Bollettino
Unione Matematica
Italiana

Luigi Bianchi

Prova di un teorema aritmetico di Jacobi

Bollettino dell'Unione Matematica Italiana, Serie 1, Vol. **1** (1922), n.2-3, p. 41–43.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=BUMI_1922_1_1_2-3_41_0>

Bollettino dell'Unione Matematica Italiana, Unione Matematica Italiana, 1922.

PICCOLE NOTE

Prova di un teorema aritmetico di Jacobi.

Nota di LUIGI BIANCHI

Nel tomo 3 del *Giornale di Crelle* (p. 497) DIRICHLET proponeva la questione seguente. Se q è un numero primo della forma $q = 4h + 3$, risulta dal teorema di WILSON la congruenza

$$\left(1 \cdot 2 \cdot 3 \ldots \frac{q-1}{2}\right)^2 \equiv 1 \pmod{q},$$

indi l'altra

$$1 \cdot 2 \cdot 3 \ldots \frac{q-1}{2} \equiv \pm 1 \pmod{q}. \tag{1}$$

DIRICHLET domandava un criterio per decidere per quali numeri primi $q \equiv 3 \pmod 4$ vale nel secondo membro della (1) il segno positivo, e per quali il segno negativo. Al che rispose JACOBI *Crelle's Journal*, Bd. 9 S. 189, *Werke* Bd. 6, S. 243) colla proposizione seguente:

Se il numero dei residui quadratici di q *che sono* $> \frac{q}{2}$ *si indica con* μ, *si ha*

$$1 \cdot 2 \cdot 3 \ldots \frac{q-1}{2} \equiv (-1)^{\mu} \pmod{q}, \tag{A}$$

e vale quindi nella (1) *il segno superiore se* μ *è pari, l'inferiore se* μ *è dispari.*

Osservo che per dimostrare la formola (A) basta imitare il procedimento tenuto da GAUSS per stabilire il lemma fondamentale della sua terza dimostrazione della legge di reciprocità (GAUSS, *Werke*, Bd. II, p. 1-8), come segue.

Ripartiamo i $\frac{q-1}{2}$ residui quadratici (mod. q) in due gruppi,

dei quali il primo contenga i μ residui $\alpha_1, \alpha_2, \ldots, \alpha_\mu$ che sono $> \frac{q}{2}$, l'altro i rimanenti $\beta_1, \beta_2, \ldots, \beta_\lambda$ $\left(\lambda+\mu=\frac{q-1}{2}\right)$ inferiori a $\frac{q}{2}$. Siccome i numeri α, β sono insieme le radici delle congruenza binomia di grado dispari

$$x^{\frac{q-1}{2}} - 1 \equiv 0 \pmod{q},$$

avremo

$$\alpha_1\alpha_2 \ldots \alpha_\mu\beta_1\beta_2 \ldots \beta_\lambda \equiv 1 \pmod{q}. \tag{2}$$

Se consideriamo i $\frac{q-1}{2}$ numeri

$$q-\alpha_1,\ q-\alpha_2, \ldots, q-\alpha_\mu,\ \beta_1,\ \beta_2, \ldots, \beta_\lambda, \tag{3}$$

questi sono inferiori tutti a $\frac{q}{2}$ e diversi fra loro, poichè non vi sono due α o due β eguali, nè un $q-\alpha$ eguale a un β, essendo il secondo residuo, il primo non residuo, a causa di $\left(\frac{-1}{q}\right)=-1$. Dunque i numeri (3) riproducono, in altro ordine, i numeri

$$1,\ 2,\ 3, \ldots, \frac{q-1}{2}$$

e facendone il prodotto risulta

$$(q-\alpha_1)(q-\alpha_2)\ldots(q-\alpha_\mu)\beta_1\beta_2\ldots\beta_\lambda = 1\cdot 2\cdot 3\ldots\frac{q-1}{2}.$$

Se qui si riduce (mod. q), osservando la (2), se ne trae subito la (A).

Come nella seconda trasformazione del lemma di GAUSS, si può dare un altro aspetto alla (A) facendo figurare, in luogo dei numeri α, β, che sono i minimi resti positivi (mod. q) dei quadrati

$$1^2,\ 2^2,\ 3^2 \ldots \left(\frac{q-1}{2}\right)^2, \tag{4}$$

i quozienti della divisione di questi per q. Pongasi in generale

$$s^2 = qE\left(\frac{s^2}{q}\right) + r_s \quad \left(s = 1, 2, 3, \ldots \frac{q-1}{2}\right),$$

avendo indicato con $E\left(\frac{s^2}{q}\right)$ il quoziente, con r_s il resto della divisione di s^2 per q. Sommando la precedente pei valori $1, 2, 3 \ldots \frac{q-1}{2}$ di s e ponendo

$$N = \sum_s E\left(\frac{s^2}{q}\right), \quad A = \alpha_2 + \alpha_2 + \ldots + \alpha\mu, \quad B = \beta_1 + \beta_2 + \ldots + \beta_\lambda,$$

col ricordare la formola

$$1^2 + 2^2 + \ldots + \left(\frac{q-1}{2}\right)^2 = \frac{q(q^2-1)}{24},$$

deduciamo

$$\frac{q(q^2-1)}{24} = qN + A + B.$$

D'altra parte, sommando i numeri (3), si ottiene, per quanto precede

$$\frac{q^2-1}{8} = \mu q - A + B,$$

che sottratta dalla precedente dà

$$\frac{(q^2-1)(q-3)}{24} = q(N-\mu) + 2A.$$

Siccome nella (A) si tratta solo di decidere se μ è pari o dispari, ed il numero a destra

$$\frac{(q^2-1)(q-3)}{24} = \frac{4h(2h^2+3h+1)}{3} \quad (q = 4h+3)$$

è pari (anzi multiplo di 4), resta

$$N \equiv \mu \pmod 2.$$

La formula (A) si può dunque anche scrivere

$$\text{(B)} \qquad 1 \cdot 2 \cdot 3 \ldots \frac{q-1}{2} \equiv (-1)^N \pmod q, \quad N = \sum_{s=1}^{s=\frac{q-1}{2}} E\left(\frac{s^2}{q}\right).$$

Pisa, novembre 1922.