Come posso dimostrare il teorema di Wilson? Perché è applicabile solo per i numeri primi?

Mi rifarò in questa mia risposta al capitolo VII del bel libro di Albert H. Beiler, "*Recreations in the Theory of Numbers – The Queen of Mathematics entertains (1964)*", dove la "regina della matematica" è, per il Beiler (e moltissimi altri) la Teoria dei Numeri. Il Beiler, volutamente elementare, illustra ma non dimostra alcuni importanti dettagli. Ma naturalmente, per un lettore attento, questi dettagli non chiariti si risolvono in altrettanti dubbi. Io ho cercato di chiarire i dettagli, e bisogna dire che essi nascondono dimostrazioni non del tutto banali.

1. Attribuzione.

Per quanto riguarda l'attribuzione del teorema di Wilson, si legge in rete che *questo teorema fu scoperto per la prima volta da Ibn al-Haytham (conosciuto anche come* ***Alhazen****) intorno all'anno mille, ma prese il nome da John Wilson (allora studente del matematico inglese Edward Waring), che lo riscoprì più di 700 anni dopo. Edward Waring annunciò il teorema nel 1770, nonostante né lui né Wilson possedessero una dimostrazione.* ***Lagrange diede la prima dimostrazione nel 1773 (1).*** *Vi sono alcune ragioni per credere che Leibniz conoscesse questo risultato già un secolo prima, ma non lo pubblicò mai* **(2).**

Fig.1: John Wilson (1741-1793)

1. Come Fermat, Wilson lavorava in un altro campo: dal 1786 al 1793 (anno della sua morte cinquantaduenne) fu *Judge of Common Pleas*, cioè giudicava le cause tra sudditi, quelle che non riguardavano il Re. Che però non fosse un qualunque nessuno in matematica lo sapeva il suo insegnante di matematica all'Università di Cambridge, il Professor Edward Waring (1736-1798). Infatti, nel 1757 Wilson fu *"Senior Wrangler"*, titolo che viene attribuito allo studente che esce primo all'esame del "Cambridge Tripos", terzo anno di matematica, che abilita agli studi superiori di matematica **(3).** Wilson non diede molta importanza alla sua scoperta, ma la comunicò a Waring, il quale la pubblicò, attribuendola a Wilson, nel 1770, e aggiungendo che la dimostrazione gli pareva inaccessibile. Lagrange dimostrò subito il teorema nel 1771 **(1).**

Il teorema di Wilson è uno dei pochi teoremi in teoria dei numeri il cui inverso è anche vero.

2. La scoperta di Wilson (o chi per esso)

La scoperta di Wilson fu la seguente. Si prenda un numero primo, per esempio 11. Si calcoli il fattoriale 1 x 2x 3 x 4 x 5 x 6 x 7 x 8 x 9 x 10 x11. Questo è un numero piuttosto grande, 39916800, ma, per come l'abbiamo formato, è evidente che è divisibile per 1, 2, 3, 4, 5 , 6, 7, 8, 9, 10, 11. Se però dal prodotto omettiamo 11, cioè calcoliamo 10!, otteniamo 3628800, che non può essere divisibile per 11. Perché? Perché 11 è un numero primo, e quindi un prodotto che non contiene 11 o un suo multiplo non può essere divisibile per 11. (4)

Però, Wilson notò che aggiungendo 1 a 10! il numero miracolosamente diventava divisibile per 11. Infatti 3628800+1 = 3628801, che, diviso per 11 , dà 329891. Wilson notò che questo valeva per 3 (infatti 2!+1 =3 è divisibile per 3, per 5 (4 x 3x 2+1= 25, che è divisibile per 5) , per 7 (6 x 5 x 4 x 3 x 2 +1 =721, divisibile per 7) e così via per **tutti e solo i numeri primi.**

Possiamo cioè congetturare che **(p-1)!+1 sia divisibile per p.**

Invece, se si esegue la stessa operazione su numeri composti, si trova che (n-1)!+1 non è divisibile per n. Per esempio, per n=4, 3!+1= 7, non divisibile per 4; per n=6, 5!+1 = 121, non divisibile per 6; per 8, 7!+1 = 5041, non divisibile per 8. Eccetera.

Possiamo quindi congetturare, dato un numero n, il

Teorema di Wilson:

1) se n è primo, (n-1)!+1 è divisibile per n

2) se e solo se (n-1)!+1 è divisibile per n, n è primo.

In teoria, il teorema di Wilson sembra essere un elegante criterio per determinare se un dato numero sia primo o no. In pratica, come criterio non vale nulla: il problema sta nel malefico fattoriale. Il fattoriale diventa presto un numero immenso. Per esempio, per numeri di sette cifre, come 1111111, il fattoriale ha circa un milione di cifre: e non ci si può sognare di usare una approssimazione, come la formula di Stirling: a noi serve anche l'ultima cifra, per applicare criteri di divisibilità, congruenze e via dicendo. Più che un test per verificare se un numero è primo, questa è un'elegante proprietà dei numeri primi, che finora non si è potuta applicare per scoprire se un numero è primo. Non per niente il Beiler battezza il Capo VII del suo testo come "La coppa di Tantalo": abbiamo una dimostrazione chiara, una proprietà inconfutabile, ma non si è ancora trovato il modo di applicarla in pratica.

3. Dimostrazione elementare

Quella di Wilson è solo l'illustrazione di una congettura. Noi procediamo nella dimostrazione. I resti possibili nella divisione di un numero x per un numero primo p sono tutti i numeri da 0 (se p è un divisore di x) a p-1. Per vedere quello che succede col teorema di Wilson, è utile mostrare le tabelle così costruite:

1) Si costruisce una tabella per ogni numero k da 5 a 11 (lascio al lettore la costruzione delle tabelle per k inferiore a 5). La tabella ha k-1 righe e k-1 colonne. Le righe hanno nome (in rosso) da 1 a k-1, e lo stesso hanno le colonne. Questi numeri sono i resti possibili della divisione per k, nel loro ordine naturale.

2) Si calcola casella per casella il prodotto del numero della riga per il numero della colonna, e nella casella si scrive il resto della divisione per k.

E' più semplice da fare che da descrivere.

I. Tabella per k =5, quindi 4 righe per 4 colonne.

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Anche per un k così piccolo, si possono fare delle osservazioni interessanti.

Anzitutto la costruzione: Per esempio la casella in riga 3 e colonna 3 riporta il valore 4: questo è semplicemente il resto della divisione per 5 del prodotto 3 * 3 = 9. Invece, ad

esempio, la casella in riga 4 e colonna 3 riporta il valore 2, resto della divisione di 4 *3 = 12, diviso 5.

Notiamo poi che in ogni riga e colonna compaiono tutti i resti della divisione di un numero non multiplo di 5 per 5. Essi sono, come si è detto, p-1, cioè, in questo caso, 4.

La proprietà più notevole è che questi quattro resti appaiono sempre in diverse righe e diverse colonne. Né in una riga né in una colonna compaiono mai due resti eguali.

Ciò può essere dimostrato:

Lavoriamo sulla riga i. Vogliamo dimostrare che in una tabella n x n il contenuto della casella a(i,k) non può essere eguale al contenuto di una qualsiasi casella a(i,j) se j è diverso da k. Ricordiamo a questo scopo che il contenuto della casella a(i,k) è dato dal resto della divisione per (n+1) del prodotto i*k in cui i è lo i-esimo resto **della divisione per n+1**, in pratica un numero da 1 a n.

Per un numero primo n = p abbiamo, in generale

i * j = m p + R, e quindi dovremmo porre nella casella il valore R.

Supponiamo ora di moltiplicare i due resti i e k. Otteniamo i * k = sp +r. Vogliamo dimostrare che r non può essere eguale a R. Se fosse R=r, sottraendo le due equazioni avremmo (con numeri interi unicamente):

i *(j -k) = (m-s)p

Ma, per il già menzionato Primo Teorema di Euclide **(vedi Nota 4),** se p divide il prodotto i *(j -k) o divide il primo fattore o divide il secondo fattore. Ma il primo fattore è un resto della divisione per p, e quindi non è divisibile per p, mentre il secondo fattore è addirittura la differenza di due resti. Quindi R ≠ r. Ma se non ci sono resti eguali nelle p-1 caselle della riga, vuol dire che , nel caso in cui n è un numero primo, in ogni riga avremo **tutti** i resti da 1 a p-1 in vario ordine, e lo stesso avremo per le colonne, alle quali si può applicare la stessa dimostrazione) ma in modo che mai due resti eguali si trovino sulla stessa riga o sulla stessa colonna della tavola**. Il punto importante è che in ogni riga e colonna ci sarà uno e un solo resto 1.**

Per i numeri non primi, *come vedremo anche in pratica, non abbiamo questa garanzia, perché il teorema di Euclide non vale per i numeri non primi. Per esempio, sia n =6 e si consideri il 9*4= 36. Ora, né 9 né 4 sono divisibili per 6, ma 36 lo è. Ciò spiega perché, almeno nel quadro di questa dimostrazione, il Teorema di Wilson sia applicabile solo ai numeri primi.*

Vediamo, a puro titolo di illustrazione, qualche altra tabella.

Per esempio, sia n =6 (non primo).

II. Tabella per k =6, quindi 5 righe per 5 colonne.

	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

Qui si vede il caos che risulta nella tabella dal fatto che 6 non è un numero primo.

(i) Alcuni resti sono zero.

(ii) I cinque resti possibili compaiono tutti solo nella prima e ultima riga, nella prima e ultima colonna.

(iii) Il resto 1 che, come vedremo, è indispensabile in ogni riga e colonna manca in tre righe e tre colonne.

Vediamo che succede con n = 7 (che è primo): qui si respira di nuovo.

III. Tabella per k =7, quindi 6 righe per 6 colonne.

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Ecco che ogni riga e ogni colonna ha i sei resti da 1 a 6, non si hanno mai due resti eguali sulla stessa riga né sulla stessa colonna, e ogni riga/colonna ha il suo 1.

IV. Tabella per k =8, quindi 7 righe per 7 colonne.

	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	0	2	4	6
3	3	6	1	4	7	2	5
4	4	0	4	0	4	0	4
5	5	2	7	4	1	6	3
6	6	4	2	0	6	4	2
7	7	6	5	4	3	2	1

Qui il caos è ancora più completo che per k =6. Ci sono quattro righe e quattro colonne "complete" di tutti i resti, altre non lo sono. Ci sono cinque zeri e quattro uno. Ma la teoria dei numeri ci lascia sospettare che ci siano simmetrie più arcane, che a noi non serviranno. Per esempio si noti che la tavola II e la tavola IV hanno due triangoli identici, che ho segnato in giallo in Tav.IV. E' facile dimostrare la persistenza del triangolo a Nord-Ovest, meno quella del triangolo Sud-Est.

Da ultimo presento la tavola per k =11, il numero primo con cui abbiamo incominciato la nostra ricerca.

V. Tabella per k =11, quindi 10 righe per 10 colonne.

	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	1	3	5	7	9
3	3	6	9	1	4	7	10	2	5	8
4	4	8	1	5	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	1	6
6	6	1	7	2	8	3	9	4	10	5
7	7	3	10	6	2	9	5	1	8	4
8	8	5	2	10	7	4	1	9	6	3
9	9	7	5	3	1	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	1

E qui siamo ritornati nella regolarità dei numeri primi.

Procediamo nella dimostrazione. In virtù , ad esempio, del primo teorema di Euclide, i numeri primi e solo i numeri primi presentano un 1 e un solo 1 in ogni riga e in ogni colonna, associando un indice i a un indice j. Per esempio, nella Tabella V, i = 9 viene associato a j = 5 per ottenere 1.

Inoltre, per qualsiasi tabella, di numeri primi e non primi, la prima casella è a(1,1) = 1*1 = 1. Similmente, l'ultima casella, a(n-1,n-1) = (n-1)^2 =n^2-2n+1 = n(n-2) +1, cioè, divisa per n, dà resto 1.

Poiché , dato un numero primo p, p-1 è sempre pari, (eccetto che per 2), abbiamo che p può essere diviso in coppie, con due sole eccezioni, la riga 1, in cui 1 è sempre al primo posto, e quindi non vengono associati due resti, ma un resto solo a sé stesso, e la riga (p-1) che è di nuovo associata a sé stessa.

Per p=11 abbiamo quindi:

2*6 ≡ 1 (dove il simbolo ≡ indica che 2*6 è ***congruente a 1, modulo 11***, ovvero 2*6/11 da resto 1)

3*4 ≡ 1

5*9 ≡ 1

7*8 ≡ 1

In 10! , sfruttando quattro congruenze, abbiamo usato tutti gli otto numeri da 2 a p-2. Restano solo 1 e p-1, che vanno associati fra loro, poiché 1 è nella casella (1,1) e (p-1,p-1). Ma il prodotto **1 *(p-1) dà (p-1) che è congruente a -1**, modulo p (qui p=11). E questa è una quinta congruenza, grazie alla quale vengono utilizzati tutti i numeri da 1 a 10 una volta sola ciascuno.

Se ora moltiplichiamo le 5 congruenze ottenute, il risultato è -1, in cui il -1 viene dalla combinazione del primo e dell'ultimo resto. In altre parole , 10! ≡ -1 mod(11), ovvero (11-1)! +1 ≡ 0. Ma è evidente, da come siamo giunti a questo risultato, che il fatto che p =11 è irrilevante. Per p qualsiasi , avremmo una tabella (p-1) x (p-1), in cui p-1 è un numero pari. Certamente la casella (1,1) resta congruente a 1 e la casella (p-1, p-1) resta congruente a -1, mentre i numeri da 2 a p-2 si dividono in coppie il cui prodotto è congruente a 1.

Resta solo da escludere un caso che l'attento lettore avrà notato: sorge un problema se abbiamo un 1 sulla diagonale principale, perché con questo interessiamo un solo resto, anche se al quadrato. Niente ci garantisce che ci sia un altro 1 sulla diagonale principale, in modo che possiamo esaurire tutti i numeri che abbiamo a disposizione (che sono in numero pari). Noi possiamo permetterci con sicurezza un 1 sulla diagonale principale solo nelle due caselle (1,1) e (p-1, p-1). Ma lo si può dimostrare, che è sempre così?

In effetti supponiamo di avere ordinato le caselle secondo i numeri naturali, come nelle tabelle precedenti. Noi vogliamo dimostrare che per n = p, primo, non può mai essere:

k^2 = np +1

Questo può essere svolto in (k-1)(k+1) = np. Occorre anche ricordare che k, essendo un resto, è compreso fra 1 e p-1, estremi inclusi. Per il solito teorema di Euclide, p deve dividere o k+1 o k-1. Ma k è inferiore o al massimo eguale a p-1. Solo se k =p-1 possiamo avere una soluzione, in quanto otteniamo p(p-2)=np, che quindi è divisibile per p, in quanto lo è p, col risultato che n=p-2.

La casella (p-2,p-2) ci dà (p-1)(p-3) =np, ma questo non è possibile, perché nessuno dei due fattori è divisibile per p, essendo più piccolo di p. Scendendo lungo la diagonale la situazione peggiora, perché abbiamo due fattori sempre più piccoli. Quando k=2, abbiamo 3*1 = np e una soluzione esiste solo se 2=p-1, cioè p =3, ricadendo nel caso precedente.

Ma c'è ancora un passo da fare. Se k =1, allora abbiamo (1+1)(1-1) = np, che ci offre una soluzione per n =0. ***Abbiamo così dimostrato che le caselle estreme della diagonale principale sono le sole che possono contenere un 1 (e di fatto lo contengono sempre).***

E con questo è "dimostrato" il teorema di Wilson.

Lagrange diede una seconda dimostrazione in nota alla dimostrazione principale. Essa è assai più immediata di quella che ho scritto, anche se forse meno intuitiva, e potrà interessare coloro che hanno qualche familiarità con il "piccolo teorema di Fermat".

NOTE:

(1) Joseph Louis Lagrange, "Demonstration d'un théorème nouveau concernant les nombres premiers", *Nouveaux Mémoires de l'Académie Royale des Sciences et Belles-Lettres* (Berlin), vol. 2, pages 125–137 (1771). Curiosamente, it.Wikipedia dà la stessa citazione e la data sbagliata, 1773. L'errore si spiega considerando che le memorie del 1771 furono pubblicate nel 1773, come si vede dal frontespizio del volume. Nondimeno, a pag.125, M. de La Grange (così viene qui chiamato l'autore) nota che questo suo contributo fu letto all?Accademia il 13 giugno 1771.

(2) Giovanni Vacca (1899) "Sui manoscritti inediti di Leibniz", *Bollettino di bibliografia e storia delle scienze matematiche* ..., vol. 2, pagine 113–116; vedi pag. 114. Vacca cita dai

manoscritti matematici di Leibniz, conservati alla Reale Pubblica Biblioteca in Hannover (Germania), vol. 3 B, fascicolo 11, page 10:

Scrive il Vacca:

Inoltre egli intravide anche il teorema di Wilson, come risulta dall'enunciato seguente:

"Productus continuorum usque ad numerum qui antepraecedit datum divisus per datum relinquit 1 (vel complementum ad unum?) si datus sit primitivus. Si datus sit derivativus relinquet numerum qui cum dato habeat communem mensuram unitate majorem."

Egli non giunse però a dimostrarlo.

(da https://en.wikipedia.org/wiki/Wilson%27s_theorem)

(3) Credo che ancora adesso il **Cambridge Mathematical Tripos** sia considerato il più infernale esame di matematica al mondo, in un corso universitario di matematica di quel livello: chi voglia vedere il tipo di problemi proposti prenda il testo di *Whittaker e Watson, A course in Modern Analysis*, e dia un'occhiata agli esercizi proposti. Molti provengono dai Cambridge Tripos. Nel 1854, vennero proposti 211 problemi, da risolversi in otto giorni, 45 ore. Naturalmente, neanche il "Senior Wrangler" arrivava in media al 50% del totale possibile.

(4) Alcuni provano difficoltà ad accettare questo concetto. Un esempio si può fare con il numero 10! =3628800, di cui vogliamo dimostrare che **non** è divisibile per 11. Per come il numero è stato costruito (fattoriale), esso non contiene il numero 11 tra i suoi fattori, non contiene suoi multipli, e non contiene neanche divisori di 11 perché 11 è un numero primo. In effetti, la sua scomposizione in fattori primi (che, come dimostrò Gauss nelle sue *Disquisitiones Arithmeticae, 1801,* è unica) è: 3628800 = 2^8 * 3^4 * 5^2 * 7^1. Inevitabilmente, la decomposizione contiene tutti i numeri primi fino a 10, e non contiene nessuno dei successivi, primo dei quali 11, né i loro multipli. Nessuno dei fattori è divisibile per 11 e quindi non lo è neanche 10!.

Se non lo si comprende a prima vista, lo si dimostra, ad esempio, come applicazione del cosiddetto "Primo teorema di Ecuclide", sua proposizione 30, Libro VII, che afferma: "Se un numero primo divide il prodotto di due interi positivi, allora il numero primo divide almeno uno dei due interi positivi". Nel nostro caso, scomponendo 10! nel prodotto di due suoi fattori qualsiasi, dalla scomposizione in fattori primi di ciascuno dei due fattori si vede che nessuno dei due può essere divisibile per 11, e quindi non lo può essere il prodotto. Incidentalmente, qualsiasi "fattoriale con un buco", in cui manchi un numero primo con tutti i suoi multipli, non è divisibile per quel numero primo. E' banale, ma si provi con 1 x 2 x 3 x 4 x 6 x 7 x 8 x 9 x 11 = 798336. Avendo escluso 5 e 10, il numero non è divisibile per 5, come si vede subito.

Tuttavia, qui non dimostro appieno l'importante "Primo Teorema di Euclide", che discende dal metodo delle divisioni successive di Euclide per trovare il MCD di due numeri.

Dirò solo che dal metodo di Euclide segue che il MCD, M , di due numeri A e B à dato da

M = (xU +yV).

Supponiamo che un numero primo P divida AB (per cui r P = AB), ma P non divida A. In altre parole, p e A sono primi fra loro. Ne segue:

M = 1 = (xp+yA) (identità di Bézout)

Si moltiplichino per B entrambi i membri: B = xBP+yAB = xBP+yrP = P(xB+yr), cioè P divide B. CDD.