Bollettino
Unione Matematica Italiana

M. Cugiani

Osservazioni relative alla questione dell'esistenza di un algoritmo euclideo nei campi quadratici

Bollettino dell'Unione Matematica Italiana, Serie 3, Vol. **3** (1948), n.2, p. 136–141.

Zanichelli

<http://www.bdim.eu/item?id=BUMI_1948_3_3_2_136_0>

Osservazioni relative alla questione dell'esistenza di un algoritmo euclideo nei campi quadratici.

Nota di M. CUGIANI (a Novara).

Sunto. - *Coll'aiuto di un lemma, esposto nella parte iniziale della presente nota, si dimostra una proposizione che rientra come caso particolare in un teorema di* HOFREITER *la cui dimostrazione sembra prestare il fianco a qualche critica, e si dimostra pure, facendo uso di mezzi elementari, una proposizione che rientra in un teorema provato da* ERDÖS *e* CHAOKO *per via non elementare, giungendosi inoltre a stabilire una limitazione, interessante per la nostra questione, che non era mai stata per l'innanzi stabilita.*

Noi diciamo che nel campo quadratico $K(\sqrt{D})$ vale l'A. E. se dati due interi qualsiasi del campo, α, β è sempre possibile trovare un terzo intero γ del campo stesso, tale che si abbia

$$|N(\alpha - \beta\gamma)| < |N(\beta)| \quad \text{ovvero} \quad \left|N\left(\frac{\alpha}{\beta} - \gamma\right)\right| < 1.$$

La questione di stabilire per quali valori di D valga l'A. E. trattata già da molti illustri autori, è stata da costoro in gran parte risolta. L'incertezza permane solo per valori di D che appartengono ad alcune particolari classi. Di tali valori è stato dimostrato che sono certamente in numero finito, e si può presumere che sono probabilmente assai pochi (1).

Noi ci ripromettiamo di fare qui alcune osservazioni, che ci sembrano di importanza sostanziale, su taluni lavori relativi a questo argomento.

Formuliamo anzitutto un lemma che ci servirà per quanto andiamo ad esporre.

Sia p un numero primo della forma $kn + h$.

Fissiamo h', k', d, t interi positivi soddisfacenti alle condizioni:

$$h' < k',\ k' \mid k\ (2),\ d = (k',\ (h - h')),\quad \left(\frac{d}{p}\right) = \left(-1\right)^{\frac{p+1}{2}},$$

$$d \geq t,\quad h' \equiv \frac{h - h'}{d} \left(\mathrm{mod}\ \frac{k'}{d}\right),\quad p > dtk'$$

e consideriamo l'insieme, che chiameremo A, di tutti i numeri

(1) Su tutto questo vedi per es.: L. RÉDEI, *Ueber den Euklidischen Algorithmus in Reellquadratischen Zahlkörpern*, « Jurn. für die reine und ang. Math. », 183 (1941), pp. 183-192.

(2) Col simbolo $a \mid b$ intendiamo significare che il numero a divide il numero b.

della forma $k'm + h'$ minori di $\frac{p}{t}$ essendo m una variabile che assume valori interi positivi.

Dico che fra i numeri dell'insieme A ne esiste certamente uno che non è residuo quadratico di p.

Possiamo dimostrare questo lemma per assurdo supponendo che, se è possibile, tutti i numeri di A siano residui quadratici di p. Consideriamo infatti un altro insieme B formato da tutti i numeri che si ottengono dividendo per d le differenze fra p e i singoli elementi di A. Ogni termine di B avrà la forma $\frac{k'}{d} w + \frac{h - h'}{d}$ $\left(\text{ove si ha } w = \frac{k}{k'} n - m\right)$ e sarà non residuo di p per la ipotesi fatta che sia $\left(\frac{d}{p}\right) = (-1)^{\frac{p+1}{2}}$. Inoltre il numero dei termini di B sarà uguale al numero dei termini di A che è $\geq d$ essendo per ipotesi $p > dtk'$ ed inoltre $h' < k'$. Notiamo ancora che tutti i numeri di B sono minori di $\frac{p}{t}$ essendo essi, per il modo stesso con cui sono definiti, minori di $\frac{p}{d}$ ed avendosi per ipotesi $d \geq t$. Ora è facile dimostrare che uno dei termini di B viene a coincidere con uno dei termini di A. Infatti i numeri w sono della forma $w = \frac{k}{k'} n - m$, e poichè i numeri m assumono valori interi consecutivi, lo stesso accadrà dei w, i quali sono in numero tanti quanti gli elementi di B e quindi formeranno almeno un sistema completo di resti mod d. Quindi la congruenza $\frac{k'}{d} x + \frac{h - h'}{d} \equiv h'$ (mod k') la quale è certamente solubile a causa dell'ipotesi $\frac{h - h'}{d} \equiv h' \left(\text{mod } \frac{k'}{d}\right)$ ammetterà almeno una soluzione x_0 coincidente con uno dei w. Quindi uno degli elementi di B avrà la forma $k'm + h'$ ed essendo $< \frac{p}{t}$ coinciderà con uno degli elementi di A. Tale numero dovrebbe quindi essere nello stesso tempo residuo e non residuo di p. Da tale assurdo segue senz'altro il nostro asserto.

Notiamo qui, che ove fosse $h = h'$ le considerazioni precedenti varrebbero ancora purchè si ponesse $d = k'$.

Ciò premesso passiamo ad esporre le annunciate osservazioni.

1. Tratterremo anzitutto del seguente teorema di HOFREITER: L'A. E. non può valere in $K(\sqrt{D})$ quando sia $D \equiv 21 \pmod{24}$, escluso il caso $D = 21$ [3].

[3] Vedi: N. HOFREITER, *Quadratische Korper mit und ohne Euklidischen Algorithmus.* « Monatsh. für Mat. und Phys. 42, (1935), pp. 397-400.

La dimostrazione di tale proposizione è condotta dall'autore in modo da lasciare dei dubbi sulla sua validità.

Egli la fa dipendere infatti dalla insolubilità della congruenza $dx^2 - 3Y^2 \equiv 0 \pmod 8$, essendo $Y = dy - 2g$, dove g è arbitrario (intero), $d = \frac{D}{3}$, x ed y devono soddisfare alla sola condizione $x \equiv y \pmod 2$. Ora della affermazione di tale insolubilità l'HOFREITER non dà alcuna giustificazione, e d'altra parte è evidente che ove si ponga $x \equiv Y \equiv 0 \pmod 4$, oppure $x \equiv Y \equiv 2 \pmod 4$, il che evidentemente è sempre possibile, anche compatibilmente colla condizione $x \equiv y \pmod 2$, la congruenza è soddisfatta. Il pensiero dello Autore appare quindi poco chiaro e ci è sembrato non inutile il tentare di dare del teorema una dimostrazione che non faccia ricorso alla insolubilità della detta congruenza. La proposizione che siamo pervenuti a dimostrare ha sfortunatamente un contenuto più ristretto di quella dell'HOFREITER. Eccola in breve.

Sappiamo anzitutto per un lemma di BEHRBOHM e RÉDEI che l'A. E. non può esistere in $K(\sqrt{D})$ con $D \equiv 21 \pmod{24}$ se non è $D = 3p$, dove p è primo (4).

Mostriamo adesso in primo luogo che *l'A. E. non può valere in* $K(\sqrt{D})$ *con* $D = 3p \equiv 21$ *(mod 24) se è possibile determinare un numero* σ *tale che si abbia* $\sigma < \frac{p}{3}$, $\sigma \equiv 1 \pmod 8$, $\left(\frac{\sigma}{3}\right) = 1$, $\left(\frac{\sigma}{p}\right) = -1$.

Sappiamo infatti da un altro lemma di BEHRBOHM e REDEI che l'A. E. non vale in $K(\sqrt{D})$ con $D \equiv 1 \pmod 4$ se esiste un r tale che la congruenza $z^2 \equiv r \pmod D$ sia solubile in interi z e che inoltre nessuna delle equazioni

$$DX^2 - Y^2 = -4r, \qquad DX^2 - Y^2 = 4(D - r)$$

sia solubile in interi X, Y (5).

Supposta ora l'esistanza del numero σ anzidetto poniamo $r = 3p \quad 9\sigma$, le due equazioni precedenti assumeranno la forma:

$$DX^2 - Y^2 = 4(9\sigma - 3p), \qquad DX^2 - Y^2 = 36\sigma$$

e si vede subito che la seconda è insolubile avendosi

$$\left(\frac{D}{\sigma}\right) = \left(\frac{3p}{\sigma}\right) = \left(\frac{\sigma}{3p}\right) = -1.$$

(4) Vedi: BEHRBOHM e REDEI, *Der Euklidischen Algorithmus in quadratischen Korpern.* « Journ. für die reine und ang. Math. », 174, (1936), pp. 192-205.

(5) Vedi: BEHRBOHM e RÉDEI, art. cit.

Per la insolubilità della seconda osserviamo che il secondo membro contiene un fattore $(p - 3\sigma)$ ora abbiamo

$$\left(\frac{p-3\sigma}{D}\right) = \left(\frac{p-3\sigma}{3p}\right) = \left(\frac{p}{3}\right)\left(\frac{-3\sigma}{p}\right) = \left(\frac{p}{3}\right)\left(\frac{p}{3}\right) = -1.$$

Inoltre vale la congruenza $p - 3\sigma \equiv 7 - 3 \cdot 1 \equiv 4 \pmod 8$ quindi $(p - 3\sigma)$ contiene il fattore 2 a potenza pari. Posto perciò $(p-3\sigma)_0 = \frac{p-3\sigma}{4}$ avremo

$$\left(\frac{p-3\sigma}{D}\right) = \left(\frac{(p-3\sigma)_0}{D}\right) = \left(\frac{D}{(p-3\sigma)_0}\right) = -1$$

di qui segue l'insolubilità della prima equazione e la dimostrazione del nostro asserto è compiuta.

Osserviamo adesso che in taluni casi è facile assicurare l'esistenza di un numero σ, definito come sopra. Consideriamo infatti il caso $p \equiv 7 \pmod{120}$ Invocando il lemma che noi abbiamo dimostrato all'inizio di questo scritto, ed applicandolo al caso di un numero primo p della forma $120n + 7$, si vede subito che tra i numeri della forma $120m + 97$ minori di $\frac{p}{3}$ deve esistere almeno un non residuo di p, purchè sia $p > 10800$. Ora tale non residuo risponde a tutti i requisiti richiesti per il numero σ.

Analogo ragionamento vale quando sia $p \equiv 103 \pmod{120}$. Il numero σ si dovrà cercare adesso fra quelli della forma $120m + 73$ ed esisterà certamente, come ci assicura il solito lemma, purchè sia $p > 10800$.

2. Trattiamo ora del seguente lemma di ERDÖS e CHAO KO: l'A. E. può esistere solo in un numero finito di $K(\sqrt{D})$ quando D sia primo della forma $24n + 13$ oppure $8n + 1$ (6).

La dimostrazione di questa proposizione, fornita dai suddetti Autori è da loro fatta dipendere dal seguente lemma:

Se p è un numero primo abbastanza grande $[p > p(n)]$ detti q_1, q_2, q_3 i tre minimi non residui quadratici dispari di p si ha

$$p^{1-n} > q_1 q_2 q_3$$

dove $n < 10^{-3}$ è una costante positiva arbitraria.

La dimostrazione di questo lemma è a sua volta fondata su teoremi anche molto riposti di aritmetica analitica. Noi ci siamo sfor-

(6) Vedi: ERDÖS e CHAO KO: *Note on the Euclidean Algorithm*, « The Journal of the London Math. Soc. ». Vol. XIII, (1938), pp. 3-8.

zati di dare invece del teorema di ERDÖS e CHAO KO una dimostrazione elementare, la quale ci permettesse inoltre di assegnare un effettivo limite superiore dei valori di D per cui può valere un A. E., limite di cui il teorema sopra enunciato ci assicura soltanto l'esistenza. Anche qui siamo riusciti nel nostro intento soltanto per valori di D meno generali di quelli contenuti nella dimostrazione primitiva.

Dall'esame della dimostrazione di ERDÖS e CHAO KO si vede intanto che limitatamente al caso $p \equiv 13 \pmod{24}$ essa procede ugualmente se alla condizione $D = p > q_1 q_2 q_3$, di cui al lemma sopra menzionato si sostituisce la condizione meno restrittiva $D = p > 3q_1 q_2$, dove q_1 e q_2 sono i minimi non residui dispari di p.

Ora si può subito dimostrare che, per p abbastanza grande, tale condizione è soddisfatta nei due casi particolari $p \equiv 13 \pmod{120}$ e $p \equiv 37 \pmod{120}$.

Per tali valori di p si ha intanto $\left(\frac{5}{p}\right) = -1$ e quindi $q_1 = 5$. Osserviamo ora che posto dapprima $p \equiv 13 \pmod{120}$, fra i numeri della forma $15m + 13$, minori di $\frac{p}{15}$, esiste certamente un non residuo di p purchè sia $p > 15^3$ come ci assicura il nostro lemma, applicato ai valori numerici $k = 120$, $k' = 15$, $h = h' = 13$, $d = t = 15$.

Ora tale non residuo o è primo o contiene in ogni caso un numero primo minore di $\frac{p}{15}$ che è non residuo di p e che è diverso da 5, poichè i numeri della forma $15m + 13$ non sono divisibili per 5. Quindi il nostro asserto è dimostrato.

Analoga dimostrazione nel caso $D = p \equiv 37 \pmod{120}$ ove si cerchi un non residuo di p fra i numeri della forma $15m + 7$ minori di $\frac{p}{15}$ col solito lemma, applicato ai valori numerici $k = 120$, $k' = 15$, $h = 37$, $h' = 7$, $d = t = 15$. Dovrà essere ancora $p > 15^3$.

Sostituendo la proposizione testè dimostrata all'analogo lemma di ERDÖS e CHAO KO, e lasciando del resto immutate le considerazioni di questi due autori, si può immediatamente stabilire il teorema:

L'A. E. non vale in $K(\sqrt{D})$ *con* $D \equiv 13,27 \pmod{120}$ *se sia* D *primo maggiore di* 15^3.

Il ragionamento da noi qui usato può essere facilmente esteso. Daremo un esempio di ciò. Consideriamo i casi precedentemeute esclusi $D \equiv 61 \pmod{120}$ e $D \equiv 109 \pmod{120}$ e scegliamo per fissare le idee il primo fra essi $D = 120n + 61$. I numeri D di questa

forma potranno anche esser rappresentati ponendo $D = 840n + \rho$ con $\rho \equiv 61 \pmod{120}$, $\rho < 840$.

I valori possibili per ρ formano un sistema completo di numeri incongrui mod 7. Uno di essi sarà divisibile per 7 ed è da scartare dovendo essere D primo, degli altri sei, tre saranno residui quadratici di 7 e tre non residui; indichiamo questi ultimi con $\rho_1\rho_2\rho_3$ e fissiamo la nostra attenzione p. es. su ρ_1. Siamo cioè condotti a considerare numeri D della forma $840n + \rho_1$. Si può facilmente dimostrare che anche per questi si ha $D > 3q_1q_2$ purchè sia $D > 21^3$. Qui intanto sarà $q_1 = 7$. Ragionando poi come poc'anzi basterà far vedere che esiste un numero non residuo di p fra quelli non divisibili per 7 che sono minori di $\frac{D}{21}$. Ora un tal numero esiste certamente fra quelli della forma $21m + \rho_1'$ (dove ρ_1' è il minimo resto positivo di ρ_1 mod 21) come ci assicura il nostro lemma applicato ai valori

$$k = 840; \quad k' = 21; \quad h = \rho_1; \quad h' = \rho_1'; \quad d = t = 21.$$

Analogamente si potrebbe operare rispetto ai valori

$$D = 840n + \rho_2, \qquad D = 840n + \rho_3.$$

Con questo esempio riteniamo di aver sufficientemente illustrato come sia possibile generalizzare il nostro schema di ragionamento estendendolo via via a tutti i casi precedentemente esclusi.