0(p)$, $x \neq 0$ ($x \in$ impar) $\wedge \ y = 0$ / $\nexists \ f_{i>0}(p) = p$

ó: $p = x^2 - \sigma \cdot y^2 = x'^2 - \sigma \cdot y'^2$, $x \neq 0$, $y = 0$

/ $x' \in \mathbb{Z} \backslash (\pm x, 0) \wedge y' \in \mathbb{Z} \backslash (\pm y, 0)$ es decir $p = f_0(p) = f_1(p)$

Además: $\exists \ \beta \in \mathbb{Z}$, $\beta \in (1,p-1)$ / $(\pm\beta)^2 \equiv \sigma \ (\text{mod } p)$

$\Rightarrow \ \sigma \in$ residuo cuadrático en $\mathbb{Z}/p$

Tal que: $\forall \ k \in \mathbb{Z}$, $k \in (p,p-1) \wedge k \not\equiv \pm\beta \ (\text{mod } p)$

entonces: $\{\pm k\}^2 \not\equiv \sigma \ (\text{mod } p)$

ó: $p = x^2 - \sigma \bullet y^2 = x'^2 - \sigma \bullet y'^2 = x''^2 - \sigma \bullet y''^2 = \ldots = (x'^w)^2 - \sigma \bullet (y'^w)^2$

es decir: $p = f_0(p) = f_1(p) = f_2(p) = \ldots = f_w(p)$ / $Card[f(p)] \geq 3$ tal que:

$Card[f(p)] \geq 3$ ý $4 \leq Card[\beta^*] \leq 2w$ **

* se cumple que: $\forall p \in$ cuadrado perfecto impar $\Rightarrow p \equiv 1 \pmod 8$ siempre.

ý además: $\exists \ \beta \in \mathbb{Z}$ / $\{\pm\beta\}^2 \equiv \sigma \pmod p$ syss: $\exists \ f_1(p) = p$

** dada la ecuación cuadrática: $p = (x'^i)^2 - \sigma \bullet (y'^i)^2 \Rightarrow (x'^i)^2 \equiv \sigma \bullet (y'^i)^2 \pmod p$

Tal que: existe β'^i si y sólo si: $mcd(x'^i, y'^i) = \pm 1$ / $x'^i \equiv \pm\beta'^i \bullet y'^i \pmod p$

pues si $mcd(x'^i, y'^i) = k$, $k \neq \pm 1$ entonces $k \mid p \Rightarrow \nexists\ k^{-1}$ en $\mathbb{Z}/p$

$\Rightarrow \nexists\ (x'^i)^{-1}, (y'^i)^{-1}$ en $\mathbb{Z}/p$, pues: $k \mid x'^i \wedge k \mid y'^i$

Importante: si β es raíz de σ en $\mathbb{Z}/p$ también lo es $(p-\beta)$ y por tanto, se expone que $4 \leq Card[\beta^*] \leq 2w$, como mímimo existen cuatro raíces de σ en $\mathbb{Z}/p$, en el intervalo (1,p-1). es decir, existen también (ý al menos): $\beta' \wedge (p-\beta')$ raíces de σ en $\mathbb{Z}/p$

iv) Sea $p = q \bullet q'$, p no primo impar, $p > 1$

siendo: $q, q' \in$ impares, $1 < q < p$

/ $q \notin$ cuadrado perfecto $\wedge\ q' \in$ cuadrado perfecto

siendo: $p = x^2 - \sigma \bullet y^2 = f_0(p)$, $x, y \in \mathbb{Z} \setminus \{0\}$

$\wedge\ p \neq f_{i>0}(p)$ es decir, siendo: $x', y' \in \mathbb{Z}$ / $\forall\ x' \neq \pm x \ \wedge\ \forall\ y' \neq \pm y$

$\Rightarrow p \neq x'^2 - \sigma \bullet y'^2$ es decir: $Card[f(p)] = 1$

Tal que en $\mathbb{Z}/p \Rightarrow x^2 \equiv \sigma y^2 \pmod p$.

pero ocurre que: $\forall \mu \in (1,p-1) \Rightarrow \{\pm\mu\}^2 \not\equiv \sigma \pmod p$

(a diferencia de si p es primo (punto Iro)

donde: $\exists \ \alpha \in (1,p-1)$ / $\{\pm\alpha\}^2 \equiv \sigma \pmod p$ (pág 5))

v) Sea $p = q \bullet q'$ (p no primo impar $p > 1$), siendo: $q, q' \in$ impares, $1 < q < p$

/ $q \wedge q' \notin$ cuadrado perfecto $\wedge\ q \neq q' \ \wedge$ <u>al menos</u> q <u>es primo</u>

siendo: $p = x^2 - \sigma \bullet y^2 = f_0(p)$, $x, y \in \mathbb{Z} \setminus \{0\}$

<u>si:</u> $\exists \ \beta \in \mathbb{Z}$, $\beta \in (1,p-1)$ / $\{\pm\beta\}^2 \equiv \sigma \pmod p$ (...)

entonces: $\exists\ f_1(p) = x'^2 - \sigma \bullet y'^2$, con: $x', y' \in \mathbb{Z}$

$/\ \forall\ x' \neq \pm x\ \wedge\ \forall\ y' \neq \pm y\ \wedge\ |\pm x'| < \frac{1}{2}(p+1)$

tal que: $p = x^2 - \sigma \bullet y^2 = x'^2 - \sigma \bullet y'^2 \iff p = f_0(p) = f_1(p)$

entonces, por ser p **no primo**:

$\Rightarrow \exists\ \beta' \in \mathbb{Z}, \beta' \in (1,p-1)\backslash\{\pm\beta\}$, es decir: $\beta' \not\equiv \pm\beta \pmod p$, equivalentemente:

$x^2 - \sigma \bullet y^2 \equiv 0 \pmod p \iff x^2 \equiv \sigma \bullet y^2 \pmod p \iff x \equiv \pm\beta \bullet y \pmod p$

$x'^2 - \sigma \bullet y'^2 \equiv 0 \pmod p \iff x'^2 \equiv \sigma \bullet y'^2 \pmod p \iff x' \equiv \pm\beta' \bullet y' \pmod p$

tal que: $\beta \not\equiv \pm\beta' \pmod p \wedge \{\pm\beta\}^2 \equiv \{\pm\beta'\}^2 \equiv \sigma \pmod p$

IIIro) por todo lo expresado en los puntos anteriores
(incluido el inciso previo de la pág 4) tendremos que:
p es primo impar, si y sólo si:
$p = x^2 - \sigma \bullet y^2$, $x,y \in \mathbb{Z}\backslash\{0\}$, con: $f_0(p) = x^2 - \sigma \bullet y^2$

ý además, si y sólo si: $\exists\ \alpha \in (1,p-1) / \{\pm\alpha\}^2 \equiv \sigma \pmod p$

siendo: $\sigma = -1$ si $p \equiv 1 \pmod 4$
$\sigma = -2$ si $p \equiv 3 \pmod 8$
$\sigma = +2$ si $p \equiv 7 \pmod 8$

Tal que: $\forall\ k \in \mathbb{Z}, k \in (p,p-1) \wedge k \not\equiv \pm\alpha \pmod p$ entonces: $\{\pm k\}^2 \not\equiv \sigma \pmod p$

Además si: $p \not\equiv 7 \pmod 8$ entonces: $p \neq x'^2 - \sigma \bullet y'^2\ \forall\ x' \neq \pm x \wedge \forall\ y' \neq \pm y$

IVto) $\forall p \in$ impar, $p > 1$, primo ó no primo.

si: $\exists$ <u>al menos</u> $f_0(p) / p = f_0(p) = x^2 - \sigma \bullet y^2$
entonces: $x \in$ impar siempre,
lo tomamos como referencia impuesta, obteniendo entonces que
la variable (y) es…: $y \in$ par si: $p \equiv 1 \pmod 4$
$y \in$ impar si: $p \equiv 3 \pmod 4$

Vto) sea $p = x^2 - \sigma \bullet y^2 / p \in$ impar, $p > 1$, primo ó no primo. ý además:
puede (<u>ó no</u>) darse la existencia de $f_1(p), f_2(p), f_3(p), \ldots, f_w(p)$, tales que;
$p = f_{i>0}(p) = (x'^i)^2 - \sigma \bullet (y'^i)^2$, $i = 1,2,\ldots,w$ entonces en $\mathbb{Z}/p$:

$\Rightarrow x^2 \equiv \sigma y^2 \pmod p$ se podrá obtener el valor β (de existir*) / $\beta \in (1,p-1)$

$\wedge \{\pm\beta\}^2 \equiv \sigma \pmod p$ es decir: $x \equiv \pm\beta \bullet y \pmod p$ syss*: $mcd(x,y) = \pm 1$

VIto) Sea q primo, $q>2$ Ý sea: $\varsigma\in$ (-[p-1],p-1) / $\varsigma\in$ residuo cuadrático en $\mathbb{Z}/q$, <u>para todos los primos</u> de la forma: q=8k+1 ý/ó q=8k+3 ý/ó q=8k+5 ý/ó q=8k+7

De manera que se cumpla además que: $q = a^2 - \varsigma \bullet b^2$, $a,b\in \mathbb{Z}\setminus\{0\}$

Entonces, tomado un número p impar positivo particular / $p \equiv q \pmod 8$ se cumple que, dicho p es primo (impar), si y sólo si:

i) $p = x^2 - \varsigma \bullet y^2$, $x,y\in \mathbb{Z}\setminus\{0\}$, con: $f_0(p) = x^2 - \varsigma \bullet y^2$

ii) ý además, si y sólo si: $\exists\ \alpha\in$ (1,p-1) / $\{\pm\alpha\}^2 \equiv \varsigma \pmod p$, $mcd(x,y)=\pm 1$

/$\forall$ $k\in \mathbb{Z}$, $k\in$ (p,p-1) $\wedge$ $k \not\equiv \pm\alpha \pmod p$ ** entonces: $\{\pm k\}^2 \not\equiv \varsigma \pmod p$

• Además si: $(-\varsigma)>0$ entonces: $p \neq x'^2 - \varsigma \bullet y'^2$ $\forall$ $x' \neq \pm x \wedge \forall\ y' \neq \pm y$

ó bien si $(-\varsigma)<0$ entonces pueden existir (al menos): $x' \neq \pm x \wedge y' \neq \pm y$,

tales que: $p = x^2 - \varsigma \bullet y^2 = x'^2 - \varsigma \bullet y'^2$

/ $x \equiv \pm\alpha y \pmod p \wedge x' \equiv \pm\alpha y' \pmod p$ **

• Pudiendo diferenciar dicho valor p primo de cualquier valor p´ <u>no primo</u> tal que: $p \equiv p' \pmod 8$ pues dicho valor compuesto p´, ó no tiene raíces en $\mathbb{Z}/p'$ para el valor ς (ς no es residuo cuadrático en $\mathbb{Z}/p'$) o bien existen al menos 4 raíces del mismo, en el intervalo (1,p´-1), ó bien p´ es un cuadrado perfecto, ó mcd $(x,y)\neq\pm 1$.

• el punto IV, aquí es irrelevante p es impar x puede ser impar ó par dependiendo de los valores del residuo cuadrático (d) ý de si la variable (y) tal que: $-\varsigma \bullet y'^2$ sea un valor impar ó par.

• Finalmente podremos tomar un valor impar p=8k+r, tal que $p=x^2-\varsigma \bullet y^2$, $x,y\in \mathbb{Z}\setminus\{0\}$ y se conozca del mismo que: ς residuo cuadrático en $\mathbb{Z}/p$ ý: $\varsigma\in$ (-[p-1],p-1) e indiferentemente de si lo es para cualquier otro primo p´=8k´+r. pudiéndose obtener además, si dicho p es primo ó no. Dependiendo de si existen más raíces de ς en $\mathbb{Z}/p$, más ecuaciones cuadráticas para dicho valor p (dependiendo de si $(-\varsigma)>0$ ó si $(-\varsigma)<0$) , si es un cuadrado perfecto, ó mcd $(x,y)\neq\pm 1$.,...etc.

//

Nota 1ra. dichas premisas están expuestas en la parte II en la (proposición 21ra. págs 39-43)

Nota 2da. se expondrá a continuación en la parte I del temario la "resolución" del valor α, es decir: las demostraciones oportunas para denotar que:

σ es residuo cuadrático en Z/p para todo p **primo** impar /

$\sigma = -1$ si $p \equiv 1 \pmod 4$, $\sigma = -2$ si $p \equiv 3 \pmod 8$, $\sigma = +2$ si $p \equiv 7 \pmod 8$

y tal que: $\exists\ \alpha\in \mathbb{Z}$, $\alpha\in$ (1,p-1) / $(\pm\alpha)^2 \equiv \sigma \pmod p$ $\forall$p primo impar

así como la ecuación/es para hallar dicho valor α.

(En la siguiente página se incluye a modo de introducción dichos resultados que se demostrarán obviamente a lo largo de la parte I del temario.)

Parte Ira. Introducción

De la cual se obtendrán, entre otros, los siguientes resultados.

Siendo $p \in \mathbb{Z}$, $p>0 \wedge p \in$ impar entonces.

$p = 2\varphi+1$ / $\varphi = 2\rho$ si: $p \equiv 1 \pmod 4$

$\varphi = 2\rho + 1$ si: $p \equiv 3 \pmod 4$

tal que: $\prod_{t=0}^{i}(2t+1) = \{1, 3, 5, 7, 9, \ldots, (2i-1), (2i+1)\}$, $t \in \mathbb{N}$

ý siendo: $i = \frac{1}{2}\varphi - 1$ si: $p \equiv 1 \pmod 4$

$i = \frac{1}{2}(\varphi-1)$ si: $p \equiv 3 \pmod 4$

entonces se cumple que:

si: $p \not\equiv 5 \pmod 8 \Rightarrow \left(\prod_{t=0}^{i}(2t+1), \rho\ !\right)^2 \equiv \sigma \pmod p$ **

si y sólo si p es primo impar

si: $p \equiv 5 \pmod 8 \Rightarrow [(2)^{\rho}]^2 \equiv \sigma \pmod p$ $\forall$ p primo impar

siendo: $\sigma = -1$ si: $p \equiv 1 \pmod 4$

$\sigma = -2$ si: $p \equiv 3 \pmod 8$

$\sigma = +2$ si: $p \equiv 7 \pmod 8$

Por lo cual, se denotará por $\alpha \in (1,p-1)$ / $\forall$ p primo impar

Siendo: $\alpha \equiv \left(\prod_{t=0}^{i}(2t+1), \rho\ !\right) \pmod p$ ** si: $p \not\equiv 5 \pmod 8$

$\alpha \equiv [(2)^{\rho}] \pmod p$ si: $p \equiv 5 \pmod 8$

/ $\alpha^2 \equiv \sigma \pmod p$, siendo: $\sigma \in$ residuo cuadrático en $\mathbb{Z}/p$

[1] $\sigma \in$ residuo cuadrático en $\mathbb{Z}/p$ siempre que p sea primo, ý σ puede ser (ó no) residuo cuadrático en $\mathbb{Z}/p$ si p es compuesto.

[2] recuérdese que: σ puede ser (ó no) residuo cuadrático en $\mathbb{Z}/p$ si p es compuesto.

En tales casos denotaremos como: β, $(p-\beta)$, β', $(p-\beta')$,..., β'^{w}, $(p-\beta'^{w})$ a las raíces de σ en Z/p (en caso de existir). y como: β^* a una de ellas cualquiera sin especificar. Y **no** por el valor α para diferenciar ambos casos (primo/compuesto)

[3] si p es compuesto impar tenemos que α no existe**. Pues no se cumplen las congruencias expuestas en las ecuaciones anteriores.

//

Proposición 1ra) Sea $p \in \mathbb{Z}$, $p>0 \wedge p \in$ impar / denotaremos por $\varphi \in \mathbb{N}$ /

$p = 2\varphi+1$ de forma que, por el teorema de Wilson:

$(p-1)! \equiv -1 \pmod p$ si ý sólo si p es primo.

- **...**tenemos equivalentemente que:

  $[p-1](p-2)! \equiv -1 \pmod p$ syss: p es primo.

- suponiendo que tomado p primo particular, entonces es trivial que:

  $\exists\ (a)^{-1}\ \forall a \in [1,p-1]$ / $a \cdot (a)^{-1} \equiv 1 \pmod p$ de forma que:

- aplicamos $(p-1)^{-1}$, a nuestra ecuación modular, obteniendo que:

  $(p-2)! \equiv +1 \pmod p$ syss: p es primo.

- es trivial que: $p-2 = 2\varphi-1 \Rightarrow$ equivalentemente tenemos que:

  $(2\varphi-1)! \equiv 1 \pmod p$ syss: p es primo.

Proposición 2da) equivalentemente resultará que:

$[2\varphi-1](2\varphi-2)! \equiv 1 \pmod p$ syss: p es primo.

es trivial que: $2^{-1} \equiv -\varphi \pmod p$, $p = 2\varphi +1$

$\varphi^{-1} \equiv -2 \pmod p$

aplicaremos un proceso de iteración semejante a la operación realizada tal que:

1ro° aplic. $(2)^{-1} \Rightarrow [\varphi+\varphi](2\varphi-2)! \equiv (2)^{-1} \pmod p$ syss: p es primo.

(es trivial que: $(2)^{-1}[2\varphi-1] \equiv [\varphi+\varphi] \pmod p$)

$\Leftrightarrow$ $[2\varphi](2\varphi-2)! \equiv (2)^{-1} \equiv -\varphi \pmod p$ syss: p es primo.

$p = 2\varphi+1 \Rightarrow 2\varphi = p-1$ / en $\mathbb{Z}/p \Rightarrow 2\varphi \equiv -1 \pmod p$

aplic. $(\varphi)^{-1} \Rightarrow [2](2\varphi-2)! \equiv -2(2)^{-1} \pmod p$ syss: p es primo.

$\Leftrightarrow [2][\ 2\varphi-2](2\varphi-3)! \equiv -1 \pmod p$* syss: p es primo.

2do° aplic. $(2)^{-1}$ / $(2)^{-1} \equiv -\varphi \pmod p \Rightarrow$

$\Leftrightarrow$ $[2][\ \varphi+2\varphi](2\varphi-3)! \equiv \varphi \pmod p$* syss: p es primo.

aplic. $(\varphi)^{-1}$ / $(\varphi)^{-1} \equiv -2 \pmod p \Rightarrow$

$\Leftrightarrow$ $[2 \cdot 3](2\varphi-3)! \equiv 1 \pmod p$ syss: p es primo.

$\Leftrightarrow$ $[2 \cdot 3][\ 2\varphi-3](2\varphi-4)! \equiv 1 \pmod p$** syss: p es primo.

3ro° aplic. $(2)^{-1} / (2)^{-1} \equiv -\varphi \pmod p$** $\Rightarrow$

$\Leftrightarrow [2 \bullet 3][\varphi+3\varphi](2\varphi-4)! \equiv -\varphi \pmod p$ syss: p es primo.

aplic. $(\varphi)^{-1} / (\varphi)^{-1} \equiv -2 \pmod p$ $\Rightarrow$

$\Leftrightarrow [2 \bullet 3 \bullet 4](2\varphi-4)! \equiv 2\varphi \equiv -1 \pmod p$ syss: p es primo.

(...)

de forma que realizadas i-ésimas iteraciones obtendríamos equivalentemente:

$$(i)!(2\varphi-i)! \equiv \{-1\}^{(i+1)} \pmod p \text{ syss: p es primo. } \forall i \in \mathbb{N}$$

demostración: tenemos que la expresión anterior es equivalente a:

$(i)![2\varphi-i] \bullet (2\varphi-[i+1])! \equiv \{-1\}^{(i+1)} \pmod p$ syss: p es primo.

aplic. $(2)^{-1} / (2)^{-1} \equiv -\varphi \pmod p$ $\Rightarrow$

$\Leftrightarrow (i)![\varphi+\varphi i] \bullet (2\varphi-[i+1])! \equiv \{-1\}^{(i+1)} \bullet (-\varphi) \pmod p$ syss: p es primo.

aplic. $(\varphi)^{-1} / (\varphi)^{-1} \equiv -2 \pmod p$ $\Rightarrow$

$\Leftrightarrow (i)![i+1] \bullet (2\varphi-[i+1])! \equiv \{-1\}^{(i+1)} \bullet (-1) \pmod p$ syss: p es primo.

$\Leftrightarrow (i+1)! \bullet (2\varphi-[i+1])! \equiv \{-1\}^{(i+2)} \pmod p$ syss: p es primo.

denotamos por $j=i+1$ /

$\Leftrightarrow (j)! \bullet (2\varphi-j)! \equiv \{-1\}^{(j+1)} \pmod p$ syss: p es primo. $\forall j \in \mathbb{N}$

fórmula equivalente.

Proposición 3ra) Sea $i = \varphi$ entonces por lo obtenido anteriormente resulta que:

$\Leftrightarrow (\varphi)!(2\varphi-\varphi)! \equiv \{-1\}^{(\varphi+1)} \pmod p$ syss: p es primo.

$\Leftrightarrow (\varphi)!(\varphi)! \equiv \{-1\}^{(\varphi+1)} \pmod p$ syss: p es primo.

$$\Leftrightarrow \{(\varphi)!\}^2 \equiv \{-1\}^{(\varphi+1)} \pmod p \text{ syss: p es primo.}$$

Proposición 4ta) Sea $n\in \mathbb{N}$, entonces es trivial que:

$$\{(\varphi)!\}^2 = \{-1\}^{(\varphi+1)} + p\bullet n, \text{ (para algún valor n)}$$

$$\Rightarrow (\varphi)! = \left(\{-1\}^{(\varphi+1)} + p\bullet n\right)^{1/2}$$

pudiendo expresar en $\mathbb{Z}/p$ que: $(\varphi)! \equiv a \pmod p$, $a\in [1,p-1]$

tal que: $a^2 \equiv \{-1\}^{(\varphi+1)} \pmod p$ syss: p es primo.

es decir: $\left(\{-1\}^{(\varphi+1)}\right)$ es un residuo cuadrático en $\mathbb{Z}/p$ porque:

$((\varphi)!)^2$ es un residuo cuadrático en $\mathbb{Z}/p$, pues es un cuadrado perfecto

denotaremos por $\varepsilon\in \mathbb{Z} \;/\; \pm\varepsilon = \left(\{-1\}^{(\varphi+1)} + p\bullet n\right)^{1/2}$

para comodidad y abreviaturas gráficas, de modo que podemos expresar que:

$\{(\varphi)!\} \equiv \pm\varepsilon \pmod p$ syss: p es primo.

Proposición 5ta) Teníamos de la proposición anterior que:

$\{(\varphi)!\} \equiv \{(\varphi)\}\bullet\{(\varphi-1)!\} \equiv \pm\varepsilon \pmod p$ syss: p es primo.

siendo: $\pm\varepsilon = \left(\{-1\}^{(\varphi+1)} + p\bullet n\right)^{1/2}\in \mathbb{Z} \wedge \{(\varphi)!\}^2 = \{-1\}^{(\varphi+1)} + p\bullet n$, $n\in \mathbb{N}$.

como sabemos que: $p = 2\varphi + 1 \;/\; 2^{-1} \equiv -\varphi \pmod p$

$$\varphi^{-1} \equiv -2 \pmod p$$

aplicando φ^{-1} a ambas partes de la congruencia, obtendremos:

$\{(\varphi-1)!\} \equiv \pm\varepsilon(-2) \pmod p$ syss: p es primo. (**[1])

Sea la aplicación $[\wedge 2]$ (elevando al cuadrado) obteniendo que:

$\{(\varphi-1)!\}^2 \equiv \{\pm\varepsilon\}^2(-2)^2 \pmod p$ syss: p es primo.

$\Leftrightarrow \{(\varphi-1)!\}^2 \equiv \left(\{-1\}^{(\varphi+1)} + p\bullet n\right)(-2)^2 \pmod p$ syss: p es primo.

$\Leftrightarrow \{(\varphi-1)!\}^2 \equiv 4\left(\{-1\}^{(\varphi+1)}\right) \pmod p$ syss: p es primo.

Proposición 6ta) De la proposición anterior y mediante un proceso iterativo equivalentemente, tendremos que:

$\{(\varphi-1)!\} \equiv \pm\varepsilon(-2) \pmod p$ syss: p es primo.

$\Leftrightarrow [\varphi-1](\varphi-2)! \equiv (-2)\{\pm\varepsilon\} \pmod p$ syss: p es primo.

siendo: $\pm\varepsilon = \left(\{-1\}^{(\varphi+1)} + p\bullet n\right)^{1/2}\in \mathbb{Z}$

aplic. $(2)^{-1} / (2)^{-1} \equiv -\varphi \pmod p \Rightarrow$

$\Leftrightarrow (2)^{-1}[\varphi-1](\varphi-2)! \equiv (-1)\{\pm\mathfrak{E}\} \pmod p$ syss: p es primo. (ver: **[1] pág anterior.)

Inciso importante:

$$(2)^{-1}[\varphi-k] \equiv (2)^{-1}\{-2^{-1}-k\} \pmod p,\ k \in \mathbb{N}$$

sabemos que $(2)^{-1} \equiv -\varphi \pmod p$ (ver: proposición 2da)

$$\Leftrightarrow (2)^{-1}[\varphi-k] \equiv (2)^{-1}\{-2^{-1}-k\} \equiv -2^{-1}\{2^{-1}+k\} \equiv \varphi\{2^{-1}+k\} \pmod p,\ k \in \mathbb{N}$$

$$\boxed{\Leftrightarrow (2)^{-1}[\varphi-k] \equiv \{k+2^{-1}\}\varphi \pmod p,\ k \in \mathbb{N}}$$

además es trivial que: $\{k+2^{-1}\} \equiv \{2k+1\}(2)^{-1} \pmod p$

◦ Sea k=1, tendremos que:

$$\Leftrightarrow (2)^{-1}[\varphi-1] \equiv -\varphi[\varphi-1] \equiv [1-\varphi]\varphi \equiv \{1+2^{-1}\}\varphi \pmod p$$

$$\Leftrightarrow (2)^{-1}[\varphi-1] \equiv \{\underline{1}+2^{-1}\}\varphi \equiv \{\underline{2}+1\}\underline{(2)^{-1}}\varphi \equiv \{3\}(2)^{-1}\varphi \pmod p$$

de forma que **[1]: $\underline{(2)^{-1}[\varphi-1]}(\varphi-2)! \equiv (-1)\{\pm\mathfrak{E}\} \pmod p$ syss: p es primo.

resulta equivalente a: $\{3\}(2)^{-1}\varphi(\varphi-2)! \equiv (-1)\{\pm\mathfrak{E}\} \pmod p$ syss: p es primo.

como: $(2)^{-1} \equiv -\varphi \pmod p \Rightarrow (2) \equiv -\varphi^{-1} \pmod p \Rightarrow -2 \equiv \varphi^{-1} \pmod p$

aplicando por $[\varphi^{-1}]$:

$$\Leftrightarrow \{3\}(2)^{-1}(\varphi-2)! \equiv (2)\{\pm\mathfrak{E}\} \pmod p \text{ syss: p es primo.}$$

$$\Leftrightarrow \{3\}(2)^{-1}[\varphi-2](\varphi-3)! \equiv (2)\{\pm\mathfrak{E}\} \pmod p \text{**[2] syss: p es primo.}$$

siendo: $\pm\mathfrak{E} = \left(\{-1\}^{(\varphi+1)} + p \bullet n\right)^{1/2}$

◦ Sea ahora k=2, tendremos que:

como: $(2)^{-1}[\varphi-k] \equiv \{k+2^{-1}\}\varphi \pmod p,\ k \in \mathbb{N}$

$\Rightarrow (2)^{-1}[\varphi-2] \equiv \{2+2^{-1}\}\varphi \pmod p$

$\Leftrightarrow (2)^{-1}[\varphi-2] \equiv \{\underline{2}+2^{-1}\}\varphi \equiv \{\underline{4}+1\}\underline{2^{-1}}\varphi \equiv \{5\}(2)^{-1}\varphi \pmod p$

de forma que: $\{3\}\underline{\mathbf{(2)^{-1}[\varphi-2]}}(\varphi-3)\mathbf{!} \equiv \mathbf{(}2\mathbf{)}\{\pm\boldsymbol{\varepsilon}\} \pmod p$**[2] syss: p es primo.
es equivalente a:

$\Leftrightarrow \{3\}\{5\}\mathbf{(2)^{-1}}\varphi\,(\varphi-3)\mathbf{!} \equiv \mathbf{(}2\mathbf{)}\{\pm\boldsymbol{\varepsilon}\} \pmod p$ syss: p es primo.

como: $\varphi^{-1} \equiv -2 \pmod p$ ý aplicando por $[\varphi^{-1}]$, tenemos que:

$\Leftrightarrow \{3\bullet 5\}\mathbf{(2)^{-1}}(\varphi-3)\mathbf{!} \equiv \mathbf{[-2^2]}\{\pm\boldsymbol{\varepsilon}\} \pmod p$ syss: p es primo.

$\Leftrightarrow \{3\bullet 5\}\mathbf{(2)^{-1}}[\varphi-3](\varphi-4)\mathbf{!} \equiv \mathbf{[-2^2]}\{\pm\boldsymbol{\varepsilon}\} \pmod p$ syss: p es primo.

◦ Sea ahora k=3, tendremos que:

como: $(2)^{-1}[\varphi-k] \equiv \{k+2^{-1}\}\varphi \pmod p$, $k\in\mathbb{N}$

$\Rightarrow (2)^{-1}[\varphi-3] \equiv \{3+2^{-1}\}\varphi \pmod p$

$\Leftrightarrow (2)^{-1}[\varphi-3] \equiv \{\underline{\mathbf{3}}+2^{-1}\}\varphi \equiv \{\underline{\mathbf{6}}+1\}\underline{2^{-1}}\varphi \equiv \{7\}\mathbf{(2)^{-1}}\varphi \pmod p$

de forma que: $\{3\bullet 5\}\underline{\mathbf{(2)^{-1}[\varphi-3]}}(\varphi-4)\mathbf{!} \equiv \mathbf{[-2^2]}\{\pm\boldsymbol{\varepsilon}\} \pmod p$ syss: p es primo.
es equivalente a:

$\Leftrightarrow \{3\}\{5\}\{7\}\mathbf{(2)^{-1}}\varphi\,(\varphi-4)\mathbf{!} \equiv \mathbf{[-2^2]}\{\pm\boldsymbol{\varepsilon}\} \pmod p$ syss: p es primo.

como: $\varphi^{-1} \equiv -2 \pmod p$ ý aplicando por $[\varphi^{-1}]$, tenemos que:

$\Leftrightarrow \{3\bullet 5\bullet 7\}\mathbf{(2)^{-1}}(\varphi-4)\mathbf{!} \equiv \mathbf{(-2)[-2^2]}\{\pm\boldsymbol{\varepsilon}\} \pmod p$ syss: p es primo.

$\Leftrightarrow \{3\bullet 5\bullet 7\}\mathbf{(2)^{-1}}(\varphi-4)\mathbf{!} \equiv \mathbf{[2^3]}\{\pm\boldsymbol{\varepsilon}\} \pmod p$ syss: p es primo.

$\Leftrightarrow \{3\bullet 5\bullet 7\}\mathbf{(2)^{-1}}[\varphi-4](\varphi-5)\mathbf{!} \equiv \mathbf{[2^3]}\{\pm\boldsymbol{\varepsilon}\} \pmod p$ syss: p es primo.

(...)

◦ Realizando las iteraciones precisas, obtenemos para el i-ésimo término que:

$\{(2i-1)(2i-3)(2i-5)\mathbf{...}(5)(3)\}\mathbf{(2)^{-1}}[\varphi-i]\bullet(\varphi-[i+1])\mathbf{!} \equiv\mathbf{...}$

$\mathbf{...}\equiv (-1)^i\mathbf{[2^{i-1}]}\{\pm\boldsymbol{\varepsilon}\} \pmod p$ syss: p es primo. (** [3])

equivalentemente:

$$\boxed{\{(2i-1)(2i-3)(2i-5)\mathbf{...}(5)(3)\underline{(1)}\}\bullet(\varphi-i)\mathbf{!} \equiv (-1)^i\mathbf{[2^i]}\{\pm\boldsymbol{\varepsilon}\} \pmod p}$$

syss: p es primo.

siendo: $\pm\boldsymbol{\varepsilon} = \left(\{-1\}^{(\varphi+1)} + p\bullet n\right)^{1/2} \in \mathbb{Z}$, $\forall i \in \mathbb{N}\backslash\{0\}$

(omitimos la demostración por resultar trivial por inducción.)

Proposición 7ma) Tomando de la ecuación modular anterior el caso concreto tal que i = φ, tendremos equivalentemente que:

$\{(2\varphi-1)(2\varphi-3)(2\varphi-5)...(5)(3)\underline{(1)}\}\bullet(\varphi-\varphi)! \equiv (-1)^{\varphi}[2^{\varphi}]\{\pm\varepsilon\} \pmod p$

syss: p es primo.

cláramente: $(0)! = 1$

$\Leftrightarrow \{(2\varphi-1)(2\varphi-3)(2\varphi-5)...(5)(3)\underline{(1)}\} \equiv (-1)^{\varphi}[2^{\varphi}]\{\pm\varepsilon\} \pmod p$

syss: p es primo. Siendo: $\pm\varepsilon = \left(\{-1\}^{(\varphi+1)} + p\bullet n\right)^{1/2} \in \mathbb{Z}$, $\forall i \in \mathbb{N}\backslash\{0\}$

Inciso importante:

Es claro que: $(p-1)! \equiv (-1) \pmod p$ syss: p es primo. (t^{ma} Wilson)

Ý habiamos denotado que: $p = 2\varphi+1 \Rightarrow$ podemos expresar que:

$(p-1)! \equiv (2\varphi)! \equiv (-1) \pmod p$

$\Leftrightarrow [2\varphi](2\varphi-1)! \equiv (-1) \pmod p$ syss: p es primo.

Ahora bien: $2\varphi \equiv (-1) \pmod p$, $p = 2\varphi+1$* trivial.

como suponemos que p es primo. $\Rightarrow \forall a \in \mathbb{N}, a \in (0,p) \Rightarrow$

$\exists\ a^{-1}$ único / $a\bullet a^{-1} \equiv 1 \pmod p \Rightarrow \exists\ (2\varphi)^{-1}$

con: $(2\varphi)^{-1} \equiv 2^{-1}\varphi^{-1} \pmod p$ ý es trivial (*) que: $(2\varphi)^{-1} \equiv (-1) \pmod p$

como teníamos que: $[2\varphi](2\varphi-1)! \equiv (-1) \pmod p$ syss: p es primo.

Aplicando $(2\varphi)^{-1}$ obtendremos que:

$$(2\varphi-1)! \equiv 1 \pmod p \text{ syss: p es primo.}$$

Corolario) podemos argumentar equivalentemente que:

$(2\varphi-1)!\bullet\{(2\varphi-1)(2\varphi-3)(2\varphi-5)...(5\bullet 3\bullet 1)\}^{-1} \equiv (2\varphi-2)(2\varphi-4)(2\varphi-6)...(4\bullet 2) \equiv ..$

$...\equiv \left\{(-1)^{\varphi}[2^{\varphi}]\{\pm\varepsilon\}\right\}^{-1} \pmod p$ syss: p es primo.

pues de la proposición 6ta pág anterior (** [3]) teníamos que:

$\{(2i-1)(2i-3)(2i-5)...(5)(3)\underline{(1)}\}\bullet(\varphi-i)! \equiv (-1)^{i}[2^{i}]\{\pm\varepsilon\} \pmod p$ trivial

$\Rightarrow (2\varphi-2)(2\varphi-4)(2\varphi-6)...(6\bullet 4\bullet 2) \equiv (-1)^{-\varphi}[2^{-\varphi}]\{\pm\varepsilon\}^{-1} \pmod p$

syss: p es primo.

◦ Teníamos que: $(2)^{-1} \equiv -\varphi \pmod p$ (prop. 2da pág 11) $\wedge$ $(-1)^{-1} \equiv (-1) \pmod p$
de forma que resulta equivalente que:

$$(2\varphi-2)(2\varphi-4)(2\varphi-6)\ldots(6 \bullet 4 \bullet 2) \equiv (-1)^{\varphi}[-\varphi]^{\varphi}\{\pm\boldsymbol{\varepsilon}\}^{-1} \pmod p$$

syss: p es primo. $\wedge$ siendo: $\pm\boldsymbol{\varepsilon} = \left(\{-1\}^{(\varphi+1)} + p \bullet n\right)^{1/2} \in \mathbb{Z}$

<u>Proposición 8va)</u> Sea {An} = {2φ-2, 2φ-4, 2φ-6,..., 6, 4, 2},
sucesión de elementos pares.
entonces: #{An} = Card(An) = (φ-1) = $\frac{1}{2}(2\varphi-2)$ trivial.

de forma que, aplicando $\left\{2^{(\varphi-1)}\right\}^{-1}$ a la ecuación modular resultante del corolario anterior, obteniéndose que:

$$(2\varphi-2)(2\varphi-4)(2\varphi-6)\ldots(6 \bullet 4 \bullet 2) \bullet \left\{2^{(\varphi-1)}\right\}^{-1} \equiv \left\{2^{(\varphi-1)}\right\}^{-1}(-1)^{\varphi}[-\varphi]^{\varphi}\{\pm\boldsymbol{\varepsilon}\}^{-1} \pmod p$$

$$\Leftrightarrow (\varphi-1)(\varphi-2)(\varphi-3)\ldots(3 \bullet 2 \bullet 1) \equiv \left\{2^{(\varphi-1)}\right\}^{-1}(-1)^{\varphi}[-\varphi]^{\varphi}\{\pm\boldsymbol{\varepsilon}\}^{-1} \pmod p$$

syss: p es primo. $\wedge$ siendo: $\pm\boldsymbol{\varepsilon} = \left(\{-1\}^{(\varphi+1)} + p \bullet n\right)^{1/2} \in \mathbb{Z}$

obteniendo equivalentemente que:

$$\Leftrightarrow (\varphi-1)! \equiv \left\{2^{(\varphi-1)}\right\}^{-1}(-1)^{\varphi}[-\varphi]^{\varphi}\{\pm\boldsymbol{\varepsilon}\}^{-1} \pmod p$$

syss: p es primo. $\wedge$ siendo: $\pm\boldsymbol{\varepsilon} = \left(\{-1\}^{(\varphi+1)} + p \bullet n\right)^{1/2} \in \mathbb{Z}$

de la proposición 2da pág 11, tenemos que: $2^{-1} \equiv -\varphi \pmod p$, $p = 2\varphi+1$

de forma que: $\Leftrightarrow \left\{2^{(\varphi-1)}\right\}^{-1} \equiv [-\varphi]^{(\varphi-1)} \pmod p$

$\wedge \Rightarrow (\varphi-1)! \equiv (-1)^{\varphi}[-\varphi]^{(\varphi-1)}[-\varphi]^{\varphi}\{\pm\boldsymbol{\varepsilon}\}^{-1} \pmod p$

$$\Leftrightarrow (\varphi-1)! \equiv (-1)^{\varphi}[-\varphi]^{(2\varphi-1)}\{\pm\boldsymbol{\varepsilon}\}^{-1} \pmod p$$

syss: p es primo. $\wedge$ siendo: $\pm\boldsymbol{\varepsilon} = \left(\{-1\}^{(\varphi+1)} + p \bullet n\right)^{1/2} \in \mathbb{Z}$

Inciso previo: por la proposición 2da. pág 11. resulta que:

$$2^{-1} \equiv -\varphi \pmod{p} \Rightarrow$$

$\Leftrightarrow [-\varphi]^{(2\varphi-1)} \equiv [2]^{-(2\varphi-1)} \equiv [2]^{-(p-2)} \pmod{p}$, por ser: $p = 2\varphi+1$

sabemos que por el pequeño t^{ma} de Fermat: $2^{(p-1)} \equiv 1 \pmod{p}$ $\forall$ p primo.

$\Leftrightarrow 2^{-(p-1)} \equiv 1 \pmod{p}$ $\forall$ p primo. $\wedge$ aplicando [$\bullet$ 2] tenemos:

$\Leftrightarrow 2^{-(p-2)} \equiv 2 \pmod{p}$ $\forall$ p primo.

(...)

$\Rightarrow (\varphi-1)! \equiv (-1)^{\varphi}[-\varphi]^{(2\varphi-1)}\{\pm\varepsilon\}^{-1} \equiv (-1)^{\varphi}[2]^{-(p-2)}\{\pm\varepsilon\}^{-1} \equiv$...

...$\equiv (-1)^{\varphi}[2]\{\pm\varepsilon\}^{-1} \pmod{p}$ si y sólo si p es primo.

$$\Leftrightarrow (\varphi-1)! \equiv (-1)^{\varphi}[2]\{\pm\varepsilon\}^{-1} \pmod{p}$$

syss: p es primo. $\wedge$ siendo: $\pm\varepsilon = \left(\{-1\}^{(\varphi+1)} + p \bullet n\right)^{1/2} \in \mathbb{Z}$

Corolario) Aplicando [%^{2}] (elevando al cuadrado) ambas partes de la ecuación modular resultante, tendremos que:

$\{(\varphi-1)!\}^2 \equiv (-1)^{2\varphi}[4]\{\pm\varepsilon\}^{-2} \equiv (-1)^{2\varphi}[4]\{\pm\varepsilon^2\}^{-1} \pmod{p}$

como: $\pm\varepsilon = \left(\{-1\}^{(\varphi+1)} + p \bullet n\right)^{1/2} \Rightarrow \{\pm\varepsilon^2\} = \left(\{-1\}^{(\varphi+1)} + p \bullet n\right)$

$\Rightarrow \{(\varphi-1)!\}^2 \equiv (-1)^{2\varphi}[4]\left(\{-1\}^{(\varphi+1)} + p \bullet n\right)^{-1} \pmod{p}$

$\Leftrightarrow \{(\varphi-1)!\}^2 \equiv (-1)^{2\varphi}[4]\left(\{-1\}^{(\varphi+1)}\right)^{-1} \equiv (-1)^{2\varphi}\{-1\}^{-(\varphi+1)}[4] \pmod{p}$

$\Leftrightarrow \{(\varphi-1)!\}^2 \equiv \{-1\}^{(\varphi-1)}[4] \pmod{p}$, syss: p es primo.

(ver proposición 5ta. Pág. 13)

Ojo: $\{-1\}^{(\varphi-1)} \equiv \{-1\}^{(\varphi+1)} \pmod{p}$

(en la prop. 5ta resultaba exponente $(\varphi+1)$, ambos resultados son equivalentes)

Proposición 9na) Por el Corolario anterior, podemos argumentar que:

$\{(\varphi-1)!\}^2 \equiv \{-1\}^{(\varphi-1)}[4] \pmod p$, syss: p es primo.

$\Leftrightarrow \{(\varphi-1)!\} \equiv \pm\{-1\}^{\{(\varphi-1)/2\}}[4]^{(1/2)} \pmod p$, syss: p es primo.

Corolario 1ro)

Del coeficiente $\pm\{-1\}^{\{(\varphi-1)/2\}}$ tenemos dos posibilidades: $2|(\varphi-1)$ ó $2\nmid(\varphi-1)$

i) $2|(\varphi-1) \Rightarrow \varphi\in$ impar $\Rightarrow p \equiv 3 \pmod 4$, trivial: $\varphi = 2n+1 \wedge p = 2\varphi+1$

$\Rightarrow p = 2(2n+1)+1 = \underline{4n+3}$

ii) $2\nmid(\varphi-1) \Rightarrow \varphi\in$ par $\Rightarrow p \equiv 1 \pmod 4$, trivial: $\varphi = 2n \wedge p = 2\varphi+1$

$\Rightarrow p = 2(2n)+1 = \underline{4n+1}$

además: $\Rightarrow 2|\varphi$ de forma que:

$\{(\varphi-1)!\} \equiv \pm\{-1\}^{\{(\varphi-1)/2\}}[4]^{(1/2)} \pmod p$

$\Leftrightarrow \{(\varphi-1)!\} \equiv \pm\{-1\}^{(\varphi/2)}\{-1\}^{(-1/2)}[2] \pmod p$

syss: p es primo.

entonces ha de existir un elemento $a\in (1,p-1) / \pm a \equiv \{-1\}^{(-1/2)} \pmod p$

demostración:

$\Leftrightarrow \{\pm a\}^2 \equiv \{-1\}^{\{-1\}} \equiv \{-1\} \pmod p$

Pero sabemos por el apartado iv) (pág. 3) [siendo p primo] que: si $p \equiv 1 \pmod 4$ ý m es un residuo cuadrático en $(\mathbb{Z}/p)$, entonces $(-m)$ es también un residuo cuadrático en $(\mathbb{Z}/p)$, ý como es trivial que 1 es un residuo cuadrático (1 es cuadrado perfecto) en $(\mathbb{Z}/p)$ $\Rightarrow$ -1 también lo es.

Por tanto $\exists\ a\in (1,p-1) / \pm a \equiv \{-1\}^{\{-1/2\}} \pmod p$ QED.

Corolario 2do)

De la proposición 8va. (pág 18) teníamos que:

$$(\varphi-1)! \equiv (-1)^{\varphi}[2]\{\pm\varepsilon\}^{-1} \pmod p$$

syss: p es primo. $\wedge$ siendo: $\pm\varepsilon = \left(\{-1\}^{(\varphi+1)} + p \bullet n\right)^{1/2} \in \mathbb{Z}$

caso i) $\varphi \in$ impar ($\Rightarrow p \equiv 3 \pmod 4$)

$$\Rightarrow (\varphi-1)! \equiv -2\{\pm\varepsilon\}^{-1} \pmod p$$

$$\Leftrightarrow (\varphi-1)! \equiv -2\{\left(\{-1\}^{(\varphi+1)} + p \bullet n\right)^{1/2}\}^{-1} \pmod p$$

$$\Leftrightarrow (\varphi-1)! \equiv -2\{\left(\{-1\}^{(\varphi+1)}\right)^{1/2}\}^{-1} \pmod p, \text{ como } (\varphi+1) \in \text{ par}$$

$$\Leftrightarrow (\varphi-1)! \equiv -2\{(1)^{1/2}\}^{-1} \equiv -2\{(1)^{-1}\}^{1/2} \pmod p, \text{ ý como } 1^{-1} \equiv 1 \pmod p$$

$$\Leftrightarrow (\varphi-1)! \equiv -2(1)^{1/2} \pmod p$$

$$\Rightarrow \{(\varphi-1)!\}^2 \equiv 4 \pmod p, \text{ syss: p es primo.}$$

caso ii) $\varphi \in$ par ($\Rightarrow p \equiv 1 \pmod 4$)

$$\Rightarrow (\varphi-1)! \equiv 2\{\pm\varepsilon\}^{-1} \pmod p$$

$$\Leftrightarrow (\varphi-1)! \equiv 2\{\left(\{-1\}^{(\varphi+1)} + p \bullet n\right)^{1/2}\}^{-1} \pmod p$$

$$\Leftrightarrow (\varphi-1)! \equiv 2\{\left(\{-1\}^{(\varphi+1)}\right)^{1/2}\}^{-1} \pmod p, \text{ como } (\varphi+1) \in \text{ impar}$$

$$\Leftrightarrow (\varphi-1)! \equiv 2\{(-1)^{1/2}\}^{-1} \equiv 2\{(-1)^{-1}\}^{1/2} \pmod p, \text{ ý como } -1^{-1} \equiv -1 \pmod p$$

$$\Leftrightarrow (\varphi-1)! \equiv -2(-1)^{1/2} \pmod p$$

$$\Rightarrow \{(\varphi-1)!\}^2 \equiv -4 \pmod p, \text{ syss: p es primo.}$$

Inciso: Si p es primo. por lo general: $(\varphi-1)! \equiv 0 \pmod p$

excepto casos, como p = 9 que no es primo / (φ=4)

$$\Rightarrow (\varphi-1)! \equiv 3! \equiv 6 \pmod p.$$

Proposición 10ma)

i) Denotaremos por $\varphi = \psi + r$, $\varphi, \psi, r \in \mathbb{N}$

/ de forma trivial resulta que: $p = 2\varphi+1 = 2\psi+\{2r+1\}$

ii) Busquemos el valor ψ^{-1} / $2\psi \equiv -\{2r+1\}$ (mod p)

$\Rightarrow \psi \equiv -2^{-1} \bullet \{2r+1\}$ (mod p), trivialmente se resuelve que:

$\Leftrightarrow \psi^{-1} \equiv -2 \bullet \{2r+1\}^{-1}$ (mod p)

Nota: el valor: $\{2r+1\}^{-1}$ (mod p) puede no resultar factible en su obtención, pero será innecesaria la resolución del mismo para nuestros procedimientos. //

iii) de la proposición 4ta. (pág 13) resultaba que:

$(\varphi)! \equiv \pm\mathfrak{E}$ (mod p) syss: p es primo.

$$\text{siendo } \pm\mathfrak{E} = \left(\{-1\}^{(\varphi+1)} + p \bullet n\right)^{1/2} \in \mathbb{Z}$$

del aptdo ii. anterior resultará equivalente que:

$(\varphi)! \equiv (\psi+r)! \equiv [\psi+r](\psi+r-1)! \equiv \pm\mathfrak{E}$ (mod p), syss: p es primo.

iv) Sea $[\psi+r-\lambda]$, $\lambda \in \mathbb{N}$, aplicando ψ^{-1} / $\left(\psi^{-1} \equiv -2 \bullet \{2r+1\}^{-1}\right.$ (mod p) aptdo ii.$\left.\right)$ obtendremos equivalentemente que:

$\psi^{-1}[\psi+r-\lambda] \equiv 1+\psi^{-1}(r-\lambda)$ (mod p)

$\Leftrightarrow \psi^{-1}[\psi+r-\lambda] \equiv 1+(-2)\{2r+1\}^{-1}(r-\lambda)$ (mod p)

$\Leftrightarrow \psi^{-1}[\psi+r-\lambda] \equiv 1+\{2r+1\}^{-1}(-2r+2\lambda)$ (mod p)

$\Leftrightarrow \psi^{-1}[\psi+r-\lambda] \equiv 1+\{2r+1\}^{-1}(-2r\underline{-1}+2\lambda\underline{+1})$ (mod p), $\left(\{2r+1\}^{-1}(-2r\underline{-1}) \equiv \underline{-1}^{*} \bmod p\right)$

$\Leftrightarrow \psi^{-1}[\psi+r-\lambda] \equiv 1\underline{-1}^{*}+\{2r+1\}^{-1}(+2\lambda+1)$ (mod p)

$$\Rightarrow \psi^{-1}[\psi+r-\lambda] \equiv \{2r+1\}^{-1}(+2\lambda+1) \text{ (mod p)}, \ \forall p \in \mathbb{N}$$

Proposición 11ra) teníamos del aptdo iii) de la proposición anterior que:

$(\varphi)! \equiv (\psi+r)! \equiv [\psi+r](\psi+r-1)! \equiv \pm\mathfrak{E}$ (mod p), syss: p es primo.

como: $\varphi = \psi + r \wedge \varphi^{-1} \equiv -2$ (mod p) $\Rightarrow (\psi+r)^{-1} \equiv \varphi^{-1} \equiv -2$ (mod p)

$$\Rightarrow [\psi+r-1]! \equiv -2\{\pm\mathfrak{E}\} \text{ (mod p), syss: p es primo.}$$

◦ De forma equivalente tenemos que:

$[\psi+r-\underline{1}^{*}](\psi+r-2)! \equiv -2\{\pm\mathfrak{E}\}$ (mod p), syss: p es primo. $\lambda_1 = 1^{*}$

(λ definida en aptdo iv) proposición anterior)

Por lo obtenido en aptdo iv) proposición anterior /

$\psi^{-1}[\psi+r-\lambda] \equiv \{2r+1\}^{-1}(+2\lambda+1) \pmod p$, $\forall p \in \mathbb{N}$, entonces:

• aplicando ψ^{-1}, $\lambda=1^* \Rightarrow$

$\Rightarrow \psi^{-1}[\psi+r-\underline{1^*}](\psi+r-2)! \equiv -2\psi^{-1}\{\pm\mathcal{E}\} \pmod p$, syss: p es primo.

$\Leftrightarrow \{2r+1\}^{-1}(+2+1)[\psi+r-2]! \equiv -2\psi^{-1}\{\pm\mathcal{E}\} \pmod p$

syss: p es primo.

(pues: $\psi^{-1}[\psi+r-1] \equiv \{2r+1\}^{-1}(+2+1) \pmod p$)

• aplicando (-2): $\underline{(-2)\{2r+1\}^{-1}}(+3)[\psi+r-2]! \equiv 4\psi^{-1}\{\pm\mathcal{E}\} \pmod p$

(pues: $\psi^{-1} \equiv \underline{(-2)\{2r+1\}^{-1}} \pmod p$ ver aptdo ii) prop. anterior)

• aplicando ψ: $(3)[\psi+r-2]! \equiv 4\{\pm\mathcal{E}\} \pmod p$

$\Leftrightarrow (3)[\psi+r-\underline{2}^*](\psi+r-3)! \equiv 4\{\pm\mathcal{E}\} \pmod p$, syss: p es primo. $\lambda_2=2^*$

◦ <u>2da iteración:</u>

• aplicando ψ^{-1}, $\lambda=2^* \Rightarrow$

$\Rightarrow (3)\psi^{-1}[\psi+r-\underline{2}^*](\psi+r-3)! \equiv 4\psi^{-1}\{\pm\mathcal{E}\} \pmod p$, syss: p es primo.

$\Leftrightarrow (3)\{2r+1\}^{-1}(+2(2)+1)[\psi+r-3]! \equiv 4\psi^{-1}\{\pm\mathcal{E}\} \pmod p$

$\Leftrightarrow (3)\{2r+1\}^{-1}(5)[\psi+r-3](\psi+r-4)! \equiv 4\psi^{-1}\{\pm\mathcal{E}\} \pmod p$, syss: p es primo.

$\Leftrightarrow (3 \cdot 5)\{2r+1\}^{-1}[\psi+r-3](\psi+r-4)! \equiv 4\psi^{-1}\{\pm\mathcal{E}\} \pmod p$, syss: p es primo.

• aplicando (-2ψ):

$\Leftrightarrow (3 \cdot 5)[\psi+r-\underline{3}^*](\psi+r-4)! \equiv -2^{[3]}\{\pm\mathcal{E}\} \pmod p$, syss p es primo. $\lambda_3=3^*$

◦ <u>3ra iteración:</u>

• aplicando ψ^{-1}, $\lambda=3^* \Rightarrow$

$\Rightarrow (3 \cdot 5)\psi^{-1}[\psi+r-\underline{3}^*](\psi+r-4)! \equiv -2^{[3]}\psi^{-1}\{\pm\mathcal{E}\} \pmod p$, syss: p es primo.

$\Leftrightarrow (3 \cdot 5)\{2r+1\}^{-1}(+2(3)+1)[\psi+r-4]! \equiv -2^{[3]}\psi^{-1}\{\pm\mathcal{E}\} \pmod p$

$\Leftrightarrow (3 \cdot 5)\{2r+1\}^{-1}(7)[\psi+r-4](\psi+r-5)! \equiv -2^{[3]}\psi^{-1}\{\pm\mathcal{E}\} \pmod p$

syss: p es primo.

$\Leftrightarrow (3\cdot 5\cdot 7)\{2r+1\}^{-1}[\psi+r-4](\psi+r-5)! \equiv -2^{[3]}\psi^{-1}\{\pm\mathcal{E}\} \pmod p$ syss: p es primo.

$\cdot$ aplicando (-2ψ):

$\Leftrightarrow (3\cdot 5\cdot 7)[\psi+r-\underline{4}^*](\psi+r-5)! \equiv +2^{[4]}\{\pm\mathcal{E}\} \pmod p$, syss: p es primo. $\lambda_4=4^*$

(...)

◦ Obteniendo equivalentemente para la i-ésima iteración / $\forall i\in\mathbb{N}$

$\{3\cdot 5\cdot 7\cdot \ldots\cdot (2i-1)(2i+1)\}[\underline{\psi+r}-(i+1)]! \equiv (-1)^{(i+1)}\cdot 2^{[i+1]}\{\pm\mathcal{E}\} \pmod p$, $\varphi = \underline{\psi+r}$

$$\Leftrightarrow \{3\cdot 5\cdot 7\cdot \ldots\cdot (2i-1)(2i+1)\}[\varphi-(i+1)]! \equiv (-1)^{(i+1)}\cdot 2^{[i+1]}\{\pm\mathcal{E}\} \pmod p^{**}$$

syss: p es primo. $\wedge$ siendo $\pm\mathcal{E} = \left(\{-1\}^{(\varphi+1)} + p\bullet n\right)^{1/2}\in \mathbb{Z}$

(trivial por inducción, omitimos la demostración)

<u>Proposición 12da)</u> es trivial que:

$\{2\cdot 4\cdot 6\cdot 8\cdot \ldots\cdot (2i-2)\cdot (2i)\} = 2^i[1\cdot 2\cdot 3\cdot 4\cdot 5\cdot \ldots\cdot (i-1)(i)] = 2^i(i)!$ <u>trivial</u>

omitimos demostración

aplicándo $[\ 2^i(i)!\ ]$ a la fórmula de la proposición anterior**, se resuelve que:

$$(2i+1)![\varphi-(i+1)]! \equiv (-1)^{(i+1)}\cdot 2^{[2i+1]}(i)!\{\pm\mathcal{E}\} \pmod p,\ \forall i\in\mathbb{N}$$

syss: p es primo. $\wedge$ siendo $\pm\mathcal{E} = \left(\{-1\}^{(\varphi+1)} + p\bullet n\right)^{1/2}\in \mathbb{Z}$

<u>Proposición 13ra)</u> (<u>Omitible</u>) a modo de corolario.

Supongamos $i = \varphi-1$, entonces la ecuación modular anterior...

$\Leftrightarrow (2[\varphi-1]+1)![\varphi-([\varphi-1]+1)]! \equiv (-1)^{([\varphi-1]+1)}\cdot 2^{[2|\varphi-1|+1]}(\varphi-1)!\{\pm\mathcal{E}\} \pmod p$

$\Leftrightarrow (2\varphi-1)![0]! \equiv (-1)^{\varphi}\cdot 2^{(2\varphi-1)}(\varphi-1)!\{\pm\mathcal{E}\} \pmod p$, syss: p es primo.

como: $(0)! = 1$

$\Leftrightarrow (2\varphi-1)! \equiv (-1)^{\varphi}\cdot 2^{(2\varphi-1)}(\varphi-1)!\{\pm\mathcal{E}\} \pmod p$, syss: p es primo.

Ahora bien: $p = 2\varphi+1 \Rightarrow 2\varphi = p-1 \Rightarrow (2\varphi)! = (p-1)!$

$\Rightarrow (2\varphi-1)! = (p-2)! = (p-2)!(p-1)(p-1)^{-1} = (p-1)!(p-1)^{-1}$

Tal que en $\mathbb{Z}/p$ resulta que:

$(2\varphi-1)! \equiv (p-1)!(p-1)^{-1} \equiv (p-1)!(-1)^{-1} \equiv (p-1)!(-1) \pmod p$

Por el t^{ma} de Wilson: $(p-1)! \equiv -1 \pmod p$ syss: p es primo.

$\Rightarrow (2\varphi-1)! \equiv 1 \pmod p$ syss: p es primo.

Por tanto resulta que:

$(2\varphi-1)! \equiv (-1)^{\varphi} \cdot 2^{(2\varphi-1)}(\varphi-1)!\{\pm\mathfrak{E}\} \pmod p$, p es primo.

es equivalente a:

$\Leftrightarrow (-1)^{\varphi} \cdot 2^{(2\varphi-1)}(\varphi-1)!\{\pm\mathfrak{E}\} \equiv 1 \pmod p^{*}$, p es primo.

◦ Además teníamos, (proposición 5ta. (**[1]) pág. 13) que:

$(\varphi-1)! \equiv -2\{\pm\mathfrak{E}\} \pmod p$, syss: p es primo.

De forma que equivalentemente tenemos que (*):

$\Leftrightarrow (-1)^{\varphi} \cdot 2^{(2\varphi-1)}(-2)\{\pm\mathfrak{E}\}^2 \equiv 1 \pmod p$, $\forall$ p primo.

(...) por el t^{ma} de Fermat: $2^{p-1} \equiv 1 \pmod p$, $\forall$ p primo.

como: $p = 2\varphi+1 \Rightarrow 2^{2\varphi} \equiv 1 \pmod p$, $\forall$ p primo. $\Rightarrow$

$\Rightarrow (-1)^{\varphi} \cdot 2^{2\varphi} \cdot 2^{-1}(-2)\{\pm\mathfrak{E}\}^2 \equiv 1 \pmod p$, $\forall$ p primo.

$\Leftrightarrow (-1)^{\varphi} \cdot 2^{-1}(-2)\{\pm\mathfrak{E}\}^2 \equiv 1 \pmod p$

como: $\pm\mathfrak{E} = \left(\{-1\}^{(\varphi+1)} + p \bullet n\right)^{1/2} \in \mathbb{Z} \Rightarrow$

$\Leftrightarrow (-1)^{\varphi} \cdot 2^{-1}(-2)\left(\{-1\}^{(\varphi+1)} + p \bullet n\right) \equiv 1 \pmod p$

$\Leftrightarrow (-1)^{\varphi} \cdot 2^{-1}(-2)\left(\{-1\}^{(\varphi+1)}\right) \equiv 1 \pmod p$

$\Leftrightarrow (-1)^{2\varphi+1} \cdot 2^{-1}(-2) \equiv 1 \pmod p$

$\Leftrightarrow (-1)^{2\varphi+2} \equiv (-1)^{2(\varphi+1)} \equiv 1 \pmod p$

trivial pues $2(\varphi+1) \in$ par $\Rightarrow$ todas las congruencias son correctas

Proposición 14ta) (Omitible) a modo de corolario.

Respecto a la proposición 11ra. tal que se resolvía que:

$\{3' 5' 7' ...' (2i-1)(2i+1)\}[\varphi-(i+1)]! \equiv (-1)^{(i+1)'} 2^{[i+1]}\{\pm\varepsilon\} \pmod p$

syss: p es primo. $\wedge$ siendo $\pm\varepsilon = \left(\{-1\}^{(\varphi+1)} + p \bullet n\right)^{1/2} \in \mathbb{Z}$

Supongamos $i = \varphi-1$ (como en la proposición anterior) obteniendo que:

$\Leftrightarrow \{3' 5' 7' ...' (2[\varphi-1]-1)(2[\varphi-1]+1)\}[\varphi-([\varphi-1]+1)]! \equiv ...$

$...\equiv (-1)^{(\varphi-1+1)'} 2^{[\varphi-1+1]}\{\pm\varepsilon\} \pmod p$

$\Leftrightarrow \{3' 5' 7' ...' (2\varphi-3)(2\varphi-1)\}[0]! \equiv (-1)^{\varphi'} 2^{\varphi}\{\pm\varepsilon\} \pmod p$

$\Leftrightarrow \{3' 5' 7' ...' (2\varphi-3)(2\varphi-1)\} \equiv (-1)^{\varphi'} 2^{\varphi}\{\pm\varepsilon\} \pmod p$ syss: p es primo.

(...) de la proposición 12da. resultaba que:

$\{2' 4' 6' 8' ...' (2i-2)' (2i)\} = 2^i(i)!$, ý como $i = \varphi-1$

$\Rightarrow$ aplicándola a la fórmula obtenemos la ecuación modular de la proposición 13ra.

$(2\varphi-1)! \equiv (-1)^{\varphi} \cdot 2^{(2^{\varphi}-1)}(\varphi-1)!\{\pm\varepsilon\} \pmod p$, syss: p es primo.

(omitimos más estudios a este respecto)

Proposición 15ta)

Inciso previo: De los resultados de las proposiciones anteriores, cabe destacar fundamentalmente, para las propiedades que derivan de las mismas, que:

Proposición 5ta.) $\{(\varphi-1)!\} \equiv \pm\varepsilon(-2) \pmod p$ syss: p es primo.

Proposición 11ra.)

$\{3' 5' 7' ...' (2i-1)(2i+1)\}[\varphi-(i+1)]! \equiv (-1)^{(i+1)'} 2^{[i+1]}\{\pm\varepsilon\} \pmod p$

syss: p es primo. $\wedge$ siendo $\pm\varepsilon = \left(\{-1\}^{(\varphi+1)} + p \bullet n\right)^{1/2}$

con: $(\varphi)! = \left(\{-1\}^{(\varphi+1)} + p \bullet n\right)^{1/2} \Rightarrow \{(\varphi)!\} \equiv \pm\varepsilon \pmod p$

syss: p es primo.

(ver proposición 4ta.)

' Expresaremos ahora por: $\rho \in \mathbb{N}$ / (*recordando que:* $p = 2\varphi+1$)

$\varphi = 2\rho$ si: $\varphi \in$ par $\Rightarrow p \equiv 1 \pmod 4$ $p = 4\rho + 1$

$\varphi = 2\rho + 1$ si: $\varphi \in$ impar $\Rightarrow p \equiv 3 \pmod 4$ $p = 4\rho + 3$

(ver: corolario 1ro. proposición 9na. pág 19)

ý finalmente expresaremos por:

$$\prod_{t=0}^{i}(2t+1) = \{1, 3, 5, 7, 9, \ldots, (2i-1), (2i+1)\},\ t \in \mathbb{N} \quad (*)$$

◦ Por todo ello, queremos ver los resultados que se observan para un caso particular tal que:

$(2i+1)^* = \varphi - 1 \Rightarrow i = \frac{1}{2}\varphi - 1$ factible si: $\varphi \in$ par $\Leftrightarrow$ si: $p \equiv 1 \pmod 4$

$(2i+1)^* = \varphi \Rightarrow i = \frac{1}{2}(\varphi - 1)$ factible si: $\varphi \in$ impar $\Leftrightarrow$ si: $p \equiv 3 \pmod 4$

<u>caso i)</u> $\varphi \in$ par $\Rightarrow i = \frac{1}{2}\varphi - 1 = \frac{1}{2}(2\rho) - 1 \Leftrightarrow i = \rho - 1$ (por ser $\varphi = 2\rho$)

de la proposición 11ra.) resultará equivalente que:

$\{3, 5, 7, \ldots, (2i-1)(2i+1)\}[\varphi-(i+1)]! \equiv (-1)^{(i+1)}, 2^{[i+1]}\{\pm\varepsilon\} \pmod p$

$\Leftrightarrow \prod_{t=0}^{i}(2t+1), [\varphi-(i+1)]! \equiv (-1)^{(i+1)}, 2^{[i+1]}\{\pm\varepsilon\} \pmod p$

$\Leftrightarrow \prod_{t=0}^{i}(2t+1), [\varphi-([\rho - 1]+1)]! \equiv (-1)^{(\rho-1+1)}, 2^{[\rho-1+1]}\{\pm\varepsilon\} \pmod p$

$\Leftrightarrow \prod_{t=0}^{i}(2t+1), [(2\rho)-[\rho]]! \equiv (-1)^{\rho}, 2^{\rho}\{\pm\varepsilon\} \pmod p$

$\Leftrightarrow \prod_{t=0}^{i}(2t+1), (\rho)! \equiv (-1)^{\rho}, 2^{\rho}\{\pm\varepsilon\} \pmod p$ (**), syss: p es primo.

ý como: $\varphi = 2\rho \Rightarrow \pm\varepsilon = \left(\{-1\}^{(\varphi+1)} + p \bullet n\right)^{1/2} = \left(\{-1\}^{(2\rho+1)} + p \bullet n\right)^{1/2}$

$$\Rightarrow \pm\varepsilon = \left(\{-1\} + p \bullet n\right)^{1/2} \in \mathbb{Z}$$

aplicando [$\%^2$] (elevando al cuadrado), se resuelve que:

$\Leftrightarrow \left\{\prod_{t=0}^{i}(2t+1), (\rho)!\right\}^2 \equiv (-1)^{2\rho}, 2^{2\rho}\{\pm\varepsilon\}^2 \pmod p$, syss: p es primo.

$\Leftrightarrow \left\{\prod_{t=0}^{i}(2t+1), (\rho)!\right\}^2 \equiv (-1)^{\varphi}, 2^{\varphi}\{(-1) + p \bullet n\} \pmod p$

syss: p es primo.

como: $\varphi \in$ par

$\Leftrightarrow \left\{\prod_{t=0}^{i}(2t+1), (\rho)!\right\}^2 \equiv 2^{\varphi}(-1) \pmod p$, syss: p es primo. **(*[ref: 1])**

◦ Ahora bien, **<u>Hipótesis caso i.</u>** **($\varphi \in$ par):**

$2^{\varphi} \equiv -1 \pmod p$, syss: $\forall$ p primo. $\rho \in$ impar

$2^{\varphi} \equiv +1 \pmod p$, syss: $\forall$ p primo. $\rho \in$ par

<u>demostración:</u>

Sea $k = 2, 4, 6, \ldots, (2\rho - 2), (2\rho) \Rightarrow k = 2^{\rho}, \rho!$ trivial

como: $\prod_{t=0}^{i}(2t+1) = \{1, 3, 5, 7, 9, \ldots, (2i-1), (2i+1)\}$

ý: $i = \rho - 1 \Rightarrow \prod_{t=0}^{i}(2t+1) = \{1, 3, 5, 7, 9, \ldots, (2[\rho - 1]-1), (2[\rho - 1]+1)\}$

$\Leftrightarrow \prod_{t=0}^{i}(2t+1) = \{1, 3, 5, 7, 9, \ldots, (2\rho - 3), (2\rho - 1)\}$

aplicando 2^{ϱ} a la ecuación (**) de la pág. anterior resultará que:

$\prod_{t=0}^{i}(2t+1) \cdot 2^{\varrho} \cdot \rho\,! \equiv \prod_{t=0}^{i}(2t+1) \cdot k \equiv \ldots$

$\ldots \equiv (2\rho)! \equiv 2^{\varrho}(-1)^{\varrho} \cdot 2^{\varrho}\{\pm\mathfrak{E}\} \pmod p$, $\varphi = 2\rho$

$\Rightarrow \varphi! \equiv (-1)^{\varrho} \cdot 2^{2\varrho}\{\pm\mathfrak{E}\} \pmod p \Leftrightarrow \varphi! \equiv (-1)^{\varrho} \cdot 2^{\varphi}\{\pm\mathfrak{E}\} \pmod p$

syss: p es primo.

como: $p = 2\varphi+1 \Rightarrow 2\varphi+1 \equiv 0 \pmod p \Leftrightarrow 2\varphi \equiv -1 \pmod p$

$\Rightarrow 2^{-1} \equiv -\varphi \pmod p \wedge \varphi^{-1} \equiv -2 \pmod p$ trivial.

Aplicando φ^{-1} tenemos que:

$\Leftrightarrow \varphi^{-1} \cdot \varphi! \equiv (-1)^{\varrho} \cdot 2^{\varphi}\, \varphi^{-1}\{\pm\mathfrak{E}\} \pmod p$

$\Leftrightarrow (\varphi-1)! \equiv (-1)^{\varrho+1} \cdot 2^{\varphi+1}\{\pm\mathfrak{E}\} \pmod p$, pues $\varphi^{-1} \equiv -2 \pmod p$

syss: p es primo.

ý además, por la proposición 5ta.)

$\{(\varphi-1)!\} \equiv (-2)\ \{\pm\mathfrak{E}\} \pmod p$ syss: p es primo.

tenemos entonces que:

$\{(\varphi-1)!\} \equiv (-2)\ \{\pm\mathfrak{E}\} \equiv (-1)^{\varrho+1} \cdot 2^{\varphi+1}\{\pm\mathfrak{E}\} \pmod p$, syss: p es primo.

$\Leftrightarrow (-1)^{\varrho} \cdot 2^{\varphi} \equiv 1 \pmod p$ siendo: $(-1)^{-\varrho} \equiv (-1)^{\varrho} \pmod p$

$\Rightarrow 2^{\varphi} \equiv (-1)^{\varrho} \pmod p$* , $\forall$ p primo. QED.

Partíamos de la Hipótesis tal que ($\varphi \in$ par):

$2^{\varphi} \equiv -1 \pmod p$, $\forall$ p primo. syss: $\rho \in$ impar ***

$2^{\varphi} \equiv +1 \pmod p$, $\forall$ p primo. syss: $\rho \in$ par

Por tanto la hipótesis se cumple y queda demostrada.

<u>corolario al caso i):</u> como teníamos (*[ref: 1] página anterior) que:

$\{\prod_{t=0}^{i}(2t+1) \cdot (\rho)!\}^2 \equiv 2^{\varphi}(-1) \pmod p$, syss: p es primo.

$\wedge\ 2^{\varphi} \equiv (-1)^{\varrho} \pmod p$*

entonces: $\Rightarrow \{\prod_{t=0}^{i}(2t+1) \cdot (\rho)!\}^2 \equiv (-1)^{\varrho+1} \pmod p$, syss: p es primo.

caso ii) $\varphi\in$ impar $\Rightarrow i=\frac{1}{2}(\varphi-1)=\frac{1}{2}(2\rho+1-1) \Leftrightarrow i=\rho$ (por ser $\varphi=2\rho+1$)

de la proposición 11ra.) resultará equivalente que:

(todo el procedimiento es análogo al caso i.)

$\{3\cdot 5\cdot 7\cdot \ldots\cdot (2i-1)(2i+1)\}[\varphi-(i+1)]! \equiv (-1)^{(i+1)}\cdot 2^{[i+1]}\{\pm\mathfrak{E}\}$ (mod p)

$\Leftrightarrow \prod_{t=0}^{i}(2t+1)\cdot[\varphi-(i+1)]! \equiv (-1)^{(i+1)}\cdot 2^{[i+1]}\{\pm\mathfrak{E}\}$ (mod p)

$\Leftrightarrow \prod_{t=0}^{i}(2t+1)\cdot[\varphi-([\rho]+1)]! \equiv (-1)^{(\rho+1)}\cdot 2^{[\rho+1]}\{\pm\mathfrak{E}\}$ (mod p)

$\Leftrightarrow \prod_{t=0}^{i}(2t+1)\cdot[(2\rho+1)-[\rho+1]]! \equiv (-1)^{(\rho+1)}\cdot 2^{(\rho+1)}\{\pm\mathfrak{E}\}$ (mod p)

$\Leftrightarrow \prod_{t=0}^{i}(2t+1)\cdot(\rho)! \equiv (-1)^{(\rho+1)}\cdot 2^{(\rho+1)}\{\pm\mathfrak{E}\}$ (mod p) (**),

syss: p es primo.

ý como: $\varphi=2\rho+1 \Rightarrow \pm\mathfrak{E}=\left(\{-1\}^{(\varphi+1)}+p\bullet n\right)^{1/2}=\left(\{-1\}^{(2\rho+2)}+p\bullet n\right)^{1/2}$

$\Rightarrow \pm\mathfrak{E}=\left(\{+1\}+p\bullet n\right)^{1/2}\in \mathbb{Z}$

aplicando [%^{2}] (elevando al cuadrado), se resuelve que:

$\Leftrightarrow\left\{\prod_{t=0}^{i}(2t+1)\cdot(\rho)!\right\}^2 \equiv (-1)^{(2\rho+2)}\cdot 2^{(2\rho+2)}\{\pm\mathfrak{E}\}^2$ (mod p),

syss: p es primo.

como: $\varphi=2\rho+1$

$\Rightarrow\left\{\prod_{t=0}^{i}(2t+1)\cdot(\rho)!\right\}^2 \equiv (-1)^{(\varphi+1)}\cdot 2^{(\varphi+1)}\{(+1)+p\bullet n\}$ (mod p)

syss: p es primo.

como: $\varphi\in$ impar

$\Leftrightarrow\left\{\prod_{t=0}^{i}(2t+1)\cdot(\rho)!\right\}^2 \equiv 2^{(\varphi+1)}$(mod p) (*$_{[\text{ref: 2}]}$), syss: p es primo.

◦ Ahora bien, **Hipótesis caso ii.** ($\varphi\in$ impar)**:**

$2^{\varphi}\equiv+1$ (mod p), $\forall$ p primo. syss: $\rho\in$ impar

$2^{\varphi}\equiv-1$ (mod p), $\forall$ p primo. syss: $\rho\in$ par

demostración:

$k=2\cdot 4\cdot 6\cdot \ldots\cdot (2\rho-2)\cdot(2\rho) \Rightarrow k=2^{\rho}\cdot\rho!$ trivial

como: $\prod_{t=0}^{i}(2t+1)=\{1\cdot 3\cdot 5\cdot 7\cdot 9\cdot \ldots\cdot (2i-1)\cdot(2i+1)\}$

ý: $i=\rho \Rightarrow \prod_{t=0}^{i}(2t+1)=\{1\cdot 3\cdot 5\cdot 7\cdot 9\cdot \ldots\cdot (2[\rho]-1)\cdot(2[\rho]+1)\}$

$\Leftrightarrow \prod_{t=0}^{i}(2t+1)=\{1\cdot 3\cdot 5\cdot 7\cdot 9\cdot \ldots\cdot (2\rho-1)\cdot(2\rho+1)\}$

aplicando 2^{ρ} a la ecuación (**) de la pág. anterior resultará que:

$$\prod_{t=0}^{i}(2t+1)\cdot 2^{\rho}\cdot \rho\ ! \equiv \prod_{t=0}^{i}(2t+1)\cdot k \equiv \ldots$$

$$\ldots \equiv (2\rho+1)! \equiv 2^{\rho}(-1)^{(\rho+1)}\cdot 2^{(\rho+1)}\{\pm\varepsilon\} \pmod p$$

con: $\varphi = 2\rho + 1$

$$\Rightarrow \varphi! \equiv (-1)^{(\rho+1)}\cdot 2^{(2\rho+1)}\{\pm\varepsilon\} \pmod p \Leftrightarrow \varphi! \equiv (-1)^{(\rho+1)}\cdot 2^{\varphi}\{\pm\varepsilon\} \pmod p$$

syss: p es primo.

como: $p = 2\varphi+1 \Rightarrow 2\varphi+1 \equiv 0 \pmod p \Leftrightarrow 2\varphi \equiv -1 \pmod p$

$$\Rightarrow 2^{-1} \equiv -\varphi \pmod p \wedge \varphi^{-1} \equiv -2 \pmod p \text{ trivial.}$$

Aplicando φ^{-1} tenemos que:

$$\Leftrightarrow \varphi^{-1}\cdot \varphi! \equiv (-1)^{\rho+2}\cdot 2^{\varphi}\ \varphi^{-1}\{\pm\varepsilon\} \pmod p$$

$$\Leftrightarrow (\varphi-1)! \equiv (-1)^{\rho+2}\cdot 2^{\varphi+1}\{\pm\varepsilon\} \pmod p, \text{ pues } \varphi^{-1} \equiv -2 \pmod p$$

syss: p es primo.

ý además, por la proposición 5ta.)

$\{(\varphi-1)!\} \equiv (-2)\ \{\pm\varepsilon\} \pmod p$ syss: p es primo.

tenemos entonces que:

$\{(\varphi-1)!\} \equiv (-2)\ \{\pm\varepsilon\} \equiv (-1)^{\rho+2}\cdot 2^{\varphi+1}\{\pm\varepsilon\} \pmod p$, syss: p es primo.

$\Leftrightarrow (-1)^{\rho+1}\cdot 2^{\varphi} \equiv 1 \pmod p$ siendo: $(-1)^{-(\rho+1)} \equiv (-1)^{(\rho+1)} \pmod p$

$\Rightarrow 2^{\varphi} \equiv (-1)^{\rho+1} \pmod p$* , $\forall$p primo. QED.

Partíamos de la Hipótesis tal que ($\varphi \in$ impar):

$2^{\varphi} \equiv +1 \pmod p$, $\forall$p primo. syss: $\rho \in$ impar

$2^{\varphi} \equiv -1 \pmod p$, $\forall$p primo. syss: $\rho \in$ par

Por tanto la hipótesis se cumple y queda demostrada.

<u>corolario al caso ii):</u> como teníamos (*[ref: 2] pág anterior) que:

$$\{\prod_{t=0}^{i}(2t+1)\cdot(\rho)!\}^2 \equiv 2^{(\varphi+1)} \pmod p, \text{ syss: p es primo.}$$

$\wedge\ 2^{\varphi} \equiv (-1)^{\rho+1} \pmod p$*

entonces:

$$\Rightarrow \{\prod_{t=0}^{i}(2t+1)\cdot(\rho)!\}^2 \equiv (-1)^{\rho+1}\cdot(2) \pmod p, \text{ syss: p es primo.}$$

Proposición 16ta)

Por todo lo obtenido en la proposición anterior, resulta trivial que: $\forall n \in \mathbb{N}$, siendo p impar primo ó no.

si: $\rho \in$ par $\Rightarrow \rho = 2n$ / **1.)** $\varphi \in$ par $\Rightarrow \varphi = 2\rho \Rightarrow \varphi = 4n$

como: $p = 2\varphi + 1 \Rightarrow \underline{p = 8n+1} = 4\rho + 1$*

ó **2.)** $\varphi \in$ impar $\Rightarrow \varphi = 2\rho + 1 \Rightarrow \varphi = 4n+1$

como: $p = 2\varphi + 1 \Rightarrow \underline{p = 8n+3} = 4\rho + 3$**

si: $\rho \in$ impar $\Rightarrow \rho = 2n+1$ / **1.)** $\varphi \in$ par $\Rightarrow \varphi = 2\rho \Rightarrow \varphi = 4n+2$

como: $p = 2\varphi + 1 \Rightarrow \underline{p = 8n+5} = 4\rho + 1$*

ó **2.)** $\varphi \in$ impar $\Rightarrow \varphi = 2\rho + 1 \Rightarrow \varphi = 4n+3$

como: $p = 2\varphi + 1 \Rightarrow \underline{p = 8n+7} = 4\rho + 3$**

Entonces:

$\varphi \in$ par syss: $p \equiv 1 \pmod 4$* $p = 4\rho + 1$

$\varphi \in$ impar syss: $p \equiv 3 \pmod 4$** $p = 4\rho + 3$

Proposición 17ma)

Por lo obtenido en las dos proposiciones anteriores

(obsérvese en especial los dos corolarios de la proposición 15ta págs. 27 ý 29)

Resulta expresable entonces que:

i) si: $p \equiv 1 \pmod 8 \Rightarrow \varphi \in$ par $\wedge\ \rho \in$ par entonces:

$$\left\{\prod_{t=0}^{i}(2t+1)\cdot(\rho)!\right\}^2 \equiv -1 \pmod p, \text{ syss: p es primo.}$$

ii) si: $p \equiv 5 \pmod 8 \Rightarrow \varphi \in$ par $\wedge\ \rho \in$ impar entonces:

$$2^{\varphi} \equiv 2^{2\rho} \equiv \left(2^{\rho}\right)^2 \equiv -1 \pmod p, \ \forall p \text{ primo. (ver pág 27***)}$$

(**ver**: corolario pág. siguiente)

iii) si: $p \equiv 3 \pmod 8 \Rightarrow \varphi \in$ impar $\wedge\ \rho \in$ par entonces:

$$\left\{\prod_{t=0}^{i}(2t+1)\cdot(\rho)!\right\}^2 \equiv -2 \pmod p, \text{ syss: p es primo.}$$

iv) si: $p \equiv 7 \pmod 8 \Rightarrow \varphi \in$ impar $\wedge\ \rho \in$ impar entonces:

$$\left\{\prod_{t=0}^{i}(2t+1)\cdot(\rho)!\right\}^2 \equiv +2 \pmod p, \text{ syss: p es primo.}$$

Corolario) (al apartado ii. pág anterior)

si: $p \equiv 5 \pmod 8$ tambien se deduce que:

$$\{\prod_{t=0}^{i}(2t+1)\cdot(\rho)!\}^2 \equiv +\underline{1} \pmod p$$, syss: p es primo.

pues teníamos del corolario caso i. (pág 27) que:

$$\{\prod_{t=0}^{i}(2t+1)\cdot(\rho)!\}^2 \equiv (-1)^{\varphi+1} \pmod p$$, syss: p es primo.

y sabemos que si: $p \equiv 5 \pmod 8 \Rightarrow \varphi \in$ par $\wedge\ \rho \in$ impar (pág. anterior)

Pero observese que en $\mathbb{Z}$: $\{\prod_{t=0}^{i}(2t+1)\cdot(\rho)!\}^2 = (+\underline{1}) + p\cdot m,\ m \in \mathbb{N}$ /

$$\Leftrightarrow \prod_{t=0}^{i}(2t+1)\cdot(\rho)! = \{\underline{1} + p\cdot m\}^{(1/2)} \in \mathbb{Z}$$

Tal que, de nuevo, en $\mathbb{Z}/p$: $\Leftrightarrow \prod_{t=0}^{i}(2t+1)\cdot(\rho)! \equiv \pm\underline{1} \pmod p$

(ó es congruente con +1 ó -1, pero no podemos asegurar cual de ellos es el correcto para los valores p=8n+5, pues dichos valores parecen variar "aleatoriamente").

Mientras que para: $(2^{\varphi})^2 \equiv -1 \pmod p$, $\forall$ p primo.

$\Rightarrow (2^{\varphi}) = \{-1 + p\cdot m'\}^{(1/2)} \in \mathbb{Z}$, $m' \in \mathbb{N}$

$\Rightarrow$ exige la existencia de un valor $k \in \mathbb{Z}$, $k \in (1,p-1)$ /

$$(2^{\varphi}) \equiv k \pmod p \ /\ \{\pm k\}^2 \equiv -1 \pmod p$$

• además los apartados i) ý ii) anteriores se pueden fusionar en argumentos realizando p (mod 4) /

Si $p \equiv 1 \pmod 4 \wedge$ p es primo entonces: $\exists\ a \in \mathbb{Z}$ / $\{\pm a\}^2 \equiv -1 \pmod p$

Nota: Si p no es primo. puede (ó no) darse la congruencia $\{\pm a\}^2 \equiv -1 \pmod p$ ó $\{\pm a\}^2 \not\equiv -1 \pmod p$ (se estudiarán más adelante estas posibilidades).

Proposición 18va) De lo obtenido en la proposición anterior (observese además el corolario correspondiente).

Sea: $\sigma \in \mathbb{Z}$ / si: $p \equiv 1 \pmod 4 \Rightarrow \sigma = -1$

si: $p \equiv 3 \pmod 8 \Rightarrow \sigma = -2$

si: $p \equiv 7 \pmod 8 \Rightarrow \sigma = +2$

Sea: $\alpha \in \mathbb{Z}$, $\alpha \in (1,p-1)$ entonces:

Si: $p \not\equiv 5 \pmod 8 \Rightarrow \prod_{t=0}^{i}(2t+1) \cdot (\rho)! \equiv \alpha \pmod p$ **

/ $\{\pm\alpha\}^2 \equiv \sigma \pmod p$, syss: p es primo.

Si: $p \equiv 5 \pmod 8 \Rightarrow (2^{\rho}) \equiv \alpha \pmod p$ **

/ $\{\pm\alpha\}^2 \equiv \sigma \pmod p$, $\forall$ p primo.

$2^{\varphi} \equiv 2^{2\rho} \equiv (2^{\rho})^2 \equiv -1 \equiv \sigma$*** $\pmod p$, $\forall$ p primo.

Recordando que: si $p \equiv 1 \pmod 4$ entonces $\sigma = -1$ ***

si $p \equiv 3 \pmod 8$ entonces $\sigma = -2$

si $p \equiv 7 \pmod 8$ entonces $\sigma = +2$

<u>Corolario)</u>

La congruencia con α se da siempre que p es primo. Esto es trivial puesto que su existencia se deriva de las hipótesis demostradas en la proposición 15ta). ý de los corolarios planteados en la misma.

Ahora bien, se cumplen las congruencias expuestas (**) y la existencia del elemento α definido, de forma que:

si: p es primo entonces $\forall k \in \mathbb{Z}$, $k \in (1,p-1)$ / $k \not\equiv \pm\alpha \pmod p$

entonces: $k^2 \not\equiv \sigma \pmod p$ / $\{\pm\alpha\}^2 \equiv \sigma \pmod p$

<u>demostración:</u> por la teoría general (ver: punto iii) pág 3.) que afirma que si:

p es primo, entonces: $\exists$ $\frac{p-1}{2}$ cuadrados perfectos comprendidos entre [1,p-1] en $(\mathbb{Z}/p)$ anillo. Por lo que, como ya existen $\pm\alpha$, raíces de σ en $(\mathbb{Z}/p)$, entonces no existen más valores posibles que tambien sean raíces de σ en $(\mathbb{Z}/p)$.

/ (α) ý $(p-\alpha) \in (1,p-1)$

<u>Proposición 19na)</u>

Si p **<u>no es</u>** primo, tenemos para los casos en que además $p \not\equiv 5 \pmod 8$... que:

$$\{\prod_{t=0}^{i}(2t+1) \cdot (\rho)!\}^2 \not\equiv \sigma \pmod p$$

y para el caso: $p \equiv 5 \pmod 8$ (seguimos suponiendo que p <u>no es</u> primo)

$(2^{\rho})^2 \equiv \sigma \pmod p$ ó $(2^{\rho})^2 \not\equiv \sigma \pmod p$, $\sigma=-1$

recordando que… si: $p=4k+1 \Rightarrow \sigma=-1$, si: $p=8k+3 \Rightarrow \sigma=-2$, si: $p=8k+7 \Rightarrow \sigma=+2$,

de manera que $\forall$p no primo impar positivo tal que: σ sea residuo cuadrático en $\mathbb{Z}/p$ denotaremos por: β, (p-β), β', (p-β'), β'', (p-β'') ,..., β'^{w}, (p-β'^{w}).

$\beta^* \in \mathbb{N}\backslash\{0\}$ con $\beta^* \in (1,p-1)$ ý además: $\{\pm\beta^*\}^2 \equiv \sigma \pmod p$

es decir: $\{\pm\beta\}^2 \equiv \{\pm\beta'\}^2 \equiv \{\pm\beta''\}^2 \equiv ... \equiv \{\pm\beta'^{w}\}^2 \equiv \sigma \pmod p$

(denotado por β^* para los compuestos en los que σ sea residuo cuadrático en $\mathbb{Z}/p$ para diferenciarlo de las raíces α ý (p-α) (para todos los primos), tal que:

$$\{\pm\alpha\}^2 \equiv \sigma \pmod p \ \forall p \text{ primo.}$$

en la parte II de este temario (págs. 36-87) podrá demostrarse claramente las diferencias entre los números primos ý los números compuestos en los que σ sea residuo cuadrático en $\mathbb{Z}/p$.

(ya sabemos que para todo primo σ siempre es residuo cuadrático en $\mathbb{Z}/p$ ver proposición 18va)

Corolario)

Si p no es primo, entonces σ puede (ó no) ser residuo cuadrático en $\mathbb{Z}/p$

importante:

es decir, puede existir (al menos) un elemento $\beta \in \mathbb{Z}$, $\beta \in (1,p-1)$ /

$$\{\pm\beta\}^2 \equiv \sigma \pmod p.$$

ó puede ocurrir que $\forall k \in (1,p-1)$ ocurra en cambio que: $\{\pm k\}^2 \not\equiv \sigma \pmod p$

(demostrado y diferenciados todos los casos posibles en la parte II del temario)

Véanse como ejemplos:

- Sea p=25 , p **no es** primo / $p \equiv 1 \pmod 4 \Rightarrow \sigma = -1 \ \nexists\alpha$, $\varphi=12$, $\rho = 6$ /

  $\prod_{t=0}^{i}(2t+1)\cdot(\rho)! \equiv \{1\cdot 3\cdot 5\cdot 7\cdot 9\cdot ...\cdot(2\rho-3)\cdot(2\rho-1)\}(\rho)! \equiv ...$

  $... \equiv \{1\cdot 3\cdot ...\cdot 9\cdot 11\}(6)! \equiv (10395)(720) \equiv 20\cdot 20 \equiv 0 \pmod p$

  cláramente: $\{\pm 0\}^2 \not\equiv \sigma \pmod p \Rightarrow \nexists\alpha$

  pero en cambio $\exists \ \beta = \pm 7$ / $\{\pm\beta\}^2 \equiv \{\pm 7\}^2 \equiv \sigma \equiv -1 \pmod p$.

- Sea p=65, p **no es** primo, siendo $\sigma=-1$ / $\nexists\alpha$, pero $\beta = \pm 8 \wedge \beta' = \pm 18$

  en cambio cumplen que: $\{\pm\beta\}^2 \equiv \{\pm\beta'\}^2 \equiv \sigma \pmod p$.

- Sea p=9, p **no es** primo, siendo $\sigma=-1$ / $\nexists\alpha$ ý además $\forall k \in (1,p-1)$

  $\Rightarrow \{\pm k\}^2 \not\equiv \sigma \pmod p$ $(\Rightarrow \nexists\beta)$

• Sea p=27, p **no es** primo, siendo $\sigma=-2$ / $\nexists\alpha$, pero $\beta=\pm5$

en cambio cumple que: $\{\pm\beta\}^2\equiv\sigma \pmod p$.

• Sea p=35, p **no es** primo, siendo $\sigma=-2$ / $\nexists\alpha$ ý además $\forall k\in (1,p-1)$

$\Rightarrow \{\pm k\}^2\not\equiv\sigma \pmod p$ $(\Rightarrow\nexists\beta)$

• Sea p=119, p **no es** primo, siendo $\sigma=+2$ / $\nexists\alpha$, pero $\beta=\pm11\wedge\beta'=\pm45$

en cambio cumplen que: $\{\pm\beta\}^2\equiv\{\pm\beta'\}^2\equiv\sigma \pmod p$.

• Sea p=15, p **no es** primo, siendo $\sigma=+2$ / $\nexists\alpha$ ý además $\forall k\in (1,p-1)$

$\Rightarrow \{\pm k\}^2\not\equiv\sigma \pmod p$ $(\Rightarrow\nexists\beta)$

recordando que:

Si: $p\not\equiv 5 \pmod 8$ $\Rightarrow \prod_{t=0}^{i}(2t+1)\cdot(\rho)!\equiv\alpha \pmod p$**

/ $\{\pm\alpha\}^2\equiv\sigma \pmod p$, syss: p es primo.

** $(\equiv 0 \pmod p$ syss: p no es primo$)$

Si: $p\equiv 5 \pmod 8$ $\Rightarrow (2^{\rho})\equiv\alpha \pmod p$

/ $\{\pm\alpha\}^2\equiv\sigma \pmod p$, $\forall$ p primo.

• Si: $\varphi\in$ par / $\varphi=2\rho$, $p=2\varphi+1$ $\wedge$ $p\equiv 1 \pmod 4$**

$\prod_{t=0}^{i}(2t+1)=\{1\cdot 3\cdot 5\cdot 7\cdot 9\cdot\ldots\cdot(2\rho-3)\cdot(2\rho-1)\}$

• Si: $\varphi\in$ impar / $\varphi=2\rho+1$, $p=2\varphi+1$ $\wedge$ $p\equiv 3 \pmod 4$**

$\prod_{t=0}^{i}(2t+1)=\{1\cdot 3\cdot 5\cdot 7\cdot 9\cdot\ldots\cdot(2\rho-1)\cdot(2\rho+1)\}$

(** ver corolario 1ro proposición 9na página 19)

tal que: $\prod_{t=0}^{i}(2t+1)=\{1\cdot 3\cdot 5\cdot 7\cdot 9\cdot\ldots\cdot(2i-1)\cdot(2i+1)\}$, $t\in\mathbb{N}$

ý siendo: $i=\frac{1}{2}\varphi-1$ si: $p\equiv 1 \pmod 4$

$i=\frac{1}{2}(\varphi-1)$ si: $p\equiv 3 \pmod 4$

(ver página 26 *)

Corolario 2do)

$\exists\ \sigma^{-1} \in \mathbb{Z}\ /\ \sigma \cdot \sigma^{-1} \equiv 1 \pmod{p}$ trivial:

si: $\sigma = -1 \Rightarrow\ \sigma^{-1} \equiv -1 \pmod{p}$

si: $\sigma = -2 \Rightarrow\ \sigma^{-1} \equiv -2^{-1} \pmod{p}$ $\sigma^{-1} = -\left(\frac{p+1}{2}\right)$

si: $\sigma = +2 \Rightarrow\ \sigma^{-1} \equiv +2^{-1} \pmod{p}$, $\sigma^{-1} = \frac{p+1}{2}$

Análogamente: $\exists\ \alpha^{-1} \in \mathbb{Z}\ ,\ \alpha^{-1} \in (0,p)\ /\ \alpha \cdot \alpha^{-1} \equiv 1 \pmod{p}$

si: $\sigma = -1 \Rightarrow\ \alpha(-\alpha) \equiv -\sigma \equiv 1 \pmod{p} \Rightarrow\ \alpha^{-1} \equiv -\alpha \pmod{p}$

si: $\sigma = -2 \Rightarrow\ \alpha(-\alpha) \equiv -\sigma \equiv 2 \pmod{p}\ \Rightarrow\ \alpha^{-1}\alpha(-\alpha) \equiv 2\alpha^{-1} \pmod{p}$

$\Rightarrow\ \alpha^{-1} \equiv -2^{-1}\alpha \pmod{p}$

si: $\sigma = +2 \Rightarrow\ \alpha(-\alpha) \equiv -\sigma \equiv -2 \pmod{p} \Rightarrow\ \alpha^{-1}\alpha(-\alpha) \equiv -2\alpha^{-1} \pmod{p}$

$\Rightarrow \alpha^{-1} \equiv 2^{-1}\alpha \pmod{p}$

Es trivial que: $\alpha^{-1} \equiv \sigma^{-1}\alpha \pmod{p}$

Inciso: En la parte final del presente temario se incluye un temario (págs. 88-99). Donde se demostraran las siguientes puntualizaciones omitidas aquí por ser irrelevantes para la hipótesis expuesta en la proposición 21ra.

- si: $p \equiv 1 \pmod{8}$, $\sigma = -1\ \Rightarrow\ (\varphi-1)! \equiv \pm 2\alpha \pmod{p}$, syss: p es primo.
- si: $p \equiv 3 \pmod{8}$, $\sigma = -2\ \Rightarrow\ (\varphi)! \equiv 2^{\varphi}\alpha \pmod{p}$, syss: p es primo.
- si: $p \equiv 5 \pmod{8}$, $\sigma = -1\ \Rightarrow\ (\varphi-1)! \equiv \pm(2)^{\varphi-1}\rho^{-1} \pmod{p}$, syss: p es primo.
- si: $p \equiv 7 \pmod{8}$, $\sigma = +2\ \Rightarrow\ (\varphi)! \equiv 2^{\varphi}\alpha \pmod{p}$, syss: p es primo.

// **(fin de la Parte Ira)**

Parte IIda. Introducción

Donde se plantea la Hipótesis principal (ver: proposición 21ra), expuesta (en parte) en la introducción general (págs 5-9) de la presente obra. Y la demostración de todas sus premisas. (*En la página 44 hay un índice para indicar la página donde se demuestran cada una de las premisas expuestas en dicha Hipótesis principal.*)

Previo Introductorio. *(De la Parte I teníamos que...:)*

i) de la proposición 15ta.

$p = 2\varphi+1$ / $\varphi = 2\rho$ si: $\varphi \in$ par $\Rightarrow p \equiv 1 \pmod 4$

$\varphi = 2\rho + 1$ si: $\varphi \in$ impar $\Rightarrow p \equiv 3 \pmod 4$ (pág 25)

$\wedge \quad \prod_{t=0}^{i}(2t+1) = \{1, 3, 5, 7, 9, \ldots, (2i-1), (2i+1)\}$, $t \in \mathbb{N}$ (pág 26)

Siendo: $i = \rho - 1$ si: $\varphi \in$ par (pág 26)

$i = \rho$ si: $\varphi \in$ impar (pág 28)

ii) de la proposición 17ma. (pág 30)

- si: $p \equiv 1 \pmod 8 \Rightarrow \varphi \in$ par $\wedge \ \rho \in$ par entonces:

$$\left\{\prod_{t=0}^{i}(2t+1), (\rho)!\right\}^2 \equiv -1 \pmod p, \text{ syss: p es primo.}$$

- si: $p \equiv 5 \pmod 8 \Rightarrow \varphi \in$ par $\wedge \ \rho \in$ impar entonces:

$$2^{\varphi} \equiv 2^{2\rho} \equiv (2^{\rho})^2 \equiv -1 \pmod p, \ \forall \text{p primo. (ver pág 30)}$$

$$\left\{\prod_{t=0}^{i}(2t+1), (\rho)!\right\}^2 \equiv +1 \equiv (-1)^{\rho+1} \pmod p, \text{ syss: p es primo.}$$

(Ver: corolario pág 27)

- si: $p \equiv 3 \pmod 8 \Rightarrow \varphi \in$ impar $\wedge \ \rho \in$ par entonces:

$$\left\{\prod_{t=0}^{i}(2t+1), (\rho)!\right\}^2 \equiv -2 \pmod p, \text{ syss: p es primo.}$$

- si: $p \equiv 7 \pmod 8 \Rightarrow \varphi \in$ impar $\wedge \ \rho \in$ impar entonces:

$$\left\{\prod_{t=0}^{i}(2t+1), (\rho)!\right\}^2 \equiv +2 \pmod p, \text{ syss: p es primo.}$$

iii) de la proposición 18va. (pág. 32)

Si: $p \not\equiv 5 \pmod 8 \Rightarrow \prod_{t=0}^{i}(2t+1), (\rho)! \equiv \alpha \pmod p$

/ $\{\pm\alpha\}^2 \equiv \sigma \pmod p$, syss: p es primo.

Si: $p \equiv 5 \pmod 8 \Rightarrow (2^{\rho}) \equiv \alpha \pmod p$ / $\{\pm\alpha\}^2 \equiv \sigma \pmod p$, $\forall$p primo.

Nota Importante: $\sigma\in$ residuo cuadrático en $\mathbb{Z}/p$ siempre que p sea primo, se denotan por $\alpha \wedge (p-\alpha)$, a sus dos únicas raíces, en el intervalo (1,p-1).

Ý σ puede ser (ó no) residuo cuadrático en $\mathbb{Z}/p$ si p es compuesto;

de ser σ residuo cuadrático en $\mathbb{Z}/p$, p compuesto se denotarán por:

β, $(p-\beta)$, β', $(p-\beta')$,..., β'^{w}, $(p-\beta'^{w})$, a sus raíces, en el intervalo (1,p-1).

recordando que si: $p=4k+1\Rightarrow\sigma=-1$, si: $p=8k+3\Rightarrow\sigma=-2$, si: $p=8k+7\Rightarrow\sigma=+2$.

Proposición 20ma) Sea p primo ó no primo y Sean $x,y \in \mathbb{Z}\backslash\{0\}$ tal que además se cumple la igualdad: $p = x^2 - \sigma y^2$, entonces en $\mathbb{Z}/p$ resulta que:

$$x^2 - \sigma y^2 \equiv 0 \pmod p \Leftrightarrow x^2 \equiv \sigma y^2 \pmod p$$

recordando que, si: $p=4k+1 \Rightarrow \sigma=-1$, si: $p=8k+3 \Rightarrow \sigma=-2$, si: $p=8k+7 \Rightarrow \sigma=+2$.

• sabemos además que si p es primo entonces:
(ver: proposiciones 18-19 págs. 31-34)

$$\exists\ \alpha \in \mathbb{Z},\ \alpha \in (1,p-1) \,/\, \{\pm\alpha\}^2 \equiv \sigma \pmod p \Rightarrow x \equiv \pm\alpha y \pmod p$$

puesto que $mcd(x,y) = \pm 1$, (trivial si: $mcd(x,y) = k$, $k \neq 1 \Rightarrow k \mid p$)

• ý si p **no es** primo puede (ó no) darse la existencia de un elemento β tal que:

$$\{\pm\beta\}^2 \equiv \sigma \pmod p$$

Es decir σ puede (ó no) ser un residuo cuadrático en $\mathbb{Z}/p$

Si: σ es un residuo cuadrático en $\mathbb{Z}/p$ entonces:

existen al menos $\beta, (p-\beta) \in (1,p-1) \,/\, \{\pm\beta\}^2 \equiv \sigma \pmod p$

además, puede darse la existencia de otros elementos (ó no) denotados por: $\beta', \beta'', \beta''', \ldots, \beta'^{w}$, distintos entre sí (no congruentes entre si, ni salvo signo).
ý en cambio: $\{\pm\beta\}^2 \equiv \{\pm\beta'\}^2 \equiv \{\pm\beta''\}^2 \equiv \ldots \equiv \{\pm\beta'^{w}\}^2 \equiv \sigma \pmod p$

• Sirva como ejemplo numérico:
sea p=1105 p no es primo, siendo: $\sigma=-1$ pues $1105 \equiv 1 \pmod 8$ $/\nexists\alpha$, debido a que:

Si: $p \not\equiv 5 \pmod 8 \Rightarrow \prod_{t=0}^{i}(2t+1) \cdot \left(\frac{p}{}\right)! \equiv \alpha \pmod p$ (ver: ** pág 34)

$/\ \{\pm\alpha\}^2 \equiv \sigma \pmod p$, syss: p es primo.

de forma que en nuestro caso tendremos que:

$$\prod_{t=0}^{i}(2t+1) \cdot \left(\frac{p}{}\right)! \equiv k \pmod p,\ k \in \mathbb{Z} \,/\, \{\pm k\}^2 \not\equiv \sigma \pmod p$$

$\Rightarrow \nexists\alpha$, pero en cambio existen unos valores $\beta^* \in \mathbb{Z}$, $\beta^* \in (1,p-1)$, tales que:

$\beta = \pm 47$, $\beta' = \pm 463$, $\beta'' = \pm 837$,

(no congruentes entre sí, ni salvo signo): $\beta'^{i} \not\equiv \pm\beta'^{j} \pmod p$, $i \not\equiv j \pmod p$

ý en cambio: $\{\pm\beta\}^2 \equiv \{\pm\beta'\}^2 \equiv \{\pm\beta''\}^2 \equiv \sigma \pmod p$ // *(fin del ejemplo)*

Proposición 21ra) **Hipótesis principal:** ***Premisas***

$\forall\ p\in \mathbb{N}$, $p\in$ **impar** entonces:

• Punto Iro) Si p es primo $\Rightarrow\ \exists\ x,y\in \mathbb{Z}\backslash\{0\}$

tal que: $p = x^2 - \sigma \bullet y^2$, siendo $x\in$ impar

con: $\sigma = -1$ si: $p = 4k+1$, $\sigma = -2$ si: $p = 8k+3\ \wedge\ \sigma = +2$ si: $p = 8k+7$ **

$\wedge\ y\in$ par si: $p \equiv 1 \pmod 4$ é $y\in$ impar si: $p \equiv 3 \pmod 4$

(ver: proposición 22da pág 45)

además:

• si: $p = 4k+1$ ó $p = 8k+3$

Entonces, sean: $x', y'\in \mathbb{Z}\backslash\{0\}\ /\ \forall\ x' \neq \pm x \wedge \forall y' \neq \pm y \Rightarrow p \neq x'^2 - \sigma \bullet y'^2$

• si: $p = 8k+7$ **

entonces $\exists\ x', y'\in \mathbb{Z}\backslash\{0\}\ /\ x' \neq \pm x \wedge y' \neq \pm y$

$/\ p = x'^2 - \sigma \bullet y'^2 = x''^2 - \sigma \bullet y''^2 = \ldots = (x'^w)^2 - \sigma \bullet (y'^w)^2$

• además $\forall p$ primo $\Rightarrow\ \sigma\in$ residuo cuadrático en $\mathbb{Z}/p$

$/\ \exists\ \alpha\in \mathbb{Z}, \alpha \in (1,p-1) / (\pm\alpha)^2 \equiv \sigma \pmod p$ ($\pm\alpha$ raíces <u>únicas</u> de σ * en $\mathbb{Z}/p$)

* Tal que: $\forall\ k\in \mathbb{Z}, k\in (p,p-1) \wedge k \not\equiv \pm\alpha \pmod p$ entonces: $\{\pm k\}^2 \not\equiv \sigma \pmod p$

• además en: $\mathbb{Z}/p \Rightarrow x^2 - \sigma \bullet y^2 \equiv 0 \pmod p \Leftrightarrow x^2 \equiv \sigma \bullet y^2 \pmod p$

con $\sigma\in$ residuo cuadrático en $\mathbb{Z}/p$ tal que: $\text{mcd}(x,y) = \pm 1 \Leftrightarrow x \equiv \pm\alpha \bullet y \pmod p$

• *Inciso***: si $p = 8k+7$ entonces: $p = x'^2 - \sigma \bullet y'^2 = x''^2 - \sigma \bullet y''^2 = \ldots = (x'^w)^2 - \sigma \bullet (y'^w)^2$

$\Rightarrow x' \equiv \pm\alpha \bullet y' \pmod p$, $x'' \equiv \pm\alpha \bullet y'' \pmod p$,..., $x'^w \equiv \pm\alpha \bullet y'^w \pmod p$.

(pues: $\pm\alpha$ raíces <u>únicas</u> de σ * en $\mathbb{Z}/p$)

(*Nota:*) estamos afirmando claramente que: -1 es residuo cuadrático en $\mathbb{Z}/p$ para los números primos de la forma $p = 4k+1$, que -2 es residuo cuadrático en $\mathbb{Z}/p$ para los números primos de la forma $p=8k+3$, y que 2 es residuo cuadrático en $\mathbb{Z}/p$ para los números primos de la forma $p=8k+7$. Debe quedar claro, que para los números primos de la forma $p = 8k+1$ los valores -2 y 2 también son residuo cuadrático en $\mathbb{Z}/p$ (esto no se demostrará). Pero que el valor σ para tales primos ($p=8k+1$ ó $p=8k+5$ es decir para: $p = 4k+1$) será $\sigma = -1$.

• Punto IIdo) Algo más compleja y extensa: caso en que p impar, p>2

Tal que: p no es primo.

recordando nuevamente que: $p=4k+1 \Rightarrow \sigma=-1$, si: $p=8k+3 \Rightarrow \sigma=-2$, si: $p=8k+7 \Rightarrow \sigma=+2$

II.a) si: $p \neq x^2 - \sigma \cdot y^2 \ \forall \ x,y \in \mathbb{Z}$, $x \in$ impar $\Rightarrow$

$$\forall \ \mu \in (1,p-1) \ \Rightarrow \ (\pm\mu)^2 \not\equiv \sigma \pmod p$$

II.b) si: $p = x^2 - \sigma \cdot y^2 = x'^2 - \sigma \cdot y'^2 = x''^2 - \sigma \cdot y''^2 = \ldots = (x'^w)^2 - \sigma \cdot (y'^w)^2$

$\forall x'^i \neq \pm x'^j$, $i \neq j$ $(\Rightarrow y'^i \neq \pm y'^j)$ con: $x'^m, y'^m \in \mathbb{Z}\backslash\{0\}$

Siendo: $f_0(p) = x^2 - \sigma \cdot y^2$, $f_1(p) = x'^2 - \sigma \cdot y'^2$, $f_2(p) = x''^2 - \sigma \cdot y''^2, \ldots,$

$, \ldots, f_w(p) = (x'^w)^2 - \sigma \cdot (y'^w)^2$ / $p = f_0(p) = f_1(p) = f_2(p) = \ldots = f_w(p)$

Y tal que: $\exists$ al menos $f_0(p)$ ý $f_1(p)$ que cumplen dicha igualdad con p

Entonces en $\mathbb{Z}/p$ ocurre que **si:** $\sigma \in$ residuo cuadrático en $\mathbb{Z}/p \Rightarrow$

$\exists \ f_i(p) = (x'^i)^2 - \sigma \cdot (y'^i)^2 \wedge f_j(p) = (x'^j)^2 - \sigma \cdot (y'^j)^2$

ecuaciones cuadráticas distintas

/ $p = (x'^i)^2 - \sigma \cdot (y'^i)^2 = (x'^j)^2 - \sigma \cdot (y'^j)^2$

$\wedge$ $\text{mcd}(x'^i, y'^i) = \pm 1$ $\wedge$ $\text{mcd}(x'^j, y'^j) = \pm 1$

es decir, existen (al menos***): $\beta \wedge \beta' \in (1,p-1)$ / $\beta \not\equiv \pm\beta' \pmod p$

y en cambio: $\{\pm\beta\}^2 \equiv \{\pm\beta'\}^2 \equiv \sigma \pmod p$

*** (Obviamente también sus opuestos $(p-\beta) \wedge (p-\beta') \in (1,p-1)$ son raíces de σ en $\mathbb{Z}/p$, es decir, existen al menos cuatro raíces en el intervalo (1,p-1). A diferencia de los números primos que sólo tienen dos raíces: α ý $(p-\alpha)$ en el intervalo (1,p-1) ý de ciertos cuadrados perfectos como se verá en el siguiente apartado II.c.)

II.c) si p no es primo ý $p \in$ cuadrado perfecto impar*, entonces:

• ó: $p = x^2 - \sigma \cdot y^2 = f_0(p)$, $x \neq 0$ ($x \in$ impar) $\wedge$ $y = 0$ / $\nexists \ f_{i>0}(p) = p$

• ó: $p = x^2 - \sigma \cdot y^2 = x'^2 - \sigma \cdot y'^2$, $x \neq 0$, $y = 0$

/ $x' \in \mathbb{Z}\backslash(\pm x,0) \wedge y' \in \mathbb{Z}\backslash(\pm y,0)$ es decir $p = f_0(p) = f_1(p)$

Además: $\exists \ \beta \in \mathbb{Z}$, $\beta \in (1,p-1)$ / $(\pm\beta)^2 \equiv \sigma \pmod p$

$\Rightarrow \ \sigma \in$ residuo cuadrático en $\mathbb{Z}/p$

Tal que: $\forall \ k \in \mathbb{Z}$, $k \in (p,p-1) \wedge k \not\equiv \pm\beta \pmod p$

entonces: $\{\pm k\}^2 \not\equiv \sigma \pmod p$

• ó: $p = x^2 - \sigma \cdot y^2 = x'^2 - \sigma \cdot y'^2 = x''^2 - \sigma \cdot y''^2 = \ldots = (x'^w)^2 - \sigma \cdot (y'^w)^2$

es decir: $p = f_0(p) = f_1(p) = f_2(p) = \ldots = f_w(p)$ / $Card[f(p)] \geq 3$ tal que:

$Card[f(p)] \geq 3$ ý $4 \leq Card[\beta^*] \leq 2w$ **

* se cumple que: $\forall p \in$ cuadrado perfecto impar $\Rightarrow p \equiv 1 \pmod 8$ siempre.

ý además: $\exists \ \beta \in \mathbb{Z}$ / $\{\pm\beta\}^2 \equiv \sigma \pmod p$ syss: $\exists \ f_1(p) = p$

** dada la ecuación cuadrática: $p = (x'^i)^2 - \sigma \cdot (y'^i)^2 \Rightarrow (x'^i)^2 \equiv \sigma \cdot (y'^i)^2 \pmod p$

Tal que: existe β'^i si y sólo si: $mcd(x'^i, y'^i) = \pm 1$ / $x'^i \equiv \pm\beta'^i \cdot y'^i \pmod p$

pues si $mcd(x'^i, y'^i) = k$, $k \neq \pm 1$ entonces $k \mid p \Rightarrow \nexists \ k^{-1}$ en $\mathbb{Z}/p$

$\Rightarrow \nexists \ (x'^i)^{-1}, (y'^i)^{-1}$ en $\mathbb{Z}/p$, pues: $k \mid x'^i \wedge k \mid y'^i$

Importante: si β es raíz de σ en $\mathbb{Z}/p$ también lo es $(p-\beta)$ y por tanto, se expone que $4 \leq Card[\beta^*] \leq 2w$, como mímimo existen cuatro raíces de σ en $\mathbb{Z}/p$, en el intervalo $(1,p-1)$. Es decir, existen también (al menos): $\beta' \wedge (p-\beta')$ raíces de σ en $\mathbb{Z}/p$

II.d) Sea $p = q \cdot q'$, p no primo impar, $p > 1$

siendo: $q, q' \in$ impares, $1 < q < p$

/ $q \notin$ cuadrado perfecto $\wedge \ q' \in$ cuadrado perfecto

siendo: $p = x^2 - \sigma \cdot y^2 = f_0(p)$, $x, y \in \mathbb{Z} \setminus \{0\}$

$\wedge \ p \neq f_{i>0}(p)$ es decir, siendo: $x', y' \in \mathbb{Z}$ / $\forall \ x' \neq \pm x \ \wedge \ \forall \ y' \neq \pm y$

$\Rightarrow p \neq x'^2 - \sigma \cdot y'^2$ es decir: $Card[f(p)] = 1$

/ en $\mathbb{Z}/p \Rightarrow x^2 \equiv \sigma y^2 \pmod p$, pero que: $\forall \mu \in (1,p-1) \Rightarrow \{\pm\mu\}^2 \not\equiv \sigma \pmod p$

(a diferencia de si p es primo (punto Iro), donde:

$\exists \ \alpha \in (1,p-1)$ / $\{\pm\alpha\}^2 \equiv \sigma \pmod p$ *(ver: Punto I pág 39)*)

II.e) Sea $p = q \cdot q'$ (p no primo impar $p > 1$), siendo: $q, q' \in$ impares, $1 < q < p$

/ $q \wedge q' \notin$ cuadrado perfecto $\wedge \ q \neq q' \ \wedge$ al menos q es primo

siendo: $p = x^2 - \sigma \cdot y^2 = f_0(p)$, $x, y \in \mathbb{Z} \setminus \{0\}$

si: $\exists \ \beta \in \mathbb{Z}$, $\beta \in (1,p-1)$ / $\{\pm\beta\}^2 \equiv \sigma \pmod p$ (...)

entonces: $\exists\ f_1(p) = x'^2 - \sigma \bullet y'^2$, con: $x', y' \in \mathbb{Z} \ / \ \forall\ x' \neq \pm x \ \wedge \ \forall\ y' \neq \pm y$

tal que: $p = x^2 - \sigma \bullet y^2 = x'^2 - \sigma \bullet y'^2 \iff p = f_0(p) = f_1(p)$ entonces:

$\Rightarrow \exists\ \beta' \in \mathbb{Z}$, $\beta' \in (1,p-1)\backslash\{\pm\beta\}$, es decir: $\beta' \not\equiv \pm\beta \pmod p$, equivalentemente:

$x^2 - \sigma \bullet y^2 \equiv 0 \pmod p \iff x^2 \equiv \sigma \bullet y^2 \pmod p \iff x \equiv \pm\beta \bullet y \pmod p$

$x'^2 - \sigma \bullet y'^2 \equiv 0 \pmod p \iff x'^2 \equiv \sigma \bullet y'^2 \pmod p \iff x' \equiv \pm\beta' \bullet y' \pmod p$

tal que: $\beta \not\equiv \pm\beta' \pmod p \ \wedge \ \{\pm\beta\}^2 \equiv \{\pm\beta'\}^2 \equiv \sigma \pmod p$

(*Nota*:) Obviamente también sus opuestos $(p-\beta) \wedge (p-\beta') \in (1,p-1)$ son raíces de σ en $\mathbb{Z}/p$, es decir, existen al menos cuatro raíces en el intervalo (1,p-1). A diferencia de los números primos que sólo tienen dos raíces: α ý $(p-\alpha)$ en el intervalo (1,p-1) ý de ciertos cuadrados perfectos como se expuso en el apartado II.c.

• Punto IIIro)

por todo lo expresado en los puntos Iro. y IIdo. anteriores

(incluido el inciso previo de la pág 4) tendremos que:

p es primo impar, si y sólo si:

$p = x^2 - \sigma \bullet y^2$, $x,y \in \mathbb{Z}\backslash\{0\}$, con: $f_0(p) = x^2 - \sigma \bullet y^2$

ý además, si y sólo si: $\exists\ \alpha \in (1,p-1) \ / \ \{\pm\alpha\}^2 \equiv \sigma \pmod p$

siendo: $\sigma = -1$ si: $p \equiv 1 \pmod 4$, $\sigma = -2$ si: $p \equiv 3 \pmod 8$, y $\sigma = +2$ si: $p \equiv 7 \pmod 8$

Tal que: $\forall\ k \in \mathbb{Z}$, $k \in (p,p-1) \wedge k \not\equiv \pm\alpha \pmod p$ entonces: $\{\pm k\}^2 \not\equiv \sigma \pmod p$

Además si: $p \not\equiv 7 \pmod 8$ entonces: $p \neq x'^2 - \sigma \bullet y'^2 \ \forall\ x' \neq \pm x \wedge \forall\ y' \neq \pm y$

• Punto IVto) $\forall p \in$ impar, $p>1$, primo ó no primo.

si: $\exists$ al menos $f_0(p) \ / \ p = f_0(p) = x^2 - \sigma \bullet y^2$ ecuación cuadrática

entonces: $x \in$ impar siempre,

lo tomamos como referencia impuesta, obteniendo entonces que la variable (y) es…: $y \in$ par si: $p \equiv 1 \pmod 4$

$y \in$ impar si: $p \equiv 3 \pmod 4$

• Punto Vto) sea $p = x^2 - \sigma \bullet y^2 \ / \ p \in$ impar, $p>1$, primo ó no primo. ý además:

puede (ó no) darse la existencia de $f_1(p), f_2(p), f_3(p), \ldots, f_w(p)$, tales que;

$p = f_{i>0}(p) = (x'^i)^2 - \sigma \bullet (y'^i)^2$, $i=1,2,\ldots,w$ entonces en $\mathbb{Z}/p$:

$\Rightarrow x^2 \equiv \sigma y^2 \pmod p$ se podrá obtener el valor β (de existir*) / $\beta \in (1,p-1)$

$\wedge \{\pm\beta\}^2 \equiv \sigma \pmod p$ es decir: $x \equiv \pm\beta \bullet y \pmod p$ syss*: $mcd(x,y) = \pm 1$

Por lo obtenido en los tres primeros puntos podremos puntualizar de forma general que:

• Punto VIto) Sea q primo, $q>2$

Ý sea: $\varsigma\in$ (-[p-1],p-1) / $\varsigma\in$ residuo cuadrático en $\mathbb{Z}/q$, para todos los primos de la forma: q=8k+1 ý/ó q=8k+3 ý/ó q=8k+5 ý/ó q=8k+7

De manera que se cumpla además que: $q = a^2 - \varsigma \bullet b^2$, $a,b\in \mathbb{Z}\setminus\{0\}$

Entonces, tomado un número p impar positivo particular / $p \equiv q \pmod 8$

se cumple que, dicho p es primo (impar), si y sólo si:

i) $p = x^2 - \varsigma \bullet y^2$, $x,y\in \mathbb{Z}\setminus\{0\}$, con: $f_0(p) = x^2 - \varsigma \bullet y^2$

ii) ý además, si y sólo si: $\exists\ \alpha\in (1,p-1)$ / $\{\pm\alpha\}^2 \equiv \varsigma \pmod p$, mcd(x,y)=±1

Tal que: $\forall\ k\in \mathbb{Z}$, $k\in (p,p-1) \wedge k \neq \pm\alpha \pmod p$ **

entonces: $\{\pm k\}^2 \neq \varsigma \pmod p$

• Además si: $(-\varsigma)>0$ entonces: $p \neq x'^2 - \varsigma \bullet y'^2\ \forall\ x' \neq \pm x \wedge \forall\ y' \neq \pm y$

ó bien si $(-\varsigma)<0$ entonces pueden existir (al menos): $x' \neq \pm x \wedge y' \neq \pm y$,

tales que: $p = x^2 - \varsigma \bullet y^2 = x'^2 - \varsigma \bullet y'^2$

/ $x \equiv \pm\alpha y \pmod p \wedge x' \equiv \pm\alpha y' \pmod p$ **

• Pudiendo diferenciar dicho valor p primo de cualquier valor p´ no primo tal que:

$p \equiv p' \pmod 8$

pues dicho valor compuesto p´, ó no tiene raíces en $\mathbb{Z}/p'$ para el valor ς (ς no es residuo cuadrático en $\mathbb{Z}/p'$) o bien existen al menos 4 raíces del mismo, en el intervalo (1,p´-1), ó bien p´ es un cuadrado perfecto, ó mcd $(x,y)\neq\pm1$.

• el punto IVto, aquí es irrelevante p es impar x puede ser impar ó par dependiendo de los valores del residuo cuadrático (ς) ý de si la variable (y) tal que: $-\varsigma \bullet y'^2$ sea un valor impar ó par.

• ***Finalmente***, podremos tomar un valor impar: $p = 8k+r$, tal que $p = x^2 - \varsigma \bullet y^2$, $x,y\in \mathbb{Z}\setminus\{0\}$ y se conozca del mismo que: ς residuo cuadrático en $\mathbb{Z}/p$ ý: $\varsigma\in$ (-[p-1],p-1) e indiferentemente de si lo es para cualquier otro primo $p'=8k'+r$. pudiéndose obtener además, si dicho p es primo ó no. Dependiendo de si existen más raíces de ς en $\mathbb{Z}/p$, más ecuaciones cuadráticas para dicho valor p (dependiendo de si $(-\varsigma)>0$ ó si $(-\varsigma)<0$), si es un cuadrado perfecto, ó mcd $(x,y)\neq\pm1$,...etc.

(fin de las premisas)

Nota: A continuación expondremos la ubicación de las demostraciones a cada uno de los apartados planteados en esta proposición.

• Conviene, no obstante, seguir paso a paso, el temario establecido para mejor comprensión del mismo y de las premisas establecidas en esta hipótesis.

- Punto Iro) demostrado en proposición 32da pág 74
- Punto IIdo) II.a) analizado en proposición 28va pág 53
- Punto IIdo) II.b) demostrado en proposición 31ra. pág 64
- Punto IIdo) II.c) demostrado en proposición 27ma. pág 49 **
- Punto IIdo) II.d) demostrado en proposición 29na. pág 54
- Punto IIdo) II.e) demostrado en proposición 30ma. pág 59
- Punto IIIro) demostrado en proposición 33ra. pág 82
- Punto IVto) demostrado en proposición 22da. pág 45
- Punto Vto) demostrado en proposición 25ta. pág 48
- Punto VIto) demostrado en proposición 34ta. pág 86

** ver también: proposición 26ta pág 48

Proposición 22da) De la hipótesis establecida en la proposición anterior se demostrará a continuación, (por su simplicidad), el punto IV tal que:

• Punto IVto) $\forall p \in$ impar, $p>1$, primo ó no primo.

si: $\exists$ al menos $f_0(p) / p = f_0(p) = x^2 - \sigma \bullet y^2$ ecuación cuadrática

entonces: $x \in$ impar siempre,

lo tomamos como referencia impuesta, obteniendo entonces que la variable (y) es…: $y \in$ par si: $p \equiv 1 \pmod 4$

$y \in$ impar si: $p \equiv 3 \pmod 4$

demostración:

si: $p \equiv 1 \pmod 4 \Rightarrow \sigma = -1 / p = x^2 - \sigma \bullet y^2 = x^2 + y^2 = f_0(p)$

como $p \in$ impar entonces ó x ó y ha de serlo tambien (obviamente no ambos).

Se estableció que $x \in$ impar siempre $\Rightarrow$ $y \in$ par necesariamente. trivial

si: $p \equiv 3 \pmod 4 \Rightarrow \sigma = \pm 2$ $\sigma = -2$ si: $p \equiv 3 \pmod 8$

$\sigma = +2$ si: $p \equiv 7 \pmod 8$

$p = x^2 - \sigma \bullet y^2 = x^2 \pm 2y^2 = f_0(p) \Rightarrow x \in$ impar necesariamente

falta demostrar que $y \in$ impar**...**:

en $\mathbb{Z}/4$ tendremos que p es equivalente: como $x \in$ impar $\Rightarrow x = 2a+1$ /

supongamos $y \in$ impar, entonces $y = 2b+1$ /

$p \equiv x^2 \pm 2y^2 \equiv (2a+1)^2 \pm 2(2b+1)^2 \equiv 4a^2+4a+1 \pm 2(4b^2+4b+1) \equiv 1 \pm 2 \equiv 3 \pmod 4$

ciertamente $p \equiv 3 \pmod 4$

supongamos $y \in$ par, entonces $y = 2b$ /

$p \equiv x^2 \pm 2y^2 \equiv (2a+1)^2 \pm 2(2b)^2 \equiv 4a^2+4a+1 \pm 2(4b^2) \equiv \underline{1} \pmod 4$

pero $p \equiv \underline{3} \pmod 4$ contradicción.

$\Rightarrow y \in$ impar si $p \equiv 3 \pmod 4$ QED.

Proposición 23ra) Por la proposición anterior, denotaremos equivalentemente para futuras demostraciones que:

$x \in$ impar siempre $\Rightarrow x = \pm(2\delta+1), \delta \in \mathbb{Z}$

si: $p \equiv 1 \pmod 4 \Rightarrow y \in$ par $\Rightarrow y = \pm(2\lambda)$ / $y^2 = 4\lambda^2$, $\lambda \in \mathbb{Z}$

si: $p \equiv 3 \pmod 4 \Rightarrow y \in$ impar $\Rightarrow y = \pm(\lambda)$ / $y^2 = \lambda^2$, $\lambda \in \mathbb{Z} \wedge \lambda \in$ impar

de forma que como teníamos que: $p = x^2 - \sigma \bullet y^2$

recordando que: $p=4k+1 \Rightarrow \sigma = -1$, si: $p=8k+3 \Rightarrow \sigma = -2$, si: $p=8k+7 \Rightarrow \sigma = +2$

de forma generalizada podremos expresar equivalentemente que:

$$p = (2\delta+1)^2 - 4\sigma^{-1}\lambda^2 = 4\delta^2+4\delta+1-4\sigma^{-1}\lambda^2$$

Puesto que:

- Si $p=4k+1 \Rightarrow \sigma = -1 \Rightarrow p = (2\delta+1)^2 - 4\sigma^{-1}\lambda^2 = (2\delta+1)^2 + 4\lambda^2 = (2\delta+1)^2 + (2\lambda)^2$

  ý como: $x = \pm(2\delta+1)$, $y = \pm(2\lambda) \Rightarrow p = x^2 + y^2 = x^2 - \sigma \bullet y^2$
- Si $p=8k+3 \Rightarrow \sigma = -2 \Rightarrow p = (2\delta+1)^2 - 4\sigma^{-1}\lambda^2 = (2\delta+1)^2 + 2\lambda^2 = (2\delta+1)^2 + 2(\lambda)^2$

  ý como: $x = \pm(2\delta+1)$, $y = \pm(\lambda) \Rightarrow p = x^2 + 2y^2 = x^2 - \sigma \bullet y^2$
- Si $p=4k+1 \Rightarrow \sigma = +2 \Rightarrow p = (2\delta+1)^2 - 4\sigma^{-1}\lambda^2 = (2\delta+1)^2 + -2\lambda^2 = (2\delta+1)^2 - 2(\lambda)^2$

  ý como: $x = \pm(2\delta+1)$, $y = \pm(\lambda) \Rightarrow p = x^2 - 2y^2 = x^2 - \sigma \bullet y^2$ trivial.

<u>Proposición 24ta)</u> (<u>Omitible</u>)

- si: $p \equiv 1 \pmod 8 \Rightarrow y \in$ par / $y = 2\lambda \wedge \lambda \in$ par
- si: $p \equiv 5 \pmod 8 \Rightarrow y \in$ par / $y = 2\lambda \wedge \lambda \in$ impar
- si: $p \equiv 3 \pmod 4 \Rightarrow y \in$ impar $\Rightarrow \lambda \in$ impar

De forma generalizada: si: $p \not\equiv 1 \pmod 8 \Rightarrow \lambda \in$ impar

<u>demostración:</u>

- <u>caso i</u>) $p \equiv 1 \pmod 8 \Rightarrow \sigma = -1 \Rightarrow p = x^2 - \sigma \bullet y^2 = (2\delta+1)^2 + 4\lambda^2$

  siendo: $\lambda = 2m+v$ con: $v = 0$ si: $\lambda \in$ par

  $v = 1$ si: $\lambda \in$ impar

  tal que: $\lambda^2 = 4m^2+4vm+v^2$

$\Rightarrow p = [4\delta^2+4\delta+1] + 4[4m^2+4vm+v^2]$

$\Rightarrow$ en $\mathbb{Z}/8$: $p \equiv 4\delta^2+4\delta+1 + 16m^2+16vm+4v^2 \pmod 8$

$\Leftrightarrow p \equiv 4\delta^2+4\delta+1+4v^2 \pmod 8 \Leftrightarrow p \equiv 4\delta(\delta+1)+1+4v^2 \pmod 8$

de forma que: $2 \mid \delta(\delta+1)$, pues ó δ es par ó lo es $(\delta+1) \Rightarrow 4\delta(\delta+1) \equiv 0 \pmod 8$

$\Rightarrow p \equiv [0] + 1 + 4v^2 \pmod 8 \Rightarrow$ como teníamos que: $p \equiv 1 \pmod 8$

$\Rightarrow p \equiv 1 \equiv 1+4v^2 \pmod 8 \Rightarrow 4v^2 \equiv 0 \pmod 8$ syss: $v = 0$

$\Rightarrow \lambda \in$ par QED.

• <u>caso ii</u>) $p \equiv 5 \pmod 8 \Rightarrow \sigma = -1 \Rightarrow p = x^2 - \sigma \bullet y^2 = (2\delta+1)^2 + 4\lambda^2$

siendo: $\lambda = 2m+v$ con: $v = 0$ si: $\lambda \in$ par

$v = 1$ si: $\lambda \in$ impar

tal que: $\lambda^2 = 4m^2+4vm+v^2$

$\Rightarrow p = [4\delta^2+4\delta+1] + 4[4m^2+4vm+v^2]$

$\Rightarrow$ en $\mathbb{Z}/8$: $p \equiv 4\delta^2+4\delta+1 + 16m^2+16vm+4v^2 \pmod 8$

$\Leftrightarrow p \equiv 4\delta^2+4\delta+1+4v^2 \pmod 8 \Leftrightarrow p \equiv 4\delta(\delta+1)+1+4v^2 \pmod 8$

de forma que: $2 \mid \delta(\delta+1)$, pues ó δ es par ó lo es $(\delta+1) \Rightarrow 4\delta(\delta+1) \equiv 0 \pmod 8$

$\Rightarrow p \equiv [0] +1+4v^2 \pmod 8 \Rightarrow$ como teníamos que: $p \equiv 5 \pmod 8$

$\Rightarrow p \equiv 5 \equiv 1+4v^2 \pmod 8 \Rightarrow 4v^2 \equiv 4 \pmod 8$ syss: $v = 1$

$\Rightarrow \lambda \in$ impar QED.

• <u>caso iii</u>) $p \equiv 3 \pmod 4 \Rightarrow \sigma \neq -1 \ / \ \sigma = -2$ si: $p \equiv 3 \pmod 8$

$\sigma = +2$ si: $p \equiv 7 \pmod 8$

$\Rightarrow p = x^2 - \sigma \bullet y^2 = x^2 \pm 2y^2 = (2\delta+1)^2 \pm 2\lambda^2$

siendo: $\lambda = 2m+v$ con: $v = 0$ si: $\lambda \in$ par

$v = 1$ si: $\lambda \in$ impar

tal que: $\lambda^2 = 4m^2+4vm+v^2$

$\Rightarrow p = [4\delta^2+4\delta+1] \pm 2[4m^2+4vm+v^2]$

$\Rightarrow$ en $\mathbb{Z}/4$: $p \equiv 4\delta^2+4\delta+1 \pm 8m^2 \pm 8vm \pm 2v^2 \pmod 4$

$\Leftrightarrow p \equiv 1 \pm 2v^2 \pmod 4$ tal que:

si: $v = 0 \Rightarrow p \equiv 1 \pmod 4$ Absurdo pues partíamos de que: $p \equiv 3 \pmod 4$

si: $v = 1 \Rightarrow p \equiv 3 \pmod 4$ correcto ý como: $\lambda = 2m+v$

$\Rightarrow \lambda \in$ impar QED.

Proposición 25ta) De la hipótesis establecida en la proposición 21ra. se demostrará a continuación, (por su simplicidad), el punto V tal que:

• Punto Vto) sea $p = x^2 - \sigma \bullet y^2$ / $p \in$ impar, $p>1$, primo ó no primo. ý además:
puede (ó no) darse la existencia de $f_1(p)$, $f_2(p)$, $f_3(p)$,..., $f_w(p)$, tales que;

$p= f_{i>0}(p) = (x'^i)^2 - \sigma \bullet (y'^i)^2$, i=1,2,...,w entonces en $\mathbb{Z}/p$:

$\Rightarrow x^2 \equiv \sigma y^2 \pmod p$ se podrá obtener el valor μ (de existir*) / $\mu \in (1,p-1)$

$\wedge \{\pm\mu\}^2 \equiv \sigma \pmod p$ es decir: $x \equiv \pm\mu \bullet y \pmod p$ syss*: $mcd(x,y)=\pm 1$

Tal que $\mu \wedge (p-\mu)$ son raíces de σ en $\mathbb{Z}/p$ (pueden existir más)

demostración:

tenemos que: $x^2 \equiv \sigma y^2 \pmod p$, entonces si: $mcd(x,y) = \pm 1 \Rightarrow \exists$ x^{-1}, y^{-1} en $\mathbb{Z}/p \Rightarrow$

$\Rightarrow \sigma$ es residuo cuadrático en $\mathbb{Z}/p \Rightarrow \exists$ $\mu \in (1,p-1)$ / $x \equiv \pm\mu \bullet y \pmod p$.

$\Rightarrow \mu \equiv \pm x \bullet y^{-1} \pmod p$. trivial.

$\Leftrightarrow x^2 \equiv \sigma y^2 \pmod p \Leftrightarrow x \equiv \sigma y^2 \bullet x^{-1} \equiv \mu \bullet \mu \bullet y^2 \bullet x^{-1} \equiv \mu y \bullet (\mu y x^{-1}) \pmod p$

$\Rightarrow \mu y x^{-1} \equiv \pm 1 \pmod p$

• si: $mcd(x,y) \neq \pm 1$ no implica que σ no sea residuo cuadrático en $\mathbb{Z}/p$, puede existir otra ecuación cuadrática tal que: $p = x'^2 - \sigma \bullet y'^2$ y cumpla que: $mcd(x',y')=\pm 1$

Proposición 26ta) si: $p \in$ cuadrado perfecto impar, entonces: $p \equiv 1 \pmod 8$ $\sigma=-1$

demostración: Sea: $q \in \mathbb{N}$, $q \in$ impar / $q^2 = p$

tal que: $q = 2m+1$, $m \in \mathbb{N}\backslash\{0\}$ (pues $p>1$)

$\Rightarrow p = q^2 = (2m+1)^2 = 4m^2+4m+1 = 4m(m+1)+1$

Entonces: ó bien $(m) \in$ par ó $(m+1) \in$ par $\Rightarrow$ en: $\mathbb{Z}/8 \Rightarrow$ $4m(m+1) \equiv 0 \pmod 8$

$\Rightarrow p \equiv \underline{4m(m+1)}+1 \equiv 1 \pmod 8$ QED.

Proposición 27ma) De la hipótesis establecida en la proposición 21ra se demostrará a continuación, el apartado II.c) tal que:

II.c) si p no es primo ý p$\in$ cuadrado perfecto impar*, entonces:

- ó: $p = x^2 - \sigma \bullet y^2 = f_0(p)$, $x \neq 0$ ($x \in$ impar) $\wedge$ $y = 0$ / $\nexists$ $f_{i>0}(p) = p$

  Recordando que: $\sigma = -1$ si: $p = 4k+1$, $\sigma = -2$ si: $p = 8k+3$ $\wedge$ $\sigma = +2$ si: $p = 8k+7$

- ó: $p = x^2 - \sigma \bullet y^2 = x'^2 - \sigma \bullet y'^2$, $x \neq 0$, $y = 0$

  / $x' \in \mathbb{Z}\backslash(\pm x, 0) \wedge y' \in \mathbb{Z}\backslash(\pm y, 0)$ es decir $p = f_0(p) = f_1(p)$

  Además: $\exists$ $\beta \in \mathbb{Z}$, $\beta \in (1, p-1)$ / $(\pm\beta)^2 \equiv \sigma \pmod p$

  $\Rightarrow$ $\sigma \in$ residuo cuadrático en $\mathbb{Z}/p$

  Tal que: $\forall$ $k \in \mathbb{Z}$, $k \in (p, p-1) \wedge k \neq \pm\beta \pmod p$

  entonces: $\{\pm k\}^2 \neq \sigma \pmod p$

- ó: $p = x^2 - \sigma \bullet y^2 = x'^2 - \sigma \bullet y'^2 = x''^2 - \sigma \bullet y''^2 = \ldots = (x'^w)^2 - \sigma \bullet (y'^w)^2$

  es decir: $p = f_0(p) = f_1(p) = f_2(p) = \ldots = f_w(p)$ / $\mathrm{Card}[f(p)] \geq 3$ tal que:

  $\mathrm{Card}[f(p)] \geq 3$ ý $4 \leq \mathrm{Card}[\beta^*] \leq 2w$ **

* se cumple que: $\forall p \in$ cuadrado perfecto impar $\Rightarrow$ $p \equiv 1 \pmod 8$ siempre.

ý además: $\exists$ $\beta \in \mathbb{Z}$ / $\{\pm\beta\}^2 \equiv \sigma \pmod p$ syss: $\exists$ $f_1(p) = p$

** dada la ecuación cuadrática: $p = (x'^i)^2 - \sigma \bullet (y'^i)^2 \Rightarrow (x'^i)^2 \equiv \sigma \bullet (y'^i)^2 \pmod p$

Tal que: existe β'^i si y sólo si: $\mathrm{mcd}(x'^i, y'^i) = \pm 1$ / $x'^i \equiv \pm\beta'^i \bullet y'^i \pmod p$

pues si $\mathrm{mcd}(x'^i, y'^i) = k$, $k \neq \pm 1$ entonces $k \mid p \Rightarrow \nexists\ k^{-1}$ en $\mathbb{Z}/p$

$\Rightarrow \nexists\ (x'^i)^{-1}, (y'^i)^{-1}$ en $\mathbb{Z}/p$, pues: $k \mid x'^i \wedge k \mid y'^i$

Importante: si β es raíz de σ en $\mathbb{Z}/p$ también lo es $(p-\beta)$ y por tanto, se expone que $4 \leq \mathrm{Card}[\beta^*] \leq 2w$, como mímimo existen cuatro raíces de σ en $\mathbb{Z}/p$, en el intervalo $(1, p-1)$. es decir, existen también (al menos): $\beta' \wedge (p-\beta')$ raíces de σ en $\mathbb{Z}/p$ (ver proposición 30ma. pág 59)

• **demostración apartado i:**

Sea $q \in \mathbb{N}\backslash\{0\}$ / $p = q^2$ entonces es trivial que: $p \neq x^2 - \sigma \bullet y^2$ es absurdo

◦ Teníamos que $p \in$ cuadrado perfecto impar, entonces:

$\Rightarrow$ $p \equiv 1 \pmod 8$ siempre. Demostrado en la proposición 26ta. (pág 48)

$\Rightarrow \sigma = -1 \Rightarrow p \neq x^2 + y^2$ es absurdo /

de la proposición 22da. pág 45. tenemos además que: $x \in$ impar é $y \in$ par

como: $p \in$ impar ý $p = q^2$, basta con tomar $y = 0$ / $p \neq x^2 + (0)^2$ es absurdo

$\Rightarrow p = q^2 = x^2 = (2\delta+1)^2$ / $q = \pm x$, $x = \pm(2\delta+1)$ QED.

$\Rightarrow p = x^2 - \sigma \bullet y^2$, $y = 0$ / σ no es residuo cuadrático en $\mathbb{Z}/p$

<u>Corolario)</u>

• del Punto Iro de la Hipótesis de la proposición 21ra (pág 39) teníamos además que:

Si p es primo $\Rightarrow$ $\exists$ $x,y \in \mathbb{Z}\backslash\{0\}$ tal que: $p = x^2 - \sigma \bullet y^2$, siendo $x \in$ impar

con: $\sigma = -1$ si: $p = 4k+1$

$\wedge$ $y \in$ par si: $p \equiv 1 \pmod 4$ (ver: proposición 22da pág 45)

Entonces: $\forall$ $x', y' \in \mathbb{Z}\backslash\{0\}$ / $\forall$ $x' \neq \pm x \wedge \forall y' \neq \pm y \Rightarrow p \neq x'^2 - \sigma \bullet y'^2$

◦ además $\forall p$ primo $\Rightarrow$ $\sigma \in$ residuo cuadrático en $\mathbb{Z}/p$

/ $\exists$ $\alpha \in \mathbb{Z}$, $\alpha \in (1,p-1)$ / $(\pm\alpha)^2 \equiv \sigma \pmod p$ ($\pm\alpha$ raíces <u>únicas</u> de σ * en $\mathbb{Z}/p$)

* Tal que: $\forall$ $k \in \mathbb{Z}$, $k \in (p,p-1) \wedge k \not\equiv \pm\alpha \pmod p$ entonces: $\{\pm k\}^2 \not\equiv \sigma \pmod p$

◦ además en: $\mathbb{Z}/p \Rightarrow x^2 - \sigma \bullet y^2 \equiv 0 \pmod p \Leftrightarrow x^2 \equiv \sigma \bullet y^2 \pmod p$

con $\sigma \in$ residuo cuadrático en $\mathbb{Z}/p$ tal que: $mcd(x,y) = \pm 1 \Leftrightarrow x \equiv \pm\alpha \bullet y \pmod p$

• quedando diferenciados los números primos de los cuadrados perfectos que tan sólo son expresables con una ecuación cuadrática, la cual sea suma de dos cuadrados.

Pues tendríamos que $q = x^2 + y^2 = f_0(p)$, $x \neq 0$ ($x \in$ impar) $\wedge$ $y = 0$

, q cuadrado perfecto / σ no es residuo cuadrático en $\mathbb{Z}/q$

Mientras que los primos de la forma ($p=4k+1$), son: $p = x^2 + y^2$, $x,y \in \mathbb{Z}\backslash\{0\}$

, p primo / σ es residuo cuadrático en $\mathbb{Z}/p$

Quedan también diferenciados de los cuadrados perfectos con múltiples ecuaciones cuadráticas tales que:

$q = x^2 + y^2 = x'^2 + y'^2 = x''^2 + y''^2 = \ldots = (x'^w)^2 + (y'^w)^2$

(no olvidar de la proposición 26 pág 48) que $\forall q \in$ cuadrado perfecto impar,

entonces: $p \equiv 1 \pmod 8 \Rightarrow \sigma = -1$)

Nota Importante:

• falta demostrar que: existen cuadrados perfectos impares p tales que $\nexists\ f_{i>0}(p) = p$

es decir: $p \neq x'^2 - \sigma \bullet y'^2\ \forall y \neq 0$

bastará con tomar unos ejemplos: p = 9, 49, 81,...

además para este tipo de caso concreto ocurre para dichos elementos que:

$\forall \mu \in (1,p-1) \Rightarrow \{\pm\mu\}^2 \not\equiv \sigma \pmod p$

trivial, tenemos que: $p = q^2 = x^2 = (2\delta+1)^2$

en $\mathbb{Z}/p$: $\Rightarrow (2\delta+1)^2 \equiv 0 \pmod p$ aplicando $[\sigma]$

$\Leftrightarrow \sigma(2\delta+1)^2 \equiv 0 \pmod p$*,

supongamos lo contrario tal que: $\exists\ \beta \in (1,p-1)\ /\ \{\pm\beta\}^2 \equiv \sigma \pmod p$

Aplicando ($\%^{1/2}$) "raíz cuadrada" tendremos que*: $\pm\beta(2\delta+1) \equiv 0 \pmod p$,

Para que se cumpla la congruencia con cero $\Rightarrow \beta \equiv \pm(2\delta+1) \pmod p$

Pero entonces: $\beta^2 \equiv (2\delta+1)^2 \equiv x^2 \equiv q^2 \equiv 0 \pmod p$ es decir: $\{\pm\beta\}^2 \not\equiv \sigma \pmod p$

Contradicción pues suponíamos que: $\{\pm\beta\}^2 \equiv \sigma \pmod p$ (lo que es falso)

$\Rightarrow$ entonces: $\sigma \notin$ residuo cuadrático en $\mathbb{Z}/p$

$\Rightarrow \forall \mu \in (1,p-1) \Rightarrow \{\pm\mu\}^2 \not\equiv \sigma \pmod p$ QED.

• **sobre el apartado ii:**

$p = x^2 - \sigma \bullet y^2 = x'^2 - \sigma \bullet y'^2,\ x \neq 0,\ y = 0$

$/\ x' \in \mathbb{Z}\backslash(\pm x,0) \wedge y' \in \mathbb{Z}\backslash(\pm y,0)$ es decir $p = f_0(p) = f_1(p)$

Además: $\exists\ \beta \in \mathbb{Z}\ ,\ \beta \in (1,p-1)\ /\ (\pm\beta)^2 \equiv \sigma \pmod p$

$\Rightarrow \sigma \in$ residuo cuadrático en $\mathbb{Z}/p$

Tal que: $\forall\ k \in \mathbb{Z}, k \in (p,p-1) \wedge k \not\equiv \pm\beta \pmod p$

entonces: $\{\pm k\}^2 \not\equiv \sigma \pmod p$

$\exists\ \beta \in \mathbb{Z}\ /\ \{\pm\beta\}^2 \equiv \sigma \pmod p$ syss: $\exists\ p = f_1(p) = x'^2 - \sigma \bullet y'^2\ /\ \text{mcd}(x',y') = \pm 1$

Sabemos ya que: $\forall\ p \in$ cuadrado perfecto impar, $\Rightarrow p \equiv 1 \pmod 8$ siempre.

$\Rightarrow \sigma = -1$ *(ver: demostración en proposición 26ta. pág. 48)*

//

No es necesaria dicha demostración, ya han quedado diferenciados dichos cuadrados perfectos de los números primos (ver corolario pág 50) , quedaría demostrar el punto Iro de dicha hipótesis ver: proposición 32da pág 74.
Sirvan como ejemplos para ver que ciertamente existen cuadrados perfectos expresables equivalentes a dos ecuaciones cuadráticas, las cuales son suma de dos cuadrados perfectos, tales que:
$q_1=25=5^2+0^2=3^2+4^2$ $q_2=169=13^2+0^2=5^2+12^2$ $q_3=289=17^2+0^2=15^2+8^2$ (...)

• Conjeturamos que:
si q es cuadrado perfecto tal que: $\sqrt{q} \equiv 1 \pmod 4$ con $\sqrt{q}$ primo, entonces:

$$q = x^2 - \sigma \bullet y^2 = x'^2 - \sigma \bullet y'^2 \ , \ \sigma = -1$$

y si: q es cuadrado perfecto tal que: $\sqrt{q} \equiv 3 \pmod 4$ con $\sqrt{q}$ primo,

entonces: $q = x^2 - \sigma \bullet y^2$, $y=0$, $\sigma = -1$.

$$/ \ \forall \ x',y' \in \mathbb{Z} \ , \ x' \neq \pm x \wedge y \neq 0 \ \Rightarrow q \neq x'^2 - \sigma \bullet y'^2$$

(Omitimos demostraciones por ser innecesarias, el apartado ii. ya ha quedado diferenciado de los números primos.)

• **sobre el apartado iii:**

$$p = x^2 - \sigma \bullet y^2 = x'^2 - \sigma \bullet y'^2 = x''^2 - \sigma \bullet y''^2 = \ldots = (x'^w)^2 - \sigma \bullet (y'^w)^2 \ , \ \sigma = -1$$

es decir: $p = f_0(p) = f_1(p) = f_2(p) = \ldots = f_w(p)$ / $Card[f(p)] \geq 3$ tal que:
$Card[f(p)] \geq 3$

diferenciado también de los números primos, sirva como ejemplo...:

$$q = 5625 = \{25^2 \bullet 3^2\} = 75^2+0^2 = 21^2+72^2 = 45^2+60^2$$

$Card[f(q)]=4 \Rightarrow$ q no es primo / *además*: $mcd(x^*,y^*) \neq \pm 1 \ \forall \ x^*,y^* \in \mathbb{Z}\backslash\{0\} \Rightarrow \nexists \beta \ldots$

Nota Importante:

Dado p impar / $p=4k+1$/ $Card[f(p)] \geq 2$ $\Rightarrow$p no es primo

Dado p impar / $p=4k+1$/ $Card[f(p)] = 1$ $\Rightarrow$p no es primo si...

si σ no es residuo cuadrático en $\mathbb{Z}/p$

p es primo, si σ es residuo cuadrático en $\mathbb{Z}/p$

Proposición 28va)

De la hipótesis establecida en la proposición 21ra se analizará a continuación, el apartado II.a) tal que:

II.a) si: $p \neq x^2 - \sigma \bullet y^2 \ \forall \ x,y \in \mathbb{Z}$, $x \in$ impar $\Rightarrow$

$$\forall \ \mu \in (1,p-1) \Rightarrow (\pm\mu)^2 \not\equiv \sigma \pmod{p}$$

demostración: omitimos demostración. Innecesaria.

Importante: Observese que la transcendencia de todas las premisas expuestas en la proposición 21ra. dan relevancia a tres demostraciones, estas son:

1ro) demostrar la conjetura de Albert Girard /
Si $p \equiv 3 \pmod 4 \wedge p$ es primo, $p>2$
Entonces: $p = x^2 \pm 2y^2$ con: $x,y \in \mathbb{N}\backslash\{0\}$

2do) demostrar el teorema de Fermat (sobre suma de cuadrados) ó Lema de Thue, mediante procedimiento análogo al utilizado para la conjetura anterior. /
Si $p \equiv 1 \pmod 4 \wedge p$ es primo, $p>2$
Entonces: $p = x^2 + y^2$ con: $x,y \in \mathbb{N}\backslash\{0\}$

ý 3ro) demostrarse si: para todo entero, impar y mayor que 2, dicho elemento es primo ó compuesto (no primo).

• Por éste último punto, y debido a la premisa Ira de la hipótesis de la proposición 21ra (pág 39), (aún por demostrar), tal que:

Si p primo $\Rightarrow \exists \ x,y \in \mathbb{Z}\backslash\{0\}$ tal que: $p = x^2 - \sigma \bullet y^2$ (...)

tenemos que cualquier $p \neq x^2 - \sigma \bullet y^2 \ \forall \ x,y \in \mathbb{Z}$, $x \in$ impar

siendo: $p \in \mathbb{N}$, $p \in$ impar $\wedge \ p>1$. entonces: p no es primo

$\Rightarrow$ es condición suficiente para omitir la demostración. Pues en tal caso ya se obtiene de forma directa que el elemento p no es primo

• bastará, así mismo, con el ejemplo numérico de algunos casos que cumplan la situación propuesta inicialmente, para saber, que el caso expuesto, es posible que exista, es decir:

$\exists \ p \in \mathbb{N}$, $p \in$ impar, $p>1 \ / \ p \neq x^2 - \sigma \bullet y^2 \ \forall \ x,y \in \mathbb{Z}$, $x \in$ impar

si: $p \equiv 1 \pmod 8$ tenemos $p=33 \Rightarrow \nexists\ f_o(p) = p$

si: $p \equiv 3 \pmod 8$ tenemos $p=35 \Rightarrow \nexists\ f_o(p) = p$

si: $p \equiv 5 \pmod 8$ tenemos $p=21 \Rightarrow \nexists\ f_o(p) = p$

si: $p \equiv 7 \pmod 8$ tenemos $p=15 \Rightarrow \nexists\ f_o(p) = p$

con: $f_o(p) = x^2 - \sigma \bullet y^2 \Rightarrow p \neq f_o(p)$

• **<u>Importante:</u>** el hecho de que en tal situación, ocurra que**…:**

$$\nexists\ \beta\ /\ \forall\ \mu \in (1,p-1) \Rightarrow (\pm\mu)^2 \not\equiv \sigma \pmod p$$

si: $p \neq x^2 - \sigma \bullet y^2\ \forall\ x,y \in \mathbb{Z}$, $x \in$ impar

está conjeturado ý también omitida la demostración pertinente.
pues difiere de los elementos primos, en que en estos últimos, sí existe $f_o(p) = p$
ý por tanto es innecesario el conocimiento y/o existencia del valor β
(El análisis al apartado II.a. queda finalizado)

<u>Proposición 29na)</u>

De la hipótesis establecida en la proposición 21ra se demostrará a continuación, el apartado II.d tal que:

<u>II.d)</u> Sea $p = q \bullet q'$, p no primo impar, $p>1$

siendo: $q,q' \in$ impares, $1 < q < p$

$/\ q \notin$ cuadrado perfecto $\wedge\ q' \in$ cuadrado perfecto

siendo: $p = x^2 - \sigma \bullet y^2 = f_0(p)$, $x,y \in \mathbb{Z}\backslash\{0\}$

recordando que: $\sigma = -1$ si: $p = 4k+1$, $\sigma = -2$ si: $p = 8k+3\ \wedge\ \sigma = +2$ si: $p = 8k+7$

$\wedge\ p \neq f_{i>0}(p)$ es decir, siendo: $x',y' \in \mathbb{Z}\ /\ \forall\ x' \neq \pm x\ \wedge\ \forall\ y' \neq \pm y$

$\Rightarrow p \neq x'^2 - \sigma \bullet y'^2$ es decir: $Card[f(p)] = 1$

tal que en $\mathbb{Z}/p$: $\Rightarrow x^2 \equiv \sigma y^2 \pmod p$

pero ocurre que: $\forall\ \mu \in (1,p-1) \Rightarrow \{\pm\mu\}^2 \not\equiv \sigma \pmod p$

$\Rightarrow \sigma$ no es residuo cuadrático en $\mathbb{Z}/p$

(a diferencia de si p es primo (punto Iro), donde:

$\exists\ \alpha \in (1,p-1)\ /\ \{\pm\alpha\}^2 \equiv \sigma \pmod p$ *(ver: Punto I pág 39)*)

• Observese de los números primos (punto Iro proposición 21ra) que:

• si: $p = 4k+1$ ó $p = 8k+3$ / $p = x^2 - \sigma \bullet y^2$

Entonces, sean: $x', y' \in \mathbb{Z}\backslash\{0\}$ / $\forall\ x' \neq \pm x \wedge \forall y' \neq \pm y \Rightarrow p \neq x'^2 - \sigma \bullet y'^2$

• si: $p = 8k+7$ entonces $\exists\ x', y' \in \mathbb{Z}\backslash\{0\}$ / $x' \neq \pm x \wedge y' \neq \pm y$

/ $p = x^2 - \sigma \bullet y^2 = x'^2 - \sigma \bullet y'^2 = x''^2 - \sigma \bullet y''^2 = ... = (x'^w)^2 - \sigma \bullet (y'^w)^2$

/ $mcd(x'^i, y'^i) = \pm 1$, $\forall i = 0,1,2,3,...,w$ / $x'^i \equiv \pm\alpha \bullet y'^i \pmod p$

• además $\forall p$ primo $\Rightarrow$ $\sigma \in$ residuo cuadrático en $\mathbb{Z}/p$

/ $\exists\ \alpha \in \mathbb{Z}$, $\alpha \in (1,p-1)$ / $(\pm\alpha)^2 \equiv \sigma \pmod p$ ($\pm\alpha$ raíces <u>únicas</u> de σ * en $\mathbb{Z}/p$)

* Tal que: $\forall\ k \in \mathbb{Z}$, $k \in (p,p-1) \wedge k \not\equiv \pm\alpha \pmod p$ entonces: $\{\pm k\}^2 \not\equiv \sigma \pmod p$

• Para finalizar, es trivial, y por tanto no necesita demostración alguna que si:

$p = q \bullet q'$, p no primo impar, $p > 1$

siendo: $q, q' \in$ impares, $1 < q < p$

/ $q \notin$ cuadrado perfecto $\wedge\ q' \in$ cuadrado perfecto

Tal que:

i) si $Card[f(p)] = 1 \Rightarrow \sigma$ no es residuo cuadrático en $\mathbb{Z}/p$

es decir: $p = x^2 - \sigma \bullet y^2 = f_0(p)$, $x,y \in \mathbb{Z}\backslash\{0\}$

$\wedge\ p \neq f_{i>0}(p)$ es decir, siendo: $x', y' \in \mathbb{Z}$ / $\forall\ x' \neq \pm x\ \wedge\ \forall\ y' \neq \pm y$

$\Rightarrow p \neq x'^2 - \sigma \bullet y'^2$

suponiendo que: $\exists\ f_0(q)$ / $q = f_0(q)$ entonces, puede ocurrir que q sea primo ó sea no primo.

$q = f_0(q) = a^2 - \sigma \bullet b^2 = (2\delta+1)^2 - 4\sigma^{-1}\lambda^2$, $\lambda \neq 0$

$q' = f_0(q') = c^2 = (2\delta'+1)^2$ pues: q' es cuadrado perfecto impar

$\Rightarrow p = q \bullet q' = (c \bullet a)^2 - \sigma \bullet (c \bullet b)^2$ / $x = ca \wedge y = (cb)$ / $p = x^2 - \sigma \bullet y^2$

$\Rightarrow mcd(x,y) \neq \pm 1 \Rightarrow \sigma$ no es residuo cuadrático en $\mathbb{Z}/p$

ii) si Card[f(p)]>1 /

$p = x^2 - \sigma \bullet y^2 = x'^2 - \sigma \bullet y'^2 = x''^2 - \sigma \bullet y''^2 = ... = (x'^w)^2 - \sigma \bullet (y'^w)^2$

$\Rightarrow \exists$ al menos una ecuación cuadrática / $p = (x'^i)^2 - \sigma \bullet (y'^i)^2$

/ $mcd(x'^i, y'^i) \neq \pm 1$

(trivial la expuesta en el apartado anterior)

σ puede ser **(ó no)** un residuo cuadrático en $\mathbb{Z}/p$ (ver: ** pág. siguiente)

bastará con unos ejemplos, queda diferenciado claramente de valores naturales primos

caso i) Card[f(p)]=1

• $q = 3 \wedge q' = 25 = 5^2 + 0 = 3^2 + 4^2$ / $mcd(q,q') = \pm 1$

/ $p = qq' = [75] = 5^2 + (2)5^2$, $p \equiv 3 \pmod 8 \Rightarrow \sigma = -2$

σ no es residuo cuadrático en $\mathbb{Z}/p$

caso ii) Card[f(p)]>1

• $q = 5 \wedge q' = 25 = 5^2 + 0 = 3^2 + 4^2$ / $mcd(q,q') \neq \pm 1$

/ $p = qq' = [125] = 5^2 + 10^2 = 11^2 + 2^2$, $p \equiv 5 \pmod 8 \Rightarrow \sigma = -1$

$mcd(11,2) = \pm 1$ / $11^2 \equiv \sigma 2^2 \pmod{125} \Leftrightarrow 11 \equiv \pm\beta 2 \pmod{125}$

$\Rightarrow \beta \equiv \pm 68 \pmod{125}$ / $\{\pm\beta\}^2 \equiv \sigma \pmod p$

$\Rightarrow \sigma$ es residuo cuadrático en $\mathbb{Z}/p$

<u>más ejemplos numéricos:</u>

1ro) $p = 17*49 = 833 = 7^2 + 28^2$, $p \equiv 1 \pmod 8 \Rightarrow \sigma = -1$ / $p = x^2 - \sigma \bullet y^2 = x^2 + y^2$

$\Rightarrow 7^2 \equiv -28^2 \equiv (-1)28^2 \equiv \sigma 28^2 \pmod p \Leftrightarrow 7 \equiv \pm 28*\beta \pmod p$

$\Leftrightarrow 7 \equiv \pm(7*4)\beta \pmod p$ / $4^{-1} \equiv 625 \pmod p$

$\Rightarrow 7*625 \equiv 210 \equiv \pm 7*\beta \pmod p \Leftrightarrow 30*7 \equiv \pm 7*\beta \pmod p \not\exists 7^{-1}$ en $\mathbb{Z}/p$

Supongamos que $\beta \equiv \pm 30 \pmod p$ pero en cambio: $\{\pm\beta\}^2 \equiv 67 \pmod p$

/ $\{\pm\beta\}^2 \not\equiv \sigma \pmod p \Rightarrow \sigma$ no es residuo cuadrático en $\mathbb{Z}/p$

otros ejemplos:

2do) con: $p \equiv 1 \pmod 8 \Rightarrow p = 17*9 = 153 = 3^2+12^2$

ó $p = 41*9 = 369 = 15^2+12^2$

con: $p \equiv 5 \pmod 8 \Rightarrow p = 5*9 = 45 = 3^2+6^2$

recordando que: $p = qq'$, $q' \in$ cuadrado perfecto impar

ý que: i) $q' = f_0(q') = f_1(q')$, $f_0(q') = x^2 - \sigma \bullet y^2 \wedge f_1(q') = x'^2 - \sigma \bullet y'^2$

ii) $q' = f_0(q') \not\exists f_1(q') / f_0(q') = x^2 - \sigma \bullet y^2 \wedge f_1(q') \neq x'^2 - \sigma \bullet y'^2$

(ver: punto II.c. págs 40-41)

entonces**..:**

- $p = 5*49 = 245 = 7^2+14^2$
- $p = 3*25 = 75 = 5^2+(2)*5^2$
- $p = 11*49 = 539 = 21^2+(2)*7^2$
- $p = 3*49 = 147 = 7^2+(2)*7^2$
- $p = 25*11 = 275 = 15^2+(2)*5^2$

en todos ellos: $Card[f(p)]=1 \wedge \forall \mu \in (1,p-1) \Rightarrow \{\pm\mu\}^2 \not\equiv \sigma \pmod p$

es decir σ no es residuo cuadrático en $\mathbb{Z}/p$

pero**..:**

- $p = 3*9 = 27 = 3^2+(2)*3^2 = 5^2+(2)*1^2$ ** / $Card[f(p)] = 2 > 1$

  $\beta \equiv \pm 5 \pmod p$, $Card(\beta^*)=2$ dos raíces 5 y (p-5) en $\mathbb{Z}/p$

- $p = 11*9 = 99 = 1^2+(2)*7^2 = 7^2+(2)*5^2$ ** / $Card[f(p)] = 2 > 1$

  $\beta \equiv \pm 85 \pmod p \wedge \beta' \equiv \pm 41 \pmod p$, $Card(\beta^*)=4$, cuatro raíces en $\mathbb{Z}/p$

en los cuales: $Card[f(p)] > 1$ (dos ecuaciones cuadráticas)

$\wedge \exists \beta^* / \{\pm\beta^*\}^2 \equiv \sigma \pmod p / Card(\beta^*) \geq 2$

si fueran primos $\Rightarrow Card[f(p)]=1 \ \forall p \not\equiv 7 \pmod 8$ p primo

con únicamente dos raíces en (1,p-1) para el valor σ en $\mathbb{Z}/p$

(ver: proposición 21 Punto Iro.)

Obsérvese con más precisión, de los ejemplos ** anteriores, tales que:

- $p = 3*9 = 27 = 3^2+(2)*3^2 = 5^2+(2)*1^2$ / $27 \equiv 3 \pmod 8 \Rightarrow \sigma=-2$
  - $3^2+(2)*3^2 \equiv 0 \pmod{27} \Leftrightarrow 3^2 \equiv (-2)*3^2 \pmod{27}$

  $\Leftrightarrow 3^2 \equiv 3^2\sigma \pmod{27}$ $\nexists$ 3^{-1}
  - $5^2+(2)*1^2 \equiv 0 \pmod{27} \Leftrightarrow 5^2 \equiv (-2)*1^2 \pmod{27}$

  $\Leftrightarrow 5^2 \equiv 1^2\sigma \pmod{27} \Leftrightarrow 5 \equiv \pm 1\beta \pmod{27} \Leftrightarrow \beta \equiv \pm 5 \pmod{27}$
- $p = 11*9 = 99 = 1^2+(2)*7^2 = 7^2+(2)*5^2$ / $99 \equiv 3 \pmod 8 \Rightarrow \sigma=-2$
  - $1^2+(2)*7^2 \equiv 0 \pmod{99} \Leftrightarrow 1^2 \equiv (-2)*7^2 \pmod{99}$ / $7^{-1} \equiv 85 \pmod{99}$

  $\Leftrightarrow 7^{-2} \equiv \sigma \pmod{99} \Leftrightarrow 85^2 \equiv \sigma \pmod{99} \Leftrightarrow \beta \equiv \pm 85 \pmod{99}$
  - $7^2+(2)*5^2 \equiv 0 \pmod{99} \Leftrightarrow 7^2 \equiv (-2)*5^2 \pmod{99}$ / $5^{-1} \equiv 20 \pmod{99}$

  $\Leftrightarrow 7^2*5^{-2} \equiv \sigma \pmod{99} \Leftrightarrow 7^2*20^2 \equiv \sigma \pmod{99} \Leftrightarrow \beta' \equiv \pm 7*20 \equiv \pm 41 \pmod{99}$

  $\Rightarrow \exists\ \beta, \beta'$ / $\beta \not\equiv \pm \beta' \pmod p \wedge$ / $\{\pm\beta\}^2 \equiv \{\pm\beta'\}^2 \equiv \sigma \pmod p$

(ver definición punto II.b) pág 40)

---

otros ejemplos numéricos:

$p = 13*(25*9) = 2925 = 3^2+54^2 = 45^2+30^2 = 51^2+18^2$ / $mcd(q,q') = \pm 1$

$p = 5*(25*9) = 1125 = 15^2+30^2 = 33^2+6^2$ / $mcd(q,q') \neq \pm 1$

$p = 13*(49*9) = 5733 = 63^2+42^2$ / $mcd(q,q') = \pm 1$

$p = 65*(49) = 3185 = 7^2+56^2 = 49^2+28^2$ / $mcd(q,q') = \pm 1$

$p = 17*(49) = 833 = 7^2+28^2$ / $mcd(q,q') = \pm 1$

/ $\forall \mu \in (1,p-1) \Rightarrow \{\pm\mu\}^2 \not\equiv \sigma \pmod p$

ó bien: $\forall p$ / $Card[f(p)]=0$ es decir: $p \neq x^2 - \sigma \bullet y^2$ $\forall x,y \in Z \setminus \{0\}$

$p = 33*25 = 825$	$p = 33*49 = 1617$
$p = 21*25 = 525$	$p = 21*49 = 1029$

Proposición 30ma) De la hipótesis establecida en la proposición 21ra se demostrará a continuación, el apartado II.e) tal que:

II.e) Sea $p = q \bullet q'$ (p no primo impar $p>1$), siendo: $q,q' \in$ impares, $1 < q < p$

$/\ q \wedge q' \notin$ cuadrado perfecto $\wedge\ q \neq q' \wedge$ al menos q es primo

siendo: $p = x^2 - \sigma \bullet y^2 = f_0(p)$, $x,y \in \mathbb{Z}\backslash\{0\}$

recordando que: $\sigma = -1$ si: $p = 4k+1$, $\sigma = -2$ si: $p = 8k+3$ $\wedge$ $\sigma = +2$ si: $p = 8k+7$

si: $\exists\ \beta \in \mathbb{Z}, \beta \in (1,p-1)\ /\ \{\pm\beta\}^2 \equiv \sigma \pmod p$

entonces: $\exists\ f_1(p) = x'^2 - \sigma \bullet y'^2$, con: $x',y' \in \mathbb{Z}\ /\ \forall\ x' \neq \pm x\ \wedge\ \forall\ y' \neq \pm y$

tal que: $p = x^2 - \sigma \bullet y^2 = x'^2 - \sigma \bullet y'^2 \iff p = f_0(p) = f_1(p)$ entonces:

$\Rightarrow \exists\ \beta' \in \mathbb{Z}$, $\beta' \in (1,p-1)\backslash\{\pm\beta\}$, es decir: $\beta' \neq \pm\beta \pmod p$, equivalentemente:

$x^2 - \sigma \bullet y^2 \equiv 0 \pmod p \iff x^2 \equiv \sigma \bullet y^2 \pmod p \iff x \equiv \pm\beta \bullet y \pmod p$

$x'^2 - \sigma \bullet y'^2 \equiv 0 \pmod p \iff x'^2 \equiv \sigma \bullet y'^2 \pmod p \iff x' \equiv \pm\beta' \bullet y' \pmod p$

tal que: $\beta \neq \pm\beta' \pmod p \wedge \{\pm\beta\}^2 \equiv \{\pm\beta'\}^2 \equiv \sigma \pmod p$

(*Nota*:) Obviamente también sus opuestos $(p-\beta) \wedge (p-\beta') \in (1,p-1)$ son raíces de σ en $\mathbb{Z}/p$, es decir, existen al menos cuatro raíces en el intervalo $(1,p-1)$. A diferencia de los números primos que sólo tienen dos raíces: α ý $(p-\alpha)$ en el intervalo $(1,p-1)$ ý de ciertos cuadrados perfectos como se expuso en el apartado II.c.

Inciso Previo: (omitimos demostrar los siguientes aptdos. por resultar triviales)

1ro) si: $a \in (1,p-1)\ /\ a \in$ residuo cuadrático en $\mathbb{Z}/p$

entonces: $a^{-1} \in$ residuo cuadrático en $\mathbb{Z}/p$ syss: $\exists\ a^{-1}$ en $\mathbb{Z}/p$

2do) si tenemos que: $a^2 b \equiv c \pmod p$ ý se asegura que:

- $b \notin$ residuo cuadrático en $\mathbb{Z}/p$, entonces: $c \notin$ residuo cuadrático en $\mathbb{Z}/p$

  $cb^{-1} \in$ residuo cuadrático en $\mathbb{Z}/p$

- $b \in$ residuo cuadrático en $\mathbb{Z}/p$, entonces: $c \in$ residuo cuadrático en $\mathbb{Z}/p$

---

demostración:

Sea $p = qq' \;/\; q,q' \notin$ cuadrado perfectos, $q \neq q'$

de forma que es condición necesaria ý suficiente, que:

q sea primo, entonces $\exists\ f_0(q)$ (existe ecuación cuadrática) /

$$q = f_0(q) = x^2 - \sigma_q \bullet y^2 = (2\delta+1)^2 - 4\sigma_q^{-1}\lambda^2 \quad *,\ \lambda \neq 0$$

recordamos que: $\sigma_q = -1$ si: $p = 4k+1$, $\sigma_q = -2$ si: $p = 8k+3$ $\wedge$ $\sigma_q = +2$ si: $p = 8k+7$

(* (argumentado en punto Iro de la hipótesis general (pág 39)
ý demostrado en la proposición 32da pág 74)

mientras que: $q' = f_0(q')$ ó $q' \neq f_0(q')$ es decir puede $\exists$ ó $\nexists\ f_0(q') = q'$

si existe, entonces: $q' = f_0(q') = x'^2 - \sigma_{q'} \bullet y'^2 = (2\delta'+1)^2 - 4\sigma_{q'}^{-1}\lambda'^2$, $\lambda' \neq 0$

* además, es trivial que existe q primo siempre / $q \mid p$

$p = p_1^a p_2^b p_3^c \ldots p_{n-1}^{w-1} p_n^w$ $\forall\ p_i$ primo / $q = p_k$, $k \in [1,n]$

suponíamos así mismo que: $p = x^2 - \sigma_p \bullet y^2 = f_0(p)$, $x,y \in \mathbb{Z}\backslash\{0\}$

tal que: $p = f_0(p) = x_p^2 - \sigma_p \bullet y_p^2 = (2\delta_p+1)^2 - 4(\sigma_p)^{-1}\lambda_p^2$

entonces, puede ocurrir que: $\sigma_q = \sigma_p$ ó $\sigma_q \neq \sigma_p$

Tenemos por tanto que: q es primo siendo: $q = (2\delta+1)^2 - 4\sigma_q^{-1}\lambda^2$, $\lambda \neq 0$

aplicando (q'^2) tenemos que:

$\Leftrightarrow\ qq'^2 = (2\delta+1)^2 q'^2 - 4\sigma_q^{-1}\lambda^2 q'^2 = pq'$, puesto que: $p = qq'$

/ en $\mathbb{Z}/p$ tenemos que: $(2\delta+1)^2 q'^2 - 4\sigma_q^{-1}\lambda^2 q'^2 \equiv 0 \pmod p$

$\Leftrightarrow (2\delta+1)^2 q'^2 \equiv 4\sigma_q^{-1}\lambda^2 q'^2 \pmod p$ aplicando σ_q tenemos:

$\Leftrightarrow (2\delta+1)^2 \sigma_q q'^2 \equiv 4\lambda^2 q'^2 \pmod p$

Sea $\xi \in \mathbb{Z}\backslash\{0\}$, $\xi \in (p,p-1)$ / $\xi\sigma_q \equiv \sigma_p \pmod p$ por tanto, aplicando ξ tenemos:

$$\Leftrightarrow (2\delta+1)^2 \sigma_p q'^2 \equiv 4\lambda^2 q'^2 \xi \pmod p$$

Inciso: **¿** $\exists\ \xi$, $\xi \in$ (p,p-1) / $\xi\sigma_q \equiv \sigma_p \pmod p$ **???**

es decir: **¿** ξ es ó no es residuo cuadrático en $\mathbb{Z}/p$**???**

veamos unos ejemplos, para mayor comprensión..:

i) $q \equiv 7 \pmod 8 \Rightarrow \sigma_q = 2 \wedge p \equiv 1 \pmod 4 \Rightarrow \sigma_p = -1$ /

$\Rightarrow A^2\sigma_q \equiv B^2 \pmod p$ aplicando (-2^{-1}) tendremos que:

$\Leftrightarrow A^2(2)(-2^{-1}) \equiv B^2(-2^{-1}) \pmod p$ siendo: $\xi = (-2^{-1})$

$\Leftrightarrow A^2(-1) \equiv A^2\sigma_p \equiv B^2(-2^{-1}) \equiv B^2\xi \pmod p$

$\Leftrightarrow A^2\sigma_p \equiv B^2\xi \pmod p$

entonces: $\xi \in$ residuo cuadrático en $\mathbb{Z}/p$

si ý sólo si: $\sigma_p \in$ residuo cuadrático en $\mathbb{Z}/p$

ii) $q \equiv 7 \pmod 8 \Rightarrow \sigma_q = 2 \wedge p \equiv 3 \pmod 8 \Rightarrow \sigma_p = -2$ /

$\Rightarrow A^2\sigma_q \equiv B^2 \pmod p$ aplicando (-1) tendremos que:

$\Leftrightarrow A^2(2)(-1) \equiv A^2(-2) \equiv A^2\sigma_p \equiv B^2(-1) \pmod p$ siendo: $\xi = (-2^{-1})$

ý sabemos por el punto iv) (pág 3) que si: $p \equiv 3 \pmod 4$ ý m es un residuo cuadrático en $(\mathbb{Z}/p)$, entonces (-m) no es un residuo cuadrático en $(\mathbb{Z}/p)$.

por tanto, como: $1 \in$ residuo cuadrático en $\mathbb{Z}/p$

entonces: $(-1) \notin$ residuo cuadrático en $\mathbb{Z}/p$

$\Rightarrow \sigma_p \notin$ residuo cuadrático en $\mathbb{Z}/p$

de forma que: $\forall \mu \in (1,p-1) \Rightarrow \{\pm\mu\}^2 \not\equiv \sigma_p \pmod p$

De manera que podemos argumentar que:

- si: $\xi \in$ residuo cuadrático en $\mathbb{Z}/p$

$\Rightarrow \exists\ \beta \in (1,p-1) \Rightarrow \{\pm\beta\}^2 \equiv \sigma_p \pmod p$

σ_p es un residuo cuadrático en $\mathbb{Z}/p$

- si: $\xi \notin$ residuo cuadrático en $\mathbb{Z}/p$

$\Rightarrow \nexists \beta$ / $\forall \mu \in (1,p-1) \Rightarrow \{\pm\mu\}^2 \not\equiv \sigma_p \pmod p$

σ_p no es un residuo cuadrático en $\mathbb{Z}/p$

Por tanto, la dificultad radica en saber si: ξ es ó no es residuo cuadrático en $\mathbb{Z}/p$

No trataremos de resolver si ξ es ó no residuo cuadrático en $\mathbb{Z}/p$, podría resultar bastante extensa la resolución del mismo problema, bastará con la siguiente argumentación:

- Supongamos que: $\xi\in$ residuo cuadrático en $\mathbb{Z}/p$, de manera que:

$$\exists\ \tau\in\ \mathbb{Z}\ ,\tau\in\ (1,p-1)\ /\quad \tau^2 \equiv \xi\ (\text{mod } p)$$

Teníamos de la pág 60 que: $(2\delta+1)^2\sigma_p q'^2 \equiv 4\lambda^2 q'^2 \xi\ (\text{mod } p)$

De forma que equivalentemente:

$$\Leftrightarrow (2\delta+1)^2\sigma_p q'^2 \equiv 4\lambda^2 q'^2\tau^2\ (\text{mod } p)\quad \left(\text{syss: } \tau^2 \equiv \xi\ (\text{mod } p)\right)$$

Aplicando ($\%^{1/2}$) "raíz cuadrada" obtenemos:

$$\Leftrightarrow (2\delta+1)\beta q' \equiv \pm 2\lambda q'\tau\ (\text{mod } p)^* \qquad \left(\text{syss: } \tau^2 \equiv \xi\ (\text{mod } p)\right)$$

Tal que en $\mathbb{Z}$ resultará que:

$$\Leftrightarrow (2\delta+1)\beta q' = \pm 2\lambda q'\tau + pz\ ,\ z\in\ \mathbb{Z}\quad \left(\text{syss: } \tau^2 \equiv \xi\ (\text{mod } p)\right)$$

- Bastará con demostrar que $\exists\ \beta'\in\ (1,p-1)\ /\ \beta \not\equiv \pm\beta'\ (\text{mod } p)$

  ý que, en cambio, se cumple que: $\{\pm\beta\}^2 \equiv \{\pm\beta'\}^2 \equiv \sigma_p\ (\text{mod } p)$

- Por tanto si: $p = qq'$, q primo ý $q'>1$ ý además:

  i) $q \wedge q' \notin$ cuadrado perfecto impares $\wedge\ q \neq q'$

  ii) ý $\exists\ \ \beta\in\ \mathbb{Z}, \beta\in\ (1,p-1)\ /\ \{\pm\beta\}^2 \equiv \sigma\ (\text{mod } p)$

  Entonces: $p = x^2 - \sigma \bullet y^2 = x'^2 - \sigma \bullet y'^2\ \forall\ x' \neq \pm x\ \wedge\ \forall\ y' \neq \pm y$

  $$\wedge\ x, x', y, y' \in\ \mathbb{Z}\backslash\{0\}$$

  siendo: $f_0(p) = x^2 - \sigma \bullet y^2\ \wedge\ \ f_1(p) = x'^2 - \sigma \bullet y'^2$

- Teníamos que: $(2\delta+1)q'\beta \equiv \pm 2\lambda q'\tau\ (\text{mod } p)^*$

  $$\text{syss: } \tau^2 \equiv \xi\ (\text{mod } p)$$

  para cumplir con la demostración, bastará con que: $\exists\ \ \beta'\ /$

Supongamos que: $\beta' = \pm\beta + qd$, $d\in\ \mathbb{Z}\backslash\{0\}$ ** siendo claro que: $q'q \equiv 0\ (\text{mod } p)$

entonces es trivial que de existir β' ocurre que: $\{\pm\beta\}^2 \equiv \{\pm\beta'\}^2 \equiv \sigma_p\ (\text{mod } p)$

equivalentemente resultará que:

$$\{\pm\beta\}^2 \equiv \{\pm\beta'\}^2 \equiv \{\pm\beta + qd\}^2 \equiv \sigma_p \pmod p$$

$$\Leftrightarrow \{\pm\beta + qd\}^2 \equiv \beta^2 \pm 2\beta qd + q^2d^2 \equiv \sigma_p \pmod p$$

$$\Leftrightarrow \beta^2 \pm 2\beta qd + q^2d^2 \equiv \sigma_p \pmod p \Leftrightarrow q^2d^2 \pm 2\beta qd + (\beta^2 - \sigma_p) \equiv 0 \pmod p$$

$$\Leftrightarrow q^2d^2 \pm 2\beta qd + (\sigma_p - \sigma_p) \equiv 0 \pmod p \Leftrightarrow q^2d^2 \pm 2\beta qd \equiv 0 \pmod p$$

$\Rightarrow$ ó: $d \equiv 0 \pmod p$ ó $q^2d \pm 2\beta q \equiv 0 \pmod p$

teníamos de la página anterior ** que: $d \in \mathbb{Z}\backslash\{0\} \Rightarrow d \not\equiv 0 \pmod p$

tomemos, por tanto: $q^2d \pm 2\beta q \equiv 0 \pmod p \Leftrightarrow q(qd \pm 2\beta) \equiv 0 \pmod p$

$/\nexists\ q^{-1} \wedge\ q \not\equiv 0 \pmod p \Rightarrow (qd \pm 2\beta) \equiv 0 \pmod p$

pero como: $d \not\equiv 0 \pmod p\ \wedge\ (qd \pm 2\beta) \equiv 0 \pmod p$ **(*[ref: 1])**

$\Rightarrow \exists\ \beta' / \beta' = \pm\beta + qd$ si y sólo si además: $d \not\equiv q' \pmod p$ **(*[ref: 2])**

($d \not\equiv q'$ Se demostrará en el corolario pág. siguiente)

En tal caso, implica que existen <u>al menos</u> cuatro residuos cuadráticos tales que:

$\pm\beta \wedge \pm\beta' \in$ residuo cuadrático en $\mathbb{Z}/p$ $\beta,(p-\beta),\beta',(p-\beta') \in (1,p-1)$

$\Rightarrow \exists\ f_0(p) \wedge f_1(p)$

pues $f_0(p)$* sólo puede resolver el valor de uno de ellos, (β)

si ý sólo si: $\tau^2 \equiv \xi \pmod p$ tal que:

$*f_0(p) = x^2 - \sigma \bullet y^2 \Rightarrow x \equiv \pm\beta y \pmod p$

$f_1(p) = x'^2 - \sigma \bullet y'^2 \Rightarrow x' \equiv \pm\beta' y' \pmod p$ con: $p = f_0(p) = f_1(p)$

QED

es claro que si: $\tau^2 \not\equiv \xi \pmod p$ entonces como $(2\delta+1)^2\sigma_p q'^2 \equiv 4\lambda^2 q'^2 \xi \pmod p$

$\Rightarrow \sigma_p \notin$ residuo cuadrático en $\mathbb{Z}/p \Rightarrow \nexists\beta \Rightarrow \nexists\beta'$

<u>*Inciso:*</u> en tal caso no se ha demostrado la existencia ó no existencia de $f_0(p)$ ó de $f_1(p)$, $f_2(p)$,...,$f_w(p)$. <u>Es innecesario.</u> pues tendríamos ante tal situación que:

$\nexists\beta \Rightarrow \forall\mu \in (1,p-1) \Rightarrow \{\pm\mu\}^2 \not\equiv \sigma_p \pmod p$

A diferencia de p primo $/\exists\ \pm\alpha$ único $/\{\pm\alpha\}^2 \equiv \sigma \pmod p$

<u>*(fin del inciso)*</u>

Nota: si: $p = qq' \ , q = q' \ / \ p = q^2 \Rightarrow \beta^2 \pm 2\beta qd + q^2d^2 \equiv \sigma_p \ (\text{mod } p)$

$\Leftrightarrow \pm 2\beta qd + (\beta^2 - \sigma_p) \equiv 0 \ (\text{mod } p) \ \Leftrightarrow \pm 2\beta qd \equiv 0 \ (\text{mod } p)$

$\Rightarrow d = qk \ , k \in \mathbb{Z} \Rightarrow \nexists \beta'$ pero puede existir β (ó no)

ver: caso punto II.c de la hipótesis general de la proposición 21 págs 40-41

ejemplo: $p=25=5^2+0^2=3^2+4^2 \ / \ \beta = \pm 7$

Corolario)

partíamos de la condición de la página anterior tal que: $d \not\equiv q' \ (\text{mod } p)$ **(*[ref: 2])**

supongamos el caso contrario: $d \equiv q' \ (\text{mod } p)$ entonces tenemos en $\mathbb{Z}$ que:

$d = q' + pm \ , m \in \mathbb{Z} \Leftrightarrow d = q' + qq'm \Rightarrow d = q'e \ **, e \in \mathbb{Z}$

de forma que como suponíamos que: $\exists \ \beta' \ / \ \beta' = \pm\beta + qd$ resultará que:

$\beta' = \pm\beta + qd = \pm\beta + qq'e = \pm\beta + pe$, por ser $p = qq' \ \Rightarrow \beta' \equiv \pm\beta \ (\text{mod } p)$

Pero teníamos **(*[ref: 1])** que: $(qd \pm 2\beta) \equiv 0 \ (\text{mod } p)$ como: $d = q'e$ **

$\Leftrightarrow (qq'e \pm 2\beta) \equiv 0 \ (\text{mod } p) \ \Rightarrow \pm 2\beta \equiv 0 \ (\text{mod } p)$ Absurdo

$\Rightarrow d \not\equiv q' \ (\text{mod } p)$ como preveíamos inicialmente QED.

Proposición 31ra) De la hipótesis establecida en la proposición 21ra se demostrará a continuación, el apartado II.b) tal que: (siendo p **no** primo)

II.b) si: $p = x^2 - \sigma \bullet y^2 = x'^2 - \sigma \bullet y'^2 = x''^2 - \sigma \bullet y''^2 = \ldots = (x'^w)^2 - \sigma \bullet (y'^w)^2$

recordando que: $\sigma = -1$ si: $p = 4k+1$, $\sigma = -2$ si: $p = 8k+3 \ \wedge \ \sigma = +2$ si: $p = 8k+7$

$\forall x'^i \neq \pm x'^j, \ i \neq j \ \ (\Rightarrow y'^i \neq \pm y'^j)$ con: $x'^m, y'^m \in \mathbb{Z} \setminus \{0\}$

Siendo: $f_0(p) = x^2 - \sigma \bullet y^2$, $f_1(p) = x'^2 - \sigma \bullet y'^2$, $f_2(p) = x''^2 - \sigma \bullet y''^2$,...,

,..., $f_w(p) = (x'^w)^2 - \sigma \bullet (y'^w)^2 \ / \ p = f_0(p) = f_1(p) = f_2(p) = \ldots = f_w(p)$

Y tal que: $\exists$ al menos $f_0(p)$ ý $f_1(p)$ que cumplen dicha igualdad con p

Entonces en $\mathbb{Z}/p$ ocurre que **si:** $\sigma \in$ residuo cuadrático en $\mathbb{Z}/p \Rightarrow$

$\exists \ f_i(p) = (x'^i)^2 - \sigma \bullet (y'^i)^2 \wedge f_j(p) = (x'^j)^2 - \sigma \bullet (y'^j)^2$

ecuaciones cuadráticas distintas

$/ \ p = (x'^i)^2 - \sigma \bullet (y'^i)^2 = (x'^j)^2 - \sigma \bullet (y'^j)^2 \ \wedge \ \text{mcd}(x'^i, y'^i) = \pm 1 \ \wedge \ \text{mcd}(x'^j, y'^j) = \pm 1$

es decir, existen (al menos***): $\beta \wedge \beta' \in (1, p-1) \ / \ \beta \not\equiv \pm\beta' \ (\text{mod } p)$

y en cambio: $\{\pm\beta\}^2 \equiv \{\pm\beta'\}^2 \equiv \sigma \ (\text{mod } p)$

*** (Obviamente también sus opuestos $(p-\beta) \wedge (p-\beta') \in (1,p-1)$ son raíces de σ en $\mathbb{Z}/p$, es decir, existen al menos cuatro raíces en el intervalo (1,p-1). A diferencia de los números primos que sólo tienen dos raíces: α ý $(p-\alpha)$ en el intervalo (1,p-1) ý de <u>ciertos</u> cuadrados perfectos como se verá en el siguiente apartado II.c.)

Argumentación similar a la planteada en el punto II.e)
de la proposición 21ra. (pág 40)

<u>Demostración:</u> Bastará con demostrar que:

Sea p **no** primo entonces, suponiendo además que:

$p = x^2 - \sigma \bullet y^2 = x'^2 - \sigma \bullet y'^2$

(pudiendo existir <u>(ó no)</u> $f_2(p)$, $f_3(p)$, $f_4(p)$,…, $f_w(p)$)

entonces en $\mathbb{Z}/p$: $\Rightarrow \exists \ \beta \wedge \beta' \ / \ \beta \not\equiv \pm\beta \pmod p \wedge \{\pm\beta\}^2 \equiv \{\pm\beta'\}^2 \equiv \sigma \pmod p$

Equivalentemente ý siendo $p = qq'$, con $q \neq q'$, tal que:

$q = x_q^2 - \sigma_q \bullet y_q^2 = (2\delta+1)^2 - 4\sigma_q^{-1}\lambda^2$

$q' = x_{q'}^2 - \sigma_{q'} \bullet y_{q'}^2 = (2\delta'+1)^2 - 4\sigma_q^{-1}\lambda'^2$ con: $\lambda, \lambda' \in \mathbb{Z}\setminus\{0\}$

aplicando q' ý q respectivamente obtendremos que:

$\Leftrightarrow \quad qq' = p = (2\delta+1)^2 q' - 4\sigma_q^{-1}\lambda^2 q'$

$q'q = p = (2\delta'+1)^2 q - 4\sigma_{q'}^{-1}\lambda'^2 q$

de manera que en $\mathbb{Z}/p$ tendremos que:

$(2\delta+1)^2 q' - 4\sigma_q^{-1}\lambda^2 q' \equiv 0 \pmod p$

$(2\delta'+1)^2 q - 4\sigma_{q'}^{-1}\lambda'^2 q \equiv 0 \pmod p$ (sabemos que: $\nexists\ q^{-1} \wedge (q')^{-1}$)

$\Leftrightarrow (2\delta+1)^2 q' \equiv 4\sigma_q^{-1}\lambda^2 q' \pmod p$

$\Leftrightarrow (2\delta'+1)^2 q \equiv 4\sigma_{q'}^{-1}\lambda'^2 q \pmod p$

$\Leftrightarrow (2\delta+1)^2 q'\sigma_q \equiv 4\lambda^2 q' \pmod p$

$\Leftrightarrow (2\delta'+1)^2 q\sigma_{q'} \equiv 4\lambda'^2 q \pmod p$

Sean: $\xi \wedge \xi' \ / \ \xi,\xi' \in \mathbb{Z}\backslash\{0\} \ / \ \xi\sigma_q \equiv \sigma \pmod p \ \wedge \ \xi'\sigma_{q'} \equiv \sigma \pmod p \ \Rightarrow$

$\Leftrightarrow (2\delta+1)^2 q'\sigma \equiv 4\lambda^2 q'\xi \pmod p \Leftrightarrow (2\delta+1)^2 q'^2\sigma \equiv 4\lambda^2 q'^2\xi \pmod p$

$\Leftrightarrow (2\delta'+1)^2 q\sigma \equiv 4\lambda'^2 q\xi' \pmod p \Leftrightarrow (2\delta'+1)^2 q^2\sigma \equiv 4\lambda'^2 q^2\xi' \pmod p$

$\Rightarrow \sigma \in$ residuo cuadrático en $\mathbb{Z}/p$ si ý sólo si: $\xi,\xi' \in$ residuo cuadrático en $\mathbb{Z}/p$

Inciso: si: ξ ó $\xi' \notin$ residuo cuadrático en $\mathbb{Z}/p \Rightarrow \sigma \notin$ residuo cuadrático en $\mathbb{Z}/p$

$\Rightarrow$ p no es primo pues $\Rightarrow \nexists \alpha$.

ý $\forall$ p primo $\Rightarrow \sigma \in$ residuo cuadrático siempre ($\exists$ α raíz) *(fin del inciso)*

• por tanto suponemos $\xi,\xi' \in$ residuo cuadrático en $\mathbb{Z}/p$

(si: $\xi \in$ res. cuad. en Z/p $\Rightarrow \sigma \in$ res. cuad. en Z/p $\Rightarrow \xi' \in$ res. cuad. en Z/p)

Tal que: $\exists \ \tau,\tau' \in \mathbb{Z}$,$\tau,\tau' \in (1,p-1) \ / \ \tau^2 \equiv \xi \pmod p \ \wedge \ \tau'^2 \equiv \xi' \pmod p$

obteniendo equivalentemente que:

$(2\delta+1)^2 q'^2\sigma \equiv 4\lambda^2 q'^2\xi \pmod p \Leftrightarrow (2\delta+1)^2 q'^2\sigma \equiv 4\lambda^2 q'^2\tau^2 \pmod p$

$(2\delta'+1)^2 q^2\sigma \equiv 4\lambda'^2 q^2\xi' \pmod p \Leftrightarrow (2\delta'+1)^2 q^2\sigma \equiv 4\lambda'^2 q^2\tau'^2 \pmod p$

• denotaremos para abreviatura ý comodidad gráfica por:

$\varsigma = \lambda q'\tau \ \wedge \ \varsigma' = \lambda' q\tau' \ \wedge \ (2\upsilon+1) = (2\delta+1)q' \ ** \wedge (2\upsilon'+1) = (2\delta'+1)q \ **$

**estas igualdades son posibles debido a que:

i) si $q^* \equiv 1 \pmod 4$ entonces $q^* = 4\rho \ * +1 \Rightarrow$

$(2\upsilon+1) = (2\delta+1)q' = 2\delta q'+q' = 2\delta q'+4\rho' +1 = 2(\delta q'+2\rho') +1$

$/ \ \upsilon = \delta q'+2\rho'$

$(2\upsilon'+1) = (2\delta'+1)q = 2\delta' q+q = 2\delta' q+4\rho +1 = 2(\delta' q+2\rho) +1$

$/ \ \upsilon' = \delta' q+2\rho$

ii) si $q^* \equiv 3 \pmod 4$ entonces $q^* = 4\rho \ * +3 = (4\rho \ *+2) +1 \Rightarrow$

$(2\upsilon+1) = (2\delta+1)q' = 2\delta q'+q' = 2\delta q'+4\rho' +2+1 = 2(\delta q'+2\rho' +1) +1$

$/ \ \upsilon = \delta q'+2\rho' +1$

$(2\upsilon'+1) = (2\delta'+1)q = 2\delta' q+q = 2\delta' q+4\rho +2+1 = 2(\delta' q+2\rho +1) +1$

$/ \ \upsilon' = \delta' q+2\rho +1$

(ver: corolario 1ro. proposición 9na. pág 19 $\wedge$ proposición 16ta pág 30)

De forma que tendremos equivalentemente que:

$(2\delta+1)^2 q'^2 \sigma \equiv 4\lambda^2 q'^2 \tau^2 \pmod p \Leftrightarrow (2\upsilon+1)^2 \sigma \equiv 4\varsigma^2 \pmod p$

$(2\delta'+1)^2 q^2 \sigma \equiv 4\lambda'^2 q^2 \xi' \tau'^2 \pmod p \Leftrightarrow (2\upsilon'+1)^2 \sigma \equiv 4\varsigma'^2 \pmod p$

Aplicando ($\%^{1/2}$) "raíz cuadrada" obtendremos que:

$2\varsigma \equiv \pm(2\upsilon+1)\beta \pmod p \Leftrightarrow 2\lambda q' \tau \equiv \pm(2\delta+1) q' \beta \pmod p$

$2\varsigma' \equiv \pm(2\upsilon'+1)\beta' \pmod p \Leftrightarrow 2\lambda' q \tau' \equiv \pm(2\delta'+1) q \beta' \pmod p$

Obteniendo de las mismas equivalencias, las siguientes posibilidades.

<u>caso i)</u> $\beta \equiv \pm\beta' \pmod p \Rightarrow \lambda q' \tau \equiv \pm\lambda' q \tau' \pmod p$ ó $\lambda q' \tau \not\equiv \pm\lambda' q \tau' \pmod p$

<u>caso ii)</u> $\beta \not\equiv \pm\beta' \pmod p \Rightarrow \lambda q' \tau \equiv \pm\lambda' q \tau' \pmod p$ ó $\lambda q' \tau \not\equiv \pm\lambda' q \tau' \pmod p$

**<u>*Inciso Importante*</u>: teníamos de la página anterior que:

$\xi\sigma_q \equiv \sigma \pmod p \wedge \xi'\sigma_{q'} \equiv \sigma \pmod p \wedge \tau^2 \equiv \xi \pmod p \wedge \tau'^2 \equiv \xi' \pmod p$

/ $\tau^2\sigma_q \equiv \sigma \pmod p$* $\wedge \tau'^2\sigma_{q'} \equiv \sigma \pmod p$ syss: $\xi, \xi' \in$ residuos cuadráticos en $\mathbb{Z}/p$

<u>*(fin del inciso)*</u>

<u>demostración:</u> ¿$\beta \equiv \pm\beta' \pmod p$? supongámos cierta la congruencia, tal que:

<u>i.a)</u> $\lambda q' \tau \equiv \pm\lambda' q \tau' \pmod p$* aplicando $(q) \Rightarrow \lambda q q' \tau \equiv 0 \equiv \pm\lambda' q^2 \tau' \pmod p$, $p = qq'$

$\Leftrightarrow \pm\lambda' q^2 \tau' \equiv 0 \pmod p$, obteniendo que:

ó: $\lambda' \equiv q' k \pmod p$, $k \in \mathbb{Z}\backslash\{0\}$ ó $q \equiv q' \pmod p$

(teníamos que: $\tau'^2\sigma_{q'} \equiv \sigma \pmod p$** $\Rightarrow$ es trivial que: $\tau' \not\equiv q' m$, $m \in \mathbb{Z}\backslash\{0\}$)

<u>i.a.1)</u> $\lambda' \equiv q' k \pmod p$, $k \in \mathbb{Z}\backslash\{0\} \Rightarrow$ * $\lambda q' \tau \equiv \pm\lambda' q \tau' \equiv \pm q' k q \tau' \equiv 0 \pmod p$

$\Rightarrow \lambda \equiv qk' \pmod p$, $k' \in \mathbb{Z}\backslash\{0\} \Rightarrow \lambda = qk' + pz$, $z \in \mathbb{Z} \wedge \lambda \in (0,q)$

/ como: $q = (2\delta+1)^2 - 4\sigma_q^{-1}\lambda^2$, tenemos que: $\lambda^2 < q < p$

pues: $p = qq'$, $q' > 1 \Rightarrow \lambda < q < p$.

como suponemos que $p \notin$ cuadrado perfecto ý como: $\lambda = qk' + pz$

entonces si: $k' = 0 \Rightarrow \lambda = pz$, <u>absurdo</u> pues: $0 \leq \lambda < q < p$

si: $k' \geq 1 \Rightarrow \lambda = qk' + qq'z = q(k' + q'z)$ <u>absurdo</u> $\lambda \in (0,q)$

i.a.2) $q \equiv q' \pmod p$ como teníamos* (pág anterior): $\lambda q'\tau \equiv \pm\lambda' q\tau' \pmod p$

$\not\exists\ q'^{-1}$ pero es trivial que: $\Leftrightarrow \lambda q\tau \equiv \pm\lambda' q\tau' \pmod p$ $q \equiv q'$

$\Rightarrow \lambda \equiv \pm\lambda'\tau'\tau^{-1} \pmod p$ para que se cumpla: $\lambda q\tau \equiv \pm\lambda' q\tau' \pmod p$

como además teníamos (pág 66) que:

$(2\delta+1)^2 q'^2\sigma \equiv 4\lambda^2 q'^2\tau^2 \pmod p \Leftrightarrow (2\delta+1)^2 q^2\sigma \equiv 4\lambda^2 q^2\tau^2 \pmod p$

$(2\delta'+1)^2 q^2\sigma \equiv 4\lambda'^2 q^2\tau'^2 \pmod p$

entonces equivalentemente resulta que:

- $(2\delta+1)^2 q^2\sigma \equiv 4[\pm\lambda'\tau'\tau^{-1}]^2 q^2\tau^2 \equiv 4\lambda'^2\tau'^2\tau^{-2} q^2\tau^2 \equiv 4\lambda'^2\tau'^2 q^2$ **$\pmod p$
- $(2\delta'+1)^2 q^2\sigma \equiv 4\lambda'^2 q^2\tau'^2$ **$\pmod p$

De forma que: $\Rightarrow (2\delta+1)^2 q^2\sigma \equiv (2\delta'+1)^2 q^2\sigma \pmod p \Rightarrow \delta \equiv \delta' \pmod p$

Como teníamos de la página 65 que:

$q = (2\delta+1)^2 - 4\sigma_q^{-1}\lambda^2 \ \wedge\ q' = (2\delta'+1)^2 - 4\sigma_q^{-1}\lambda'^2$,con: $\lambda,\lambda' \in \mathbb{Z}\backslash\{0\}$

$/\ \delta \in [0,q) \wedge \delta' \in [0,q') \wedge \delta \equiv \delta' \pmod p \Rightarrow \delta = \delta' + pm \Rightarrow \delta = \delta'$, $m = 0$

$\Rightarrow q = q' \Rightarrow p \in$ cuadrado perfecto impar

Pero partíamos de que: $p = (x'^w)^2 - \sigma \bullet (y'^w)^2$ (ver página 64)

siendo: $\forall\, x'^w, y'^w \in \mathbb{Z}\backslash\{0\}$ (ver pág 64)

$\Rightarrow p \notin$ cuadrado perfecto impar: <u>contradicción</u>

Si: $p \in$ cuadrado perfecto impar, es un caso ya analizado y demostrado en la proposición 27ma. (pág 49) por tanto; este apartado tampoco será factible para el presente análisis.

<u>i.b)</u> $\lambda q'\tau \not\equiv \pm\lambda' q\tau' \pmod p$ sea $\varepsilon \in \mathbb{Z}\ /\ \lambda q'\tau\varepsilon \equiv \pm\lambda' q\tau' \pmod p$*

aplicando (q) $\Rightarrow \lambda qq'\tau\varepsilon \equiv 0 \equiv \pm\lambda' q^2\tau' \pmod p$, $p = qq'$

$\Leftrightarrow \pm\lambda' q^2\tau' \equiv 0 \pmod p$, obteniendo que:

ó: $\lambda' \equiv q'k \pmod p$, $k \in \mathbb{Z}\backslash\{0\}$ ó $q \equiv q' \pmod p$

(teníamos que: $\tau'^2\sigma_{q'} \equiv \sigma \pmod p$** inciso pág anterior

$\Rightarrow$ es trivial que: $\tau' \not\equiv q'm$, $m \in \mathbb{Z}\backslash\{0\}$)

i.b.1) $\lambda' \equiv q' k \pmod p$, $k \in \mathbb{Z}\setminus\{0\}$ de la página anterior teníamos que:

$$\lambda q'\tau\varepsilon \equiv \pm\lambda' q\tau' \pmod p *$$

$\Leftrightarrow \lambda q'\tau\varepsilon \equiv \pm\lambda' q\tau' \equiv \pm q' kq\tau' \equiv 0 \pmod p \Rightarrow \lambda q'\tau\varepsilon \equiv 0 \pmod p$

aplicando (2): $\Leftrightarrow 2\lambda q'\tau\varepsilon \equiv 0 \pmod p$

de la pág 66, teníamos que: $2\lambda q'\tau \equiv \pm(2\delta+1)q'\beta \pmod p$

$\Rightarrow 2\lambda q'\tau\varepsilon \equiv 0 \equiv \pm(2\delta+1)q'\beta\varepsilon \pmod p$

$\Leftrightarrow \pm(2\delta+1)q'\beta\varepsilon \equiv 0 \pmod p$

en $\mathbb{Z}$ tendremos: $\pm(2\delta+1)q'\beta\varepsilon = 0 + pz$, $z \in \mathbb{Z}$

$\Leftrightarrow \pm(2\delta+1)q'\beta\varepsilon = qq'z \Leftrightarrow \pm(2\delta+1)\beta\varepsilon = qz$

en $\mathbb{Z}/q$ tendremos: $\pm(2\delta+1)\beta\varepsilon \equiv 0 \pmod q$ aplicando $(\%^2)$

$\Leftrightarrow (2\delta+1)^2\sigma\varepsilon^2 \equiv 0 \pmod q$ es trivial que $\varepsilon \neq 0$

$\Rightarrow (2\delta+1)^2\sigma \equiv 0 \pmod q$ de la pág 65, teníamos que:

$q = (2\delta+1)^2 - 4\sigma_q^{-1}\lambda^2 \Leftrightarrow (2\delta+1)^2\sigma_q \equiv 4\lambda^2 \pmod q$

Sea $e \in \mathbb{Z}\setminus\{0\}$ / $\sigma e \equiv \sigma_q \pmod q \Rightarrow (2\delta+1)^2\sigma e \equiv 0 \pmod q$

$\Leftrightarrow (2\delta+1)^2\sigma_q \equiv 0 \pmod q \Rightarrow (2\delta+1)^2\sigma_q \equiv 4\lambda^2 \equiv 0 \pmod q$

$\Rightarrow$ en $\mathbb{Z}$ tendremos: $4\lambda^2 = 0 + qm$,como: $0 \leq 4\lambda^2 < q \Rightarrow \lambda = 0$

además: $\lambda q'\tau\varepsilon \equiv \pm\lambda' q\tau' \pmod p * \Rightarrow \lambda \equiv 0 \equiv \lambda' q\tau' \pmod p$

$\Leftrightarrow \lambda q'\tau\varepsilon \equiv 0 \equiv \lambda' q\tau' \pmod p \Leftrightarrow \lambda q'\tau \equiv 0 \equiv \lambda' q\tau'\varepsilon^{-1} \equiv \lambda' q\tau' \pmod p$

y partíamos inicialmente de que: i.b) $\lambda q'\tau \neq \pm\lambda' q\tau' \pmod p$ Contradicción

i.b.2) $q \equiv q' \pmod p$ de la página anterior teníamos que:

$$\lambda q'\tau\varepsilon \equiv \pm\lambda' q\tau' \pmod p *$$ aplicando (q) tendremos:

$\Leftrightarrow \lambda qq'\tau\varepsilon \equiv 0 \equiv \pm\lambda' q^2\tau' \pmod p$ / $\nexists (q')^{-1}$ pero es trivial que:

$\Leftrightarrow \lambda q'\tau\varepsilon \equiv 0 \equiv \pm\lambda' q\tau' \pmod p **$

de la página 67 teníamos que:

$$2\lambda q'\tau \equiv \pm(2\delta+1)q'\beta \pmod p *^1 \ \wedge \ 2\lambda' q\tau' \equiv \pm(2\delta'+1)q\beta' \pmod p *^2$$

Aplicando ε a la primera ecuación modular*[1], tenemos que:

$\Leftrightarrow 2\lambda\varepsilon q'\tau \equiv \pm(2\delta+1)q'\beta\varepsilon \pmod p$

ý teníamos que: $\lambda q'\tau\varepsilon \equiv 0 \equiv \pm\lambda' q\tau' \pmod p$ **pág anterior

$\Leftrightarrow 2\lambda\varepsilon q'\tau \equiv 0 \equiv \pm 2\lambda' q\tau' \pmod p$

de la segunda ecuación modular resultaba que:

$2\lambda' q\tau' \equiv \pm(2\delta'+1)q\beta' \pmod p$*[2]

$\Rightarrow \pm(2\delta'+1)q\beta' \equiv 0 \pmod p$

de forma que equivalentemente tenemos que:

$2\lambda\varepsilon q'\tau \equiv \pm 2\lambda' q\tau' \equiv 0 \equiv \pm(2\delta'+1)q\beta' \equiv \pm(2\delta+1)q'\beta\varepsilon \pmod p$***

En $\mathbb{Z}$ tendremos: $\pm(2\delta+1)q'\beta\varepsilon = 0 + pz$, $z \in \mathbb{Z}$

$\Leftrightarrow \pm(2\delta+1)q'\beta\varepsilon = qq'z \Leftrightarrow \pm(2\delta+1)\beta\varepsilon = qz$

en $\mathbb{Z}/q$: $\Rightarrow \pm(2\delta+1)\beta\varepsilon \equiv 0 \pmod q$ es trivial que $\varepsilon \neq 0$

aplicando $(\%^2)$ $\Rightarrow (2\delta+1)^2\sigma\varepsilon^2 \equiv 0 \pmod q$

de la pág 65 teníamos que:

$q = (2\delta+1)^2 - 4\sigma_q^{-1}\lambda^2 \Leftrightarrow (2\delta+1)^2\sigma_q \equiv 4\lambda^2 \pmod q$

Sea $e \in \mathbb{Z}\backslash\{0\}$ / $\sigma e \equiv \sigma_q \pmod q$ $\Rightarrow (2\delta+1)^2\sigma e \equiv (2\delta+1)^2\sigma_q \pmod q$

$\Rightarrow (2\delta+1)^2\sigma\varepsilon^2(e) \equiv 0 \equiv (2\delta+1)^2\sigma_q\varepsilon^2 \pmod q$

$\Leftrightarrow (2\delta+1)^2\sigma_q\varepsilon^2 \equiv 0 \pmod q \Rightarrow (2\delta+1)^2\sigma_q \equiv 0 \pmod q$

ý como: $(2\delta+1)^2\sigma_q \equiv 4\lambda^2 \pmod q$

$\Rightarrow (2\delta+1)^2\sigma_q \equiv 0 \equiv 4\lambda^2 \pmod q \Rightarrow \lambda \equiv 0 \pmod q$

$\Rightarrow \lambda q' \equiv 0 \pmod p \Rightarrow \lambda \equiv 0 \pmod p$ ý como teníamos que:

$2\lambda\varepsilon q'\tau \equiv \pm 2\lambda' q\tau' \equiv 0 \equiv \pm(2\delta'+1)q\beta' \equiv \pm(2\delta+1)q'\beta\varepsilon \pmod p$***

tal que: $\pm 2\lambda' q\tau' \equiv 0 \pmod p$

$\Rightarrow \pm 2\lambda'\tau' \equiv q' \pmod p$* ó $\pm 2\lambda'\tau' \equiv 0 \pmod p$

* en $\mathbb{Z}$ tendríamos: $2\lambda'\tau' = \pm q' + pz'$, $z' \in \mathbb{Z}$ pero: $q' = (2\delta'+1)^2 - 4\sigma_q^{-1}\lambda'^2$

siendo: $2\lambda' < p \Rightarrow z' = 0 \Rightarrow 2\lambda'\tau' = \pm q'$ absurdo $\Rightarrow x' = 0$ ý eso no es posible

pues $x' = \pm(2\delta'+1)$, $x' \in$ impar siempre ý $x' \neq 0$

$\Rightarrow \pm 2\lambda'\tau' \equiv 0 \pmod p \Rightarrow \lambda' \equiv 0 \pmod p$ pues: $\tau^2 \equiv \xi \pmod p \wedge \xi \not\equiv 0 \pmod p$

$\Rightarrow \lambda \equiv 0 \equiv \lambda' \pmod p$

Como teníamos de la página 65 que:

$q = (2\delta+1)^2 - 4\sigma_q^{-1}\lambda^2 \wedge q' = (2\delta'+1)^2 - 4\sigma_q^{-1}\lambda'^2$,con: $\lambda,\lambda' \in \mathbb{Z}\backslash\{0\}$

$/\ \lambda \in [0,q) \wedge \lambda' \in [0,q') \wedge \lambda \equiv \lambda' \pmod p \Rightarrow \lambda = \lambda' + pm \Rightarrow \lambda = \lambda'$, $m = 0$

$\Rightarrow q = q' \Rightarrow p \in$ cuadrado perfecto impar

Pero partíamos de que: $p = (x'^w)^2 - \sigma \bullet (y'^w)^2$ (ver página 64)

siendo: $\forall x'^w, y'^w \in \mathbb{Z}\backslash\{0\}$ (ver pág 64)

$\Rightarrow p \notin$ cuadrado perfecto impar: <u>contradicción</u>

Si: $p \in$ cuadrado perfecto impar, es un caso ya analizado y demostrado en la proposición 27va. (pág 49) por tanto; este apartado tampoco será factible para el presente análisis.

<u>Nota final al caso i)</u>

Si p no es primo $\wedge\ p \notin$ cuadrado perfecto impar, entonces p no puede hayarse en ninguna de las situaciones planteadas en este caso supuesto. Por tanto obtenemos que: $\beta \not\equiv \pm\beta' \pmod p$ situación que no es necesario analizar.

Tenemos por tanto que si existe $\beta\ /\ \{\pm\beta\}^2 \equiv \sigma \pmod p$

Es decir: si $\sigma \in$ residuo cuadrático en $\mathbb{Z}/p$ entonces:

$\Rightarrow \exists\ \beta'\ /\ \beta \not\equiv \pm\beta' \pmod p\ /\ \{\pm\beta\}^2 \equiv \{\pm\beta'\}^2 \equiv \sigma \pmod p$ QED.

(ver ejemplo numérico página siguiente)

<u>Corolario)</u> <u>(Omitible)</u>

ya hemos demostrado que: $\beta \not\equiv \pm\beta' \pmod p$

realizaremos un breve análisis del mismo:

$\beta \not\equiv \pm\beta' \pmod p$ tal que, teníamos de la página 66 que:

$(2\delta+1)^2 q'^2 \sigma \equiv 4\lambda^2 q'^2 \tau^2 \pmod p \Leftrightarrow 2\lambda q'\tau \equiv \pm(2\delta+1)q'\beta \pmod p$

$(2\delta'+1)^2 q^2 \sigma \equiv 4\lambda'^2 q^2 \tau'^2 \pmod p * \Leftrightarrow 2\lambda' q\tau' \equiv \pm(2\delta'+1)q\beta' \pmod p$

Sea $e \in \mathbb{Z}\backslash\{0\}\ /\ \beta e \equiv \pm\beta' \pmod p \Rightarrow 2\lambda' q\tau' \equiv \pm(2\delta'+1)q\beta e \pmod p$

aplicando ($\%^2$) "elevando al cuadrado", tendremos que:

$\Leftrightarrow 4\lambda^2 q'^2 \tau^2 \equiv (2\delta+1)^2 q'^2 \sigma \pmod p$

$\Leftrightarrow 4\lambda'^2 q^2 \tau'^2 \equiv (2\delta'+1)^2 q^2 \sigma e^2 \pmod p$* $\Rightarrow (2\delta'+1)^2 q^2 \sigma \equiv (2\delta'+1)^2 q^2 \sigma e^2 \pmod p$

$\Rightarrow e^2 \equiv 1 \pmod p$ pero como: $\beta \not\equiv \pm\beta' \pmod p \ \wedge \ \beta e \equiv \pm\beta' \pmod p$

$\Rightarrow e \not\equiv \pm 1 \pmod p$

De las páginas 66 ý 67 teníamos que:

$(2\upsilon+1)^2\sigma \equiv 4\varsigma^2 \pmod p \ \wedge \ (2\upsilon'+1)^2\sigma \equiv 4\varsigma'^2 \pmod p$

siendo: $\varsigma = \lambda q'\tau \ \wedge \ \varsigma' = \lambda' q\tau' \ \wedge \ (2\upsilon+1) = (2\delta+1)q' \wedge (2\upsilon'+1) = (2\delta'+1)q$

equivalentemente:

$(2\upsilon+1)^2 - 4\sigma^{-1}\varsigma^2 \equiv 0 \pmod p \Leftrightarrow (2\upsilon+1)^2 - 4\sigma^{-1}\varsigma^2 = pz = p'$

$(2\upsilon'+1)^2 - 4\sigma^{-1}\varsigma'^2 \equiv 0 \pmod p \Leftrightarrow (2\upsilon'+1)^2 - 4\sigma^{-1}\varsigma'^2 = pz' = p''$

¿ $p' = p''$?

dependera de los valores ξ, ξ', τ, τ' previamente definidos en la página 66.

teníamos de la página 65 que:

$qq' = p = (2\delta+1)^2 q' - 4\sigma_q^{-1}\lambda^2 q'$

$q'q = p = (2\delta'+1)^2 q - 4\sigma_{q'}^{-1}\lambda'^2 q$

Ejemplo: Sirva como ejemplo numérico para finalizar la proposición.

Sea $p = 5*13*17 = 1105$ / $p \equiv 1 \pmod 4 \Rightarrow \sigma = -1$ /

$p = 9^2+32^2 = 23^2+24^2 = 31^2+12^2 = 33^2+4^2$ / $x'^m < x'^{m+1}$, $m \in (0,w)$

$f_0(p) = 9^2+32^2$ / $f_1(p) = 23^2+24^2$ / $f_2(p) = 31^2+12^2$ / $f_3(p) = 33^2+4^2$

$p = f_i(p) = x^{*2} - \sigma \bullet y^{*2} = (2\delta^*+1)^2 - 4\sigma^{-1}\lambda^{*2} = (2\delta^*+1)^2 + 4\lambda^{*2}$, i=0,1,2,3

(ver proposiciones: 23ra ý 24ta págs 45-46)

$\Rightarrow$ tenemos que: $p = 1105$ / $2^{-1} = \frac{1}{2}(p+1) \Rightarrow 2^{-1} \equiv 553 \pmod p \wedge 3^{-1} \equiv 737 \pmod p$

(Inciso:) de la proposición 19na. Corolario 2do. (pág 35) /

si: $\sigma = -1 \Rightarrow \beta^{-1} \equiv -\beta \pmod p$ *(fin del inciso)*

Obteniendo que:

$p = f_0(p) = 9^2+32^2 = (9)^2 +4(16)^2 \quad / \delta = 4 \quad \lambda = 16$

$p = f_1(p) = 23^2+24^2 = (23)^2 +4(12)^2 \; / \delta = 11 \; \lambda = 12$

$p = f_2(p) = 31^2+12^2 = (31)^2 +4(6)^2 \; / \delta = 15 \; \lambda = 6$

$p = f_3(p) = 33^2+4^2 = (33)^2 +4(2)^2 \quad / \delta = 16 \; \lambda = 2$

- $f_0(p) \; / \; \delta = 4, \lambda = 16 \Rightarrow 2(16) \equiv \pm(2[4]+1)\beta \pmod p \Leftrightarrow 32 \equiv \pm 9\beta \pmod p$

$$\Rightarrow 1 \equiv \pm 242\beta \pmod p \Leftrightarrow \beta \equiv \pm 242 \pmod p$$

- $f_1(p) \; / \; \delta' = 11, \lambda' = 12 \Rightarrow 2(12) \equiv \pm(2[11]+1)\beta' \pmod p \Leftrightarrow 24 \equiv \pm 23\beta' \pmod p$

$$\Rightarrow 1 \equiv \pm 47\beta' \pmod p \Leftrightarrow \beta' \equiv \pm 47 \pmod p$$

- $f_2(p) \; / \; \delta'' = 15, \lambda'' = 6 \Rightarrow 2(6) \equiv \pm(2[15]+1)\beta'' \pmod p \Leftrightarrow 12 \equiv \pm 31\beta'' \pmod p$

$$\Rightarrow 1 \equiv \pm 463\beta'' \pmod p \Leftrightarrow \beta'' \equiv \pm 463 \pmod p$$

- $f_3(p) \; / \delta''' = 16, \lambda''' = 2 \Rightarrow 2(2) \equiv \pm(2[16]+1)\beta''' \pmod p \Leftrightarrow 4 \equiv \pm 33\beta''' \pmod p$

$$\Rightarrow 1 \equiv \pm 837\beta''' \pmod p \Leftrightarrow \beta''' \equiv \pm 837 \pmod p$$

Tal que: $\beta'^{k} \not\equiv \pm\beta'^{m} \pmod p$ con: $k \neq m$

Pero en cambio: $\{\pm\beta'^{k}\}^2 \equiv \{\pm\beta'^{m}\}^2 \equiv \sigma \equiv -1 \pmod p$

Proposición 32da) De la hipótesis establecida en la proposición 21ra se demostrará a continuación, el punto I. tal que:

• Punto Iro) Si p es primo $\Rightarrow$ $\exists$ $x,y \in \mathbb{Z}\backslash\{0\}$

tal que: $p = x^2 - \sigma \bullet y^2$, siendo $x \in$ impar

con: $\sigma = -1$ si: $p = 4k+1$, $\sigma = -2$ si: $p = 8k+3$ $\wedge$ $\sigma = +2$ si: $p = 8k+7$ **

$\wedge$ $y \in$ par si: $p \equiv 1 \pmod 4$ é $y \in$ impar si: $p \equiv 3 \pmod 4$

(ver: proposición 22da pág 45)

además:

• si: $p = 4k+1$ ó $p = 8k+3$

Entonces, sean: $x', y' \in \mathbb{Z}\backslash\{0\}$ / $\forall$ $x' \neq \pm x \wedge \forall y' \neq \pm y \Rightarrow p \neq x'^2 - \sigma \bullet y'^2$

• si: $p = 8k+7$ **

entonces $\exists$ $x', y' \in \mathbb{Z}\backslash\{0\}$ / $x' \neq \pm x \wedge y' \neq \pm y$

/ $p = x'^2 - \sigma \bullet y'^2 = x''^2 - \sigma \bullet y''^2 = \ldots = (x'^w)^2 - \sigma \bullet (y'^w)^2$

• además $\forall p$ primo $\Rightarrow$ $\sigma \in$ residuo cuadrático en $\mathbb{Z}/p$

/ $\exists$ $\alpha \in \mathbb{Z}$, $\alpha \in (1,p-1)$ / $(\pm\alpha)^2 \equiv \sigma \pmod p$ ($\pm\alpha$ raíces únicas de σ * en $\mathbb{Z}/p$)

* Tal que: $\forall$ $k \in \mathbb{Z}$, $k \in (p,p-1) \wedge k \not\equiv \pm\alpha \pmod p$ entonces: $\{\pm k\}^2 \not\equiv \sigma \pmod p$

• además en: $\mathbb{Z}/p \Rightarrow x^2 - \sigma \bullet y^2 \equiv 0 \pmod p \Leftrightarrow x^2 \equiv \sigma \bullet y^2 \pmod p$

con $\sigma \in$ residuo cuadrático en $\mathbb{Z}/p$ tal que: $\text{mcd}(x,y) = \pm 1 \Leftrightarrow x \equiv \pm\alpha \bullet y \pmod p$

• *Inciso***: si $p = 8k+7$ entonces: $p = x'^2 - \sigma \bullet y'^2 = x''^2 - \sigma \bullet y''^2 = \ldots = (x'^w)^2 - \sigma \bullet (y'^w)^2$

$\Rightarrow x' \equiv \pm\alpha \bullet y' \pmod p$, $x'' \equiv \pm\alpha \bullet y'' \pmod p$,..., $x'^w \equiv \pm\alpha \bullet y'^w \pmod p$.

(pues: $\pm\alpha$ raíces únicas de σ * en $\mathbb{Z}/p$)

(*Nota:*) estamos afirmando claramente que: -1 es residuo cuadrático en $\mathbb{Z}/p$ para los números primos de la forma $p = 4k+1$, que -2 es residuo cuadrático en $\mathbb{Z}/p$ para los números primos de la forma $p=8k+3$, y que 2 es residuo cuadrático en $\mathbb{Z}/p$ para los números primos de la forma $p=8k+7$. Debe quedar claro, que para los números primos de la forma $p = 8k+1$ los valores -2 y 2 también son residuo cuadrático en $\mathbb{Z}/p$ (esto no se demostrará). Pero que el valor σ para tales primos ($p=8k+1$ ó $p=8k+5$ es decir para: $p = 4k+1$) será $\sigma = -1$.

demostración:

Es trivial que $\forall$ p primo, $p>2$: $\exists\ \alpha\in (1,p-1) / \{\pm\alpha\}^2 \equiv \sigma \pmod p$

recordando que: $\sigma=-1$ si: $p = 4k+1$, $\sigma=-2$ si: $p = 8k+3$ $\wedge$ $\sigma=+2$ si: $p = 8k+7$

además: $\forall\ k\in \mathbb{Z}$, $k\in (p,p-1) \wedge k\not\equiv\pm\alpha \pmod p$ entonces: $\{\pm k\}^2\not\equiv \sigma \pmod p$

• Sean $x,y\in \mathbb{Z}\backslash\{0\} / p=\{\pm y\alpha +pz\}^2-\sigma y^2 /$ $\{\pm y\alpha +pz\}^2=x^2$

Sabiendo además que: $y\in$ par si: $p \equiv 1 \pmod 4$
$y\in$ impar si: $p \equiv 3 \pmod 4$
(ver: proposición 22da. pág 45)

$\Rightarrow$ con: $x\in$ impar siempre

Inciso: Es trivial que:

• si: $\sigma<0$ / *

caso i) $p=4k+1 \Rightarrow \sigma=-1 \Rightarrow p= x^2-\sigma y^2 / p= x^2+y^2 / p=\{\pm y\alpha +pz\}^2+y^2$

entonces: $y^2<p \wedge \{\pm y\alpha +pz\}^2<p$

caso ii) $p=8k+3 \Rightarrow \sigma=-2 \Rightarrow p= x^2-\sigma y^2 / p= x^2+2y^2 / p=\{\pm y\alpha +pz\}^2+2y^2$

entonces: $2y^2<p \wedge \{\pm y\alpha +pz\}^2<p$

• si: $\sigma>0$ / $p=8k+7 \Rightarrow \sigma=+2 \Rightarrow p= x^2-\sigma y^2 / p= x^2-2y^2 / p=\{\pm y\alpha +pz\}^2-2y^2$

entonces: $\{\pm y\alpha +pz\}^2>p$

ejemplos: $p=23=[11]^2-2[7]^2=[19]^2-2[13]^2=...$

$p=31=[7]^2-2[3]^2=[9]^2-2[5]^2=[47]^2-2[33]^2=...$

$p= 7 =[3]^2-2[1]^2=[5]^2-2[3]^2=[13]^2-2[9]^2=[27]^2-2[19]^2=...$

/ $p = x'^2-\sigma\bullet y'^2= x''^2-\sigma\bullet y''^2=...=(x'^w)^2-\sigma\bullet (y'^w)^2$

$\Leftrightarrow x'\equiv\pm\alpha\bullet y'(\text{mod } p)$, $x''\equiv\pm\alpha\bullet y''(\text{mod } p)$,..., $x'^w\equiv\pm\alpha\bullet y'^w \pmod p$.

fin del inciso:

• denotaremos por: $\xi = \pm|\sqrt{p}| \in \mathbb{Z}\backslash\{0\}$, tomaremos una de las dos signaturas

ý sean tomados unos valores particulares: $\delta \in \mathbb{Z}\backslash\{0\}$ / $\delta \in (0,\xi] \wedge k \in \mathbb{Z}$

de forma que: $\delta \bullet \alpha + pk = \xi + c \bullet \alpha + r$, $r \in \mathbb{Z} \wedge r \in (-\alpha,0]$

es claro además que: $(\xi + r) \in [-\xi,\xi]$

puesto que: $\xi^2 \leq \alpha^2 \leq p+\sigma$ ó $\xi^2 \leq p+\sigma < \alpha^2$

de manera que equivalentemente resulta que:

$\Leftrightarrow (\delta - c) \bullet \alpha + pk = (\xi + r) \in [-\xi,\xi]$ / $(\xi + r)^2 < p$ (ver:* pág anterior)

de forma que: $\{(\delta - c) \bullet \alpha + pk\}^2 - \sigma(\delta - c)^2 \equiv 0 \pmod p$ **

recordando que: $\sigma = -1$ si: $p = 4k+1$, $\sigma = -2$ si: $p = 8k+3$ $\wedge$ $\sigma = +2$ si: $p = 8k+7$

** sabemos que: $\{\pm\alpha\}^2 \equiv \sigma \pmod p$ aplicando por un valor entero: $y^2 \in \mathbb{Z}\backslash\{0\}$

$\Rightarrow \{\pm y\alpha\}^2 \equiv \sigma y^2 \pmod p \Leftrightarrow \{\pm y\alpha + pz\}^2 \equiv \sigma y^2 \pmod p$ / $z \in \mathbb{Z}$

$\Leftrightarrow \{\pm y\alpha + pz\}^2 - \sigma y^2 \equiv 0 \pmod p$

en $\mathbb{Z} \Rightarrow \{\pm y\alpha + pz\}^2 - \sigma y^2 = 0 + pm$ / $m \in \mathbb{N}\backslash\{0\}$

si: $mcd(\{\pm y\alpha + pz\}, y) = \pm 1 \Rightarrow \sigma$ es residuo cuadrático en $\mathbb{Z}/(pm)$

si: $mcd(\{\pm y\alpha + pz\}, y) \neq \pm 1 \Rightarrow \sigma$ puede ser **(<u>ó no</u>)** residuo cuadrático en $\mathbb{Z}/(pm)$

depende de si existen: $x', y' \in \mathbb{Z}\backslash\{0\}$ / $pm = (x')^2 - \sigma(y')^2 \wedge mcd(x', y') = \pm 1$

** de forma que: $\{(\delta - c) \bullet \alpha + pk\}^2 - \sigma(\delta - c)^2 = pm$, $m \in \mathbb{N}\backslash\{0\}$, donde: $y = (d - c)$

$\Rightarrow \{(\delta - c) \bullet \alpha + pk\}^2 - \sigma(\delta - c)^2 \equiv 0 \pmod p$ como se afirmaba.

$\Leftrightarrow \{(\delta - c) \bullet \alpha + pk\}^2 - \sigma(\delta - c)^2 = pm$

$\Leftrightarrow (\delta - c)^2 \bullet \alpha^2 + 2(\delta - c)pk \bullet \alpha + p^2k^2 - \sigma(\delta - c)^2 - pm = 0 = f(\alpha)$

Tenemos que el discriminante de dicha función es:

$\Delta = [2(\delta - c)pk]^2 - 4(\delta - c)^2\{p^2k^2 - \sigma(\delta - c)^2 - pm\}$

$\Leftrightarrow \Delta = 4(\delta - c)^2\{p^2k^2\} - 4(\delta - c)^2\{p^2k^2\} - 4(\delta - c)^2\{-\sigma(\delta - c)^2 - pm\}$

$\Leftrightarrow \Delta=-4(\delta-c)^2\{-\sigma(\delta-c)^2-pm\} \Leftrightarrow \Delta=4(\delta-c)^2\{\sigma(\delta-c)^2+pm\}$

Es trivial que: $\Delta^{1/2} = \pm 2(\delta-c)\{\sigma(\delta-c)^2+pm\}^{1/2} \in \mathbb{Z}\backslash\{0\}$ (syss: $\exists\ \alpha$)

tal que como: $f(\alpha) = (\delta-c)^2 \bullet \alpha^2 + 2(\delta-c)pk \bullet \alpha + p^2k^2 - \sigma(\delta-c)^2 - pm = 0$

$\Rightarrow \alpha = \frac{1}{2} \bullet \frac{1}{(\delta-c)^2} \bullet \{\Delta^{1/2} - 2(\delta-c)pk\}$ es decir: $(2a)^{-1}\{\Delta^{1/2}-b\}$

y como sabemos que $\forall$ p primo impar existe $\alpha \in \mathbb{Z} / \{\pm\alpha\}^2 \equiv \sigma \pmod p$

si tomamos que m=1 aseguramos que $\forall$ p primo impar por tanto existe α

$\Rightarrow \alpha = \frac{1}{2} \bullet \frac{1}{(\delta-c)^2} \bullet \{\Delta^{1/2} - 2(\delta-c)pk\} \in \mathbb{Z}\backslash\{0\}$

$\Rightarrow \Delta^{1/2} \in \mathbb{Z}\backslash\{0\} \Rightarrow \pm 2(\delta-c)\{\sigma(\delta-c)^2+pm\}^{1/2} \in \mathbb{Z}\backslash\{0\}$

$\Rightarrow \exists$ δ,c,k definidos en la página anterior.

Tal que: $f(\alpha) = (\delta-c)^2 \bullet \alpha^2 + 2(\delta-c)pk \bullet \alpha + p^2k^2 - \sigma(\delta-c)^2 - pm = 0$

son todos coeficientes enteros.

Como además ya sabemos que m=1 lo cumple, (marcha atrás, tenemos que)

$\Rightarrow \{(\delta-c) \bullet \alpha + pk\}^2 - \sigma(\delta-c)^2 = pm = p$

ý como p es primo mcd $\Rightarrow (\{(\delta-c) \bullet \alpha + pk\},(\delta-c)) = \pm 1$ obligatoriamente

para ciertos valores (δ,c,k) particulares

QED

<u>Corolario 1ro)</u>

• recordamos que si tomamos m>1 puede ocurrir que: $\Delta^{1/2} \notin \mathbb{Z}\backslash\{0\}$ en cuyo caso no podemos afirmar en principio que: $\{\pm\alpha\}^2 \not\equiv \sigma \pmod p$

ó bien que: $\forall \mu \in \mathbb{Z}$, $\mu \in (p,p-1)$ entonces: $\{\pm\mu\}^2 \not\equiv \sigma \pmod p$

puesto que hemos tomado un valor δ particular en principio.

Tendremos, por tanto que estudiar todos los valores posibles tales que:

$\delta = 1,2,3,...,\xi$, siendo: $\xi = \pm|\sqrt{p}| \in \mathbb{Z}\backslash\{0\}$ tomado uno de los dos signos

pues teníamos que: $\delta \in \mathbb{Z}\backslash\{0\}$ / $\delta \in (0,\xi]$

de forma que: $\delta \bullet \alpha + pk = \xi + c \bullet \alpha + r$, $r \in \mathbb{Z} \wedge r \in (-\alpha,0]$

pudiendo (ó no) obtener finalmente al menos, una ecuación cuadrática:

$$\{(\delta'-c')\bullet \alpha + pk'\}^2 - \sigma(\delta'-c')^2 = pm$$

lo cual tampoco implica que σ sea residuo cuadrático en $\mathbb{Z}/p$ pues para ello es necesario además que $mcd(\{(\delta'-c')\bullet \alpha + pk'\}, [\delta'-c']) = \pm 1$

• si: $\Delta^{1/2} \in \mathbb{Z}\backslash\{0\}$ no podemos afirmar en principio que: $\{\pm\alpha\}^2 \equiv \sigma \pmod p$

es decir puede que σ sea (ó no) residuo cuadrático en $\mathbb{Z}/p$

pues puede ocurrir que: $mcd(\{(\delta-c)\bullet \alpha + pk\}, [\delta-c]) \neq \pm 1$ (ó no)

en cuyo caso, también habría que tomar otros valores posibles tales que: $\delta=1,2,3,...,\xi$ hasta obtener, (de existir), una ecuación cuadrática tal que:

$\{(\delta'-c')\bullet \alpha + pk'\}^2 - \sigma(\delta'-c')^2 = pm$, $mcd([(\delta'-c')\bullet \alpha + pk'], [\delta'-c']) = \pm 1$

• recordamos así mismo que dado p compuesto tal que se denotaban por:

$\beta, (p-\beta), \beta', (p-\beta'), \beta'', (p-\beta''), ..., \beta'^{w}, (p-\beta'^{w})$ a las raíces (de existir) de σ en $\mathbb{Z}/p$. Para diferenciarlas de la expresión α que era la dada (como raíz de σ) para los valores p primos impares)

<u>Corolario 2do)</u> (*<u>importante</u>*)

Afirmábamos que dado p primo impar, entonces:

• si: $p = 4k+1$ ó $p = 8k+3 \Rightarrow p = x^2 - \sigma\bullet y^2$

Entonces, sean: $x', y' \in \mathbb{Z}\backslash\{0\} \ / \ \forall\, x' \neq \pm x \wedge \forall y' \neq \pm y \Rightarrow p \neq x'^2 - \sigma\bullet y'^2$

sólo existe una ecuación cuadrática para p

• si: $p = 8k+7$ entonces $\exists\ x', y' \in \mathbb{Z}\backslash\{0\} \ / \ x' \neq \pm x \wedge y' \neq \pm y$

$/\ p = x^2 - \sigma\bullet y^2 = x'^2 - \sigma\bullet y'^2 = x''^2 - \sigma\bullet y''^2 = ... = (x'^{w})^2 - \sigma\bullet (y'^{w})^2$

$/\ x' \equiv \pm\alpha\bullet y' \pmod p,\ x'' \equiv \pm\alpha\bullet y'' \pmod p, ..., x'^{w} \equiv \pm\alpha\bullet y'^{w} \pmod p.$

(pues: $\pm\alpha$ raíces <u>únicas</u> de σ en $\mathbb{Z}/p$)

existe más de una ecuación cuadrática para p

(recordando que: $\sigma = -1$ si: $p = 4k+1$, $\sigma = -2$ si: $p = 8k+3 \ \wedge \ \sigma = +2$ si: $p = 8k+7$)

es decir si: $p = 4k+1$ ó $p = 8k+3$ entonces $Card[f(p)]=1$

si: $p = 8k+7$ entonces $Card[f(p)] > 1$

demostración: **(caso $\sigma<0$)** $p = 4k+1$ $(\Rightarrow\sigma=-1)$ ó $p = 8k+3$ $(\Rightarrow\sigma=-2)$

• si $\sigma<0 \Rightarrow$ Card[f(p)]=1 es decir $\Rightarrow$ $p = x^2 - \sigma \bullet y^2$

tal que: $\forall\ x' \neq \pm x \wedge \forall y' \neq \pm y\ /\ x', y' \in \mathbb{Z}\backslash\{0\} \quad \Rightarrow\ p \neq x'^2 - \sigma \bullet y'^2$

sólo existe una ecuación cuadrática para p

siempre que: $p = 4k+1$ $(\Rightarrow\sigma=-1)$ ó $p = 8k+3$ $(\Rightarrow\sigma=-2)$

tenemos que: $\delta \bullet \alpha + pk = \xi + c \bullet \alpha + r\ ,\ r \in \mathbb{Z} \wedge r \in (-\alpha, 0]$

$$\Leftrightarrow (\delta - c) \bullet \alpha + pk = \{\xi + r\} \in [-\xi, \xi] \ *$$

De forma que se demuestra trivialmente que: $\exists\ y \in (0,\xi]$

$/\ y^2 < p$ (ver: caso i. pág 75) $\wedge\ \xi = \pm|\sqrt{p}| \in \mathbb{Z}\backslash\{0\}$ (pág 76)

Tal que: $p = x^2 - \sigma \bullet y^2 \quad x,y \in \mathbb{Z}\backslash\{0\}$

y que por tanto: $y \leq |\sqrt{p}| = \xi \Rightarrow y \in (0,\xi]$ trivial

obtuvimos que: $\{\pm y\alpha + pz\}^2 - \sigma y^2 = 0 + pm\ /\ m \in \mathbb{N}\backslash\{0\}$ (pág 76)

que para $m=1 \Rightarrow \{\pm y\alpha + pz\}^2 - \sigma y^2 = p$ (pág 77)

de forma que tenemos claramente que: $\{(\delta - c) \bullet \alpha + pk\}^2 - \sigma(\delta - c)^2 = p$

$$\Rightarrow y = \pm(\delta - c) \ \wedge\ x = \pm\{(\delta - c) \bullet \alpha + pk\} = \pm\{\xi + r\}$$

recordando que: $\sigma = -1$ si: $p = 4k+1$, $\sigma = -2$ si: $p = 8k+3$

• Sea $t \in \mathbb{N}\backslash\{0\}\ /\quad t \bullet \alpha = p \bullet s + s'\ ,\ s' < 0$

es trivial que $s' \neq 0$ puesto que: $\alpha \nmid p\ \ \forall p$ primo impar

como imponemos que: $s' < 0 \Rightarrow t \bullet \alpha > p \bullet s$

de manera que como teníamos que: $(\delta - c) \bullet \alpha + pk = \{\xi + r\} \in [-\xi, \xi]$ *

equivalente tendremos que: $(\delta + t - c) \bullet \alpha + p(k-s) - s' = \{\xi + r\}$

$$\Leftrightarrow (\delta + t - c) \bullet \alpha + p(k-s) = \{\xi + r + s'\}$$

"obteniendo" unos supuestos valores: $x', y' \in \mathbb{Z}\backslash\{0\}$

$/\ x' = \pm\{\xi + r + s'\} \ \wedge\ y' = \pm(\delta + t - c)$

tales que: $p = x^2 - \sigma \bullet y^2 = x'^2 - \sigma \bullet y'^2$; x, x' impares ý $x \neq \pm x'$

• lleguemos a contradicción, de forma que:

tenemos que $(\delta+t-c)\bullet \alpha + p(k-s) = \{\xi + r + s'\}$

es claro que debe ocurrir que: $\{\xi + r + s'\} \in [-\xi,\xi]$ necesariamente.

pues si no, tendríamos que: $\{\xi + r + s'\}^2 > p$ absurdo

$\Rightarrow (\delta+t-c)\bullet \alpha + p(k-s) = \{\xi + r + s'\} \in [-\xi,\xi]$ siendo $r \leq 0$, $s' \in [-2\xi,0)$

trivial si: $r=0 \Rightarrow s' \in [-2\xi,0)$

como: $t\bullet \alpha = p\bullet s + s'$, $s' < 0$ / $\alpha^2-\sigma = pb$, $b \in \mathbb{N}\backslash\{0\}$

pues tenemos que: $\alpha^2 \equiv \sigma \pmod p$

ý a su vez, es trivial que: $\xi \leq \alpha$, puesto que: $\xi = \pm|\sqrt{p}| \in \mathbb{Z}\backslash\{0\} \wedge \alpha^2-\sigma = pb$

como: $s \neq 0 \Rightarrow t \geq \alpha \Rightarrow y' = \pm(\delta+t-c) = \pm(\delta+[\alpha+\upsilon]-c)$, $\upsilon \in \mathbb{N}$

$\Rightarrow \quad (y')^2 = (\delta+[\alpha+\upsilon]-c)^2 > \alpha^2 \geq p+\sigma \geq \xi^2 \quad \Rightarrow (y')^2 > p$ **Absurdo**

pues teníamos que: $p = x'^2 - \sigma\bullet y'^2$ ý como $\sigma < 0$

$p = 4k+1$ $(\Rightarrow \sigma=-1)$ ó $p = 8k+3$ $(\Rightarrow \sigma=-2)$

$\Rightarrow$ si: $p = 4k+1$ $(\Rightarrow \sigma=-1) \Rightarrow p = x'^2+y'^2 \wedge (y')^2 > p$ absurdo

ý si: $p = 8k+3$ $(\Rightarrow \sigma=-2) \Rightarrow p = x'^2+2y'^2 \wedge (y')^2 > p$ absurdo

$\Rightarrow$ si $\sigma < 0 \Rightarrow$ Card[f(p)]=1 es decir $\Rightarrow$ $p = x^2 - \sigma\bullet y^2$

tal que: $\forall\, x' \neq \pm x \wedge \forall y' \neq \pm y$ / $x', y' \in \mathbb{Z}\backslash\{0\} \quad \Rightarrow p \neq x'^2 - \sigma\bullet y'^2$

sólo existe una ecuación cuadrática para p

siempre que: $p = 4k+1$ $(\Rightarrow \sigma=-1)$ ó $p = 8k+3$ $(\Rightarrow \sigma=-2)$ QED

<u>demostración:</u> **(caso $\sigma > 0$)** $p = 4k+7$ $(\Rightarrow \sigma=+2)$

• si $\sigma > 0 \Rightarrow$ Card[f(p)]>1 es decir $\Rightarrow$

$p = x^2 - \sigma\bullet y^2 = x'^2 - \sigma\bullet y'^2 = x''^2 - \sigma\bullet y''^2 = \ldots = (x'^w)^2 - \sigma\bullet (y'^w)^2$

/ $x'^i \neq \pm x'^j \wedge y'^i \neq \pm y'^j$, i,j=0,1,2,3,...,w

• además $\forall$ p primo $\Rightarrow$ $\sigma \in$ residuo cuadrático en $\mathbb{Z}/p$

/ $\exists$ $\alpha \in \mathbb{Z}$, $\alpha \in (1,p-1)$ / $(\pm\alpha)^2 \equiv \sigma \pmod p$ ($\pm\alpha$ raíces <u>únicas</u> de σ * en $\mathbb{Z}/p$)

* Tal que: $\forall$ $k \in \mathbb{Z}$, $k \in (p,p-1) \wedge k \not\equiv \pm\alpha \pmod p$ entonces: $\{\pm k\}^2 \not\equiv \sigma \pmod p$

• entonces si p = 8k+7 primo

$\Rightarrow p = x^2 - \sigma \cdot y^2 = x'^2 - \sigma \cdot y'^2 = x''^2 - \sigma \cdot y''^2 = ... = (x'^w)^2 - \sigma \cdot (y'^w)^2$

$\Rightarrow x \equiv \pm\alpha \cdot y \pmod p$, $x' \equiv \pm\alpha \cdot y' \pmod p$, $x'' \equiv \pm\alpha \cdot y'' \pmod p$,...,

..., $x'^w \equiv \pm\alpha \cdot y'^w \pmod p$.

(pues: $\pm\alpha$ raíces <u>únicas</u> de σ * en $\mathbb{Z}/p$)

---

bastará con tomar como ejemplo...: p=7 primo / p es de la forma p=8k+7$\Rightarrow$ σ=+2

tal que: $p=7= x^2 - \sigma \cdot y^2 = x^2 - 2y^2$

/ $7 = 3^2 - 2 \cdot 1^2 = 5^2 - 2 \cdot 3^2 = 13^2 - 2 \cdot 9^2 = 27^2 - 2 \cdot 19^2 = ...$ / Card[f(p)]>1

Otros ejemplos serían tales que p=8k+7 primo $\Rightarrow$ σ=+2 ...:

$23 = 5^2 - 2 \cdot 1^2 = 11^2 - 2 \cdot 7^2 = 19^2 - 2 \cdot 13^2 = ...$

$31 = 7^2 - 2 \cdot 3^2 = 9^2 - 2 \cdot 5^2 = 33^2 - 2 \cdot 23^2 = ...$

$47 = 7^2 - 2 \cdot 1^2 = 17^2 - 2 \cdot 11^2 = 25^2 - 2 \cdot 17^2 = ...$

$71 = 11^2 - 2 \cdot 5^2 = 13^2 - 2 \cdot 7^2 = 53^2 - 2 \cdot 37^2 = ...$ Card[f(p)]>1

Pero obviamente se obtiene en todos ellos que:

$$xy^{-1} \equiv x'y'^{-1} \equiv x''y''^{-1} \equiv x'''y'''^{-1} \equiv ... \equiv x'^w y'^w \equiv \pm\alpha \pmod p$$

puesto que: $\exists$ $\alpha \in \mathbb{Z}$, $\alpha \in (1,p-1)$ / $(\pm\alpha)^2 \equiv \sigma \pmod p$

($\pm\alpha$ raíces <u>únicas</u> de σ * en $\mathbb{Z}/p$)

* Tal que: $\forall$ $k \in \mathbb{Z}$, $k \in (p,p-1) \wedge k \not\equiv \pm\alpha \pmod p$ entonces: $\{\pm k\}^2 \not\equiv \sigma \pmod p$

omitimos analizar más dichos resultados.

El punto I. de la proposición 21ra queda demostrado en su totalidad.

Proposición 33ra) De la hipótesis establecida en la proposición 21ra se demostrará a continuación, el punto III. tal que:

• Punto IIIro) p es primo impar, si y sólo si:

$p = x^2 - \sigma \bullet y^2$, $x,y \in \mathbb{Z}\backslash\{0\}$, con: $f_0(p) = x^2 - \sigma \bullet y^2$ / $mcd(x,y)=\pm 1$

ý además, si y sólo si: $\exists\ \alpha \in (1,p-1)$ / $\{\pm\alpha\}^2 \equiv \sigma \pmod p$

siendo: $\sigma = -1$ si: $p \equiv 1 \pmod 4$, $\sigma = -2$ si: $p \equiv 3 \pmod 8$, y $\sigma = +2$ si: $p \equiv 7 \pmod 8$

Tal que: $\forall\ k \in \mathbb{Z}$, $k \in (p,p-1) \wedge k \not\equiv \pm\alpha \pmod p$ entonces: $\{\pm k\}^2 \not\equiv \sigma \pmod p$

Además:

si: $p \not\equiv 7 \pmod 8$ entonces: $p \neq x'^2 - \sigma \bullet y'^2\ \forall\ x' \neq \pm x \wedge \forall\ y' \neq \pm y$

ý si: $p \equiv 7 \pmod 8$ entonces:

$$p = x^2 - \sigma \bullet y^2 = x'^2 - \sigma \bullet y'^2 = x''^2 - \sigma \bullet y''^2 = \ldots = (x'^w)^2 - \sigma \bullet (y'^w)^2$$

$\Rightarrow x' \equiv \pm\alpha \bullet y' \pmod p$, $x'' \equiv \pm\alpha \bullet y'' \pmod p$,..., $x'^w \equiv \pm\alpha \bullet y'^w \pmod p$.

/ $mcd(x'^i, y'^i) = \pm 1$

demostración:

Basta diferenciar todas las posibilidades demostradas con anterioridad tales que p sea compuesto y expuestas en los puntos II.a.-II.b.-II.c.-II.d. ý II.e. págs. 40-42

II.a) si: $p \neq x^2 - \sigma \bullet y^2\ \forall\ x,y \in \mathbb{Z}$, $x \in$ impar $\Rightarrow$

$$\forall\ \mu \in (1,p-1) \Rightarrow (\pm\mu)^2 \not\equiv \sigma \pmod p$$

[analizado en proposición 28va pág 53]

(Queda diferenciado de los números primos, puesto que...)

$\forall$ p primo entonces: $p = x^2 - \sigma \bullet y^2$, $x,y \in \mathbb{Z}\backslash\{0\}$

recordando que: $\sigma = -1$ si: $p = 4k+1$, $\sigma = -2$ si: $p = 8k+3 \wedge \sigma = +2$ si: $p = 8k+7$

II.b) si: $p = x^2 - \sigma \bullet y^2 = x'^2 - \sigma \bullet y'^2 = x''^2 - \sigma \bullet y''^2 = \ldots = (x'^w)^2 - \sigma \bullet (y'^w)^2$

$\forall\ x'^i \neq \pm x'^j$, $i \neq j$ ($\Rightarrow y'^i \neq \pm y'^j$) con: $x'^m, y'^m \in \mathbb{Z}\backslash\{0\}$

Siendo: $f_0(p) = x^2 - \sigma \bullet y^2$, $f_1(p) = x'^2 - \sigma \bullet y'^2$, $f_2(p) = x''^2 - \sigma \bullet y''^2$,...,

,..., $f_w(p) = (x'^w)^2 - \sigma \bullet (y'^w)^2$ / $p = f_0(p) = f_1(p) = f_2(p) = \ldots = f_w(p)$

Y tal que: $\exists$ al menos $f_0(p)$ ý $f_1(p)$ que cumplen dicha igualdad con p

Entonces en $\mathbb{Z}/p$ ocurre que **si:** $\sigma \in$ residuo cuadrático en $\mathbb{Z}/p \Rightarrow$

$\exists\ f_i(p) = (x'^i)^2 - \sigma \bullet (y'^i)^2 \wedge f_j(p) = (x'^j)^2 - \sigma \bullet (y'^j)^2$

ecuaciones cuadráticas distintas

$/\ p = (x'^{i})^2 - \sigma \bullet (y'^{i})^2 = (x'^{j})^2 - \sigma \bullet (y'^{j})^2$

$\wedge \quad mcd(x'^{i}, y'^{i}) = \pm 1 \quad \wedge \quad mcd(x'^{j}, y'^{j}) = \pm 1$

es decir, existen (al menos***): $\beta \wedge \beta' \in (1,p-1) \ / \ \beta \not\equiv \pm\beta' \pmod p$

y en cambio: $\{\pm\beta\}^2 \equiv \{\pm\beta'\}^2 \equiv \sigma \pmod p$

*** (Obviamente también sus opuestos $(p-\beta) \wedge (p-\beta') \in (1,p-1)$ son raíces de σ en $\mathbb{Z}/p$, es decir, existen al menos cuatro raíces en el intervalo (1,p-1). A diferencia de los números primos que sólo tienen dos raíces: α ý $(p-\alpha)$ en el intervalo (1,p-1) ý de <u>ciertos</u> cuadrados perfectos como se verá en el siguiente apartado II.c.)

[analizado en proposición 31ra. pág 64]

(Queda diferenciado de los números primos, puesto que...)

$\forall$ p primo entonces: $p = x^2 - \sigma \bullet y^2 \ / \ mcd(x,y) = \pm 1$

$\exists \ \alpha \in (1,p-1) \ / \ \{\pm\alpha\}^2 \equiv \sigma \pmod p$

siendo: $\sigma = -1$ si: $p \equiv 1 \pmod 4$, $\sigma = -2$ si: $p \equiv 3 \pmod 8$, y $\sigma = +2$ si: $p \equiv 7 \pmod 8$

Tal que: $\forall \ k \in \mathbb{Z}, k \in (p,p-1) \wedge k \not\equiv \pm\alpha \pmod p$ entonces: $\{\pm k\}^2 \not\equiv \sigma \pmod p$

existen tan solo dos raíces de σ en $\mathbb{Z}/p$ en el intervalo (1,p-1).

<u>II.c)</u> si p no es primo ý p$\in$ cuadrado perfecto impar*, entonces:

- ó: $p = x^2 - \sigma \bullet y^2 = f_0(p)$, $x \neq 0$ ($x \in$ impar) $\wedge \ y = 0 \ / \ \nexists \ f_{i>0}(p) = p$
- ó: $p = x^2 - \sigma \bullet y^2 = x'^2 - \sigma \bullet y'^2$, $x \neq 0$, $y = 0$

  $/ \ x' \in \mathbb{Z} \backslash (\pm x, 0) \wedge y' \in \mathbb{Z} \backslash (\pm y, 0)$ es decir $p = f_0(p) = f_1(p)$

  Además: $\exists \ \beta \in \mathbb{Z}$, $\beta \in (1,p-1) \ / \ (\pm\beta)^2 \equiv \sigma \pmod p$

  $\Rightarrow \ \sigma \in$ residuo cuadrático en $\mathbb{Z}/p$

  Tal que: $\forall \ k \in \mathbb{Z}, k \in (p,p-1) \wedge k \not\equiv \pm\beta \pmod p$

  entonces: $\{\pm k\}^2 \not\equiv \sigma \pmod p$
- ó: $p = x^2 - \sigma \bullet y^2 = x'^2 - \sigma \bullet y'^2 = x''^2 - \sigma \bullet y''^2 = \ldots = (x'^{w})^2 - \sigma \bullet (y'^{w})^2$

  es decir: $p = f_0(p) = f_1(p) = f_2(p) = \ldots = f_w(p) \ / \ Card[f(p)] \geq 3$ tal que:

  $Card[f(p)] \geq 3$ ý $4 \leq Card[\beta^*] \leq 2w$ **

* se cumple que: $\forall p \in$ cuadrado perfecto impar $\Rightarrow p \equiv 1 \pmod 8$ siempre.

ý además: $\exists \ \beta \in \mathbb{Z} \ / \ \{\pm\beta\}^2 \equiv \sigma \pmod p$ syss: $\exists \ f_1(p) = p$

** dada la ecuación cuadrática: $p = (x'^{i})^2 - \sigma \bullet (y'^{i})^2 \Rightarrow (x'^{i})^2 \equiv \sigma \bullet (y'^{i})^2 \pmod p$

Tal que: existe β'^{i} si y sólo si: $mcd(x'^{i}, y'^{i}) = \pm 1 \ / \ x'^{i} \equiv \pm \beta'^{i} \bullet y'^{i} \pmod p$

pues si $mcd(x'^{i}, y'^{i}) = k$, $k \neq \pm 1$ entonces $k|p \Rightarrow \nexists\ k^{-1}$ en $\mathbb{Z}/p$

$\Rightarrow \nexists\ (x'^{i})^{-1}, (y'^{i})^{-1}$ en $\mathbb{Z}/p$, pues: $k|x'^{i} \wedge k|y'^{i}$

Importante: si β es raíz de σ en $\mathbb{Z}/p$ también lo es $(p-\beta)$ y por tanto, se expone que $4 \leq Card[\beta^*] \leq 2w$, como mímimo existen cuatro raíces de σ en $\mathbb{Z}/p$, es decir, existen también (al menos): $\beta' \wedge (p-\beta')$ raíces de σ en $\mathbb{Z}/p$

[analizado en proposición 27ma. pág 49]

(Queda diferenciado de los números primos, puesto que...)

Si p es no primo entonces existe al menos una ecuación cuadrática $p = x^2 - \sigma \bullet y^2$

tal que: $mcd(x,y) \neq \pm 1$

los números primos no son cuadrados perfectos ý además:
por la proposición 26ta pág 48 tenemos que:

si: $p \in$ cuadrado perfecto impar, entonces: $p \equiv 1 \pmod 8$ $\sigma = -1$

tal que si: $Card[f(p)]=1$ entonces $p = x^2 - \sigma \bullet [0]^2 = f_0(p)$, $x \neq 0$ ($x \in$ impar) $\wedge\ y = 0$

$\Rightarrow$ p no es primo

ý si: $Card[f(p)] > 1 \Rightarrow$ p no es primo, puesto que todos los primos de la forma:

$p = 4k+1 \Rightarrow p = x^2+y^2$, $x,y \in \mathbb{Z}\backslash\{0\}$, tal que además

$p \neq x'^2 - \sigma \bullet y'^2 \ \forall\ x' \neq \pm x \wedge \forall\ y' \neq \pm$ y es decir: $Card[f(p)]=1$

II.d) Sea $p = q \bullet q'$, p no primo impar, $p > 1$

siendo: $q,q' \in$ impares, $1 < q < p$

$/\ q \notin$ cuadrado perfecto $\wedge\ q' \in$ cuadrado perfecto

siendo: $p = x^2 - \sigma \bullet y^2 = f_0(p)$, $x,y \in \mathbb{Z}\backslash\{0\}$

$\wedge\ p \neq f_{i>0}(p)$ es decir, siendo: $x',y' \in \mathbb{Z} \ / \ \forall\ x' \neq \pm x \ \wedge \ \forall\ y' \neq \pm y$

$\Rightarrow p \neq x'^2 - \sigma \bullet y'^2$ es decir: $Card[f(p)] = 1$

tal que en $\mathbb{Z}/p$: $\Rightarrow x^2 \equiv \sigma y^2 \pmod p$

pero ocurre que: $\forall\ \mu \in (1,p-1) \Rightarrow \{\pm\mu\}^2 \not\equiv \sigma \pmod p$

[analizado en proposición 29na. pág 54]

(Queda diferenciado de los números primos, puesto que...)

si p es primo: $\exists\ \alpha \in (1,p-1) \,/\, \{\pm\alpha\}^2 \equiv \sigma \pmod p$ *(ver: Punto I pág 39)*)

recordando que: $\sigma = -1$ si: $p = 4k+1$, $\sigma = -2$ si: $p = 8k+3$ $\wedge$ $\sigma = +2$ si: $p = 8k+7$

II.e) Sea $p = q \bullet q'$ (p no primo impar $p>1$), siendo: $q,q' \in$ impares, $1 < q < p$

$/\ q \wedge q' \notin$ cuadrado perfecto $\wedge\ q \neq q' \wedge$ al menos q es primo

siendo: $p = x^2 - \sigma \bullet y^2 = f_0(p)$, $x,y \in \mathbb{Z}\backslash\{0\}$

si: $\exists\ \beta \in \mathbb{Z}, \beta \in (1,p-1) \,/\, \{\pm\beta\}^2 \equiv \sigma \pmod p$ (...)

entonces: $\exists\ f_1(p) = x'^2 - \sigma \bullet y'^2$, con: $x',y' \in \mathbb{Z} \,/\, \forall\ x' \neq \pm x \wedge \forall\ y' \neq \pm y$

tal que: $p = x^2 - \sigma \bullet y^2 = x'^2 - \sigma \bullet y'^2 \Leftrightarrow p = f_0(p) = f_1(p)$ entonces:

$\Rightarrow \exists\ \beta' \in \mathbb{Z}$, $\beta' \in (1,p-1)\backslash\{\pm\beta\}$, es decir: $\beta' \not\equiv \pm\beta \pmod p$, equivalentemente:

$x^2 - \sigma \bullet y^2 \equiv 0 \pmod p \Leftrightarrow x^2 \equiv \sigma \bullet y^2 \pmod p \Leftrightarrow x \equiv \pm\beta \bullet y \pmod p$

$x'^2 - \sigma \bullet y'^2 \equiv 0 \pmod p \Leftrightarrow x'^2 \equiv \sigma \bullet y'^2 \pmod p \Leftrightarrow x' \equiv \pm\beta' \bullet y' \pmod p$

tal que: $\beta \not\equiv \pm\beta' \pmod p \wedge \{\pm\beta\}^2 \equiv \{\pm\beta'\}^2 \equiv \sigma \pmod p$

Obviamente también sus opuestos $(p-\beta) \wedge (p-\beta') \in (1,p-1)$ son raíces de σ en $\mathbb{Z}/p$, es decir, existen al menos cuatro raíces en el intervalo (1,p-1). A diferencia de los números primos que sólo tienen dos raíces: α ý $(p-\alpha)$ en el intervalo (1,p-1) ý de ciertos cuadrados perfectos como se expuso en el apartado II.c.

[analizado en proposición 30ma. pág 59]

(Queda,por tanto, diferenciado de los números primos.)

---

el punto III. queda por tanto, analizado y concluido.

Proposición 34ta) De la hipótesis establecida en la proposición 21ra se demostrará a continuación, el punto VI. tal que:

• Punto VIto) Sea q primo, $q>2$

Ý sea: $\varsigma\in$ (-[p-1],p-1) / $\varsigma\in$ residuo cuadrático en $\mathbb{Z}/q$, para todos los primos de la forma: q=8k+1 ý/ó q=8k+3 ý/ó q=8k+5 ý/ó q=8k+7

De manera que se cumpla además que: $q = a^2 - \varsigma \bullet b^2$, $a,b\in \mathbb{Z}\backslash\{0\}$

Entonces, tomado un número p impar positivo particular / $p \equiv q \pmod 8$
se cumple que, dicho p es primo (impar), si y sólo si:
i) $p = x^2 - \varsigma \bullet y^2$, $x,y\in \mathbb{Z}\backslash\{0\}$, con: $f_0(p) = x^2 - \varsigma \bullet y^2$
ii) ý además, si y sólo si: $\exists\ \alpha\in$ (1,p-1) / $\{\pm\alpha\}^2 \equiv \varsigma \pmod p$, mcd(x,y)=±1
Tal que: $\forall\ k\in \mathbb{Z}$, $k\in$ (p,p-1) $\wedge\ k \not\equiv \pm\alpha \pmod p$ **
entonces: $\{\pm k\}^2 \not\equiv \varsigma \pmod p$

• Además si: $(-\varsigma)>0$ entonces: $p \neq x'^2 - \varsigma \bullet y'^2\ \forall\ x' \neq \pm x \wedge \forall\ y' \neq \pm y$

ó bien si $(-\varsigma)<0$ entonces pueden existir (al menos): $x' \neq \pm x \wedge y' \neq \pm y$,
tales que: $p = x^2 - \varsigma \bullet y^2 = x'^2 - \varsigma \bullet y'^2$
/ $x \equiv \pm\alpha y \pmod p \wedge x' \equiv \pm\alpha y' \pmod p$ **

• Pudiendo diferenciar dicho valor p primo de cualquier valor p´ no primo tal que:
$p \equiv p' \pmod 8$
pues dicho valor compuesto p´, ó no tiene raíces en $\mathbb{Z}/p'$ para el valor ς (ς no es residuo cuadrático en $\mathbb{Z}/p'$) o bien existen al menos 4 raíces del mismo, en el intervalo (1,p´-1), ó bien p´ es un cuadrado perfecto, ó mcd (x,y)≠±1.

• el punto IVto, aquí es irrelevante p es impar x puede ser impar ó par dependiendo de los valores del residuo cuadrático (d) ý de si la variable (y) tal que: $-\varsigma \bullet y'^2$ sea un valor impar ó par.

• ***Finalmente***, podremos tomar un valor impar: p = 8k+r, tal que $p = x^2 - \varsigma \bullet y^2$, $x,y\in \mathbb{Z}\backslash\{0\}$ y se conozca del mismo que: ς residuo cuadrático en $\mathbb{Z}/p$ ý: $\varsigma\in$ (-[p-1],p-1) e indiferentemente de si lo es para cualquier otro primo $p'=8k'+r$. pudiéndose obtener además, si dicho p es primo ó no. Dependiendo de si existen más raíces de ς en $\mathbb{Z}/p$, más ecuaciones cuadráticas para dicho valor p (dependiendo de si $(-\varsigma)>0$ ó si $(-\varsigma)<0$) , si es un cuadrado perfecto, ó mcd (x,y)≠±1,...etc.

demostración:

La demostración es trivial y está ya realizada.

Basta con tomar las demostraciones oportunas realizadas a cada una de las premisas de la proposición 21ra. págs. 39-43, tanto el análisis realizado para cuando p es primo (punto I ý punto III), como el realizado para la suposición de p compuesto (puntos II-a. II-b. II-c. II-d. II-e.), omitiendo en todos ellos la premisa de que:

$$\sigma = -1 \text{ si: } p = 4k+1,\ \sigma = -2 \text{ si: } p = 8k+3 \ \wedge\ \sigma = +2 \text{ si: } p = 8k+7$$

ý sustituyendo el valor σ por la expresión ς expuesta antes tal que:

$$p = x^2 - \varsigma \bullet y^2$$

donde $\varsigma \in$ residuo cuadrático en $\mathbb{Z}/p$

Todas las demostraciones son, por tanto, análogas excepto si los valores de x,y son elementos impares ó pares pues dependerá del valor numérico asignado para ς.

Sean como ejemplos numéricos:

- p =13 primo, tomando ς=-4 pues es residuo cuadrático en $\mathbb{Z}/p$

  como $(-\varsigma)=4>0 \Rightarrow$ Card[f(p)]=1 / $p = 3^2 - \varsigma \bullet 1^2 = 3^2 + 4 \bullet 1^2$

- p =41 primo, tomando ς=-4 pues es residuo cuadrático en $\mathbb{Z}/p$

  como $(-\varsigma)=4>0 \Rightarrow$ Card[f(p)]=1 / $p = 5^2 - \varsigma \bullet 2^2 = 5^2 + 4 \bullet 2^2$

- p =41 primo, tomando ς=-5 pues es residuo cuadrático en $\mathbb{Z}/p$

  como $(-\varsigma)=5>0 \Rightarrow$ Card[f(p)]=1 / $p = 6^2 - \varsigma \bullet 1^2 = 6^2 + 5 \bullet 1^2$

- p =13 primo, tomando ς=3 pues es residuo cuadrático en $\mathbb{Z}/p$

  como $(-\varsigma)= -3<0 \Rightarrow$ Card[f(p)] >1

  / $p = 5^2 - \varsigma \bullet 2^2 = 11^2 - \varsigma \bullet 6^2 = 59^2 - \varsigma \bullet 34^2 =$

  que es lo mismo que: $p = 5^2 - 3 \bullet 2^2 = 11^2 - 3 \bullet 6^2 = 59^2 - 3 \bullet 34^2 = \ldots$

  tal que: $5 \bullet 2^{-1} \equiv 11 \bullet 6^{-1} \equiv 59 \bullet 34^{-1} \equiv \ldots \equiv 3^{(1/2)} \equiv \varsigma^{(1/2)} \equiv \pm\alpha \equiv \pm 4 \pmod p$

  Si existiera al menos: $p = a^2 - \varsigma \bullet b^2$ tal que $mcd(a,b) \neq \pm 1$

  entonces p no sería primo

  ó bien si: $a \bullet b^{-1} \not\equiv \pm 4 \pmod p$ entonces existen al menos 4 raíces en el intervalo (1,p-1) en $\mathbb{Z}/p$ lo que implicaría en ambos casos que p no es primo.

  Como no se dan estas situaciones tenemos finalmente que p es primo.

// (fin de la Parte IIda)

Anexo

Esta parte puede ser omitida en su totalidad, debido a que los resultados que de ella derivan, aunque interesantes, carecen de interés aplicativo para la resolución de las hipótesis de la proposición 21ra. y para la demostración de la conjetura de Albert Girard y primalidad de los elementos pertenecientes al conjunto de los enteros.

Simplemente se trata de una prolongación complementaria a la Parte Ira del temario (págs. 10-35).

Entre los resultados que se obtienen, en esta parte, se encuentran por ejemplo:

- si: $p \equiv 1 \pmod 8$, $\sigma = -1 \Rightarrow (\varphi-1)! \equiv \pm 2\alpha \pmod p$, syss: p es primo.
  $\wedge \quad (2^{\varphi}) \equiv \pm 1 \pmod p$, $\forall$ p primo.**
- si: $p \equiv 3 \pmod 8$, $\sigma = -2 \Rightarrow (\varphi)! \equiv 2^{\varphi}\alpha \pmod p$, syss: p es primo.
  $\wedge \quad (2)^{\varphi+1} \equiv \alpha \pmod p$, $\forall$ p primo.**
- si: $p \equiv 5 \pmod 8$, $\sigma = -1 \Rightarrow (\varphi-1)! \equiv \pm(2)^{\varphi-1}\rho^{-1} \pmod p$, syss: p es primo.
  $\wedge \quad (2)^{\varphi} \equiv \pm\alpha \pmod p$, $\forall$ p primo.**
- si: $p \equiv 7 \pmod 8$, $\sigma = +2 \Rightarrow (\varphi)! \equiv 2^{\varphi}\alpha \pmod p$, syss: p es primo.
  $\wedge \quad (2)^{\varphi+1} \equiv \alpha \pmod p$, $\forall$ p primo.**

$\forall$ p primo $\Rightarrow \{\pm\alpha\}^2 \equiv \sigma \pmod p$, $\sigma \in$ residuo cuadrático en $\mathbb{Z}/p$

siendo: $\forall p \in \mathbb{Z}$, $p \in$ impar $p>1$ / $p = 2\varphi+1$ entonces:

si: $p \equiv 1 \pmod 4 \Rightarrow \varphi \in$ par, $\varphi = 2\rho$

si: $p \equiv 3 \pmod 4 \Rightarrow \varphi \in$ impar, $\varphi = 2\rho + 1$

(ver: corolario 1ro. proposición 9na. pág 19)

(** en estos casos, el recíproco no es cierto, pueden existir (ó no) valores compuestos que cumplan la congruencia $(2)^{\varphi+1} \equiv \beta \pmod p$

Recordando que:

Si: $p \not\equiv 5 \pmod 8 \Rightarrow \prod_{t=0}^{i}(2t+1) \cdot (\rho)! \equiv \alpha \pmod p$

$/ \{\pm\alpha\}^2 \equiv \sigma \pmod p$, syss: p es primo.

Si: $p \equiv 5 \pmod 8 \Rightarrow (2^{\rho}) \equiv \alpha \pmod p$

$/ \{\pm\alpha\}^2 \equiv \sigma \pmod p$, $\forall$ p primo.

$2^{\varphi} \equiv 2^{2\rho} \equiv (2^{\rho})^2 \equiv -1 \equiv \sigma \pmod p$, $\forall$ p primo.

(ver pág 30)

$\{\prod_{t=0}^{i}(2t+1) \cdot (\rho)!\}^2 \equiv +1 \equiv (-1)^{\rho+1} \pmod p$, syss: p es primo.

(Ver: corolario pág 27)

//

Previo Introductorio.

i) de la proposición 15ta.

$p = 2\varphi+1$ / $\varphi = 2\rho$ si: $\varphi \in$ par $\Rightarrow p \equiv 1 \pmod 4$

$\varphi = 2\rho + 1$ si: $\varphi \in$ impar $\Rightarrow p \equiv 3 \pmod 4$ (pág 25)

$\wedge \prod_{t=0}^{i}(2t+1) = \{1 \cdot 3 \cdot 5 \cdot 7 \cdot 9 \cdot \ldots \cdot (2i-1) \cdot (2i+1)\}$ (pág 26)

Siendo: $i = \rho - 1$ si: $\varphi \in$ par (pág 26)

$i = \rho$ si: $\varphi \in$ impar (pág 28)

ii) de la proposición 17ma. (pág 30)

- si: $p \equiv 1 \pmod 8 \Rightarrow \varphi \in$ par $\wedge\ \rho \in$ par entonces:

$$\left\{\prod_{t=0}^{i}(2t+1) \cdot (\rho)!\right\}^2 \equiv -1 \pmod p, \text{ syss: p es primo.}$$

- si: $p \equiv 5 \pmod 8 \Rightarrow \varphi \in$ par $\wedge\ \rho \in$ impar entonces:

$$2^{\varphi} \equiv 2^{2\rho} \equiv \left(2^{\rho}\right)^2 \equiv -1 \pmod p, \ \forall \text{ p primo. (ver pág 27 ***)}$$

- si: $p \equiv 3 \pmod 8 \Rightarrow \varphi \in$ impar $\wedge\ \rho \in$ par entonces:

$$\left\{\prod_{t=0}^{i}(2t+1) \cdot (\rho)!\right\}^2 \equiv -2 \pmod p, \text{ syss: p es primo.}$$

- si: $p \equiv 7 \pmod 8 \Rightarrow \varphi \in$ impar $\wedge\ \rho \in$ impar entonces:

$$\left\{\prod_{t=0}^{i}(2t+1) \cdot (\rho)!\right\}^2 \equiv +2 \pmod p, \text{ syss: p es primo.}$$

iii) de la proposición 18va. (pág. 32)

Si: $p \not\equiv 5 \pmod 8 \Rightarrow \prod_{t=0}^{i}(2t+1) \cdot (\rho)! \equiv \alpha \pmod p$**

/ $\{\pm\alpha\}^2 \equiv \sigma \pmod p$, syss: p es primo

Si: $p \equiv 5 \pmod 8 \Rightarrow \left(2^{\rho}\right) \equiv \alpha \pmod p$**

/ $\{\pm\alpha\}^2 \equiv \sigma \pmod p$, syss: $\forall$ p primo.

(** ver proposición 18va pág 32)

Proposición 35ta)

como: $\prod_{t=0}^{i}(2t+1)$ = {1• 3• 5• 7• 9• ...• (2i-1)• (2i+1)} (ver prop. 15ta. pág. 26)

$\Leftrightarrow \prod_{t=0}^{i}(2t+1)$ =...

...={1• 3• 5• 7• 9• ...• (2i-1)• (2i+1)}[2• 4• 6• ...• (2i)][2• 4• 6• ...• (2i)] $^{-1}$

$\Rightarrow \prod_{t=0}^{i}(2t+1)$ =(2i+1)!• [2^{i}• i!]$^{-1}$ puesto que: [2• 4• 6• ...• (2i)] $^{-1}$= [2^{i}• i!]$^{-1}$

• caso p ≡ 1 (mod 8) $\Rightarrow \prod_{t=0}^{i}(2t+1)$}• ρ ! ≡ α (mod p), syss: p es primo.

siendo: σ = -1 / φ, ρ ∈ par $\Rightarrow$ φ = 2 ρ ∧ i = ρ -1 (pág 26)

$\Rightarrow \prod_{t=0}^{i}(2t+1)$ = (2[ρ -1] + 1)!• [(2)$^{\varphi-1}$ (ρ -1)!]$^{-1}$=...

... = (2 ρ -1)!• [(2)$^{\varphi-1}$ (ρ -1)!]$^{-1}$ =...

...= (2 ρ -1)!• [(2)$^{\varphi-1}$ (ρ -1)!]$^{-1}$• ρ • ρ $^{-1}$= ρ (2 ρ -1)!• [(2)$^{\varphi-1}$ (ρ)!]$^{-1}$

$\Leftrightarrow \prod_{t=0}^{i}(2t+1)$ = ρ (φ-1)!• [(2)$^{\varphi-1}$ (ρ)!]$^{-1}$

como: $\prod_{t=0}^{i}(2t+1)$• (ρ)! ≡ α (mod p) (prop 18va)

en $\mathbb{Z}$/p:$\Rightarrow$ $\prod_{t=0}^{i}(2t+1)$• (ρ)! ≡ (ρ)! ρ (φ-1)!• [(2)$^{\varphi-1}$ (ρ)!]$^{-1}$ (mod p)

$\Leftrightarrow$ α ≡ ρ (φ-1)!• [(2)$^{\varphi-1}$]$^{-1}$ (mod p), syss: p es primo

$\Leftrightarrow$ (φ-1)! ≡ (2)$^{\varphi-1}$ ρ $^{-1}$• α (mod p)**, syss: p es primo.

ii) por el t^{ma} de Fermat (2)$^{p-1}$ ≡ 1 (mod p), ∀ p primo

como: φ = 2 ρ $\Rightarrow$ (2)$^{p-1}$ ≡ $2^{2\varphi}$≡$2^{4\varphi}$ ≡ 1 (mod p), ∀ p primo

aplicando $2^{3\varphi+1}$, tenemos que:

$\Leftrightarrow 2^{3\varphi+1}$(φ-1)! ≡ $2^{3\varphi+1}$(2)$^{\varphi-1}$ ρ $^{-1}$• α ≡ ρ $^{-1}$• α (mod p), syss: p es primo

como: $2^{4\varphi}$ ≡ 1 (mod p), ∀ p primo

$\Rightarrow 2^{2\varphi}$ ≡ ±1 (mod p), ∀ p primo

$\Rightarrow 2^{\varphi}$ ≡ <±1,α*> (mod p), ∀ p primo

(*Nota:* " ≡<a,b> " indica que es ≡a ó ≡b, no sabemos con exactitud cuál de esas congruencias, ±1 ó α*, es la correcta, recordando que: $(-1)^{1/2}$ ≡ $\sigma^{1/2}$ ≡ α (mod p))

$\Rightarrow 2^{3\varphi}$ ≡ $2^{2\varphi}$• 2^{φ} ≡ ±1• <±1,α> ≡ <±1,±α> (mod p), ∀ p primo

$\Rightarrow 2^{3\varphi+1}$ ≡ ±2• <±1,α> (mod p), ∀ p primo

Teníamos: $(\varphi-1)! \equiv (2)^{\varphi-1}\rho^{-1}\cdot\alpha \pmod p$, syss: p es primo (**pág. anterior)

aplicando $(\varphi-1)! \Rightarrow \pm 2\cdot\langle\pm 1,\alpha\rangle(\varphi-1)! \equiv 2^{3\varphi+1}\cdot(2)^{\varphi-1}\rho^{-1}\cdot\alpha \pmod p$

$\Rightarrow \pm 2\cdot\langle 1,\alpha\rangle(\varphi-1)! \equiv 2^{4\varphi}\rho^{-1}\cdot\alpha \pmod p$, (siendo $2^{4\varphi}\equiv 1$)

$\Leftrightarrow \pm 2\cdot\langle 1,\alpha\rangle(\varphi-1)! \equiv \rho^{-1}\cdot\alpha \pmod p$, syss: p es primo

$\Leftrightarrow \pm 2\rho\cdot\langle 1,\alpha\rangle(\varphi-1)! \equiv \alpha \pmod p$, syss: p es primo, aplic α^{-1}

$\Leftrightarrow \pm 2\rho\cdot\langle \alpha^{-1},1\rangle(\varphi-1)! \equiv 1 \pmod p$, syss: p es primo

Del corolario 2do de la proposición 19na. (pág 35) tenemos que: $\alpha^{-1} \equiv -\alpha \pmod p$

$\Leftrightarrow \pm 2\rho\cdot\langle -\alpha,1\rangle(\varphi-1)! \equiv 1 \pmod p$, syss: p es primo

$\Leftrightarrow \pm^{*} 2\rho\cdot\langle \alpha^{*},1\rangle(\varphi-1)! \equiv 1 \pmod p$, syss: p es primo

$$\Leftrightarrow \pm 2\rho\cdot\langle \alpha,1\rangle(\varphi-1)! \equiv 1 \pmod p \text{ , syss: p es primo}$$

iii) tenemos así mismo que:

$(\varphi-1)! \equiv (2)^{\varphi-1}\rho^{-1}\cdot\alpha \pmod p$, syss: p es primo (**pág. anterior)

$\wedge$ por el t^{ma} Wilson / $(p-1)! \equiv -1 \pmod p$ si y sólo si p es primo /

$1\cdot 2\cdot 3\cdot\ldots\cdot(\varphi-1)[\varphi][\varphi+1](\varphi+2)(\varphi+3)\cdot\ldots\cdot(p-2)(p-1) \equiv (p-1)! \equiv -1 \pmod p$

syss: p es primo.

dónde: $1\cdot 2\cdot 3\cdot\ldots\cdot(\varphi-1) \equiv (\varphi-1)! \pmod p$

$(\varphi+2) \equiv p-(\varphi-1) \pmod p$

$(\varphi+3) \equiv p-(\varphi-1)+1 \pmod p$

$\Rightarrow (\varphi+2)(\varphi+3)\cdot\ldots\cdot(p-2)(p-1) \equiv (-1)^{\varphi-1}(\varphi-1)! \pmod p$

como: $\varphi\in$ par $\Rightarrow$ $(p-1)! \equiv (\varphi-1)![\varphi][\varphi+1]\cdot(-1)^{\varphi-1}(\varphi-1)! \pmod p$

syss: p es primo.

Inciso: $p = 2\varphi+1 \Rightarrow \varphi \equiv -2^{-1} \pmod p$ / $(\varphi+1) \equiv -2^{-1}+1 \equiv 2^{-1} \pmod p$

demostración: $-2^{-1}+1 \equiv 2^{-1} \pmod p$ aplicando (2): $\Rightarrow -1+2 \equiv 1 \pmod p$ QED

$\Rightarrow \varphi(\varphi+1) \equiv -2^{-1}\cdot 2^{-1} \equiv -2^{-2} \pmod p$. *Fin del inciso.*

teníamos por tanto que:

$(p-1)! \equiv (\varphi-1)![\varphi][\varphi+1]\cdot(-1)^{\varphi-1}(\varphi-1)! \pmod p$, syss: p es primo.

$\Leftrightarrow (-1) \equiv (-1)^{\varphi-1}\{(\varphi-1)!\}^2[\varphi][\varphi+1] \pmod p$, syss: p es primo. , $\varphi\in$ par

$\Leftrightarrow (-1) \equiv (-1)^{-1}\{(\varphi-1)!\}^2(-2^{-2}) \pmod p$, syss: p es primo.

$\Leftrightarrow (-1)(-2^2) \equiv (-1)\{(\varphi-1)!\}^2 \pmod p$, syss: p es primo.

$\Leftrightarrow -2^2 \equiv \{(\varphi-1)!\}^2 \pmod p$, syss: p es primo. , $\sigma = -1$

$\Leftrightarrow \sigma 2^2 \equiv \{(\varphi-1)!\}^2 \pmod p$, syss: p es primo.

ý como: $\{\pm\alpha\}^2 \equiv \sigma \pmod p$ tenemos que aplicando ($\%^{1/2}$) "raíz cuadrada"

$$\Leftrightarrow (\varphi-1)! \equiv \pm 2\alpha \pmod p, \text{ syss: p es primo.}$$

como: $(\varphi-1)! \equiv (2)^{\rho-1}\,\rho^{-1}\cdot\alpha \pmod p$, syss: p es primo. (**pág. 91)

$\Rightarrow \pm 2\alpha \equiv (2)^{\rho-1}\,\rho^{-1}\cdot\alpha \pmod p$, $\forall$ p primo.

$\Leftrightarrow \pm 1 \equiv (2)^{\rho-2}\,\rho^{-1} \pmod p$, $\forall$ p primo.

como: $\varphi = 2\rho \Leftrightarrow \rho \equiv 2^{-1}\varphi \pmod p \Rightarrow \rho^{-1} \equiv 2\varphi^{-1} \pmod p$

sabemos que: $\varphi^{-1} \equiv -2 \pmod p \Rightarrow \rho^{-1} \equiv -2^2 \pmod p$

$\Rightarrow \pm 1 \equiv (2)^{\rho-2}\,\rho^{-1} \equiv (2)^{\rho-2}(-2^2) \equiv -(2)^{\rho} \pmod p$, $\forall$ p primo.

$$\Rightarrow (2)^{\rho} \equiv \pm 1 \pmod p, \forall \text{ p primo.}$$

• <u>caso p ≡ 5 (mod 8)</u> $\Rightarrow \prod_{t=0}^{i}(2t+1)\cdot\rho! \equiv \pm 1 \pmod p$, syss: p es primo.

(ver: pág 90, ý ver proposiciones 17ma + <u>corolario</u> ý 18va. Págs 30-32)

siendo: $\sigma = -1$ / $\varphi\in$ par $\wedge\ \rho \in$ impar $\Rightarrow \varphi = 2\rho \wedge i = \rho - 1$ (pág 26)

ý como teníamos que: $\prod_{t=0}^{i}(2t+1) = (2i+1)!\cdot[2^i\cdot i!]^{-1}$ (ver: pág 91)

$\Rightarrow \prod_{t=0}^{i}(2t+1) = (2[\rho-1]+1)!\cdot[(2)^{\rho-1}(\rho-1)!]^{-1} = \ldots$

$\ldots = (2\rho-1)!\cdot[(2)^{\rho-1}(\rho-1)!]^{-1} = \ldots$

$\ldots = (2\rho-1)!\cdot[(2)^{\rho-1}(\rho-1)!]^{-1}\cdot\rho\cdot\rho^{-1} = \rho\,(2\rho-1)!\cdot[(2)^{\rho-1}(\rho)!]^{-1}$

$\Leftrightarrow \prod_{t=0}^{i}(2t+1) = \rho\,(\varphi-1)!\cdot[(2)^{\rho-1}(\rho)!]^{-1}$

como: $\prod_{t=0}^{i}(2t+1)\cdot(\rho)! \equiv \pm 1 \pmod p$ (corolario de prop. 17ma pág 31)

en $\mathbb{Z}/p$: $\Rightarrow \prod_{t=0}^{i}(2t+1)\cdot(\rho)! \equiv (\rho)!^{\rho}\ (\varphi\text{-}1)!\cdot[(2)^{\rho-1}(\rho)!]^{-1} \pmod p$

$\Leftrightarrow \pm 1 \equiv \rho\ (\varphi\text{-}1)!\cdot[(2)^{\rho-1}]^{-1} \pmod p$, syss: p es primo.

$\Leftrightarrow (\varphi\text{-}1)! \equiv \pm(2)^{\rho-1}\rho^{-1} \pmod p$**, syss: p es primo.

ii) por el t^ma de Fermat $(2)^{p-1} \equiv 1 \pmod p$, $\forall$ p primo.

como: $\varphi = 2\rho \Rightarrow (2)^{p-1} \equiv 2^{2\varphi} \equiv 2^{4\rho} \equiv 1 \pmod p$, $\forall$ p primo.

aplicando $2^{3\rho+1}$, tenemos que:

$\Leftrightarrow 2^{3\rho+1}(\varphi\text{-}1)! \equiv \pm 2^{3\rho+1}(2)^{\rho-1}\rho^{-1} \equiv \pm\rho^{-1} \pmod p$, syss: p es primo.

como: $2^{4\rho} \equiv 1 \pmod p$, $\forall$ p primo.

$\Rightarrow 2^{2\rho} \equiv \pm 1 \pmod p$, $\forall$ p primo.

$\Rightarrow 2^{\rho} \equiv <\pm 1, \alpha^*> \pmod p$, $\forall$ p primo.

(*Nota:* " $\equiv$<a,b> " indica que es $\equiv$a ó $\equiv$b, no sabemos con exactitud cual de esas congruencias, ± 1 ó α^*, es la correcta, recordando que: $(-1)^{1/2} \equiv \sigma^{1/2} \equiv \alpha \pmod p$)

$\Rightarrow 2^{3\rho} \equiv 2^{2\rho}\cdot 2^{\rho} \equiv \pm 1\cdot <\pm 1, \alpha> \equiv <\pm 1, \pm\alpha> \pmod p$, $\forall$ p primo.

$\Rightarrow 2^{3\rho+1} \equiv \pm 2\cdot <\pm 1, \alpha> \pmod p$, $\forall$ p primo.

Teníamos: $(\varphi\text{-}1)! \equiv \pm(2)^{\rho-1}\rho^{-1} \pmod p$, syss: p es primo. (**pág. actual)

aplicando $(\varphi\text{-}1)!$ $\Rightarrow \pm 2\cdot <\pm 1, \alpha>(\varphi\text{-}1)! \equiv \pm 2^{3\rho+1}\cdot(2)^{\rho-1}\rho^{-1} \pmod p$

$\Rightarrow \pm 2\cdot <1, \alpha>(\varphi\text{-}1)! \equiv \pm 2^{4\rho}\rho^{-1} \pmod p$, (siendo $2^{4\rho} \equiv 1$)

$\Leftrightarrow \pm 2\cdot <1, \alpha>(\varphi\text{-}1)! \equiv \pm\rho^{-1} \pmod p$, syss: p es primo.

$\Leftrightarrow \pm 2\rho\cdot <1, \alpha>(\varphi\text{-}1)! \equiv \pm 1 \pmod p$, syss: p es primo. , aplic ∓ 1

$\Leftrightarrow \pm 2\rho\cdot <\alpha^{-1}, 1>(\varphi\text{-}1)! \equiv 1 \pmod p$, syss: p es primo.

Del corolario 2do de la proposición 19na. (pág 35) tenemos que: $\alpha^{-1} \equiv -\alpha \pmod p$

$\Leftrightarrow \pm 2\rho\cdot <-\alpha, 1>(\varphi\text{-}1)! \equiv 1 \pmod p$, syss: p es primo.

$\Leftrightarrow \pm^* 2\rho\cdot <\alpha^*, 1>(\varphi\text{-}1)! \equiv 1 \pmod p$, syss: p es primo.

$\Leftrightarrow \pm 2\rho\cdot <\alpha, 1>(\varphi\text{-}1)! \equiv 1 \pmod p$, syss: p es primo.

iii) tenemos así mismo que:

$(\varphi-1)! \equiv \pm(2)^{\varphi-1}\rho^{-1} \pmod p$, syss: p es primo. (**pág. anterior)

$\wedge$ por el t^{ma} Wilson / $(p-1)! \equiv -1 \pmod p$ si y sólo si p es primo. /

$1 \cdot 2 \cdot 3 \cdot \ldots \cdot (\varphi-1)[\varphi][\varphi+1](\varphi+2)(\varphi+3) \cdot \ldots \cdot (p-2)(p-1) \equiv (p-1)! \equiv -1 \pmod p$

syss: p es primo.

dónde: $1 \cdot 2 \cdot 3 \cdot \ldots \cdot (\varphi-1) \equiv (\varphi-1)! \pmod p$

$(\varphi+2) \equiv p-(\varphi-1) \pmod p$

$(\varphi+3) \equiv p-(\varphi-1)+1 \pmod p$

$\Rightarrow (\varphi+2)(\varphi+3) \cdot \ldots \cdot (p-2)(p-1) \equiv (-1)^{\varphi-1}(\varphi-1)! \pmod p$

como: $\varphi \in$ par $\Rightarrow$ $(p-1)! \equiv (\varphi-1)![\varphi][\varphi+1] \cdot (-1)^{\varphi-1}(\varphi-1)! \pmod p$

syss: p es primo.

Inciso: $p = 2\varphi+1 \Rightarrow \varphi \equiv -2^{-1} \pmod p$ / $(\varphi+1) \equiv -2^{-1}+1 \equiv 2^{-1} \pmod p$

demostración: $-2^{-1}+1 \equiv 2^{-1} \pmod p$ aplicando (2): $\Rightarrow -1+2 \equiv 1 \pmod p$ QED

$\Rightarrow \varphi(\varphi+1) \equiv -2^{-1} \cdot 2^{-1} \equiv -2^{-2} \pmod p$. *Fin del inciso.*

teníamos por tanto que:

$(p-1)! \equiv (\varphi-1)![\varphi][\varphi+1] \cdot (-1)^{\varphi-1}(\varphi-1)! \pmod p$, syss: p es primo.

$\Leftrightarrow (-1) \equiv (-1)^{\varphi-1}\{(\varphi-1)!\}^2[\varphi][\varphi+1] \pmod p$, syss: p es primo., $\varphi \in$ par

$\Leftrightarrow (-1) \equiv (-1)^{-1}\{(\varphi-1)!\}^2(-2^{-2}) \pmod p$, syss: p es primo.

$\Leftrightarrow (-1)(-2^2) \equiv (-1)\{(\varphi-1)!\}^2 \pmod p$, syss: p es primo.

$\Leftrightarrow -2^2 \equiv \{(\varphi-1)!\}^2 \pmod p$, syss: p es primo.. , $\sigma = -1$

$\Leftrightarrow \sigma 2^2 \equiv \{(\varphi-1)!\}^2 \pmod p$, syss: p es primo.

ý como: $\{\pm\alpha\}^2 \equiv \sigma \pmod p$ tenemos que aplicando (%$^{1/2}$) "raíz cuadrada"

$\Leftrightarrow (\varphi-1)! \equiv \pm 2\alpha \pmod p$, syss: p es primo.

como: $(\varphi-1)! \equiv \pm(2)^{\varphi-1}\rho^{-1} \pmod p$, syss: p es primo. (**pág. anterior)

$\Rightarrow \pm 2\alpha \equiv \pm(2)^{\varphi-1}\rho^{-1} \pmod p$, $\forall$ p primo.

$\Leftrightarrow \pm\alpha \equiv (2)^{\varphi-2}\rho^{-1} \pmod p$, $\forall$ p primo.

como: $\varphi = 2\rho \iff \rho \equiv 2^{-1}\varphi \pmod p \Rightarrow \rho^{-1} \equiv 2\varphi^{-1} \pmod p$

sabemos que: $\varphi^{-1} \equiv -2 \pmod p \Rightarrow \rho^{-1} \equiv -2^2 \pmod p$

$\Rightarrow \pm\alpha \equiv (2)^{\varphi-2}\rho^{-1} \equiv (2)^{\varphi-2}(-2^2) \equiv -(2)^{\varphi} \pmod p$, $\forall$ p primo.

$\Rightarrow (2)^{\varphi} \equiv \pm\alpha \pmod p$, syss: $\forall$ p primo.

• <u>caso p ≡ 3 (mod 8)</u> $\Rightarrow \prod_{t=0}^{i}(2t+1)\cdot \rho\,! \equiv \alpha \pmod p$, syss: p es primo.
(ver: pág 90, ý ver proposiciones 17ma + <u>corolario</u> ý 18va. Págs 30-32)
siendo: $\sigma = -2$ / $\varphi \in$ impar, $\rho \in$ par $\Rightarrow \varphi = 2\rho + 1 \wedge i = \rho$ (pág 28)
ý como teníamos que: $\prod_{t=0}^{i}(2t+1) = (2i+1)!\cdot [2^i\, i!]^{-1}$ (ver: pág 91)
$\Rightarrow \prod_{t=0}^{i}(2t+1) = (2\rho+1)!\cdot [(2)^{\varphi}(\rho)!]^{-1} = (2\rho+1)!\cdot [(2)^{\varphi}(\rho)!]^{-1} = \ldots$
$\ldots = (\varphi)!\cdot [(2)^{\varphi}(\rho)!]^{-1}$
$\Leftrightarrow \prod_{t=0}^{i}(2t+1)\cdot (\rho)! = (\varphi)!\cdot [(2)^{\varphi}]^{-1}$
como: $\prod_{t=0}^{i}(2t+1)\cdot (\rho)! \equiv \alpha \pmod p$ (prop 18va pág 32)
en $\mathbb{Z}/p$: $\Rightarrow \prod_{t=0}^{i}(2t+1)\cdot (\rho)! \equiv (\varphi)!\cdot [(2)^{\varphi}]^{-1} \pmod p$
$\Leftrightarrow \alpha \equiv (\varphi)!\cdot [(2)^{\varphi}]^{-1} \pmod p$, syss: p es primo.

$\Leftrightarrow (\varphi)! \equiv (2)^{\varphi}\cdot \alpha \pmod p$**, syss: p es primo.

<u>ii)</u> por el t^{ma} de Fermat $(2)^{p-1} \equiv 1 \pmod p$, $\forall$ p primo.
como: $\varphi = 2\rho + 1 \Rightarrow (2)^{p-1} \equiv 2^{2\varphi} \equiv 2^{4\rho+2} \equiv 1 \pmod p$, $\forall$ p primo.
$\Rightarrow 2^{2\varphi+1} \equiv \pm 1 \pmod p \Leftrightarrow 2^{2\varphi+2} \equiv \pm 2 \pmod p$, $\forall$ p primo.
$\Rightarrow$ en $\mathbb{Z}$: $2^{2\varphi+2} = \pm 2 + p\cdot z$, z p$\in \mathbb{N}$ /
$\Rightarrow 2^{\varphi+1} = \{\pm 2 + p\cdot z\}^{1/2}$, $\forall$ p primo.
Tal que: $2^{\varphi+1} \equiv k \pmod p$ / $\{\pm k\}^2 \equiv \pm 2 \pmod p$, k$\in \mathbb{Z} \wedge$ k$\in$ (p,p-1)

sabemos que: $\{\pm\ \alpha\}^2 \equiv \sigma \equiv -2 \pmod p$

ý por la teoría de cuadrados perfectos, punto iv) pág 3. tal que:

Si $p \equiv 3 \pmod 4$ ý m es un residuo cuadrático en $(\mathbb{Z}/p)$, entonces:

(-m) <u>no es</u> un residuo cuadrático en $(\mathbb{Z}\ /p)$. con: p primo.

como teníamos: $2^{2(\rho+2)} \equiv \pm 2 \pmod p,\ \forall$ p primo.

$\Rightarrow 2^{2(\rho+2)} \equiv -2 \pmod p,\ \forall$ p primo. $\quad \left(2^{2(\rho+2)} \not\equiv 2 \pmod p\right)$

$\Leftrightarrow 2^{2(\rho+2)} \equiv -2 \equiv \sigma \pmod p,\ \forall$ p primo.

$$\Leftrightarrow 2^{(\rho+1)} \equiv \alpha \pmod p,\ \forall \text{ p primo.}$$

$\Rightarrow 2^{3(\rho+3)} \equiv 2^{3(\rho+1)} \equiv \alpha^3 \equiv \alpha^2\alpha \equiv \sigma\alpha \equiv -2\alpha \pmod p,\ \forall$ p primo.

Teníamos además: $(\varphi)! \equiv (2)^{\rho}\cdot \alpha \pmod p$, syss: p es primo. (**pág anterior)

Aplicando a la mísma: $2^{3(\rho+2)}$ tenemos equivalentemente:

$2^{3(\rho+2)}(\varphi)! \equiv 2^{3(\rho+2)}(2)^{\rho}\cdot \alpha \pmod p$, syss: p es primo.

$\Leftrightarrow 2^{3(\rho+2)}(\varphi)! \equiv 2^{4(\rho+2)}\cdot \alpha \pmod p$, syss: p es primo.

como: $\varphi = 2\rho + 1 \wedge 2^{3(\rho+3)} \equiv -2\alpha \pmod p,\ \forall$ p primo.

$\Rightarrow 2^{3(\rho+2)} \equiv -\alpha \pmod p,\ \forall$ p primo.

Entonces:

$\Leftrightarrow -\alpha(\varphi)! \equiv (2)^{2\varphi}\cdot \alpha \pmod p$, syss: p es primo.

$\Leftrightarrow (\varphi)! \equiv -(2)^{2\varphi} \pmod p$, syss: p es primo.

ý como: $p = 2\varphi+1\ /\ (2)^{p-1} \equiv (2)^{2\varphi} \equiv 1 \pmod p,\ \forall$ p primo.

peq. t^{ma} de Fermat./ $(2)^{p-1} \equiv 1 \pmod p,\ \forall$ p primo.

entonces:

$$\Leftrightarrow (\varphi)! \equiv -1 \pmod p, \text{ syss: p es primo.}$$

• <u>caso $p \equiv 7 \pmod 8$</u> $\Rightarrow \prod_{t=0}^{i}(2t+1)\cdot \rho\ ! \equiv \alpha \pmod p$, syss: p es primo.

(ver: pág 90, ý ver proposiciones 17ma + <u>corolario</u> ý 18va. Págs 30-32)

siendo: $\sigma = +2\ /\ \varphi, \rho \in$ impar $\Rightarrow\ \varphi = 2\rho + 1 \wedge i = \rho$ (pág 28)

ý como teníamos que: $\prod_{t=0}^{i}(2t+1) = (2i+1)!\cdot [2^{i}\, i!]^{-1}$ (ver: pág 91)

$\Rightarrow \prod_{t=0}^{i}(2t+1) = (2\rho+1)!\cdot [(2)^{\rho}(\rho)!]^{-1} = (2\rho+1)!\cdot [(2)^{\rho}(\rho)!]^{-1} = \ldots$

$\ldots = (\varphi)!\cdot [(2)^{\rho}(\rho)!]^{-1}$

$\Leftrightarrow \prod_{t=0}^{i}(2t+1)\cdot (\rho)! = (\varphi)!\cdot [(2)^{\rho}]^{-1}$

como: $\prod_{t=0}^{i}(2t+1)\cdot (\rho)! \equiv \alpha \pmod p$ (prop 18va pág 32)

en $\mathbb{Z}/p$: $\Rightarrow \prod_{t=0}^{i}(2t+1)\cdot (\rho)! \equiv (\varphi)!\cdot [(2)^{\rho}]^{-1} \pmod p$

$\Leftrightarrow \alpha \equiv (\varphi)!\cdot [(2)^{\rho}]^{-1} \pmod p$, syss: p es primo.

$\Leftrightarrow (\varphi)! \equiv (2)^{\rho}\cdot \alpha \pmod p$**, syss: p es primo.

ii) por el t^{ma} de Fermat $(2)^{p-1} \equiv 1 \pmod p$, $\forall$ p primo.

como: $\varphi = 2\rho + 1 \Rightarrow (2)^{p-1} \equiv 2^{2\varphi} \equiv 2^{4\rho+2} \equiv 1 \pmod p$, $\forall$ p primo.

$\Rightarrow 2^{2\rho+1} \equiv \pm 1 \pmod p \Leftrightarrow 2^{2\rho+2} \equiv \pm 2 \pmod p$, $\forall$ p primo.

$\Rightarrow$ en $\mathbb{Z}$: $2^{2\rho+2} = \pm 2 + p\cdot z$, z p$\in \mathbb{N}$ /

$\Rightarrow 2^{\rho+1} = \{\pm 2 + p\cdot z\}^{1/2}$, $\forall$ p primo.

Tal que: $2^{\rho+1} \equiv k \pmod p$ / $\{\pm k\}^2 \equiv \pm 2 \pmod p$, k$\in \mathbb{Z} \wedge$ k$\in$ (p,p-1)

sabemos que: $\{\pm \alpha\}^2 \equiv \sigma \equiv +2 \pmod p$

ý por la teoría de cuadrados perfectos, punto iv) pág 3. tal que:

Si p ≡ 3 (mod 4) ý m es un residuo cuadrático en ($\mathbb{Z}$/p), entonces:

(-m) no es un residuo cuadrático en ($\mathbb{Z}$ /p). con: p primo

como teníamos: $2^{2\rho+2} \equiv \pm 2 \pmod p$, $\forall$ p primo.

$\Rightarrow 2^{2\rho+2} \equiv +2 \pmod p$, $\forall$ p primo. $\left(2^{2\rho+2} \not\equiv -2 \pmod p\right)$

$\Leftrightarrow 2^{2\rho+2} \equiv +2 \equiv \sigma \pmod p$, $\forall$ p primo.

$\Leftrightarrow 2^{\rho+1} \equiv \alpha \pmod p$, $\forall$ p primo.

$\Rightarrow 2^{3\rho+3} \equiv 2^{3(\rho+1)} \equiv \alpha^3 \equiv \alpha^2\alpha \equiv \sigma\alpha \equiv +2\alpha \pmod p$, $\forall$ p primo.

Teníamos además: $(\varphi)! \equiv (2)^{\rho}\cdot \alpha \pmod p$, syss: p es primo. (**pág actual)

Aplicando a la mísma: $2^{3\rho+2}$ tenemos equivalentemente:

$2^{3\rho+2}(\varphi)! \equiv 2^{3\rho+2}(2)^{\rho} \cdot \alpha \pmod p$, syss: p es primo.

$\Leftrightarrow 2^{3\rho+2}(\varphi)! \equiv 2^{4\rho+2} \cdot \alpha \pmod p$, syss: p es primo.

como: $\varphi = 2\rho + 1 \wedge 2^{3\rho+3} \equiv +2\alpha \pmod p$, $\forall$ p primo.

$\Rightarrow 2^{3\rho+2} \equiv +\alpha \pmod p$, $\forall$ p primo.

Entonces:

$\Leftrightarrow +\alpha(\varphi)! \equiv (2)^{2\varphi} \cdot \alpha \pmod p$, syss: p es primo.

$\Leftrightarrow (\varphi)! \equiv (2)^{2\varphi} \pmod p$, syss: syss: p es primo.

ý como: $p = 2\varphi+1$ / $(2)^{p-1} \equiv (2)^{2\varphi} \equiv 1 \pmod p$, $\forall$ p primo.

peq. t^{ma} de Fermat./ $(2)^{p-1} \equiv 1 \pmod p$ $\forall$ p primo.

entonces:

$\Leftrightarrow (\varphi)! \equiv 1 \pmod p$, syss: p es primo.

Nota: Apreciese que cada uno de los casos expuestos en esta proposición, tienen procedimientos de resolución similares pero no análogos.

Corolario)

Valor ρ -numérico equivalente.

siendo trivial que: $2\varphi+1 \equiv 0 \pmod p$ / $\varphi \equiv -2^{-1} \pmod p$ entonces:

si: $\varphi \in$ par $\Rightarrow \varphi = 2 \cdot \rho \quad \Rightarrow \rho \equiv -2^{-2} \pmod p$

si: $\varphi \in$ impar $\Rightarrow \varphi = 2 \cdot \rho + 1 \Rightarrow \rho \equiv -3 \cdot 2^{-2} \pmod p$*

(*): $2 \cdot \rho \equiv \varphi - 1 \equiv -2^{-1} - 1 \equiv -(2^{-1}+1) \equiv -2^{-1}2(2^{-1}+1) \equiv -2^{-1}(1+2) \equiv -3 \cdot 2^{-1} \pmod p$

$\Leftrightarrow 2 \cdot \rho \equiv -3 \cdot 2^{-1} \pmod p \Rightarrow \rho \equiv -3 \cdot 2^{-2} \pmod p$* trivial.

// **(fin del Anexo)**

(y fin de la obra) ///

M.A. Rey Bonet Fecit MMXIV