N3

R. DVORNICICH

Titolo nota 11/09/2008

Interi di Gauss: $\mathbb{Z}[i]$.

$\{a+bi \mid a,b \in \mathbb{Z}\}$.

modulo: $|a+bi| = \sqrt{a^2+b^2}$

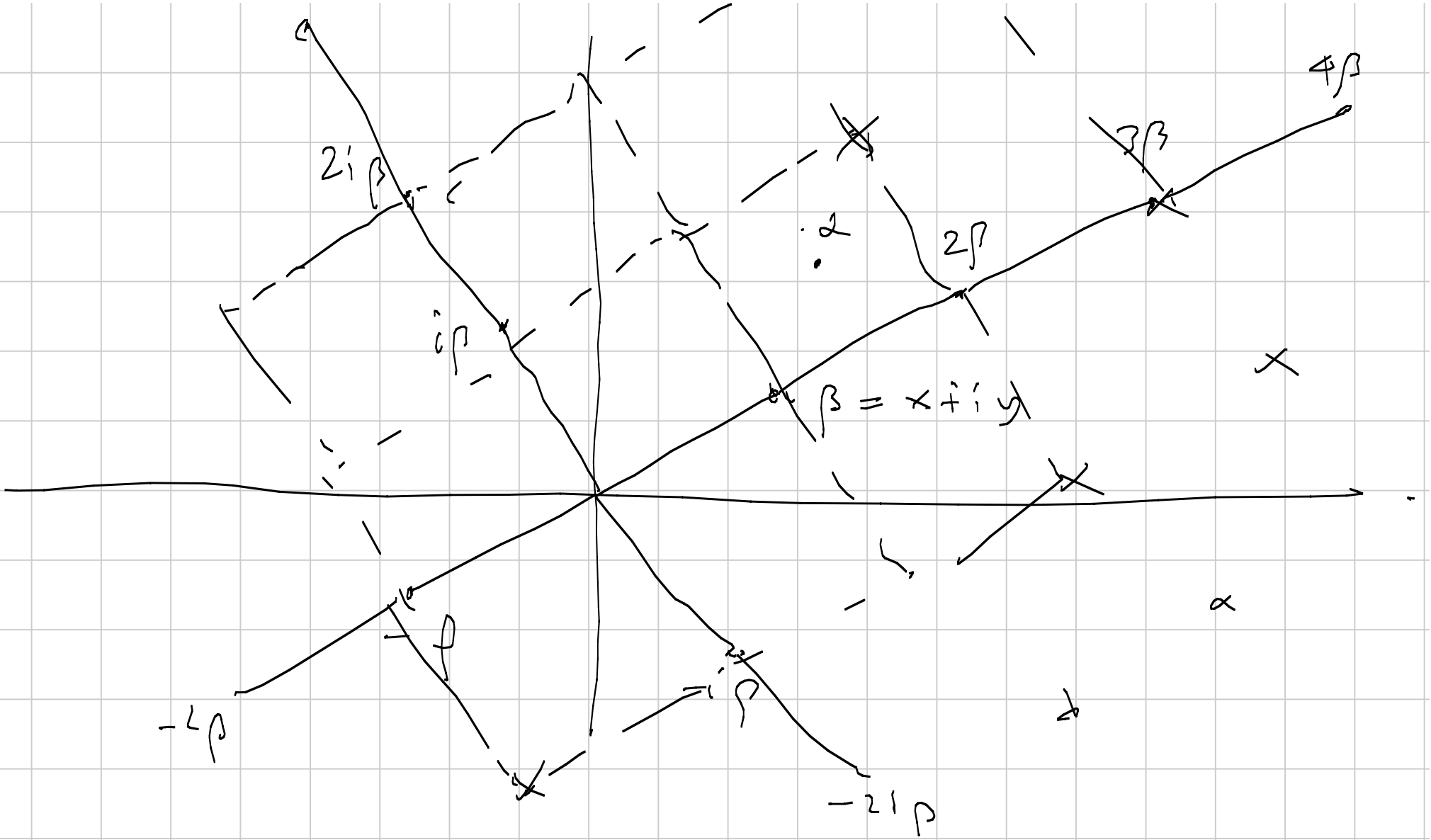
modulo^2: $|a+bi|^2 = a^2+b^2$

Divisione euclidea: (in $\mathbb{Z}$) $a = qb+r$ $0 \le r < |b|$

(in $\mathbb{Z}[i]$) $\alpha = q\beta + r$ con $0 \le |r| < |\beta|$.

$\beta = x+iy$, $x,y \in \mathbb{Z}$

Quanti sono i multipli di β $(q\beta)$ $q \in \mathbb{Z}[i]$?



Mode che rende α sta nel centro di un quadrato $|\alpha - \nu| = \frac{1}{\sqrt{2}} e = |\beta|$ $\nu = q\beta$

unità di misura

$$|\alpha - q\beta| \leq \frac{1}{\sqrt{2}}|\beta| < |\beta|$$

$\|$

r

	$\mathbb{Z}$	$\mathbb{Z}[i]$
DIV. EUCL	SI'	SI'
ALG EUCLIDE	SI'	SI'
PRIMI	$p \mid ab \Rightarrow p \mid a \circ p \mid b$	$p \mid ab \Rightarrow p \mid a \vee p \mid b$
F.U.	SI'	SI'

↓

(A MENO DI FATTORI INVERTIBILI)

Elementi invertibili: $(a+bi)$ t.c. $\exists\ (c+di)$

con $(a+bi)(c+di)=1$

$|a+bi|^2\,|c+di|^2=1$

$(a^2+b^2)(c^2+d^2)=1$

invertibili in $\mathbb{Z}[i]$: $\pm 1, \pm i$

TERNE PITAGORICHE: $a^2+b^2=c^2$

(primitive) $(a+bi)(a-bi)=c^2$

$MCD(a+bi, a-bi) \mid (2a, 2ib) \mid 2$

$2=(1+i)(1-i)=-i(1+i)^2$ $\qquad 1-i=-i(1+i)$

$|1+i|^2=1^2+1^2=2$

Se $(1+i) \mid (a+ib)$ allora $a+b$ è pari.

$(1+i)(c+id) = (a+ib) \rightarrow$ IMPOSSIBILE

$a+ib$ e $a-ib$ SONO PRIMI FRA LORO

$a+ib = \varepsilon (x+iy)^2$

$a-ib = \varepsilon^{-1} (x-iy)^2$ ε invertibile

$(x+iy)^2 = x^2 - y^2 + 2ixy$.

QUALI SONO GLI ELEMENTI PRIMI DI $\mathbb{Z}[i]$?

$\boxed{1+i}$

$p \in \mathbb{Z}$ primo dispari.

Si può scomporre in $\mathbb{Z}[i]$?

$$p = (a+bi)(c-di)$$

$$p^2 = (a^2+b^2)(c^2+d^2)$$

$$p^2 = \begin{cases} p^2 \cdot 1 \\ 1 \cdot p^2 \\ p \cdot p \end{cases}$$

Considerando solo le possibilità $a^2+b^2 = c^2+d^2 = p$

si ha che l'unica possibilità è

$$p = (a+bi)(a-bi) = a^2+b^2$$

$p \equiv 3 \pmod 4$ NO.

$p \equiv 3 \pmod 4$ è primo ANCHE in $\mathbb{Z}[i]$.

TEOREMA DI APPROSSIMAZIONE.

$\alpha \in \mathbb{R}$, $\alpha \notin \mathbb{Q}$. N intero positivo.
Allora esistono m, n interi, $0 < n \leq N$ tali che

$$\left|\alpha - \frac{m}{n}\right| < \frac{1}{nN} \qquad \left(< \frac{1}{n(N+1)}\right).$$

Dim. Consideriamo $0, \{\alpha\}, \{2\alpha\}, \dots, \{N\alpha\}, (1)$.
$\subseteq [0,1]$.
Sono $N+2$ numeri distinti
Un intervallo $\left[\frac{i}{N+1}, \frac{i+1}{N+1}\right)$ ne contiene 2.
cioè esistono h, k con $h < k$ tali che

$$|\{k\alpha\} - \{h\alpha\}| < \frac{1}{N+1}$$

$\{k\alpha\} = k\alpha - [k\alpha]$ $\quad \{h\alpha\} = h\alpha - [h\alpha]$

$$|(k-h)\alpha - m| < \frac{1}{N+1}$$

$\downarrow$

n

Se $\alpha \in \mathbb{Q}$? lo stesso con una restrizione

Se $\alpha = \frac{a}{b}$ $(a,b) = 1$ $b > N$.

$$\left|\alpha - \frac{m}{n}\right| \leq \frac{1}{n(N+1)}$$

Es $\alpha = \frac{1}{3}$ $N = 2$ $0, \frac{1}{3}, \frac{2}{3}, 1$

Parentesi (frazioni continue):

$\alpha \notin \mathbb{Q} \Rightarrow \exists$ infinite razionali $\frac{m}{n}$

tali che $\left|\alpha - \frac{m}{n}\right| < \frac{1}{n^2}$

$$\sqrt{2} = 1 + (\sqrt{2}-1) = 1 + \frac{1}{\sqrt{2}+1} = 1 + \frac{1}{2+(\sqrt{2}-1)} =$$

$$1 + \frac{1}{2 + \frac{1}{\sqrt{2}+1}} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + 1}}}$$

$1, \frac{3}{2}, \frac{7}{5}, \ldots$

Teo 2 Siano n, A interi positivi.
Se $n \mid A^2+1$, allora $n = s^2+t^2$.

Dim. Se $n=1$ è banale. Se $n>1$ allora, ponendo $N = [\sqrt{n}]$ si ha $n > N$.
Considero $\alpha = \frac{A}{n}$, Teo. approx. $\Rightarrow$

$\exists\, r, s$ con $\left| \frac{A}{n} - \frac{r}{s} \right| \le \frac{1}{s(N+1)}$ $\qquad s \le N \le \sqrt{n}$

$$|As - rn| \le \frac{n}{N+1} = \frac{n}{[\sqrt{n}]+1} < \sqrt{n}$$

$t = As - rn$

$$s^2 + t^2 = s^2(A^2+1) - 2Asrn + r^2n^2$$

$n \mid A^2+1$

quindi $n \mid s^2+t^2$.

Ho che $s^2+t^2 < n+n = 2n$ $\qquad (s^2+t^2>0)$

$\Rightarrow \quad s^2+t^2 = n.$

Esercizio: si dimostra che $(s,t)=1$.

<u>Corollario</u> Se $n>0$ è tale che $n \mid A^2+B^2$ con $(A,B)=1$, allora $n = s^2+t^2$.

<u>Dim.</u> $(A,B)=\underline{1} \Rightarrow AC-BD=\underline{1}$.

$$(A^2+B^2)(C^2+D^2) = (AD+BC)^2 + (AC-BD)^2$$

$$= E^2 + 1$$

<u>Parentesi</u>:

$$(a+ib)(c+di) = (ac-bd) + i(ad+bc)$$

$$(a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2$$

$p \equiv 1 \mod 4$

Posso risolvere $x^2 + 1 \equiv 0 \pmod p$

$p \mid x^2+1 \Rightarrow$ OK.

$p \equiv 1 \pmod 4 \Rightarrow p = (x+yi)(x-yi)$

$x^2+y^2 = p \qquad x+yi = (a+bi)(c+di)$

$p = x^2+y^2 = (a^2+b^2)(c^2+d^2)$

$a+bi \in \mathbb{Z}[i]$ qualcosa

La fattorizzazione di $a+bi$ sarà "una parte" della fatt. di $(a+bi)(a-bi) = a^2+b^2 =$ prodotto di primi $\in \mathbb{Z}$.

Se $q \equiv 3 \pmod 4$ $\quad q = x^2 + y^2$ IMPOSSIBILE

$\equiv 0, 1, 2 \pmod 4$

$q^2 = q^2 + 0^2$

$2,\ p \equiv 1\ (4),\ q^2 \quad (q \equiv ?\ \pmod 4)$

$n = 2^{\gamma}\ p_1^{a_1} \cdots p_r^{a_r}\ q_1^{2b_1} \cdots q_s^{2b_s}$

$p_i \equiv 1 \pmod 4 \qquad q_j \equiv ? \pmod 4$

$\Rightarrow \quad n = x^2 + y^2.$

Sono gli unici: se $n = x^2 + y^2$ e $q \mid n$ ($q \equiv 3\ (4)$) allora la potenza di q che divide n è pari.

$$q \mid n = x^2 + y^2$$

Se $q \nmid x$ $(q \nmid y)$ allora $\frac{x^2}{y^2} + 1 \equiv 0 \pmod q$

IMPOSSIBILE

Quando $q \mid x$ $q \mid y$ $\quad \frac{n}{q^2} = \left(\frac{x}{q}\right)^2 + \left(\frac{y}{q}\right)^2$

. . . . . .

I numeri rappresentabili $n = x^2 + y^2$ $\quad n \leq X$

sono all'incirca $\frac{X}{\sqrt{\log X}}$.

$n = x^2 + y^2 + z^2$

$x^2 \equiv 0, 1, 4 \pmod 8$

$n \equiv 7 \pmod 8$ IMPOSSIBILE

$n = 4^a (8k + 7)$ IMPOSSIBILE

(Induzione su a. $a > 1$ $\quad \frac{n}{4} = \left(\frac{x}{2}\right)^2 + \left(\frac{y}{2}\right)^2 + \left(\frac{z}{2}\right)^2$

TEOREMA IN TUTTI GLI ALTRI CASI È POSSIBILE.

$n = x^2+y^2+z^2 \iff n \neq 4^a(8b+7)$.

NON BUONI:

$\equiv 7 \ (8)$ $\quad \frac{1}{8}$ $\quad \frac{1}{8}\left(1+\frac{1}{4}+\frac{1}{4^2}+\cdots\right)$

$\equiv 7\cdot 4 \ (32)$ $\quad \frac{1}{32}$ $\quad = \frac{1}{8}\cdot\frac{4}{3} = \frac{1}{6}$,

$\equiv 7\cdot 16 \ (128)$ $\quad \frac{1}{128}$

BUONI : $5/6$.

TEOREMA Ogni $n \geq 0$ è somma di 4 quadrati.

DIM. $m = x_1^2 + x_2^2 + x_3^2 + x_4^2$

$n = y_1^2 + y_2^2 + y_3^2 + y_4^2$ $\Rightarrow mn = z_1^2 + z_2^2 + z_3^2 + z_4^2$

quaternioni: $a + bi + cj + dk$ $\quad i^2 = j^2 = k^2 = -1$

$ij = k \quad jk = i \quad ki = j$

$ji = -k \quad kj = -i \quad ik = -j$.

$x, y \quad |x|^2 \cdot |y|^2 = |xy|^2$

È sufficiente verificare il teo per $n = 0, 1$

e per $n = p$ primo

Problema: scrivere p primo nella forma

$$p = x_1^2 + x_2^2 + x_3^2 + x_4^2.$$

$p = 2 \qquad 1^2 + 1^2 + 0^2 + 0^2.$

p dispari. $\qquad x^2 + y^2 + 1^2 \equiv 0 \pmod p$

è risolubile.

$$x^2 \equiv -1 - y^2$$

(si risolve $x^2 + y^2 \equiv a \pmod p$)

posso scegliere $\frac{p+1}{2}$ $\qquad$ $\frac{p+1}{2}$

So che se può scrivere

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = m_0 p \qquad m_0 < p.$$

(posso prendere $|x_i| < \frac{p}{2}$).

Prendo m_0 minimo possibile. ($m_0 = 1$?)

m_0 è dispari.

m_0 fan' $\sum x_i^2 \equiv 0 \pmod 2$

Posso supporre $x_1 \equiv x_2$, $x_3 \equiv x_4 \pmod 2$

$$\frac{m_0 p}{2} = \left(\frac{x_1+x_2}{2}\right)^2 + \left(\frac{x_1-x_2}{2}\right)^2 + \left(\frac{x_3+x_4}{2}\right)^2 + \left(\frac{x_3-x_4}{2}\right)^2$$

$$= \frac{x_1^2+x_2^2}{2} \qquad = \frac{x_3^2+x_4^2}{2}$$

Supponiamo $m_0 \geq 3$ dispari

$x_i = b_i m_0 + y_i \qquad |y_i| < \frac{m_0}{2}$

$\sum y_i^2 \equiv \sum x_i^2 \equiv 0 \pmod{m_0}$

$\sum y_i^2 < m_0^2$

$\sum y_i^2 \equiv m_0 m_1$

$m_1 < m_0$ -

$$m_0 p = \sum x_i^2 \qquad m_0 m_1 = \sum y_i^2$$

$$m_0^2 m_1 p = \sum z_i^2$$

BASTA VERIFICARE CHE TUTTI i z_i sono divisibili per m_0.

Per esempio, $z_1 = x_1 y_1 + x_2 y_2 + x_3 y_3 + x_4 y_4$

$$y_i \equiv x_i - b_i m_0 \qquad y_i \equiv x_i \pmod{m_0}$$

$$z_1 \equiv \sum x_i^2 \pmod{m_0}$$

$$\equiv 0$$

$p \equiv 1 \pmod 4 \implies p = x^2 + y^2$

(p non è primo in $\mathbb{Z}[i]$)

Oss. Se p fosse primo in $\mathbb{Z}[i]$,
avrei che $\mathbb{Z}[i]/(p)$ sarebbe un campo.

OGNI POLINOMIO A COEFFICIENTI IN UN CAMPO HA UN NUMERO DI RADICI $\leq$ GRADO.

($2x \in \mathbb{Z}/6\mathbb{Z}[x]$)

$x^2 + 1$ $\quad i, -i$

$0, 3$ $\quad a^2 = -1$ $\quad a, -a$

$c + di \quad 0 \leq c < p \quad 0 < d < p$

$$\chi(n) = \begin{cases} 0 & \text{se } 2 \mid n \\ (-1)^{\frac{n-1}{2}} & \text{se } 2 \nmid n. \end{cases}$$

χ è moltiplicativa

($\chi(mn) = \chi(m)\chi(n)$ se $(m,n)=1$).

$$\delta(n) = \sum_{d \mid n} \chi(d) = (\chi * 1)(n)$$

<u>Oss.</u> Se $V(n) = \#$ sol di $x^2 \equiv -1 \pmod{n}$,

allora

$$V(n) = \begin{cases} 0 & \text{se } 4 \mid n \\ \prod_{p \mid n} (1+\chi(p)) & \text{se } 4 \nmid n. \end{cases}$$

Sia $r(n) = n^\circ$ sol. (x,y) di $n = x^2+y^2$.
$(x, y \in \mathbb{Z})$.

Teo. $r(n) = 4\delta(n)$

Dim. Sia $n = 2^\gamma p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1} \cdots q_s^{b_s}$

Se $q_1^{b_1} \| n$ e b_1 è dispari $\quad q \equiv 3 \pmod 4$

$\delta(q_1^{b_1}) = (\chi(1) + \chi(q_1) + \cdots + \chi(q_1^{b_1}))$

$= (1 - 1 + 1 \quad -1) = 0.$

Sia n "buono" $\quad n = 2^\gamma p_1^{a_1} \cdots p_r^{a_r} q_1^{2b_1} \cdots q_s^{2b_s}$.

In $\mathbb{Z}[i]$

$n = \varepsilon (1+i)^{2\gamma} (x_1+y_1 i)^{a_1} (x_1-y_1 i)^{a_1} \cdots$

$$\cdots (x_r+y_r i)^{a_r}(x_r-y_r i)^{a_r}\cdot q_1^{2b_1}\cdots q_s^{2b_s}$$

$$n = a^2+b^2 = (a+bi)(a-bi)$$

$$a+bi = \varepsilon (1+i)^{\gamma}\cdots (x_j+y_j i)^{l_i}(x_j-y_j i)^{a_i-l_i}\cdots q_1^{b_1}\cdots q_s^{b_s}$$

$\varepsilon \to 4$ pos. $0 \le l_i \le a_i \to a_i+1$ pos.

$$1+\chi(p_1)+\cdots+\chi(p_1^{a_i}) \qquad \chi(q_i^{2b_i}) = 1$$

RECIPROCITÀ QUADRATICA

Simbolo di Legendre: p primo

$$\left(\frac{n}{p}\right) = \begin{cases} 0 & \text{se } p \mid n \\ 1 & \text{se } p \nmid n \text{ e } n \equiv x^2 \ (p) \\ -1 & \text{se } p \nmid n \text{ e } n \not\equiv x^2 \ (p) \end{cases}$$

Gauss: $p > 2$ $p \nmid n$. Consideriamo i resti modulo p di $n, 2n, 3n, \dots, \frac{p-1}{2} n$ (compresi fra 0 e p).

$$0 \cdot \times\times\times \; ; \; \circ\circ\circ\circ \cdot p$$

$p/2$

Sia m il n° di questi resti $> p/2$

Teo. $\left(\frac{n}{p}\right) = (-1)^m$.

Es: $p=7$ $n=10$ $10, 20, 30$ $3, 6, 2$ $\times\ \circ\ \times$ $m=-1$ $\left(\frac{10}{7}\right)=-1$

$\ell = \frac{p-1}{2} - m$ ci sono ℓ resti $< \frac{p}{2}$.

$a_1, \dots, a_\ell$ resti $< \frac{p}{2}$ $\quad b_1, \dots, b_m$ resti $> \frac{p}{2}$.

$$\prod a_i \prod b_j \equiv \prod_{k=1}^{(p-1)/2} k n = \left(\frac{p-1}{2}\right)! \, n^{\frac{p-1}{2}} \pmod p$$

$$\left(\frac{n}{p}\right).$$

$a_1, \dots, a_\ell \quad p-b_1, \dots, p-b_m$

sono $\ell + m = \frac{p-1}{2}$ compresi fra 1 e $\frac{p-1}{2}$.

SONO TUTTI DISTINTI: se fosse

$a_i = p - b_{j'} \qquad a_i + b_{j'} = p$

Si dà resto a_i nt_j dà resto b_j

$s_i, t_j < \frac{p}{2}$ $\qquad n(s_i + t_{j'}) \equiv n(a_{i'} + b_j) \equiv 0 \pmod p$

Quindi $\prod a_i \prod (p - b_j) = \left(\frac{p-1}{2}\right)!$

Confrontando

$$(-1)^m = n^{\frac{p-1}{2}} = \left(\frac{n}{p}\right).$$

$\boxed{n=2}$ $\qquad p > 2$ $\qquad 2, 2\cdot 2, 2\cdot 3, \dots, 2\cdot\frac{p-1}{2} = p-1$

Resti della divisione per p. $\qquad k\ \frac{p}{2} < 2k < p$

$$m = \left[\frac{p}{2}\right] - \left[\frac{p}{4}\right]$$

$p = 8k + r \qquad r = 1, 3, 5, 7$

$$m = \begin{cases} 0 & r \\ 1 & 1 \\ 1 & 3 \\ 0 & 5 \\ & 7 \end{cases}$$

Cor $\left(\frac{2}{p}\right) = (-1)^m = (-1)^{\frac{p^2-1}{8}}$

(Cria $+1$ se $p \equiv \pm 1 \pmod 8$)

-1 se $p \equiv \pm 3 \pmod 8$)