La Matematica nella Società e nella Cultura

Rivista dell'Unione Matematica Italiana

Maria Cocozza, Alessio Russo

Numeri colorati e Ultimo Teorema di Fermat

La Matematica nella Società e nella Cultura. Rivista dell'Unione Matematica Italiana, Serie 1, Vol. **4** (2011), n.2, p. 171–179.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=RIUMI_2011_1_4_2_171_0>

La Matematica nella Società e nella Cultura. Rivista dell'Unione Matematica Italiana, Unione Matematica Italiana, 2011.

La Matematica nella Società e nella Cultura
Rivista dell'Unione Matematica Italiana
Serie I, Vol. IV, Agosto 2011, 171-179

Numeri colorati e Ultimo Teorema di Fermat

Maria Cocozza - Alessio Russo

1. – Introduzione

Immaginiamo di essere in aula, di scegliere quattro studenti e di dare a ciascuno di essi un gessetto colorato. Prendiamo poi un cesto della tombola contenente i numeri da 1 a 90, e dopo aver sorteggiato uno studente fra i quattro, questi estragga un numero dal cesto e lo riporti sulla lavagna con il proprio gessetto. Facciamo ripetere l'operazione fino a che il cesto resti vuoto. Supponiamo, il che è abbastanza ragionevole, che ogni ragazzo abbia scritto almeno un numero con il suo gessetto sulla lavagna. Allora i numeri da 1 a 90 vengono ripartiti in quattro insiemi a seconda del colore con cui sono stati scritti; a questo punto chiediamo di verificare se tra questi insiemi ne esista uno contenente dei numeri x, y e z (con x non necessariamente diverso da y) tali che $x + y = z$.

La risposta a tale domanda è affermativa, anzi la situazione presentata è un caso particolare di un risultato dimostrato nel 1916 dal matematico I. Schur ([9]), che assicura *che per ogni numero intero* $k \geq 1$, *esiste un intero positivo* s *tale che, colorando i numeri da* 1 *a* s *con* k *colori, esistono dei numeri* x, y *e* z *aventi lo stesso colore tali che* $x + y = z$. La motivazione che portò Schur al teorema precedente, fu lo studio della cosiddetta "versione locale" dell'equazione di P. Fermat

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

Come è noto, tale equazione è priva di soluzioni intere non banali se $n > 2$; è questo il contenuto del famoso *Ultimo Teorema di Fermat* dimostrato nel 1995 dal matematico inglese A. Wiles ([13] e [12]), quasi 300 anni dopo la pubblicazione postuma dell'edizione speciale dell'*Aritmetica di Diofanto con le Osservazioni di P. Fermat*, in cui il matematico francese congetturava la validità di tale risultato (per una

esposizione divulgativa della storia dell'Ultimo Teorema di Fermat si può, ad esempio, far riferimento ad uno dei libri [1], [7] e [10]). L'idea di Schur fu quella di analizzare l'equazione congruenziale

$$x^n + y^n \equiv z^n (mod p)$$

dove p è un numero primo fissato. Egli sperava di dimostrare che, al variare del primo p, nessuna di tali equazioni ha soluzioni intere non banali, cosa che avrebbe provato la congettura di Fermat. Tuttavia, come vedremo più avanti, utilizzando il teorema sulle colorazioni prima ricordato, Schur dimostrò il seguente risultato:

Versione locale dell'Ultimo Teorema di Fermat. *Sia n un numero intero positivo. Allora esiste un primo q tale che, per ogni numero primo $p \geq q$ l'equazione congruenziale $x^n + y^n \equiv z^n (mod p)$ ha una soluzione intera tale che xyz non è divisibile per p.*

Ovviamente la condizione che xyz non è multiplo di p è utile per evitare le soluzioni banali dell'equazione come $x \equiv y \equiv z \equiv 0 (mod p)$ oppure $x \equiv 0 (mod p)$ e $y \equiv z (mod p)$. Il teorema precedente è molto interessante dal punto di vista didattico, oltre che storico, poiché mostra come una possibile dimostrazione della congettura di Fermat non può essere di tipo elementare come, invece, si legge nella famosa nota a margine dell'*Arithmetica* di Diofanto scritta da Fermat nel 1637.

Scopo di quest'articolo è quello di fornire un'esposizione elementare dei risultati di Schur. In molti testi di matematica combinatoria (cfr., ad esempio, [3], [2] e [5]) il teorema di Schur sulle colorazioni precedemente citato, viene ottenuto come corollario di un famoso teorema di F. P. Ramsey pubblicato nel 1930 ([6]) che è stato il punto di partenza di un settore molto ampio della matematica combinatoria, oggi noto come *"Teoria di Ramsey"*. In realtà, quello che serve è un caso particolare del teorema di Ramsey, che assicura che *se k è un numero intero positivo, allora esiste un poligono avente un numero di vertici dipendente da k tale che, comunque si colorano con k colori i suoi lati e le sue diagonali, resta determinato almeno un triangolo i cui lati hanno tutti lo stesso colore*. Nel prossimo paragrafo riporteremo una dimo-

strazione diretta di quest'ultimo risultato dovuta a R. E. Greenwood e A. M. Gleason ([4]). Come vedremo, il ragionamento sviluppato non è altro che la naturale generalizzazione della soluzione del ben noto *problema della festa*.

2. – Grafi colorati

Nella matematica combinatoria uno degli strumenti più semplici è sicuramente il *principio dei cassetti*, formulato per la prima volta in modo esplicito da P. G. L. Dirichlet nel 1834:

Siano n e k dei numeri naturali tali che $k < n$. Allora se n oggetti sono distribuiti in k scatole, qualche scatola deve contenere più di un oggetto.

Formalmente, possiamo dire che se A e B sono insiemi finiti di ordini, rispettivamente, n e k, con $k < n$, e $\Delta : A \longrightarrow B$ è un'applicazione, allora esiste un elemento $b \in B$ tale che $|\Delta^{-1}(b)| \geq 2$. A dispetto della sua semplicità il principio dei cassetti spesso trova utilizzazione nella dimostrazione di risultati interessanti e non sempre del tutto banali. Ad esempio, si può dimostrare che sono vere le seguenti affermazioni:

(i) Se si colorano i punti del piano cartesiano aventi coordinate intere di rosso e di blu, allora esiste un rettangolo i cui vertici hanno tutti lo stesso colore.
(ii) Si considerino i numeri $1, 2, 3, \ldots, 2n$ e se ne scelgano $n + 1$ arbitrariamente. Allora due fra questi $n + 1$ numeri sono primi fra loro.
(iii) Nell'ipotesi di (ii) si ha che esistono due numeri fra gli $n + 1$ scelti tali che uno divide l'altro.

È simpatico ricordare che P. Erdös era solito proporre il quesito (iii) a giovani allievi che si avviavano allo studio della matematica (combinatoria).

Il principio dei cassetti si può facilmente generalizzare al modo seguente.

LEMMA 2.1. – *Siano n e k dei numeri naturali tali che $n = mk + r$ con $r \geq 1$. Se $\Delta : \{1, 2, \ldots, n\} \longrightarrow \{1, 2, \ldots, k\}$ è un'applicazione, allora esiste un elemento $i \in \{1, 2, \ldots, k\}$ tale che $|\Delta^{-1}(i)| \geq m + 1$.*

DIMOSTRAZIONE – Per assurdo sia $|\Delta^{-1}(i)| \leq m$ per ogni i. Allora

$$n = mk + r = |\Delta^{-1}(1)| + |\Delta^{-1}(2)| + \ldots + |\Delta^{-1}(k)| \leq mk,$$

una contraddizione. □

Ovviamente, per $m = 1$ si riottiene il principio dei cassetti. Per le considerazioni successive è utile introdurre alcune notazioni. Innanzitutto, se k è un numero naturale, denoteremo con I_k l'insieme $\{1, 2, \ldots, k\}$. Ciò premesso, se S è un insieme non vuoto, si dice *k-colorazione* di S ogni applicazione $\Delta : S \longrightarrow I_k$. Sia $s \in S$. Allora l'elemento $\Delta(s)$ è il *colore* di s. Inoltre, una parte (non vuota) T di S è *monocromatica* se la restrizione di Δ a T è costante.

Un ben noto problema di matematica combinatoria, spesso proposto in occasione di gare matematiche (cfr. [11], Problem 27.1) è il cosiddetto *problema della festa*:

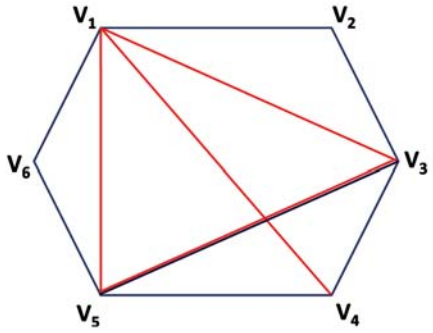
Ad una festa sono presenti sei persone. Allora sicuramente ve ne sono tre che a due a due si conoscono oppure tre che a due a due non si conoscono.

Proviamo a riformulare tale questione nel linguaggio espressivo della *teoria dei grafi*. Sia n un numero naturale, e denotiamo con K_n il *grafo completo* su n vertici, cioè il grafo che ha come lati tutte le possibili $\binom{n}{2}$ coppie di vertici. Ciò premesso, il problema della festa si può formulare al modo seguente:

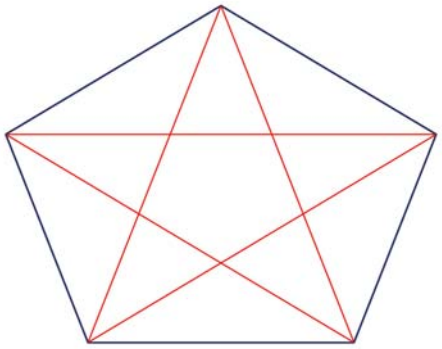
Comunque si considera una 2-colorazione dell'insieme dei lati del grafo completo K_6 (usando, ad esempio, come colori, rosso e blu) esiste un sottografo completo K_3 (triangolo) monocromatico.

Dimostriamo questo risultato. Fissiamo un vertice v_1 di K_6. Poiché v_1 è connesso con altri cinque vertici, allora per il Lemma 2.1, almeno tre lati uscenti da v_1 hanno lo stesso colore, e per co-

modità sia il rosso. Ad esempio, siano questi lati $\{v_1, v_3\}$, $\{v_1, v_4\}$ e $\{v_1, v_5\}$. Se uno dei lati $\{v_i, v_j\}$, con $3 \leq i < j \leq 5$ è rosso, allora il triangolo indotto da $\{v_1, v_i, v_j\}$ è monocromatico (rosso). Invece, se ognuno dei lati $\{v_i, v_j\}$ è blu, allora il triangolo $\{v_3, v_4, v_5\}$ è monocromatico (blu).



Si noti che 6 è il minimo intero positivo n tale che, colorando K_n con due colori, vi è un triangolo monocromatico in K_n. Infatti, se si colora K_5 con due colori, utilizzando un colore per i lati e l'altro per le diagonali, allora non vi sono triangoli monocromatici.



Generalizzeremo ora la situazione precedente.

TEOREMA 2.2 (Greenwood, Gleason, 1955). – *Sia k un intero positivo. Allora esiste un intero $f(k)$ maggiore di k tale che per ogni k-colorazione dei lati del grafo completo $K_{f(k)}$ esiste un sottografo completo K_3 monocromatico. Inoltre, $f(k) \leq 3k!$.*

DIMOSTRAZIONE – Ovviamente, se $k = 1$, allora basta porre $f(1) = 3$, mentre per $k = 2$, abbiamo appena provato che si può porre $f(2) = 6$. Sia pertanto $k > 2$ e supponiamo per induzione che esista un intero positivo $f(k) > k$ con le proprietà richieste. Si ponga

$$f(k+1) = (k+1)(f(k) - 1) + 2,$$

e consideriamo una $(k+1)$-colorazione di $K_{f(k+1)}$. Fissiamo un vertice v. Allora v è estremo di $(k+1)(f(k)-1)+1$ lati, sicché per il Lemma 2.1 esiste un colore s tale che v è estremo di $f(k)$ lati $\{v, v_1\}, \{v, v_2\}, \cdots, \{v, v_{f(k)}\}$ ciascuno di colore s. A questo punto, se fra gli estremi (diversi da v) di questi $f(k)$ lati ve ne sono due v_i e v_j tali che il lato $\{v_i, v_j\}$ ha colore s, allora il triangolo $\{v, v_i, v_j\}$ ha lati di colore s, e l'asserto è dimostrato. In caso contrario, possiamo considerare il sottografo completo $K_{f(k)}$ di vertici $v_1, v_2, \cdots, v_{f(k)}$ che per ipotesi di induzione possiede un triangolo monocromatico.

Infine, la disuguaglianza $f(k) \leq 3k!$ si ottiene facilmente ragionando per induzione su k e ricordando la definizione della funzione f. □

Ovviamente, dal Teorema 2.2 segue immediatamente che se k è un intero positivo, allora per ogni $n \geq f(k)$ e per ogni k-colorazione dei lati del grafo completo K_n esiste un triangolo monocromatico.

3. – Versione locale dell'Ultimo Teorema di Fermat

Consideriamo una k-colorazione dell'insieme $\mathbb{N}$ dei numeri naturali. Allora esiste un intero positivo $t \leq k$ tale che $\mathbb{N}$ è unione disgiunta di t sottoinsiemi monocromatici

$$\mathbb{N} = S_1 \cup S_2 \cup \cdots \cup S_t.$$

Il prossimo risultato, di cui abbiamo già parlato nell'introduzione, mostra in particolare che ogni equazione del tipo

$$x + y = z$$

ha in $\mathbb{N}$ almeno una soluzione monocromatica.

LEMMA 3.1 (Teorema di Schur, 1916). – *Sia k un numero intero positivo. Allora esiste un numero naturale $S(k)$ tale che per ogni intero $n \geq S(k)$ e per ogni k-colorazione $\Delta : I_n \longrightarrow I_k$ di I_n, esistono $x, y, z \in I_n$ tali che $\Delta(x) = \Delta(y) = \Delta(z)$ e $x + y = z$.*

DIMOSTRAZIONE – Si ponga $S(k) = f(k) - 1$, dove f è la funzione definita nel Teorema 2.2. Utilizzando la k-colorazione Δ definiamo una k-colorazione Δ^* sui lati del grafo completo K_{n+1} al modo seguente. Se i e j sono vertici distinti di K_{n+1}, si ponga

$$\Delta^*(\{i,j\}) = \Delta(|i - j|).$$

Poiché $n + 1 \geq f(k)$, per il Teorema 2.2 K_{n+1} possiede un triangolo monocromatico $\{i,j,l\}$, cioè esistono $i,j,l \in I_{n+1}$ tali che $i > j > l$ e $\Delta^*(\{i,j\}) = \Delta^*(\{j,l\}) = \Delta^*(\{i,l\})$. Posto $x = i - j$, $y = j - l$ e $z = i - l$, risulta $\Delta(x) = \Delta(y) = \Delta(z)$ e $x + y = z$. □

Ovviamente, se $k \leq h$, allora $S(k) \leq S(h)$. Una terna monocromatica (x, y, z) verificante l'equazione $x + y = z$ si dice *terna di Schur*. Gli interi $S(k)$ relativi ai primi quattro numeri naturali sono $S(1) = 2$, $S(2) = 5$, $S(3) = 16$ e $S(4) = 65$. Quest'ultimo valore spiega perché nel gioco dei quattro gessetti colorati e dei numeri della tombola la risposta alla domanda finale è affermativa. Osserviamo inoltre che dalla dimostrazione del Lemma 3.1 e dal Teorema 2.2 si ottiene la seguente maggiorazione per gli interi $S(k)$ utile per valori elevati di k:

$$S(k) \leq 3k! - 1.$$

Infine, è interessante ricordare che esiste una *versione forte* del Teorema di Schur, in cui si prova l'esistenza di una terna di Schur (x, y, z) con $x \neq y$. Una dimostrazione elementare di tale risultato può essere consultata a p. 303 di [11].

Quanto premesso finora ci consente di provare la versione locale dell'Ultimo Teorema di Fermat, dovuta a Schur nel 1916. Nel corso della dimostrazione faremo anche uso di nozioni elementari di teoria dei gruppi per le quali si può, ad esempio, far riferimento al capitolo 4 di [8].

TEOREMA 3.2 (Versione locale dell'Ultimo Teorema di Fermat). – *Sia n un numero intero positivo. Allora per ogni primo $p > S(n)$*

l'equazione congruenziale $x^n + y^n \equiv z^n (mod p)$ *ha una soluzione intera tale che* p *non divide* xyz.

DIMOSTRAZIONE – Denotiamo con $\mathbb{Z}_p^* = \{[1]_p, [2]_p, \cdots, [p-1]_p\}$ il gruppo moltiplicativo del campo $\mathbb{Z}_p$ delle classi dei resti modulo p. Consideriamo poi il sottogruppo $H = \{[a]_p^n \mid [a]_p \in \mathbb{Z}_p^*\}$ di $\mathbb{Z}_p^*$. Siano $[a]_p, [b]_p \in \mathbb{Z}_p^*$, e si ponga $[a]_p \sim_H [b]_p$ se e solo se esiste un elemento $[x]_p \in H$ tale che $[a]_p = [x]_p[b]_p$. È facile verificare che $\sim_H$ è una relazione di equivalenza in $\mathbb{Z}_p^*$ e la classe di equivalenza di un elemento $[a]_p$ di $\mathbb{Z}_p^*$ è data dall'insieme $[a]_pH = \{[a]_p[h]_p \mid [h]_p \in H\}$. Come è noto, l'operazione del gruppo $\mathbb{Z}_p^*$ si trasferisce in modo naturale sull'insieme quoziente $\mathbb{Z}_p^*/\sim_H$ che acquista la struttura di gruppo (quoziente). Inoltre, se $\mathbb{Z}_p^*/\sim_H = \{[a_1]_pH, [a_2]_pH, \cdots, [a_k]_pH\}$, allora risulta che $k \leq n$ poiché la potenza n-esima di ogni elemento di $\mathbb{Z}_p^*/\sim_H$ è identica.

Se x è un elemento di I_{p-1}, poniamo $\Delta(x) = i$, dove i è l'unico elemento di I_k tale che $[x]_p \in [a_i]_pH$. Resta in tal modo definita una k-colorazione $\Delta : I_{p-1} \longrightarrow I_k$ di I_{p-1}. Poiché $p - 1 \geq S(n) \geq S(k)$, per il Lemma 3.1 esistono degli elementi $\alpha, \beta, \gamma \in I_{p-1}$ tali che $\Delta(\alpha) = \Delta(\beta) = \Delta(\gamma) = i$ e $\alpha + \beta = \gamma$. Ne segue che $[\alpha]_p, [\beta]_p, [\gamma]_p \in [a_i]_pH$ e $[\alpha + \beta]_p = [\gamma]_p$. Allora esistono degli interi x, y e z non divisibili per p tali che $[\alpha]_p = [a_i]_p[x]_p^n$, $[\beta]_p = [a_i]_p[y]_p^n$ e $[\gamma]_p = [a_i]_p[z]_p^n$. Pertanto, $a_i x^n + a_i y^n \equiv a_i z^n (mod p)$, e quindi

$$x^n + y^n \equiv z^n (mod p),$$

poiché p non divide a_i. L'asserto è dimostrato. □

RIFERIMENTI BIBLIOGRAFICI

[1] A. D. ACZEL, *L'Enigma di Fermat*, Net, Milano, 2003.

[2] B. BOLLOBÁS, *Modern Graph Theory*, Springer, New York, 1991.

[3] R. GRAHAM - B. ROTHSCHILD - J. SPENCER, *Ramsey Theory*, Wiley-Interscience, New York, 1990.

[4] R. E. GREENWOOD - A. M. GLEASON, *Combinatorial relations and chromatic graphs*, Can. J. Math., **7** (1955), 1-7.

[5] B. M. LANDMAN - A. ROBERTSON, *Ramsey Theory on the Integers*, American Mathematical Society, New York, 2004.
[6] F. P. RAMSEY, *On a problem of formal logic*, Proc. London Math. Soc., **30** (1930), 264-286.
[7] P. RIBENBOIM, *Fermat's Last Theorem*, Springer, New York, 1999.
[8] A. RUSSO, *Numeri, Gruppi, Polinomi. Un'introduzione all'Algebra*, Aracne, Roma, 2008.
[9] I. SCHUR, *Uber die Kongruenz* $x^m + y^m = z^m (mod p)$, Jahresberich der Deutschen Matematiker-Vereinigung, **25** (1916), 114-117.
[10] S. SINGH, *L'Ultimo Teorema di Fermat*, Rizzoli, Milano, 1997.
[11] A. SOIFER, *The Mathematical Coloring Book*, Springer, New York, 2009.
[12] R. TAYLOR - A. WILES, *Ring theoretic properties of certain Hecke algebras*, Ann. of Math., **141** (1995), 553-572.
[13] A. WILES, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math., **141** (1995), 443-551.

Maria Cocozza
Liceo Scientifico "G. Galilei", Mondragone, Caserta
e-mail: maria.cocozza@istruzione.it

Alessio Russo
Dipartimento di Matematica, Seconda Università di Napoli
Via Vivaldi 43, I - 81100 Caserta
e-mail: alessio.russo@unina2.it