PRIMA PARTE: una nuova natura dei numeri Primi

Come noto a tutti, si definiscono Primi i numeri Naturali non divisibili.
Dividere per 1 vuol dire lasciare intero, e dividere per 'sé stesso' vuol dire 'atomizzare' un numero Naturale a una somma di unità. Quindi ci sembra ridondante la classica definizione di numero Primo come un numero divisibile solo per sé stesso e per l'unità, e preferiamo evidenziare la sostanza della Primalità: un numero Primo non si può dividere in due o più parti uguali, cioè non si può mettere in relazione con nessun altro numero Naturale.
Ne consegue che dividendo un numero Primo per un altro numero Naturale non si ottiene mai un numero Naturale.
Per indicare un generico numero Primo d'ora in poi sarà usato il simbolo **P**.

Si definiscono Composti tutti i numeri Naturali non Primi, e che di conseguenza possono sempre essere scomposti in un prodotto di potenze di numeri Primi:

(1) $C=P_1^a * P_2^b * P_3^c \ldots..$

La densità

Quando si divide un numero Naturale qualsiasi per un numero N dispari non multiplo di 5 si ottiene un quoziente periodico. Il numero di cifre di cui è fatto questo periodo ha un'importanza molto cruciale in questa nuova concezione dei numeri Primi, e quindi abbiamo voluto dargli un nome speciale ed evocativo: l'abbiamo chiamato *densità* (simbolo ***d***). Si può definire la densità *d* del numero dispari N il numero di cifre da cui è costituito il periodo del quoziente ottenuto dalla divisioni di un numero Naturali per N.
E' stato osservato che per i numeri Primi la densità è sempre unica, cioè dividendo un numero Naturale per un numero Primo si ottiene un numero periodico il cui periodo ha lo stesso numero di cifre indipendentemente dal dividendo considerato. Viceversa per i numeri Composti la densità può assumere valori diversi a seconda del dividendo considerato. I valori assunti dalla densità dipendono dalle densità dei fattori Primi di cui il numero è formato, secondo relazioni che inizialmente sono state desunte empiricamente, e che riportiamo di seguito:

<u>Multipli di due Primi</u>
Dato un $N=P_1*P_2$, *d* assume i valori:
- d_{P1} per i dividendi multipli di P_2;
- d_{P2} per i dividendi multipli di P_1;
- mcm (minimo comune multiplo) delle due densità in tutti gli altri casi.

In generale un numero Composto, al variare del dividendo considerato, esprimerà sia le *d* dei Primi che lo compongono che una *d* che è il loro minimo comune multiplo. Questa *densità mcm* si manifesta per tutti i dividendi che non sono multipli dei Primi di cui è formato il Composto, e quindi anche per il dividendo n=1. Abbiamo chiamato ***densità fondamentale*** la *d* espressa per *n*=1, poiché è il valore di densità che contiene più informazioni (o è l'unica *d* o è la *d mcm*). Se non diversamente specificato, per *densità* intenderemo sempre la *densità fondamentale*.

Quindi per la densità fondamentale di un numero N composto dal prodotto di *i* Primi assumiamo la relazione:

(2) $d_N = \text{m.c.m.}\ (d_{P1}, d_{P2}, \ldots d_{Pi})$

Ad esempio, la densità fondamentale di 21 è 6, perché 1/21 = 0,047619047619… (periodo di 6 cifre). 21 è il prodotto dei primi 3 e 7, di densità rispettivamente 1 e 6. Applicando la (2) si ottiene correttamente il valore 6 per la densità di 21 (1*6). Consideriamo un altro esempio: 5863=11*13*41, fattori Primi di densità 2, 6 e 5 rispettivamente. Secondo la (2) possiamo prevedere che la densità fondamentale di 5291 sia il mcm di 2, 6 e 5, cioè 30. Infatti 1/5863 produce un quoziente con periodo di 30 cifre.

Potenze di un Primo

Una potenza di un numero Primo, così come tutti i numeri Composti, presenta vari valori di densità al variare del dividendo. In particolare si è *osservato* che dato un $N=P^n$ con $P\geq 7$ si ha:

(3) $d=P^{n-i} * d_P$

dove *i* assume tutti i valori compresi tra 1 e n secondo il seguente schema:

dividendo	*i*
P o suoi multipli	2
P^2 o suoi multipli	3
P^3 o suoi multpli	4
…	…
P^{n-1}	n
Tutti gli altri dividendi (compreso 1)	1

In sintesi, *i* è pari a 1 nella maggior parte dei casi, e assume valori diversi da 1 quando il dividendo considerato è un multiplo del Primo o di una sua potenza.

Notare che la relazione (3) vale anche per n=1, nel qual caso diventa una identità.

Notare anche che per la densità fondamentale, essendo per definizione il dividendo pari a 1, si ha i=1, e quindi la (3) diventa:

(3b) $d=P^{n-1} * d_P$

Riportiamo alcuni esempi per la regola osservata sulle potenze di Primi. Consideriamo $N=49=7^2$: secondo la (3b), la densità fondamentale di 49 sarà il prodotto del Primo base della potenza per la sua densità. Quindi $d_{49}=7*d_7=7*6=42$. Infatti il quoziente 1/49 ha 42 cifre decimali periodiche. Se invece di un quadrato consideriamo un cubo, per esempio $343=7^3$, applicando la (3b) avremo: $d_{343}=7^2*d_7=49*6=294$, confermato dal fatto che effettivamente il quoziente 1/343 ha 294 cifre decimali periodiche.

Eccezioni: arbitrarietà della densità

La relazione (3) sembra non valere per P=3. Probabilmente questo si può spiegare con il fatto che quando il quoziente della divisione 1/N è dato dalla ripetizione di una sola cifra, l'attribuzione della densità diventa un fatto arbitrario. Siamo portati a dire immediatamente che la densità in questi casi sia 1, ma in realtà potrebbe essere un valore qualsiasi, visto che una sequenza infinita di ripetizioni della medesima cifra può essere letta in modi alternativi altrettanto infiniti. Prendiamo ad esempio il quoziente 1/3:

1/3=0,333333333333333333333333…..

Che può essere letto come un'infinita ripetizione della cifra 3 o del gruppo 33 o 333 e così via.
Lo stesso vale per 1/9:

1/9=0,111111111111111111111111…..

La relazione (3), osservata per $P\geq 7$, può essere valida formalmente anche per P=3 se consideriamo altri modi di raggruppare le cifre del periodo dei quozienti 1/N quando N è una potenza di 3. Infatti applicando la (3) alle potenze di 3 si avrebbe:

n	$N=3^n$	$d=3^{n-1*}d_3$ (con $d_3=1$)	*d* reale "minima"
1	3	1	1
2	9	3	1
3	27	9	3
4	81	27	9

1/9=0,11111111…..., che può essere arbitrariamente letto come 0,111 (d=3). Quindi la (2) resta valida anche per P=3 solo se ammettiamo di poter considerare per le potenze di 3 le densità arbitrarie multiple di quella "minima". In realtà queste ed altre anomalie del Primo 3 lascerebbero pensare che la densità unitaria gli conferisca una serie di proprietà

speciali. Potrebbe essere interessante approfondire la questione per valutare se il 3 non possa essere una sorta di zero in questo nuovo sistema algebrico.

Relazione generale

E' stato osservato anche che le relazioni (2) e (3) si combinano in modo da consentirci di calcolare la *d* di qualsiasi tipo di N Composto. Infatti per il caso più generale $N= P_1^a * P_2^b * P_3^c$….. possiamo scrivere la relazione:

(4) d_N=m.c.m.($P_1^{a-1} * d_{P1}$, $P_2^{b-1} * d_{P2}$, $P_3^{c-1} * d_{P3}$…)

Cioè vale sempre la (2): la densità è comunque il mcm delle densità dei singoli fattori, e laddove questi fattori siano potenze di Primi si applica la (3b) (ricordiamo che parliamo sempre di densità fondamentale) per il calcolo delle loro *d*. Anche qui sarà più chiaro con un esempio. Consideriamo il caso di N=77077=7*7*11*11*13. Abbiamo tre fattori Primi, di cui due sono elevati al quadrato. Per calcolare la densità fondamentale di 77077 basterà calcolare le densità relative a ogni fattore già elevato al suo esponente, e poi farne il mcm. I fattori da considerare sono quindi 7^2, 11^2 e 13. Con la (3b) calcoliamo le densità dei due quadrati: d_{7^2}=7*6=42, d_{11^2}=11*2=22. La densità di 13 è 6. Il mcm di 42, 22 e 6 è 462, che infatti è la lunghezza del periodo del quoziente 1/77077.
E' importante sottolineare ancora una volta che per il calcolo del mcm le densità da considerare non sono quindi quelle dei singoli fattori Primi, ma dei Primi elevati alla loro potenza. Cioè, se un Primo appare più di una volta nella scomposizione di un dato N, devo prima calcolare la *d* delle potenze e solo dopo fare il mcm tra tutte le *d* trovate.
Nell'esempio precedente, 77077=7*7*11*11*13, se attribuissi le densità ai singoli fattori Primi avrei 6, 6, 2, 2 e ancora 6, facendo il mcm di queste *d* arriverei a un risultato scorretto. La procedura corretta è 1) Calcolare la *d* delle singole potenze, 2) Calcolarne il mcm.

Teoria della densità

Le relazioni fin qui esposte sono state osservate, e rappresentano l'assunto di partenza della nostra "teoria della densità". La teoria può essere riassunta in questo enunciato: definita la densità *d* di N come il numero di cifre del quoziente periodico *n*/N, ogni N Primo genera un UNICO valore di *d*, cioè una *d* costante al variare del dividendo *n*; mentre ogni N Composto genera valori di *d* che possono cambiare al variare di *n*. La densità fondamentale di un Composto riassume in sé tutti i valori che la *d* può assumere perché è sempre il mcm delle densità dei fattori che formano il numero Composto, intendendo per fattori i Primi elevati alle loro potenze.
Di seguito elenchiamo alcune definizioni e proprietà che rappresentano il *corpus* della Teoria della densità. Molte delle proprietà che qui verranno solo enunciate troveranno spiegazione e dimostrazione nei capitoli successivi.

I Primi come Generatori di densità

Negli esempi presentati per chiarire meglio le regole della *Teoria della densità*, abbiamo citato i valori di densità di alcuni Primi. Possiamo definire *Generatore* (simbolo G) di densità *d* un numero Primo di densità *d*.
Dato un Generatore, si definisce Grado di quel Generatore la sua densità. Ad es: ^{3}G indica un Generatore di densità 3, cioè un numero Primo che, quando usato come divisore, genera sempre quozienti con periodo di 3 cifre.
Si può dimostrare (vedi avanti) che ogni valore di *d* definisce un insieme di Generatori, e che questo insieme è FINITO.
Per comodità elenchiamo nella tabella 1 i generatori delle prime 32 densità.

Tab. 1: Generatori per *d* da 1 a 32

d	**G**
1	3
2	11
3	37
4	101
5	41, 271
6	7, 13
7	239, 4649
8	73, 137
9	333667
10	9091
11	21649, 513239
12	9901

13	53, 79, 265371653
14	909091
15	31, 2906161
16	17, 5882353
17	2071723, 5363222357
18	19, 52579
19	1111111111111111111
20	3541, 27961
21	43, 1933, 10838689
22	23, 4093, 8779
23	11111111111111111111111
24	99990001
25	21401, 25601, 182521213001
26	859, 1058313049
27	757, 440334654777631
28	29, 281, 121499449
29	3191, 16763, 43037, 62003, 77843839397
30	211, 241, 2161
31	2791, 6943319, 57336415063790604359
32	353, 449, 641, 1409, 69857

Composti "Incestuosi"

Poiché la densità di un Composto è sempre il mcm delle *d* dei Primi che lo compongono, si ha il caso particolare dei Composti formati da Primi della medesima densità, che avranno necessariamente anch'essi quel valore di densità, e che soprattutto avranno una proprietà identica ai Primi: l'unicità della *d*. Infatti, essendo formati da Primi della stessa densità, questa *d* sarà l'unico valore espresso al variare del dividendo *n*. Abbiamo definito ***Incesti*** questi Composti originati dalla moltiplicazioni di Primi della stessa famiglia.

Quindi definiamo *Incesto* il prodotto di due o più Generatori della stessa *d*.

Essendo l'insieme dei G di una data *d* un insieme finito, possiamo definire l'Incesto Totale di densità *d* come il prodotto di tutti i G di quella densità. D'ora in avanti indicheremo l'Incesto Totale della densità *d* con il simbolo $[{}^{d}G]$, cioè

$[{}^{d}G] = {}^{d}G_1 * {}^{d}G_2 * {}^{d}G_3 * {}^{d}G_4 \ldots$. Ad esempio, l'Incesto Totale per d=6 sarà:

$[{}^{6}G] = {}^{6}G_1 * {}^{6}G_2 = 7 * 13 = 91$

Il Periodo e alcune sue proprietà

Il *Periodo* di un N dispari è definito come il Periodo del quoziente n/N, dove n è un numero Naturale non multiplo di N. Il numero di cifre che costituiscono il Periodo è la già definita densità di N. Si osserva che, per ogni valore di n, N e il suo Periodo hanno la stessa densità.

Abbiamo già visto che se N è Primo, *d* è costante, cioè i Periodi ottenuti per tutti i valori di *n* (diversi da N e dai suoi multipli, condizione necessaria per avere un quoziente periodico) hanno il medesimo numero di cifre. Viceversa se N è Composto, in genere *d* assume valori diversi al variare di n, secondo le regole già enunciate.

Una proprietà osservata dei periodi di N Primi è che essi sono SEMPRE divisibili per 9 (ricordare che N è per definizione un numero dispari ≥7. Comunque per N=3 questa regola è rispettata in una maniera particolare: 1/3=0,333333333….. Se si considera il periodo formato da un numero di cifre pari a 3 o a un suo multiplo, si vede che questi periodi "arbitrari" sono divisibili per 9). Questa proprietà si può dimostrare. Infatti, se il quoziente 1/N è un numero decimale con periodo *p*, mentre moltiplicando questo numero decimale periodico per N ottengo ovviamente l'unità, dalla moltiplicazione p*N ottengo un numero formato da tante cifre 9 quanto è la lunghezza del periodo. Ad esempio, 1/7=0,142857142857142857……, ma se faccio 142857*7 ottengo 999999. Questa è una regola che ci insegnano alle elementari, e che è alla base del calcolo della frazione generatrice a partire da un numero decimale periodico dato. La regola deriva dal fatto che il periodo preso come singola ripetizione è un'approssimazione del reale quoziente fatto da infinite cifre, e pertanto quello che otteniamo anziché l'unità è una sua approssimazione: cioè, mentre 0,142857142857142857…. *7=1, se uso l'approssimazione non periodica ho 0,142857*7=0,999999, e quindi 142857*7=999999.

Fin qui quello che era già noto sui periodi. Quello che possiamo aggiungere noi è che, se vale sempre questa regola e quindi p*N dà sempre un numero fatto da sole cifre 9, poiché un numero così fatto deve essere divisibile per 9, se N è Primo la divisibilità per 9 deve necessariamente essere a carico dell'altro fattore del prodotto, cioè p. **Ne consegue che i periodi degli N Primi sono sempre divisibili per 9**.

E' chiaro che non si tratta di una corrispondenza biunivoca: la divisibilità del periodo per 9 è una condizione soddisfatta da tutti i Primi, ma non solo da loro. Però può essere già un primo elemento di selezione quando vogliamo sapere se un dato N è Primo o Composto.

Ciclo

Il Periodo di N è, come è a tutti noto, la parte del quoziente della divisione n/N che si ripete ciclicamente all'infinito. Se però consideriamo come varia il Periodo di un N al variare di n, osserviamo che per ogni N si possono osservare uno o più periodi ma che ognuno di essi compare in varie forme "correnti": cioè la stessa sequenza ricompare iniziando in punti diversi. Ad esempio, nella Tabella 2 sono riportati i periodi di N=7.

Tab. 2: Periodi di N=7

n	Periodo	Ciclo
1	142857	142857
2	285714	142857
3	428571	142857
4	571428	142857
5	714285	142857
6	857142	142857

(Notare che per n=7 non c'è ovviamente un Periodo – e infatti nella definizione di Periodo abbiamo inserito la condizione $n \neq N$. Inoltre per n=8, 9, 10 ecc.. i Periodi si ripetono identici – quello che cambia nel quoziente n/N è la cifra intera, che per $1 \leq n \leq 6$ è zero, per $8 \leq n \leq 13$ è 1 ecc. Quindi per esaminare tutti i periodi possibili di un dato N basta considerare i primi N-1 dividendi.)

La Tabella 2 mostra come i Periodi delle N-1 divisioni n/N per n che va da 1 a N-1 siano tutti diversi, ma in realtà possano essere formati dalla stessa sequenza 'fondamentale' che inizia da punti differenti.
Definiamo questa sequenza fondamentale ***Ciclo***. Il 7 presenta un unico Ciclo, che compare in 6 diverse *varianti correnti*. Ma un N può avere più Cicli. Si veda l'esempio seguente:

Tab. 3: Periodi di N=13

n	Periodo	Ciclo	
1	076923	076923	a
2	153846	153846	b
3	230769	076923	a
4	307692	076923	a
5	384615	153846	b
6	461538	153846	b
7	538461	153846	b
8	615384	153846	b
9	692307	076923	a
10	769230	076923	a
11	856153	153846	b
12	923076	076923	a

Quindi per N=7 abbiamo un solo Ciclo, che per comodità possiamo far coincidere col periodo della divisione 1/7, 142857. Per N=13 abbiamo due Cicli: 076923 e 153846, che corrispondono rispettivamente alle divisioni 1/13 e 2/13.

Alcune curiosità sui Cicli

I Cicli presentano alcune proprietà che potrebbero essere semplici curiosità o che invece potrebbero dirci qualcosa sulla natura della loro composizione. Ad esempio, che cosa determina la sequenza delle cifre di un Ciclo? Esiste una relazione tra i Cicli di uno stesso Primo? E tra i Cicli di Primi della stessa densità?
Col Primo 7 abbiamo la situazione di "massimo ordine": infatti c'è un unico Ciclo – cioè una sola sequenza possibile - e i 6 resti (7-1) si distribuiscono TUTTI in quest'unica sequenza, producendo di conseguenza UN SOLO CICLO (in tutte le sue varianti correnti) per qualsiasi dividendo considerato. Questo deve accadere tutte le volte che d=N-1, ma il 7 è il caso più semplice e anche l'unico caso di d=N-1 con d<9, e quindi l'unico caso in cui il Ciclo non ha mai due volte la stessa cifra. Invece nel Ciclo del 7, ovvero la sequenza 142857, possiamo vedere con la massima chiarezza come i 6 resti si organizzino in una sequenza unica. In altre parole c'è un solo modo per saltare da un resto all'altro quando si divide un numero Naturale per 7. La sequenza potrà cominciare in punti diversi, ma i sei resti saranno comunque agganciati in quell'ordine.
In realtà questo non deve sorprendere più di tanto, visto che quando facciamo una divisione, ogni resto vincola necessariamente anche il resto successivo. Il caso del 7 è davvero esemplare perché è quello più semplice: tutti i resti partecipano all'unica sequenza possibile, e ogni divisione per 7 si comporterà nello stesso modo: ad esempio in 1/7 la sequenza di resti sarà 3-2-6-4-5-1. In 2/7 la sequenza sarà la medesima, ma inizierà dal 6. Cambiando il dividendo (non multiplo di 7) potremo solo cambiare il punto di inizio, ma i sei resti saranno comunque percorsi secondo quella sequenza (Fig. 1).

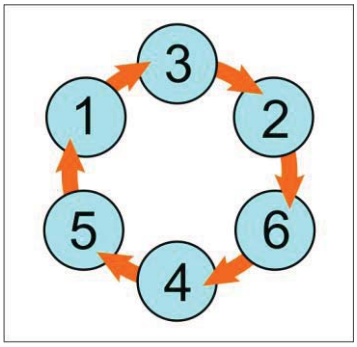

Figura 1: Sequenza di resti del Ciclo del 7

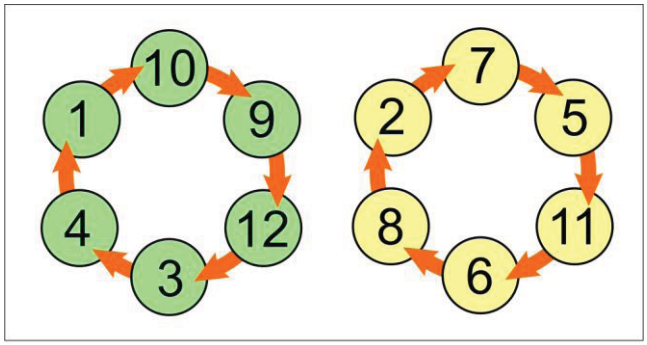

Figura 2: Sequenze di resti dei due Cicli del 13

Qualche curiosità sul Ciclo del 7: nella sequenza 142857 sommando tra loro il numero formato da prima e seconda cifra (14) con quello formato da terza e quarta cifra (28) si ottiene il numero formato da seconda e terza (42). La stessa cosa accade se sommiamo $3^a4^a + 5^a6^a$: otteniamo 4^a5^a (28+57=85). E si ha anche $5^a6^a + 1^a2^a = 6^a1^a$ (14+57=71). Non sembra solo un gioco, sembra più che altro la manifestazione del modo in cui le cifre della sequenza sono vincolate tra loro nel gioco resti-quozienti.

Per l'altro Primo di *d*=6, il 13, la situazione è già leggermente più complessa: i Cicli sono 2 e i 12 resti si suddividono in due gruppi distinti, con alcuni dividendi che creano periodi del primo tipo (varianti correnti del Ciclo 076923) e altri che creano periodi del secondo tipo (varianti correnti del Ciclo 153846). Passando ad esaminare i resti, abbiamo che i 12 resti risultano separati in due gruppi di 6, e ogni dividendo afferirà a uno dei due gruppi di resti, senza possibilità di saltare tra un gruppo e l'altro durante la divisione. Ad esempio in 1/13 la sequenza di resti sarà 10-9-12-3-4-1, mentre in 2/13 sarà 7-5-11-6-8-2. Qualsiasi altra divisione per 13 (con dividendo non multiplo di 13 ovviamente) si "aggancerà" a una di queste due sequenze, che non si mescolano mai (Fig. 2).
Anche i due Cicli del 13 presentano quella curiosa proprietà vista per il Ciclo del 7 sulla somma dei numeri formati dalle coppie di cifre vicine: 07+69=76, 69+23=92, 23+07=30; 15+38=53, 38+46=84, 46+15=61.
Ci sono inoltre anche curiose relazioni tra i tre Cicli di densità 6 se li consideriamo tutti insieme. Chiamiamo ***A*** il Ciclo del 7 142857, ***B*** il primo Ciclo del 13 076923 e ***C*** il secondo Ciclo del 13 153846. Se sommiamo ***A***+***C*** otteniamo 296703, che non è altro che il contrario di ***B***. Se sommiamo ***A*** al contrario di ***B*** otteniamo il contrario di ***A***. Queste relazioni potrebbero essere solo curiosità ma in qualche modo devo anche essere una manifestazione delle leggi che determinano la sequenza dei resti nelle divisioni, leggi che si vedono nella loro essenza quando i divisori sono Primi.

Varietà
Dato un N Primo, si definisce *varietà* ***v*** il suo numero di Cicli.
Si dimostra (vedi paragrafo successivo) che N-1=*d* * *v*.

Tab. 4: densità e varietà di alcuni Primi

P	***d***	***v***
7	6	1
11	2	5
13	6	2
17	16	1
19	18	1
23	22	1
29	28	1
31	15	2
37	3	12
41	5	8

Significato di densità e varietà: la struttura dei Primi e dei Composti

Abbiamo definito la densità di un numero dispari N come il numero di cifre decimali che costituiscono il periodo del quoziente 1/N. Quando facciamo una divisione con quoziente decimale periodico non facciamo altro che ripetere una sequenza di divisioni "elementari", ognuna delle quali ci dà una cifra decimale (tra 0 e 9) e un resto. Questo resto moltiplicato per 10 diventa il nuovo dividendo, dal quale otteniamo la successiva cifra decimale e il successivo resto.

Un quoziente periodico significa pertanto una serie di divisioni elementari alla fine della quale si ottiene un resto uguale al dividendo originale. La densità è allora il numero di divisioni elementari che portano a chiudere un Ciclo. Se consideriamo la 'tabellina' del divisore originale N - cioè la sequenza N, 2N, 3N, 4N, 5N, 6N, 7N, 8N, 9N – quando operiamo una divisione del tipo n/N non facciamo altro che saltare lungo questa tabellina ottenendo ogni volta una cifra (quoziente elementare) e un resto. I resti possibili sono ovviamente 1, 2, 3…. ecc fino a N-1, quindi N-1 casi possibili. Un quoziente periodico non è altro che un percorso di quozienti elementari e di resti. Un *Ciclo* è quindi una catena di quozienti elementari, la *densità* è la lunghezza della catena e la *varietà* è il numero di catene possibili. E' ovvio a questo punto che con N-1 resti posso avere (N-1)/*d* catene di lunghezza *d*. Abbiamo chiamato *varietà v* questa grandezza.
Quando N è Primo, le catene possibili di resti e quozienti sono tutte della stessa lunghezza e in numero pari a *v*, tale che:

(5) $N-1=d * v$

Questa relazione, già enunciata prima, ora appare più chiara: quando N è Primo, gli N-1 resti possibili formano *v* catene di lunghezza *d*. E' come dire che ci sono *v* modi ben definiti e fissi di saltare lungo la tabellina di N quando si fa una divisione n/N, e che ogni dividendo n si 'aggancia' a una di queste catene. Ogni catena corrisponde a un Ciclo e corrisponde a un insieme di valori di *n*. Il Ciclo individua quindi un insieme di dividendi *n* che 'afferiscono' alla stessa catena e possono differenziarsi solo per il punto in cui iniziano a percorrerla.
Quindi potremmo dire che quella dei divisori Primi è la regola, mentre i divisori Composti creano una più rumorosa eccezione. Infatti se N non è Primo, essendo un multiplo di altri Primi, nella divisione *n*/N le cose si complicheranno molto: compariranno catene che afferiscono ai Primi di cui è formato N, e quindi potranno esserci varie densità e un numero di Cicli che non soddisfa la relazione $N-1=d * v$. In realtà vedremo che quello che appare complicato e caotico a una prima osservazione non è altro che il risultato della combinazione della regola fondamentale $N-1=d * v$ applicata ai fattori Primi che formano il numero Composto.
Infatti se consideriamo un $N=P_1*P_2$, data la (5) possiamo scrivere:

$P_1-1=d_1v_1$
$P_2-1=d_2v_2$

$P_1=d_1v_1+1$
$P_2=d_2v_2+1$

$P_1P_2=(d_1v_1+1)(d_2v_2+1)= d_1v_1d_2v_2+ d_1v_1+ d_2v_2+1$

(6) $P_1P_2-1= d_1v_1+d_2v_2+d_1d_2v_1v_2$

Questo vuol dire che dato un N formato dal prodotto di due Primi, possiamo conoscere a priori che gli N-1 resti si distribuiscono in tre gruppi, rappresentati dai tre termini della somma a destra dell'uguaglianza (6).

Facciamo l'esempio del multiplo 21. Nella tabella sono riepilogati i Cicli ottenuti al variare di *n* tra 1 e 20:

Tab. 5: Periodi per N=21

n	**Periodo**	**Ciclo**	
1	047619	047619	a
2	095238	095238	b
3	142857	142857	c
4	190476	047619	a
5	238095	095238	b
6	285714	142857	c
7	3	3	α
8	380952	095238	b
9	428571	142857	c
10	476190	047619	a
11	523809	095238	b
12	571428	142857	c
13	619047	047619	a
14	6	6	β
15	714285	142857	c
16	761904	047619	a
17	809523	095238	b
18	857142	142857	c
19	904761	047619	a

20	952380	095238	b

La *d* è mista, essendo 6 per tutti gli *n* tranne che per *n*=7 e *n*=14, in cui abbiamo *d*=1. La varietà *v* è pure mista, perché è 3 per i Cicli di lunghezza 6, mentre è 2 per i Cicli di lunghezza 1.
Quindi le densità dei due Primi 7 e 3, che compongono il 21, si combinano per dare 18 catene di resti a lunghezza 6, suddivise in 3 diverse varietà, e 2 catene fatte da un solo resto. Il totale dei periodi possibili è sempre N-1 (20 in questo caso), ed N-1 sono pure i resti possibili nelle divisioni elementari, ma si tratta della somma di due gruppi distinti: un gruppo di 3 Cicli a lunghezza 6 (3*6=18), e un gruppo separato di 2 Cicli di lunghezza 1 (2*1=2). Quindi il totale dei resti è dato dalla somma di più addendi.
La relazione (6) prevede correttamente questo risultato. Infatti per N=21 si ha P_1=7, d_1=6, v_1=1, P_2=3, d_2=1, v_2=2.
Sostituendo nella (6) abbiamo:

21-1=6*1+1*2+6*1*1*2

Nel caso di N=21, una delle due densità è unitaria, e questo nella pratica riduce i gruppi di resti da 3 a 2: infatti empiricamente avevamo trovato 18 Cicli di lunghezza 6 e 2 Cicli di lunghezza 1.
Se consideriamo invece l'esempio di N=407=37*11, con P_1=37, d_1=3, v_1=12, P_2=11, d_2=2, v_2=5, la (6) prevede:

407-1=3*12+2*5+3*2*12*5=3*12+2*5+6*60

E quindi avremo 12 Cicli di lunghezza 3, 2 Cicli di lunghezza 5 e 60 Cicli di lunghezza 6.

Nel caso precedente le due densità coinvolte non erano una multipla dell'altra, né avevano sottomultipli in comune, e quindi d_1d_2=mcm(d_1,d_2). Ma cosa succede se invece le densità coinvolte hanno dei sottomultipli in comune?
Consideriamo ad esempio N=259=7*37, con P_1=7, d_1=6, v_1=1, P_2=37, d_2=3, v_2=12. La (6) prevede:

259-1=6*1+3*12+6*3*1*12

Perché la *d* fondamentale osservata è il mcm di 6 e 3, cioè 6, e non il prodotto 6*3, cioè 18?
E' come se i resti delle divisioni elementari dovessero arrangiarsi in sequenze secondo un ordine imposto da quello che accade per i singoli Primi. Il mcm rappresenta allora letteralmente la minima lunghezza in grado di contenere tutte le catene di resti (e quindi di quozienti elementari) possibili. Il prodotto della lunghezza delle due catene è invece una struttura in qualche modo ridondante, che comunque contiene sempre il mcm.
Potremmo azzardare che i Cicli della teorica densità prodotto 6*3 non si formino realmente con una sequenza di 18 quozienti, ma come "supercicli" formati dalla ripetizione di 3 Cicli di lunghezza 6. In altre parole, quando le *d* dei Primi che formano il Composto sono una multipla dell'altra, le sequenze di quozienti elementari formerebbero comunque al massimo Cicli della *d* mcm, coincidendo i Cicli di lunghezza d_1*d_2 con dei supercicli. Quando viceversa (come nell'esempio di N=407) le densità coinvolte non hanno multipli in comune, il prodotto è anche il mcm.
In accordo con questa ipotesi, per i casi in cui d_1*$d_2 \neq$ mcm(d_1,d_2), la reale varietà dei Cicli di densità mcm non sarà v_1v_2, ma sarà maggiorata di quella quota del prodotto d_1*d_2 che non è compresa nel mcm. Tornando all'esempio di N=259 pertanto, essendo la *d* mcm pari a 6, il contributo del primo termine della somma a destra dell'uguaglianza nella relazione (6) va letto come 36 Cicli di lunghezza 6 e non come 12 Cicli di densità 18. Quindi la varietà apparente viene aumentata quando il prodotto delle *d* è "eccedente" rispetto al mcm. Quello che si osserva è coerente con questa lettura della (6): 259 produce un totale di 37 Cicli di lunghezza 6 e 12 Cicli di lunghezza 3.
La relazione (6), derivata dalla (5) per N=P_1*P_2, corrisponde molto bene a quello che si osserva esaminando tutti i Cicli prodotti dalle divisioni n/N. Infatti quando esaminiamo i periodi dei quozienti delle divisioni n/N, dove n è un numero Naturale che varia da 1 a N-1, troviamo che la densità assume i seguenti valori:

- d_2 quando n è multiplo di P_1 (infatti se n=aP_1, n/(P_1*P_2)=aP_1/(P_1*P_2)=a/P_2, e quindi ha d=d_2)
- d_1 quando n è multiplo di P_2 (il caso speculare)
- *d* mcm in tutti gli altri casi.

Se si contano i Cicli di ognuno di questi tre gruppi, si trova che anche le varietà sono determinate da P_1 e P_2: infatti il primo gruppo conterrà v_2 Cicli, il secondo v_1 Cicli, e il terzo un numero di Cicli che dipende dal prodotto v_1v_2.

Come esempio consideriamo ancora N=259. La (6) ci dice che gli N-1 quozienti delle divisioni n/N si distribuiscono in tre gruppi secondo la somma:

259-1=6*1+3*12+6*3*1*12

Se si sviluppano le 258 divisioni si trovano proprio tre gruppi:

- 6 volte il medesimo Ciclo di lunghezza 6, in corrispondenza dei 6 multipli di 37 presenti nell'intervallo 1-258
- 12 Cicli di lunghezza 3, che compaiono ciascuno più volte per dare un totale di 36 periodi di lunghezza 3, tutti in corrispondenza dei 36 multipli di 7 presenti nell'intervallo 1-258
- i restanti 216 quozienti hanno periodi di lunghezza 6 (il mcm) e tra loro si riconoscono solo 36 Cicli, che compaiono ognuno più volte

Quindi il Primo 7 contribuisce direttamente con la sua densità – 6 – e la sua varietà – 1- a determinare i quozienti delle divisioni n/N per i 6 multipli del Primo 37 (anche la composizione del Ciclo è quella del 7, cioè 142857); analogamente il Primo 37 contribuisce direttamente con la sua densità – 3 – e con la sua varietà – 12 – a determinare i 36 quozienti in corrispondenza dei 36 multipli di 7. Gli altri quozienti sono determinati insieme dai Primi 7 e 37, con una combinazione delle loro densità e varietà.
Questi tre gruppi corrispondono esattamente ai tre termini della somma (6), da cui appare anche chiaro come la varietà apparente del terzo gruppo sarà data dal prodotto v_1v_2 moltiplicato per la parte del prodotto d_1d_2 che "eccede" il mcm di d_1 e d_2.

La relazione (6) ha un'importanza formale a nostro avviso molto rilevante: mentre i numeri Primi possono sempre essere scritti con la relazione N-1=*dv*, i numeri Composti manifestano la loro non primalità con una relazione anch'essa "composta", nella quale compaiono diversi addendi.
Un aspetto invece molto pratico della questione è che se per i numeri Primi vale sempre la relazione N-1=*dv*, allora quando N è Primo deve esistere un intero *v* tale che *v*=N-1/*d*, cioè N-1 deve essere divisibile per *d*. Quindi se ho un N e ne calcolo la *d* fondamentale, posso fare subito il test di divisibilità di N-1 per *d*.
Purtroppo questo test consente di stabilire con certezza solo la non primalità. Infatti tutti i Primi seguono la (5), ma non SOLO i Primi. Esiste il caso particolare degli Incesti, cioè dei Composti formati dal prodotto di Primi di medesima densità. In questo caso infatti la relazione generale (6) valida per tutti i Composti acquisisce la forma semplificata che ha per i Primi, essendo *d* uguale per tutti i P coinvolti. Infatti per $d_1 = d_2 = d$ si ha:

(6) $N-1 = P_1P_2-1= d_1v_1+ d_2v_2 + d_1d_2v_1v_2$

$N-1 = d(v_1+ v_2) + ddv_1v_2 = d(v_1+ v_2 + dv_1v_2)$

Che può essere scritta come

$N-1= dv$

Dove *d* sarà la densità dell'Incesto (uguale a quella di tutti i P che lo compongono) e *v* la varietà apparente. Vale a dire che anche per gli Incesti, come per i Primi, esiste una relazione lineare tra N-1 e la *d* di N.
Abbiamo esaminato diversi casi di Incesti semplici (91=7*13 ad esempio) e la relazione è sempre verificata. Inoltre, non solo esiste una relazione lineare tra N-1 e *d*, ma il coefficiente *v* corrisponde anche al numero totale di Cicli, e quindi rappresenta la reale varietà dell'N dato.
Possiamo dunque suddividere l'insieme dei Numeri Naturali in due grandi insiemi: l'insieme dei **Numeri Omogenei**, formato dai Primi e dagli Incesti, accomunati dall'espressione di un valore unico di densità, e per i quali vale la relazione (5) N-1=*dv*; e l'insieme dei **Numeri Eterogenei**, che viceversa esprimono più valori di densità e per i quali valgono relazioni non lineari tra N-1 e queste densità, e cioè N-1 è uguale sempre alla somma di più termini. I Numeri Eterogenei sono tutti i Composti che non sono Incesti.

Abbiamo pertanto individuato una relazione di linearità estremamente semplice che vale per TUTTI i Primi e per gli Incesti, che rappresentano una forma molto particolare di Composti, in fondo non così frequente. Infatti un Incesto deve contenere solo Primi della stessa *d*, e inoltre ognuno di questi Primi deve essere presente una sola volta. Non ci devono essere cioè potenze di un Primo: abbiamo visto infatti che quando un Primo è elevato a potenza, la densità assume dei valori maggiori della *d* del Primo, secondo regole osservate ma di cui non abbiamo ancora prodotto una dimostrazione.
Comunque l'unica cosa che fin qui possiamo dire applicando la relazione N-1=*dv* è che se un dato N di densità *d* non la soddisfa (cioè se non esiste un *v* intero tale che la relazione sia soddisfatta, che equivale a dire che N-1 non è divisibile per *d*), allora quell'N sicuramente NON E' Primo.
Abbiamo quindi individuato un criterio estremamente semplice per escludere la primalità di un N dato.
Riepilogando si può procedere così:

1) calcolo della densità di N
2) verifica della divisibilità di N-1 per la *d* trovata

Questo importantissimo filtro per arrivare alla diagnosi di primalità è anche il passaggio chiave per un nuovo algoritmo capace di trovare tutti i Primi di ogni *d*, in un modo che, come vedremo, eliminerà anche il problema degli Incesti. Questo sarà l'argomento del prossimo capitolo. Ma prima riassumiamo alcuni criteri di non primalità che fin qui sono emersi.

Criteri di non primalità

Primo Criterio: divisibilità del Periodo per 9

Abbiamo visto in precedenza che dato un N dispari non multiplo di 5, dalla divisione 1/N si ottiene sempre un quoziente periodico, e una nota regola ci dice che moltiplicando quel periodo per N si ottiene sempre una sequenza di tante volte la cifra 9 quante sono le cifre del periodo. In altri termini, dato un N di densità *d*, si ha sempre che il prodotto N*Periodo=$^{d}(9)$. Un numero del tipo $^{d}(9)$ è necessariamente divisibile per 9. Ne consegue che, se N è Primo, la divisibilità per 9 deve essere a carico del Periodo. Quindi i Periodi dei numeri Primi sono sempre divisibili per 9.
Questo può essere quindi un criterio per filtrare l'accesso ai test di primalità: se l'N dato genera un periodo non divisibile per 9, quell'N non può essere Primo.

Secondo Criterio: divisibilità di N-1 per *d*

Abbiamo dimostrato che dato un N di densità *d*, se N-1 non è divisibile per *d*, sicuramente N non è Primo.
Questo ci consente di applicare un filtro preliminare a tutti i test di primalità. Infatti potremo portare avanti test di primalità solo per quei candidati che soddisfano questo Primo Criterio.

Terzo Criterio: divisibilità di N per numeri di struttura $dv+1$

Se ad esempio vogliamo usare il classico test di primalità che consiste nel provare a dividere l'N dato per tutti i Primi noti fino alla radice quadrata di N, possiamo ottenere un notevole risparmio intanto applicando i primi due criteri come filtri preliminari. Poi possiamo ottenere un notevole risparmio nel numero delle divisioni se dividiamo solo per i Primi che possono essere scritti come $dv+1$, dove *d* è la densità del nostro N e *v* è un intero qualsiasi. Infatti poiché un numero di una data *d* o è Primo o è il prodotto di Primi con densità tali che il loro mcm sia *d*, allora se un dato N ha densità *d* e non è Primo, potrebbe esistere un Primo di densità *d* che divida quell'N. Un Primo di densità d può sempre essere scritto come $dv+1$, e quindi se un dato N non è Primo, deve esistere un N'=$dv+1$ tale che N divisibile per N'.
Quindi, se stiamo usando il metodo tradizionale di provare a dividere l'N dato per tutti i Primi tra 7 e $\sqrt{N}$, possiamo risparmiare molte divisione selezionando solo i Primi che possono essere scritti come dv+1.
Molto spesso si arriva velocemente a escludere la primalità con questo filtro, facendo molte meno divisioni del metodo standard. Ad esempio, consideriamo N=4187. Troviamo che ha densità 13, che tra l'altro è un numero Primo. Quindi se 4187 non è Primo, deve necessariamente avere un Primo di densità 13 tra i suoi divisori. Nella sequenza dei Primi noti, il 53 è il primo che soddisfa la relazione N=13**v* +1, cioè potrebbe essere un Primo di densità 13 (non ci interessa neanche accertarlo). Allora proviamo direttamente questa divisione saltando tutti i Primi precedenti: 4187/53=79, quindi con una sola divisione ho potuto escludere la primalità di 4187. Al limite potrei anche non conoscere i Primi da provare come divisori, ma semplicemente provare a dividere l'N dato per i vari candidati $dv+1$ non pari: farei comunque meno divisioni rispetto al metodo tradizionale, e in più non avrei bisogno di conoscere tutti i Primi compresi tra 3 e $\sqrt{4187}$.

Bisogna notare che mentre i primi due criteri sono soddisfatti da tutti i Numeri Omogenei (Primi e Incesti), il terzo, essendo comunque un test di divisibilità, non risente della presenza degli Incesti, perché col terzo criterio possiamo comunque trovare un divisore di un N Incesto. Infatti se $N=P_1*P_2$, dove P_1 e P_2 sono Primi della medesima densità *d*, deve per forza esistere un N'<N tale che N'=$dv+1$: infatti sia P_1 che P_2 sono divisori di N ed entrambi possono essere scritti rispettivamente come dv_1+1 e dv_2+1.

Riportiamo alcuni esempi di velocizzazione del metodo tradizionale con l'applicazione di questi tre criteri.

N=36243

- La densità calcolata è 2013
- Primo Criterio: un Periodo di 2013 cifre evidenzia quanto questo primo criterio sia in realtà di utilità pratica molto limitata. Proviamo a usare il secondo criterio.
- Secondo Criterio: 36243-1 non risulta divisibile per 2013, allora sicuramente 36243 non è Primo

N=2629

- La densità calcolata è 14
- Primo Criterio: il Periodo 00038037276531 risulta divisibile per 9, e quindi non ci consente di escludere la primalità.

- Secondo Criterio: 2629-1 non risulta divisibile per 14, e quindi possiamo escludere la primalità.

N=12345679

- La densità calcolata è 9
- Primo Criterio: il Periodo di 1/12345679 è 000000081, divisibile per 9. Non possiamo escludere la primalità.
- Secondo Criterio: 12345679-1 risulta divisibile per 9, non consentendo ancora di escludere la primalità.
- Terzo Criterio: dividiamo 12345679 per i candidati $9v+1$, con v pari (in modo che il candidato sia dispari). Il primo candidato è 9*2+1=19, che non risulta essere un divisore di N. Il secondo candidato è 9*4+1=37, e 12345679 risulta divisibile per 37. Abbiamo escluso la primalità con 2 divisioni.

Dagli esempi presentati appare chiaro che il Primo Criterio è in realtà spesso poco praticabile visto che diventa tanto più complesso quanto più lunghi sono i periodi. Inoltre basta che N non sia un multiplo di 9 perché viceversa lo sia il Periodo, e quindi è un criterio soddisfatto per moltissimi numeri non Primi (tutti i non multipli di 9).
Viceversa il Secondo Criterio è molto più selettivo, essendo soddisfatto solo da Primi e Incesti. Quindi si potrebbe usare il Secondo Criterio come filtro iniziale per escludere tutti i Numeri Eterogenei, e con il Terzo (il test di divisibilità per i candidati N=dv+1) determinare la primalità in maniera inequivocabile e con un minor numero di divisioni rispetto al metodo tradizionale.