Raffaele Paolantonio

Alcune relazioni fra i coefficienti binomiali e nuove dimostrazioni che ne discendono per due teoremi aritmetici

Bollettino dell'Unione Matematica Italiana, Serie 1, Vol. **10** (1931), n.4, p. 205–209.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=BUMI_1931_1_10_4_205_0>

Bollettino dell'Unione Matematica Italiana, Unione Matematica Italiana, 1931.

Alcune relazioni fra i coefficienti binomiali e nuove dimostrazioni che ne discendono per due teoremi aritmetici.

Nota di Raffaele Paolantonio (a Torino).

Sunto. - *Utilizzando la nota formula per la moltiplicazione del coseno, si stabiliscono alcune relazioni fra i coefficienti binomiali, dalle quali discendono facilmente due noti teoremi sui residui quadratici.*

1. Essendo m un numero intero positivo e θ un numero reale qualunque, si consideri la nota relazione:

$$\cos m\theta = \cos^m \theta - \binom{m}{2} \cos^{m-2} \theta \operatorname{sen}^2 \theta + \binom{m}{4} \cos^{m-4} \theta \operatorname{sen}^4 \theta - \dots .$$

Pongasi

$$m = 2nh + \nu,$$

$$\theta = \frac{\pi}{h},$$

dove n, h, ν sono numeri interi; siccome

$$\cos (2nh + \nu)\frac{\pi}{h} = \cos \left(2n\pi + \nu \frac{\pi}{h}\right) = \cos \nu \frac{\pi}{h},$$

ne viene:

$$\cos \nu \frac{\pi}{h} = \cos^m \frac{\pi}{h} - \binom{m}{2} \cos^{m-2} \frac{\pi}{h} \operatorname{sen}^2 \frac{\pi}{h} + \binom{m}{4} \cos^{m-4} \frac{\pi}{h} \operatorname{sen}^4 \frac{\pi}{4} \dots$$

Se $\nu = \pm 1$ oppure $\nu = \pm (h-1)$, essendo

$$\cos (\pm 1) \frac{\pi}{h} = \cos \frac{\pi}{h},$$

$$\cos \pm (h-1) \frac{\pi}{h} = \cos \left(\pi - \frac{\pi}{h}\right) = -\cos \frac{\pi}{h},$$

ne segue:

$$(1) \quad \pm \cos \frac{\pi}{h} = \cos^m \frac{\pi}{h} - \binom{m}{2} \cos^{m-2} \frac{\pi}{h} \operatorname{sen}^2 \frac{\pi}{h} + \binom{m}{4} \cos^{m-4} \frac{\pi}{h} \operatorname{sen}^4 \frac{\pi}{h} - \dots$$

Il segno $+$ del primo membro della (1) si riferisce a $\nu = \pm 1$ e quello $-$ a $\nu = \pm (h-1)$.

2. Si faccia nella (1):

$h = 4$ e quindi $m = 8n + \nu$, $\nu = \pm 1$ oppure $\nu = \pm 3$;

ricordando che

$$\operatorname{sen} \frac{\pi}{h} = \cos \frac{\pi}{4} = \frac{1}{\sqrt{2}},$$

si ha:

$$(2) \quad \pm \frac{1}{\sqrt{2}} = \left(\frac{1}{\sqrt{2}}\right)^m - \binom{m}{2}\left(\frac{1}{\sqrt{2}}\right)^m + \binom{m}{4}\left(\frac{1}{\sqrt{2}}\right)^m - \dots + (-1)^{\frac{m-1}{2}} \binom{m}{m-1}\left(\frac{1}{\sqrt{2}}\right)^m.$$

In questa relazione e nelle tre seguenti il segno superiore del primo membro si riferisce a $m = 8n \pm 1$ e quello inferiore a $m = 8n \pm 3$.

Moltiplicando entrambi i membri della (2) per $(\sqrt{2})^m$ risulta:

$$\pm (\sqrt{2})^{m-1} = 1 - \binom{m}{2} + \binom{m}{4} - \dots + (-1)^{\frac{m-1}{2}} \binom{m}{m-1},$$

cioè

$$(3) \quad \pm 2^{\frac{m-1}{2}} = 1 - \binom{m}{2} + \binom{m}{4} - \dots + (-1)^{\frac{m-1}{2}} \binom{m}{m-1}.$$

Se m è un numero primo, tenendo presente che ciascun termine [1] (eccetto il primo) del secondo membro della (3) è divisi-

[1] Se m è un numero primo e $\alpha_1 \dots \alpha_a$ sono numeri interi positivi o nulli ciascuno minore di m e la cui somma è uguale ad m, è noto che $\dfrac{m!}{\alpha_1! \dots \alpha_a!}$ è un numero intero divisibile per m.

In particolare $\binom{m}{k} = \dfrac{m!}{k!\,(m-k)!}$ è divisibile per m, se m è un numero primo e k un numero intero tale che $0 < k < m$.

bile per m, si ottiene:

$$(4) \qquad \pm 2^{\frac{m-1}{2}} \equiv 1 \pmod{m}.$$

3. Si faccia nella (1):

$h=6$ e quindi $m=12n+\nu$, $\nu=\pm 1$ oppure $\nu=\pm 5$;

ricordando che

$$\operatorname{sen}\frac{\pi}{6}=\frac{1}{2},$$

$$\cos\frac{\pi}{6}=\frac{\sqrt{3}}{2},$$

si ha:

$$(5) \qquad \pm\frac{\sqrt{3}}{2}=\left(\frac{\sqrt{3}}{2}\right)^m-\binom{m}{2}\left(\frac{\sqrt{3}}{2}\right)^{m-2}\left(\frac{1}{2}\right)^2+$$

$$+\binom{m}{4}\left(\frac{\sqrt{3}}{2}\right)^{m-4}\left(\frac{1}{2}\right)^4-\ldots+(-1)^{\frac{m-1}{2}}\binom{m}{m-1}\frac{\sqrt{3}}{2}\left(\frac{1}{2}\right)^{m-1}.$$

In questa relazione e nelle quattro seguenti il segno superiore del primo membro si riferisce a $m=12n\pm 1$ e quello inferiore a $m=12n\pm 5$.

Moltiplicando entrambi i membri della (5) per $\frac{2^m}{\sqrt{3}}$ risulta:

$$\pm 2^{m-1}=(\sqrt{3})^{m-1}-\binom{m}{2}(\sqrt{3})^{m-3}+\binom{m}{4}(\sqrt{3})^{m-5}-\ldots+(-1)^{\frac{m-1}{2}}\binom{m}{m-1},$$

cioè

$$(6) \qquad \pm 2^{m-1}=3^{\frac{m-1}{2}}-\binom{m}{2}3^{\frac{m-3}{2}}+\binom{m}{4}3^{\frac{m-5}{2}}-\ldots+(-1)^{\frac{m-1}{2}}\binom{m}{m-1},$$

ovvero

$$(6') \qquad \pm(2^{m-1}-1)=\left(3^{\frac{m-1}{2}}\mp 1\right)-\binom{m}{2}3^{\frac{m-3}{2}}+\binom{m}{4}3^{\frac{m-5}{2}}-\ldots+(-1)^{\frac{m-1}{2}}\binom{m}{m-1}.$$

Se m è un numero primo, tenendo presente che il primo membro [1] e ciascun termine (dal secondo in poi) del secondo membro della (6′) sono divisibili per m, si ottiene:

$$(7) \qquad \pm 3^{\frac{m-1}{2}} \equiv 1 \pmod{m}.$$

[1] Essendo m un numero primo ed a primo con m, si ha (Teorema di FERMAT): $a^{m-1}\equiv 1 \pmod{m}$.

In particolare per $a=2$ ed m uguale ad un numero primo dispari, risulta $2^{m-1}-1$ divisibile per m.

4. Osserviamo che non possono coesistere nè le due congruenze

$$\begin{cases} 2^{\frac{m-1}{2}} \equiv 1 \pmod{m} \\ 2^{\frac{m-1}{2}} \equiv -1 \pmod{m} \text{ per } m = 8n+3 \ (n \text{ numero intero } \geq 0), \\ \qquad\qquad \text{oppure } m = 8n-3 \ (n \text{ numero intero } > 0 \end{cases}$$

e nè le altre due

$$\begin{cases} 3^{\frac{m-1}{2}} \equiv 1 \pmod{m} \\ 3^{\frac{m-1}{2}} \equiv -1 \pmod{m} \text{ per } m = 12n+5 \ (n \text{ numero intero } \geq 0). \\ \qquad\qquad \text{oppure } m = 12n-5 \ (n \text{ numero intero } > 0) \end{cases}$$

altrimenti si avrebbe la relazione assurda $1 \equiv -1 \pmod{m}$ (1).

Da ciò e dalle stabilite relazioni (4) e (7), e per il criterio di EULERO discendono i seguenti due teoremi:

1°) Il numero 2 è residuo quadratico di tutti i numeri primi delle forme $8n+1$ e $8n-1$, ed è non residuo quadratico dei numeri primi delle forme $8n+3$ e $8n-3$.

Osservando che i numeri interi positivi delle forme $8n-1$ ed $8n-3$ (n numero intero > 0) sono rispettivamente delle forme $8n+7$ ed $8n+5$ (n numero intero ≥ 0) e viceversa, tale risultato può enunciarsi così:

Il numero 2 è residuo quadratico di tutti i numeri primi delle forme $8n+1$ e $8n+7$, ed è non residuo quadratico dei numeri primi delle forme $8n+3$ e $8n+5$.

Questo teorema conosciuto da FERMAT, fu dimostrato per la prima volta da LAGRANGE (« Nouv. Mém. de l'Ac. de Berlin », 1775).

2°) Il numero 3 è residuo quadratico di tutti i numeri primi delle forme $12n+1$ e $12n-1$, ed è non residuo quadratico dei numeri primi delle forme $12n+5$ e $12n-5$.

Questo teorema conosciuto da FERMAT, fu dimostrato per la prima volta da EULERO (« Nov. Comment. Ac. Petrop. », T. VIII, pag. 105).

5. Con considerazioni analoghe alle precedenti si possono stabilire facilmente altre relazioni utilizzando le seguenti note for-

(1) Cfr. ad. es. DIRICHLET-DEDEKIND, *Lezioni sulla Teoria dei Numeri*, pag. 72.

mule:

$$\operatorname{sen} m\theta = \binom{m}{1} \operatorname{sen}\theta \cos^{m-1}\theta - \binom{m}{3} \operatorname{sen}^3\theta \cos^{m-3}\theta + \\ + \binom{m}{5} \operatorname{sen}^5\theta \cos^{m-5}\theta - \ldots$$

$$\tan m\theta = \frac{\binom{m}{1}\tan\theta - \binom{m}{3}\tan^3\theta + \binom{m}{5}\tan^5\theta - \ldots}{1 - \binom{m}{2}\tan^2\theta + \binom{m}{4}\tan^4\theta - \ldots}.$$