Bollettino
Unione Matematica Italiana

Edoardo Storchi

Alcuni criteri di divisibilità per i numeri di Mersenne e il carattere 6^{co}, 12^{mo}, 24^{mo}, 48^{mo}, dell'intero 2.

Bollettino dell'Unione Matematica Italiana, Serie 3, Vol. **10** (1955), n.3, p. 363–375.

Zanichelli

<http://www.bdim.eu/item?id=BUMI_1955_3_10_3_363_0>

L'utilizzo e la stampa di questo documento digitale è consentito liberamente per motivi di ricerca e studio. Non è consentito l'utilizzo dello stesso per motivi commerciali. Tutte le copie di questo documento devono riportare questo avvertimento.

Articolo digitalizzato nel quadro del programma bdim (Biblioteca Digitale Italiana di Matematica) SIMAI & UMI
http://www.bdim.eu/

Bollettino dell'Unione Matematica Italiana, Zanichelli, 1955.

Alcuni criteri di divisibilità per i numeri di Mersenne e il carattere 6^{co}, 12^{mo}, 24^{mo}, 48^{mo}, dell'intero 2.

Nota di EDOARDO STORCHI (*) (a Milano)

Sunto. - *Tenendo conto di due classici teoremi sui residui biquadratici e cubici ed inoltre dei risultati di una recente ricerca di* A. WHITEMAN, *viene determinato il carattere* 6^{co}, 12^{mo}, 24^{mo}, 48^{mo} *dell'intero 2. Dei teoremi stabiliti viene poi fatta applicazione alla teoria dei numeri di* MERSENNE *(i numeri della forma* $2^q - 1$ *con* q *primo). Vengono ritrovati i due soli criteri di divisibilità finora noti: quello di* $2^q - 1$ *per* $2q + 1$ *dovuto ad* EULERO *e* LAGRANGE *e quello di* $2^q - 1$ *per* $6q + 1$ *dovuto a* PELLET *e* KRAITCHIC. *Vengono inoltre segnalati i nuovi criteri di divisibilità di* $2^q - 1$ *per* $8q + 1$, $16q + 1$, $24q + 1$, $48q + 1$, *nell'ipotesi che* q, $8q + 1$ *ecc. siano tutti numeri primi.*

Introduzione. - Recentemente A. L. WHITEMAN [1], facendo uso della teoria della ciclotomia, ideata da GAUSS, ha dimostrato alcuni teoremi che permettono di individuare il carattere ottavico e sestodecimo di 2.

Il teorema che riguarda il carattere ottavico di 2, scoperto da C. G. REUSCHLE nel 1856, fu dimostrato per la prima volta soltanto nel 1914, da A. F. WESTERN [2]. Il teorema che concerne il carattere sestodecimo di 2, scoperto da A. CUNNINGHAM nel 1895 sulle basi dell'evidenza sperimentale, fu ritrovato e dimostrato per la prima volta da A. AIGNER [3] nel 1939, con l'impiego della teoria dei numeri algebrici.

Applicando questi teoremi, il teorema di GAUSS sul carattere biquadratico di 2 ed un classico teoroma sui residui cubici, nel

(*) Lavoro eseguito presso l'Institute for Advanced Study di Princeton New Jersey.

(1) A. L. WHITEMAN, *The sixteenth power residue character of 2.* Canadian Journal of Mathematics 1954, pag. 364-373. Alla nota del WHITEMAN rimandiamo anche per una più completa bibliografia.

(2) A. WESTERN, *Some criteria for the residues of eighth and other powers.* Proc. London Math. Society (2), 9 (1911). 244-272.

(3) A. AIGNER, *Kriterium zum 8 und 16 Potenzcharacter der Reste 2 und* -2. Deutsche Math., 4 (1939), 44-52.

presente lavoro stabilirò e dimostrerò alcune proposizioni che permettono di individuare il carattere 6^{co}, 12^{mo}, 24^{mo}, 48^{mo} di 2, subordinando i criteri corrispondenti alla rappresentabilità dei numeri primi mediante forme quadratiche.

Dei teoremi stabiliti verrà poi fatta applicazione alla teoria dei numeri di MERSENNE e verranno stabiliti i criteri che regolano la divisibilità di $2^q - 1$ per $2q+1$, $6q+1$, $8q+1$, $16q+1$, $24q+1$, $48q+1$ rispettivamente, nell'ipotesi che q e $p = 2q+1$, q e $p = 6q+1$ ecc. siano tutti numeri primi.

Il carattere sestico di 2. - Incominciamo col segnalare una dimostrazione del tutto elementare del ben noto seguente:

TEOREMA I. - «Il numero 2 è residuo quadratico dei numeri primi della forma $8k \pm 1$ e non-residuo quadratico dei numeri primi della forma $8k \pm 3$ ».

Si parta dall'identità:

$$(2n)! = 1 \cdot 2 \cdot 3 \ldots (2n) = 1 \cdot 3 \cdot 5 \ldots (2n-1) \cdot 2 \cdot 4 \cdot 6 \ldots (2n) = n! \cdot 2^n \cdot 1 \cdot 3 \ldots (2n-1)$$

valida per $n \geq 1$. Da essa segue:

$$2n(2n-1) \ldots (n+1) = 1 \cdot 3 \cdot 5 \ldots (2n-1) \cdot 2^n \tag{1}$$

a) Sia n dispari. In tal caso si possono sopprimere in ambo i membri della (1) i fattori comuni $n+2, \ldots 2n-1$ e si ottiene:

$$2n(2n-2)(2n-4) \ldots (n+1) = 1 \cdot 3 \cdot 5 \ldots n \cdot 2^n$$

da cui:

$$2^n = \frac{2n(2n-2)(2n-4) \ldots (n+1)}{1 \cdot 3 \cdot 5 \ldots n}. \tag{2}$$

D'altra parte sussistono le $\frac{n+1}{2}$ congruenze

$$2n \equiv -1, \; 2n-2 \equiv -3, \; \ldots \; n+1 \equiv -n \pmod{2n+1}$$

dalle quali si ricava:

$$2n(2n-2) \ldots (n+1) \equiv (-1)^{\frac{n+1}{2}} \cdot 1 \cdot 3 \cdot 5 \cdot \ldots n \pmod{2n+1}$$

Se ora supponiamo $p = 2n+1$ primo (e quindi $1 \cdot 3 \cdot 5 \ldots n$ primo con p), da quest'ultima e dalla (2) segue:

$$2^n \equiv (-1)^{\frac{n+1}{2}} \pmod{p = 2n+1}.$$

Se $n = 4k + 1$ si trova allora:

$$2^{\frac{p-1}{2}} = 2^{4k+1} \equiv -1 \pmod{p = 8k + 3}. \tag{3}$$

Se $n = 4k + 3$ si trova:

$$2^{\frac{p-1}{2}} = 2^{4k+3} \equiv 1 \pmod{p = 8k + 7 = 8(k + 1) - 1} \tag{4}$$

b) Sia ora n pari. Dalla (1) sopprimendo i fattori comuni n, $n + 2$, ... $(2n - 1)$, segue:

$$2^n = \frac{2n(2n - 2) \dots (n + 4)(n + 2)}{1 \cdot 3 \dots (n - 3)(n - 1)} . \tag{2'}$$

Dalle congruenze:

$$2n \equiv -1,\ 2n - 2 \equiv -3,\ \dots\ n + 2 \equiv -(n - 1) \pmod{2n + 1}$$

si trae poi:

$$2n(2n - 2) \dots (n + 2) \equiv (-1)^{\frac{n}{2}} \cdot 1 \cdot 3 \cdot 5 \cdot 7 \dots (n - 1)$$

e quindi, supposto $2n + 1$ primo:

$$2^n \equiv (-1)^{\frac{n}{2}} \pmod{2n + 1}.$$

Se allora $n = 4k$, segue di qui:

$$2^{\frac{p-1}{2}} = 2^{4k} \equiv 1 \pmod{p = 8k + 1}. \tag{5}$$

Se invece $n = 4k - 2$, si ottiene:

$$2^{\frac{p-1}{2}} = 2^{4k-2} \equiv -1 \pmod{p = 8k - 3}. \tag{6}$$

Dalle (3), (4), (5), (6) segue pertanto il teorema 1 che, scoperto da EULERO, fu per la prima volta dimostrato da LAGRANGE facendo uso della legge di reciprocità.

Ciò premesso richiamiamo il seguente teorema fondamentale sui residui cubici (4):

TEOREMA 2 « Ogni numero primo della forma $p = 6n + 1$ è rappresentabile (in un sol modo) nella forma:

$$p = a^2 + 3b^2 \tag{7}$$

(4) Per questo teorema vedasi ad esempio L. E. DICKSON, *Cyclotomy, higher congruences, and Waring's problem*, Amer. J. Math., 57 (1935) pag. 400.

ed anche l'equazione $4p = x^2 + 27y^2$ ammette una e una sola soluzione. Posto allora:

$$4p = L^2 + 27M^2 \tag{8}$$

il numero 2 è residuo cubico di p se e solo se L è pari e l'equazione:

$$p = z^2 + 27t^2 \tag{9}$$

ammette in tal caso soluzione».

Se $L = 2l$ è pari (e quindi $M = 2m$ è pari), la rappresentazione (7) di p, che è unica, non può d'altra parte che coincidere con la rappresentazione (9) e quindi, quale corollario del teorema precedente, ha luogo il seguente:

TEOREMA 3. - «Se $p = 6m + 1$ è un numero primo e nella rappresentazione

$$p = a^2 + 3b^2$$

che esiste ed è unica, l'intero b è divisibile per 3, il numero 2 è residuo cubico di p cioè $2^{\frac{p-1}{3}} = 2^{2m} \equiv 1 \pmod{p}$ e viceversa»

Osserviamo poi che un numero primo p della forma $6m + 1$ presenta contemporaneamente una delle due forme $8k + 1$, $8k - 1$ se e solo se $m = 4h$ oppure $m = 4h + 1$ rispettivamente, mentre presenta contemporaneamente una delle due forme $8k - 3$, $8k + 3$ se e solo se $m = 4h + 2$ oppure $m = 4h + 3$ rispettivamente.

Abbinando i risultati contenuti nei teoremi 1 e 3 e tenendo conto di questa ultima osservazione, è facile pervenire alla proposizione che determina il carattere sestico di 2.

Conviene tuttavia premettere un lemma che ci sarà utile nel seguito:

LEMMA «*Sia* $p = 2^\alpha \gamma m + 1$ *un numero primo e sia inoltre* $\alpha \geq 1$ *e* $\gamma > 1$ *dispari.*

Dalle congruenze simultanee:

$$2^{\gamma m} = 2^{\frac{p-1}{2^\alpha}} \equiv (-1)^\lambda \pmod{p} \tag{10}$$

$$2^{2^\alpha m} = 2^{\frac{p-1}{\gamma}} \equiv 1 \pmod{p} \tag{11}$$

segue allora la congruenza:

$$2^m = 2^{\frac{p-1}{2^\alpha \gamma}} \equiv (-1)^\lambda \pmod{p}». \tag{12}$$

Dimostrazione.

a) Sia λ pari. Indicato con $\delta > 0$ l'esponente al quale appartiene 2 (mod. p) (cioè il minimo intero positivo x soddisfacente la congruenza $2^x \equiv 1$ (mod. p)) in base alle (10) e (11) segue che δ divide simultaneamente gli interi γm e $2^\alpha m$. Essendo $\gamma > 1$ e 2^α primi fra loro, si conclude allora che δ divide m ed ha quindi luogo la congruenza:

$$2^m = 2^{2^\alpha \gamma \frac{p-1}{}} \equiv 1 \pmod{p}$$

coincidente appunto con la (12) per λ pari.

b) Sia λ dispari. In tal caso dalla (10) che si scrive:

$$2^{\gamma m} \equiv -1 \pmod{p} \tag{10'}$$

segue la congruenza:

$$2^{2\gamma m} \equiv 1 \pmod{p} \tag{13}$$

L'intero positivo δ, a causa delle (11), (13), deve dunque dividere simultaneamente gli interi $2m\gamma$ e $2^\alpha m = 2m \cdot 2^{\alpha-1}$. Essendo $2^{\alpha-1}$ e γ primi fra loro, si conclude allora che δ deve dividere $2m$, per modo che ha luogo la congruenza:

$$2^{2m} \equiv 1 \pmod{p}. \tag{14}$$

Da quest'ultima discende:

$$2^m \equiv \pm 1 \pmod{p}.$$

Il segno superiore è però da scartarsi perchè la congruenza $2^m \equiv 1$ (mod. p) implica l'altra $2^{\gamma m} \equiv 1$ (mod. p) che è in contrasto con la (10'). In definitiva dunque sussiste la congruenza $2^m \equiv -1$ (mod. p) che è appunto la (12) corrispondente a λ dispari.

Applichiamo ora il lemma dimostrato al caso dei numeri primi della forma:

$$p = 6m + 1 = 2^1 \cdot 3 \cdot m + 1$$

(per i quali risulta $\alpha = 1$, $\gamma = 3$). Se $m = 4h$, $4h + 1$ cioè $p = 24h + 1$ $p = 24h + 7$, hanno luogo le congruenze simultanee:

$$2^{3m} = 2^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

$$2^{2m} = 2^{\frac{p-1}{3}} \equiv 1 \pmod{p}$$

e da esse discende:

$$2^m = 2^{\frac{p-1}{6}} \equiv 1 \pmod{p}.$$

Se $m = 4h + 2$, $4h + 3$ cioè $p = 24h + 13$, $p = 24h + 19$, hanno luogo le congruenze simultanee:

$$2^{3m} = 2^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

$$2^{2m} = 2^{\frac{p-1}{3}} \equiv 1 \pmod{p}$$

dalle quali segue:

$$2^m = 2^{\frac{p-1}{6}} \equiv -1 \pmod{p}.$$

Siamo così in grado di enunciare il seguente teorema che rivela il carattere sestico di 2:

TEOREMA A. - *Sia* $p = 6m + 1$ *un numero primo e sia:*

$$p = a^2 + 3b^2$$

la sua rappresentazione nella forma $x^2 + 3y^2$. *Se allora* $b \equiv 0 \pmod 3$ *ed* $m = 4h, 4h + 1$, *sussiste la congruenza:*

$$2^{\frac{p-1}{6}} \equiv 1 \pmod{p}.$$

Se $b \equiv 0 \pmod 3$ *ed* $m = 4h + 2, 4h + 3$, *sussiste l'altra congruenza:*

$$2^{\frac{p-1}{6}} \equiv -1 \pmod{p}$».$$

Il carattere 12mo di 2. - GAUSS ha dimostrato il seguente teorema che rivela il carattere biquadratico di 2:

TEOREMA 4. - « Sia $p = a^2 + b^2$, a dispari, b pari, $p = 4n + 1$. Se 2 è residuo quadratico del numero primo p, ha luogo la congruenza:

$$2^{\frac{p-1}{4}} \equiv (-1)^{\frac{b}{4}} \pmod{p}».$$

Questo teorema si può enunciare anche in forma lievemente diversa. Infatti già sappiamo che se n è dispari, 2 è non-residuo quadratico del numero primo $p = 4n + 1 = 4(2h - 1) + 1 = 8h - 3$. Rimane solo da considerare perciò il caso $n = 2m$ pari, cioè $p = 8m + 1$.

In questo caso poi nella rappresentazione $p = 8m + 1 = a^2 + b^2$ (a dispari, b pari), l'intero b è divisibile per 4; infatti l'ipotesi $b = 2c$ con c dispari, si rivela assurda poichè nella relazione $a^2 - 1 = 4(2m - c^2)$ che da essa segue, il primo membro è divisibile per 8 mentre non lo è il secondo.

Il teorema di GAUSS può quindi enunciarsi semplicemente così:

TEOREMA 4'. - « Se $p = 8n + 1 = a^2 + 16b^2$ è un numero primo, sussiste la congruenza:

$$2^{\frac{p-1}{4}} \equiv (-1)^b \pmod{p} \text{ ».}$$

Supponiamo ora che il numero primo p sia della forma $12m + 1 = 4(3m) + 1 = 6(2m) + 1$. Esso ammetterà le due rappresentazioni $p = a^2 + b^2 = c^2 + 3d^2$ con b pari, a dispari. Perchè 2 sia residuo quadratico di p occorre e basta che p presenti la forma $8h \pm 1$. Il caso $p = 12m + 1 = 8h + 1$ comporta $3m = 2h$, $m \equiv 0 \pmod 2$ e quindi $p = 24t + 1$. Il caso $p = 12m + 1 = 8h - 1$ comporta $6m + 1 = 4h$ cioè un assurdo.

Desiderando che 2 sia residuo quadratico di p, rimane perciò solo da studiare il caso $p = 24t + 1$.

Sia $p = 24t + 1 = a^2 + f^2 = c^2 + 3d^2$ (f pari), un numero primo. In queste condizioni, come si è detto, 2 è residuo quadratico di p Se poi è $d \equiv 0 \pmod 3$, in forza al teorema 3, l'intero 2 risulta anche residuo cubico di p. Poichè $p = 8(3t) + 1$, f è poi divisibile per 4: $f = 4b$ e quindi: $p = a^2 + 16b^2$.

Per il teorema di GAUSS allora:

$$2^{\frac{p-1}{4}} \equiv (-1)^b \pmod{p}.$$

Applicando il lemma fondamentale, tenuto conto che nel caso attuale:

$$p = 24t + 1 = 2^2 \cdot 3(2t) + 1 \quad \alpha = 2 \quad \gamma = 3 \quad m = 2t$$

$$2^{3m} = 2^{6t} = 2^{\frac{p-1}{4}} \equiv (-1)^b \pmod{p}$$

$$2^{2^2 m} = 2^{8t} = 2^{\frac{p-1}{3}} \equiv 1 \pmod{p}$$

si conclude subito con la congruenza:

$$2^m = 2^{2t} = 2^{\frac{p-1}{12}} \equiv (-1)^b \pmod{p}.$$

Siamo così giunti a formulare il teorema che rivela il carattere 12^{mo} di 2:

TEOREMA B. - « *Se* $p = 24t + 1 = a^2 + 16b^2 = c^2 + 3d^2$ *è un numero primo ed inoltre* $d \equiv 0 \pmod 3$, *sussiste la congruenza:*

$$2^{\frac{p-1}{12}} \equiv (-1)^b \pmod p \text{ ».}$$

Il carattere 24mo di 2. - WHITEMAN ha recentemente dimostrato, come si è detto, la congettura di REUSCHLE facendo uso del metodo della ciclotomia. Il teorema in oggetto viene dall'autore enunciato così:

TEOREMA 5. - « Sia 2 residuo biquadratico di $p = a^2 + b^2$, a dispari, b pari, $p = 8n + 1$. Se n è pari, allora:

$$2^{\frac{p-1}{8}} \equiv (-1)^{\frac{b}{8}} \pmod p$$

Se n è dispari:

$$2^{\frac{p-1}{8}} \equiv (-1)^{8+1} \pmod p \text{ ».}$$

D'altra parte è bene osservare che, essendo p della forma $8n + 1$, 2 è certamente residuo quadratico di p; per di più, se si postula per p la rappresentabilità nella forma $p = a^2 + 64b^2$, p risulta anche residuo biquadratico di p per il teorema 4' di GAUSS. Conviene allora enunciare il teorema di REUSCHLE-WESTERN-WHITEMAN nella forma seguente:

TEOREMA 5'. - « Sia $p = 8n + 1$ un numero primo il quale ammette la rappresentazione:

$$p = a^2 + 64b^2.$$

Se allora n è pari, sussiste la congruenza:

$$2^{\frac{p-1}{8}} \equiv (-1)^b \pmod p.$$

Se n è dispari, sussiste invece l'altra congruenza:

$$2^{\frac{p-1}{8}} \equiv (-1)^{b+1} \pmod p \text{ ».}$$

Supponiamo allora che $p = 6h + 1$ ammetta la rappresentazione $p = a^2 + 3b^2$ con $b \equiv 0 \pmod 3$ e che sia contemporaneamente p della forma $8n + 1$. Dall'eguaglianza $p = 8n + 1 = 6h + 1$ discende $4n = 3h$ cioè $n \equiv 0 \pmod 3$ e quindi $p = 24m + 1$.

In queste condizioni 2 è residuo quadratico di p perchè p ha la forma $8r + 1$. Se inoltre nella rappresentazione $p = c^2 + 16g^2$, g è pari, per il teorema 4' di GAUSS, 2 è anche residuo biquadra-

tico di p. Supponiamo allora che $p = 24m + 1$ ammetta la rappresentazione:

$$p = a^2 + 3b^2 = c^2 + 64d^2$$

con $b \equiv 0 \pmod 3$. In tal caso, per quanto fin qui dimostrato, 2 è certamente residuo quadratico, cubico e biquadratico di p.

Applichiamo ora il teorema di REUSCHLE-WESTERN-WHITEMAN.

Poichè $p = 8(3m) + 1$, se $3m$ è pari, cioè m è pari, sussiste la congruenza:

$$2^{\frac{p-1}{8}} \equiv (-1)^d \pmod p. \tag{15}$$

Se m è dispari, sussiste al contrario l'altra congruenza:

$$2^{\frac{p-1}{8}} \equiv (-1)^{d+1} \pmod p. \tag{16}$$

Facciamo ora nuovamente uso del lemma fondamentale distinguendo i due casi m pari ed m dispari.

a) Sia m pari. In tal caso risultando:

$$p = 24m + 1 = 2^3 \cdot 3m + 1 \quad \alpha = 3 \quad \gamma = 3$$

$$2^{3m} = 2^{\frac{p-1}{8}} \equiv (-1)^d \pmod p \tag{15}$$

$$2^{3m} = 2^{\frac{p-1}{3}} \equiv 1 \pmod p$$

si conclude con la congruenza:

$$2^m = 2^{\frac{p-1}{24}} \equiv (-1)^d \pmod p.$$

b) Sia m dispari. Quanto si è scritto sopra relativamente al caso m pari rimane immutato, all'infuori della (15) che deve sostituirsi con la (16); ne segue pertanto la congruenza:

$$2^{\frac{p-1}{24}} \equiv (-1)^{d+1} \pmod p$$

La breve analisi svolta ci porta dunque a formulare il seguente:

TEOREMA C. - « *Sia* $p = 24m + 1$ *un numero primo il quale ammette la rappresentazione:*

$$p = a^2 + 3b^2 = c^2 + 64d^2$$

con $b \equiv 0 \pmod 3$. *Se allora* m *è pari, sussiste la congruenza:*

$$2^{\frac{p-1}{24}} \equiv (-1)^d \pmod p.$$

Se m è dispari, sussiste la congruenza:

$$2^{\frac{p-1}{24}} \equiv (-1)^{a+1} \pmod{p}\text{ ».}$$

Il carattere 48mo di 2. - WHITEMAN, nel citato lavoro, dimostra con il metodo della ciclotomia, anche il seguente teorema, scoperto da A. CUNNINGHAM e dimostrato, come si disse, per la prima volta, da A. AIGNER nel 1939:

TEOREMA 6. « Sia $p = a^2 + b^2 = c^2 + 2d^2$, a e c dispari, $p = 16n + 1$ un numero primo. Se allora $2^{\frac{p-1}{8}} \equiv 1 \pmod{p}$, risulta:

$$2^{\frac{p-1}{16}} \equiv (-1)^{\frac{b}{16}+\frac{d}{4}} \pmod{p}\text{ ».}$$

D'altra parte è bene osservare che, essendo p della forma $8n + 1$, 2 è certamente residuo quadratico di p; inoltre se si postula per p la rappresentabilità nella forma $p = a^2 + 64b^2$, 2 risulta anche residuo biquadratico di p, per il teorema 4' di GAUSS. Infine il teorema 5' ci dice che se il numero primo $p = 8n + 1$ con n pari ammette la rappresentazione $p = a^2 + 64b^2$, sussiste la congruenza: $2^{\frac{p-1}{8}} \equiv (-1)^b \pmod{p}$. Questo teorema in particolare per b pari dà luogo alla seguente proposizione:

TEOREMA 7. - « Se $p = 16m + 1$ ammette la rappresentazione:

$$p = a^2 + 256f^2,$$

sussiste la congruenza:

$$2^{\frac{p-1}{8}} \equiv 1 \pmod{p}$$

cioè 2 è residuo ottavico di p ».

In base a queste considerazioni riteniamo pertanto conveniente enunciare il teorema di CUNNINGHAM-AIGNER-WHITEMAN nel modo seguente:

TEOREMA 6'. - « Se $p = 16n + 1$ è un numero primo il quale ammette la rappresentazione:

$$p = a^2 + 256f^2 = c^2 + 32d^2$$

sussiste la congruenza:

$$2^{\frac{p-1}{16}} \equiv (-1)^{f+d} \pmod{p}\text{ ».} \tag{17}$$

Ciò premesso consideriamo un numero primo della forma $48m + 1 = 6(8m) + 1 = 16(3m) + 1$ e supponiamo che nella sua rap-

presentazione nella forma $p = q^2 + 3t^2$, l'intero t sia divisibile per 3.

In queste condizioni 2 è residuo cubico del numero primo $p = 48m + 1$. Se poi $p = 16(3m) + 1$ ammette anche la rappresentazione:

$$p = a^2 + 256f^2$$

in forza al teorema 7, il numero 2 è anche residuo ottavico di p. Se per di più infine lo stesso p ammette la rappresentazione:

$$p = c^2 + 32d^2$$

in base al teorema 6' sussiste la congruenza (17).

Se si tien conto che attualmente risulta:

$$p = 48m + 1 = 2^4 \cdot 3m + 1 \quad \alpha = 4 \quad \gamma = 3$$

$$2^{3m} = 2^{\frac{p-1}{16}} \equiv (-1)^{f+d} \pmod{p}$$

$$2^{24m} = 2^{\frac{p-1}{3}} \equiv 1 \pmod{p}$$

e si applica il lemma fondamentale, si conclude allora subito con la congruenza:

$$2^{\frac{p-1}{48}} \equiv (-1)^{f+d}.$$

Possiamo pertanto enunciare il seguente teorema che rivela il carattere 48mo di 2:

TEOREMA D. - « *Se* $p = 48m + 1$ *è un numero primo il quale ammette le rappresentazioni:*

$$p = a^2 + 3b^2 = c^2 + 256d^2 = e^2 + 32f^2$$

con $b \equiv 0 \pmod 3$, *sussiste la congruenza:*

$$2^{\frac{p-1}{48}} \equiv (-1)^{f+d} \pmod{p} \text{ }».$$

Applicazione ai numeri di Mersenne.

1) Dal teorema 1 relativo al carattere quadratico di 2, si desume in particolare il criterio che regola la divisibilità di $2^p - 1$ per $2p + 1$ nell'ipotesi che p e $2p + 1$ siano ambedue numeri primi:

TEOREMA 8. - « Se $p = 4k + 3$ è un numero primo e anche

$2p+1=8k+7$ è un numero primo, il numero di MERSENNE 2^p-1 è composto, risultando:

$$2^p-1\equiv 0 \pmod{2p+1}\text{».}$$

(Teorema di EULERO-LAGRANGE)

Osserviamo ora che, se p e $4p+1$ sono ambedue numeri primi, non può sussistere in nessun caso la congruenza:

$$2^p-1\equiv 0 \pmod{4p+1}$$

Infatti poichè $p=2k+1$ è dispari, 2 è non-residuo quadratico del numero primo $4p+1=8k+5=8(k+1)-3$ e quindi $2^{2p}\equiv -1 \pmod{4p+1}$.

2) Dal teorema A si desume il seguente criterio che regola la divisibilità di 2^q-1 per $6q+1$ nell'ipotesi che q e $6q+1$ siano ambedue numeri primi:

TEOREMA 9. - « Se $q=4h+1$ e $p=6q+1=a^2+3b^2$ sono ambedue numeri primi ed inoltre b è divisibile per 3, il numero di MERSENNE 2^q-1 è composto, risultando:

$$2^q-1\equiv 0 \pmod{6q+1}$$

(Teorema di PELLET-KRAITCHIC).

3) Dal teorema 5' di REUSCHLE si desume in particolare il seguente criterio che regola la divisibilità di 2^q-1 per $8q+1$ nell'ipotesi che q ed $8q+1$ siano ambedue primi:

TEOREMA 10. - *Se* q *e* $p=8q+1=a^2+64b^2$ *sono ambedue numeri primi e* b *è dispari, il numero di* MERSENNE 2^q-1 *è composto, risultando:*

$$2^q-1\equiv 0 \pmod{p=8q+1}\text{».}$$

Osserviamo ora che, se q e $12q+1$ sono ambedue numeri primi, non può in alcun caso sussistere la congruenza: $2^q-1\equiv 0 \pmod{12q+1}$. Infatti il numero 2 è non-residuo quadratico di $p=12q+1=12(2m+1)+1=8(3m+2)-3$.

4) Dal teorema 6' di CUNNINGHAM-AIGNER-WHITEMAN si desume in particolare il seguente criterio che regola la divisibilità di 2^q-1 per $p=16q+1$ nell'ipotesi che q e p siano ambedue primi:

TEOREMA 11. - « *Se* q *e* $p=16q+1=a^2+256f^2=c^2+32d^2$ *sono ambedue numeri primi ed inoltre* f *e* d *hanno la stessa parità, il numero* 2^q-1 *è composto risultando:*

$$2^q-1\equiv 0 \pmod{p=16p+1}\text{».}$$

5) Dal teorema C si desume il criterio seguente che regola la divisibilità di $2^q - 1$ per $p = 24q + 1$ nell'ipotesi che q e p siano ambedue numeri primi:

TEOREMA 12. - « *Se* q e $p = 24q + 1 = a^2 + 3b^2 = c^2 + 64d^2$ *sono ambedue primi ed inoltre* d *è dispari e* b *divisibile per* 3, *il numero* $2^q - 1$ *è composto, risultando:*

$$2^q - 1 \equiv 0 \pmod{p = 24p + 1}\text{ }».$$

6) Infine dal teorema D si può desumere il criterîo che regola la divisibilità di $2^q - 1$ per $p = 48q + 1$ nell'ipotesi che q e p siano ambedue primi:

TEOREMA 13. - « *Se* q e $p = 48q + 1 = a^2 + 3b^2 = c^2 + 256d^2 = e^2 + 32f^2$ *sono ambedue numeri primi ed inoltre* f, d *hanno la stessa parità e* b *è divisibile per* 3, *il numero* $2^q - 1$ *è composto, risultando:*

$$2^q - 1 \equiv 0 \pmod{p = 48q + 1}\text{ }».$$

Questi sono tutti e soli i criteri di divisibilità che si conoscono relativamente ai numeri di MERSENNE. Se si riflette sul fatto che i divisori dei numeri di MERSENNE $2^q - 1$ sono della forma $2kq + 1$, ci si avvede che, in base ai teoremi richiamati o dimostrati in questo lavoro, rimangono esauriti i soli casi $k = 1, 2, 3, 4, 6, 8, 12, 16, 24, 48$.

Riteniamo opportuno per maggiore chiarezza riunire tutte le congruenze che rappresentano i risultati della presente ricerca sui numeri di MERSENNE:

1ª) $2^q - 1 \equiv 0 \pmod{p = 2q + 1}$ se $q = 4k + 3$ e $p = 2q + 1$ sono primi.

2ª) $2^q - 1 \equiv 0 \pmod{p = 6q + 1}$ se $q = 4k + 1$ e $p = 6q + 1 = a^2 + 27c^2$ sono primi.

3ª) $2^q - 1 \equiv 0 \pmod{p = 8q + 1}$ se q e $p \equiv 8q + 1 = a^2 + 64b^2$ (b dispari) sono primi.

4ª) $2^q - 1 \equiv 0 \pmod{p = 16q + 1}$ se q e $16q + 1 = a^2 + 256f^2 = c^2 + 32d^2$ ($f + d$ pari) sono primi.

5ª) $2^q - 1 \equiv 0 \pmod{p = 24q + 1}$ se q e $p = 24q + 1 = a^2 + 27b^2 = c^2 + 64d^2$ (d dispari) sono primi.

6ª) $2^q - 1 \equiv 0 \pmod{p = 48q + 1}$ se q e $p = 48q + 1 = a^2 + 27b^2 = c^2 + 256d^2 = e^2 + 32f^2$ ($f + d$ pari) sono primi.