L'insieme ϕ

pubblicazione web del 31-03-2016

Riprendiamo il discorso che precedentemente ci ha condotto al teorema di Eulero e approfondiamo l'analisi dell'insieme ϕ_q degli interi maggiori di zero, minori del numero dispari q e coprimi con q, allo scopo di dimostrare quel teorema che ho indicato con la sigla «V-V».
Per una migliore comprensione di quanto viene asserito qui, è opportuno che il lettore inizi dalle relazioni:
«Da Wilson a Fermat» e «Teorema di Eulero»
Ciò che si vuole dimostrare complessivamente è che c'è un unico filo conduttore tra i tre più famosi teoremi della «Teoria dei numeri» : teorema di Wilson ; piccolo teorema di Fermat ; teorema di Eulero - Fermat

Teorema V-V

Siano: q un qualsiasi intero dispari ; ϕ_q l'insieme dei numeri maggiori di zero, minori di q e coprimi con q ; $\phi(q)$ la quantità degli elementi di ϕ_q ; $\phi_q!$ il prodotto di tutti gli elementi di ϕ_q: $\phi_q! = 1 \cdot c_2 \cdot c_3 \cdot \ldots \cdot c_{\phi(q)}$

- Se q è composto da due o più fattori primi, oppure da potenze di due o più fattori primi,

$$\phi_q! \equiv 1 \pmod{q}$$

$$a^{\phi(q)/2} \equiv \phi_q! \equiv 1 \pmod{q} \;,\; a \in \phi_q$$

- Se q è primo, oppure la potenza di un solo primo:

$$\phi_q! \equiv -1 \pmod{q}$$

$$a^{\phi(q)/2} \equiv \phi_q! \equiv -1 \pmod{q} \;,\; a \in \phi_q \quad \text{non-residuo quadratico}$$

$$-a^{\phi(q)/2} \equiv \phi_q! \quad ; \quad a^{\phi(q)/2} \equiv 1 \pmod{q} \;,\; a \in \phi_q \quad \text{residuo quadratico}$$

* Dimostriamo che:
- se q è multiplo dispari, necessariamente deve essere valida la congruenza $\phi_q! \equiv 1 \pmod{q}$

A questo fine rivediamo la precedente relazione sul teorema di Eulero e riprendiamo la discussione al punto in cui ci si proponeva di calcolare il valore del prodotto di tutti gli elementi di ϕ_q.
Questa volta affronteremo la questione in modo più preciso e la risolveremo.

***

Quando la base è $a = 1$, l'insieme ϕ_q ha la struttura di gruppo abeliano rispetto alla moltiplicazione, per cui, se nessun degli elementi $c \in \phi_q$ dovesse avere sé stesso come simmetrico, il calcolo sarebbe immediato: $\phi_q! = c_1 \cdot c_2 \cdot c_3 \cdot \ldots \cdot c_{\phi(q)} \equiv 1 \pmod{q}$
Ma il calcolo di $\phi_q!$ lo possiamo eseguire in modo corretto solo dopo avere constatato se c'è qualche elemento $c \in \phi_q$ in coppia con sé stesso, cioè tale che $c \cdot c \equiv 1 \pmod{q}$.

Se supponiamo che questo elemento $c \in \phi_q$ esiste, avremo l'uguaglianza: $c^2 = t \cdot q + 1$, cioè: $(c-1)\cdot(c+1) = t \cdot q$
Quindi, per accertarci che tale supposizione sia reale, dobbiamo stabilire se c'è qualche elemento $c \in \phi_q$ con questi requisiti: il prodotto del suo precedente per il suo successivo deve essere multiplo di q.
Così come succede per i numeri primi, anche per gli altri numeri dispari, l'uguaglianza $(c-1)\cdot(c+1) = t \cdot q$ è sempre vera per $c=1$ e $c=q-1$. Questi due valori di c determinano rispettivamente le uguaglianze: $0 \cdot 2 = 0$; $(q-2)\cdot q = m \cdot q$.
Una osservazione di rilievo, importante per la comprensione dell'intera relazione, è che nell'uguaglianza $(c-1)\cdot(c+1)=t\cdot q$, quando $c=1$ e $c=q-1$, i fattori primi di q sono, rispettivamente, o tutti in $(c-1)$ o tutti in $(c+1)$.

Per questi due elementi, sempre presenti nell'insieme ϕ_q, qualunque sia q dispari, si ha:

$$1^2 \equiv 1 \pmod{q} \quad ; \quad (q-1)^2 \equiv 1 \pmod{q} \quad ; \quad 1 \cdot (q-1) \equiv -1 \pmod{q}$$

A motivo di quest'ultima congruenza, se in ϕ_q ci fossero soltanto questi due elementi in coppia con sé stessi, così come accade con tutti i numeri primi, il calcolo sarebbe: $\phi_q! \equiv -1 \pmod{q}$
Ma per trarre le giuste conclusioni dobbiamo andare alla ricerca di altri eventuali elementi di ϕ_q in coppia con sé stessi, tali da rendere valida l'uguaglianza $(c-1)\cdot(c+1) = t \cdot q$ anche per $c \neq 1$ e $c \neq (q-1)$.

A questo fine ci chiediamo se esiste:
- qualche elemento $c \in \phi_q$ $(c \neq 1)$ tale che $(c-1) \notin \phi_q$, cioè tale che $(c-1)$ abbia tra i suoi fattori primi qualche divisore di q.
- qualche elemento $c' \in \phi_q$ $(c' \neq q-1)$ tale che $(c'+1) \notin \phi_q$, cioè tale che $(c'+1)$ abbia tra i suoi fattori primi qualche divisore di q.

L'insieme ϕ_q non è un gruppo rispetto alla sottrazione e nemmeno rispetto all'addizione, perché queste operazioni non sono leggi di composizione interne di ϕ_q.
Infatti, supposto che ϕ_q sia chiuso rispetto alla sottrazione, consideriamo due dei suoi elementi: $c_1 = 1$ e $c_{\phi(q)} = q-1$ e calcoliamo la loro differenza d_1. Avendo supposto ϕ_q chiuso, dovremo ammettere anche che d_1 appartenga a ϕ_q.
Calcoliamo allora la differenza $d_2 = d_1 - 1$. Anche d_2 apparterrà a ϕ_q.
Procediamo con le differenze successive, fino all'ultima differenza $d_o = 1$: $(q-1)-1 = q-2$; $(q-2)-1 = q-3$; $(q-3)-1 = q-4 \ldots$
Così facendo dovremo ammettere che ϕ_q coincide con l'insieme completo dei resti modulo q.
Poiché ciò si verifica soltanto quando q è primo, cadiamo in contradizione con l'ipotesi che q invece sia composto.
Quindi, necessariamente, se q è numero composto, esiste qualche elemento $c \in \phi_q$ $(c \neq 1)$, tale che $(c-1) \notin \phi_q$.
Con ragionamento analogo, considerando questa volta l'operazione di addizione e i due elementi 1 e 2 di ϕ_q, arriviamo alla conclusione che esiste qualche elemento $c' \in \phi$ $(c' \neq q-1)$, tale che $(c'+1) \notin \phi_q$.
Tornando ad esaminare l'uguaglianza $(c-1)\cdot(c+1) = t \cdot q$, possiamo così essere certi che esiste qualche divisore di q della forma: $0 < (c-1) < q$, $c \in \phi_q$, $c \neq 1$ e qualche divisore di q della forma: $0 < (c'+1) < q$, $c' \in \phi$, $c' \neq q-1$
Ma dobbiamo rispondere a qualche altro quesito.

- Quando $[(c-1), q] \neq 1$, è possibile che (c-1) contenga tutti i divisori primi di q ?
La risposta è negativa, perché $0 < (c-1) < q$, $(c \neq 1)$.
- Quando $[(c'+1), q] \neq 1$, è possibile che (c'+1) contenga tutti i divisori primi di q ?
Anche in questo caso la risposta è negativa, perché $0 < (c'+1) < q$, $c' \neq q-1$.

Pertanto, l'elemento c "doppio" di ϕ_q esiste solo quando $c = c'$. Ciò implica che nell'uguaglianza $(c-1)\cdot(c+1) = t \cdot q$, sia (c-1) , sia (c+1) , abbiano dei divisori di q contemporaneamente: alcuni fattori primi di q in (c-1) e tutti gli altri fattori primi di q necessariamente in (c+1).

Andiamo alla ricerca di tutti i numeri c "doppi" di ϕ_q $(c \neq 1 , q-1)$, relativi alla base **a**=1, sempre che ne esista qualcuno.
Osserviamo anzitutto che nell'espressione $(c-1)\cdot(c+1)=t\cdot q$, assunta come riferimento per la nostra ricerca, se poniamo $c-1 = k$ e $c+1 = j$, si ha: $j = k+2$, per cui i numeri (c-1) e (c+1) della nostra ricerca devono essere coprimi.
Infatti, se $d|k$ ne segue che $d \nmid (k+2)$, $(d \neq 2$, perché consideriamo q dispari) .
Dopodiché, procediamo nel modo seguente.

* Scomponiamo in fattori primi il numero multiplo dispari q: $q = g \cdot j \cdot \ldots \cdot k$
Raggruppiamo questi fattori primi, nessuno appartenente a ϕ_q , in due gruppi disgiunti: A={g , j , . . . , h} ; B= {e , f , . . . , k}
Sia: $\mathbf{w} = g \cdot j \cdot \ldots \cdot h$ e $\mathbf{y} = e \cdot f \cdot \ldots \cdot k$
w e **y** sono coprimi e nessuno dei due appartiene a ϕ_q , mentre il loro prodotto è: $\mathbf{w}\cdot\mathbf{y} = q$
Se $\mathbf{w} < \mathbf{y}$, consideriamo l'insieme ϕ_y dei numeri maggiori di zero, minori di **y** e coprimi con **y** .
(Se $\mathbf{w} > \mathbf{y}$, invertiamo w con y e consideriamo l'insieme ϕ_w dei numeri maggiori di zero, minori di w e coprimi con w).
Tra gli elementi di ϕ_y ci sono sicuramente: 1 e y-1 , tutte le potenze di 2 minori di **y** e i corrispondenti $y\text{-}2^n$, **w** e **y-w**.
Come abbiamo avuto occasione di constatare, scelta in ϕ_y la base **a**=2 , esiste ed è unico un altro elemento s di ϕ_y , tale che $s\cdot\mathbf{w} \equiv 2$ (mod. y) , cioè: $s\mathbf{w}\text{-}2 = m\mathbf{y}$, per cui: $s\mathbf{w}\text{-}1 = m\mathbf{y}+1$; $(s , y) = 1$, perché $s \in \phi_y$; $(m , w) = 1$, altrimenti un loro divisore comune sarebbe divisore anche di 2, in contraddizione con l'ipotesi che q è dispari.
Avendo impegnato in **w** e in **y** tutti i fattori primi di q, abbiamo trovato un elemento "doppio" di ϕ_q , esso è $s\mathbf{w}\text{-}1$
Infatti questo numero ha i requisiti cercati:
- $(s\mathbf{w}\text{-}1)$ è un elemento di ϕ_q , perché è maggiore di 0, minore di q e coprimo con q.
Dall'uguaglianza $q=\mathbf{w}\cdot\mathbf{y}$, essendo $s < \mathbf{y}$, ne segue che $(s\mathbf{w}\text{-}1) < q$; $s\mathbf{w}\text{-}1 > 0$, perché $s > 0$ e $\mathbf{w} > 1$.
Dall'uguaglianza $s\mathbf{w}\text{-}1 = m\mathbf{y}+1$, se (sw-1) avesse un divisore primo h di q, dal momento che h è, per ipotesi, un fattore primo o di **w** o di **y**, h risulterebbe divisore anche di 1 . Il che è assurdo.
- $(s\mathbf{w}\text{-}1)+1 = s\mathbf{w}$; $(s\mathbf{w}\text{-}1)\text{-}1 = s\mathbf{w}\text{-}2=m\mathbf{y}$, quindi: $[(s\mathbf{w}\text{-}1)+1] \cdot [(s\mathbf{w}\text{-}1)\text{-}1] = s\mathbf{w} \cdot m\mathbf{y} = nq$, perché in **w** e in **y** ci sono tutti i divisori primi di q , alcuni in **w** e tutti gli altri in **y**. (Abbiamo dimostrato sopra che s ed m sono coprimi con q)
- Poiché $[(s\mathbf{w}\text{-}1)+1]\cdot[(s\mathbf{w}\text{-}1)\text{-}1] = (s\mathbf{w}\text{-}1)^2 - 1 = nq$, ne segue che: $(s\mathbf{w}\text{-}1)^2 \equiv 1$ (mod. q)
Cosicché $s\mathbf{w}\text{-}1$ è una radice quadrata di 1 in ϕ_q e quindi è un elemento doppio di ϕ_q .

Questo elemento doppio è stato trovato in corrispondenza a una scelta specifica dei fattori primi di q.
Sia ora w' il prodotto di un altro raggruppamento di fattori primi di q e y' il prodotto dei rimanenti fattori primi di q.
Procedendo alla stessa maniera di come abbiamo descritto sopra, troviamo un altro elemento doppio: s'w' - 1 .
Ma è possibile che (s'w' - 1) sia lo stesso elemento doppio trovato prima?
Se poniamo sw-1=s'w'-1 , si avrà l'uguaglianza: sw=s'w' . Sia d un divisore di w' , ma non di w.
Data l'uguaglianza $s\mathbf{w}= m\mathbf{y}+2$, sostituendo s'w' a sw , si avrà: $s'w' = m\mathbf{y}+2$
Il divisore d di w' , se non divide **w**, deve, per ipotesi, dividere **y**, per cui si arriva all'assurdo che d divide anche 2, che invece è coprimo con q dispari.
Quindi l'elemento doppio (s'w'-1) relativo a w' non può essere uguale all'elemento doppio (sw-1) relativo a w.

Tenuto conto di quest'ultima osservazione, dato che **w** è il prodotto di un qualsiasi raggruppamento di fattori primi di q , arriviamo alla conclusione che i numeri "doppi" di ϕ_q sono tanti quante sono le possibilità di distribuire in due gruppi disgiunti i fattori primi di q. Il calcolo di tutte le combinazioni è sintetizzato dalla formula:

$m = 2^n$ (n è la quantità dei divisori primi di q , m è la quantità degli elementi doppi di ϕ_q .

n	m
1	2
2	4
3	8
4	16
n	2^n

Adesso possiamo calcolare con esattezza il valore di ϕ_q!
Infatti, come abbiamo già stabilito, gli elementi di ϕ_q si possono associare:

- alcuni in coppie simmetriche, tali che $c_1 \cdot c_2 \equiv 1$ (mod. q)
- gli altri, quelli che hanno sé stessi come simmetrici, in coppie della forma (c ; q-c) , tali che $c \cdot (q-c) \equiv -1$ (mod. q) :

$$\phi_q! = (c_1 \cdot c_j) \cdot (c_2 \cdot c_t) \cdot \ldots \cdot [c_h \cdot (q - c_h)] \cdot \ldots \cdot [c_k \cdot (q - c_k)]$$

Come si può notare dalla formula, quando i divisori primi di q sono due o più di due $(n > 1)$, le coppie (c ; q-c) sono in numero pari, per cui il valore di $\phi_q!$ è dato dalla congruenza:

$$\phi_q! \equiv 1 \text{ (mod. q) , qualunque sia il numero multiplo dispari q}$$

Solo quando l'esponente è n=1, cioè quando q è primo, si forma una sola coppia (c ; q-c) e questo evento determina il valore:
$\phi_q! \equiv -1$ (mod. q) riscontrato nel teorema di Wilson: $(p-1)! \equiv -1$ (mod. p) , p numero primo.

Per il calcolo della formula $m = 2^n$, cliccare su "Combinazione ϕ"

***

Stabilito il valore di $\phi_q!$, passiamo a considerare una qualsiasi base **a** dell'insieme ϕ_q

* Dimostriamo che per ciascuna base sono valide le congruenze:

$$\mathbf{a}^{\phi(q)/2} \equiv \phi_q! \equiv 1 \pmod{q} , \quad \mathbf{a} \in \phi_q$$

Nella relazione sul teorema di Eulero abbiamo già dimostrato che, dato un numero dispari q , e scelto nell'insieme ϕ_q un qualsiasi elemento **a**, che denominiamo base, tutti gli elementi $c \in \phi_q$ si possono accoppiare, univocamente, nella congruenza: $c' \cdot c'' \equiv \mathbf{a}$ (mod. q)
Ma, per potere calcolare il valore di $\mathbf{a}^{\phi(q)/2}$, occorre stabilire anche se ci sono coppie formate dallo stesso elemento e, se ci sono, è necessario contare quante sono queste coppie.

Se si sceglie come base **a** un <u>non-residuo</u> quadratico, il calcolo è subito fatto, perché la radice quadrata di **a** in ϕ_q non esiste, per cui le coppie delle congruenze $c' \cdot c'' \equiv \mathbf{a}$ (mod. q) sono formate tutte da due elementi distinti $(c' \neq c'')$:

$$\mathbf{a}^{\phi(q)/2} \equiv \phi_q! \equiv 1 \pmod{q} , \quad \mathbf{a} \in \phi_q \text{ non-residuo quadratico}$$

Rimane il problema di calcolare il valore di $\mathbf{a}^{\phi(q)/2}$ quando si sceglie come base **a** un <u>residuo</u> quadratico $(a \neq 1)$.

I residui quadratici, per loro stessa definizione, hanno almeno una radice quadrata in ϕ_q , per cui c'è sempre qualche elemento v "doppio" di ϕ_q relativo alla scelta della base **a** , cioè tale che: $v^2=tq+\mathbf{a}$; $v^2 \equiv \mathbf{a}$ (mod. q)
Ma, se v è una radice quadrata di **a** in ϕ_q , anche (q - v) lo è. Infatti: $(q-v)^2 \equiv \mathbf{a}$ (mod. q)

Possiamo quindi asserire:
*qualunque sia il numero q dispari, per ogni residuo quadratico **a** ci sono sempre almeno due radici quadrate in ϕ_q : v e v-c , e il loro prodotto è:* $v \cdot (q-v) \equiv -\mathbf{a}$ (mod. q)

Se gli elementi doppi fossero solo due, il calcolo di $\phi_q!$ sarebbe ancora una volta ben determinato, ma alcuni esempi pratici ci fanno intravedere che le radici del residuo quadratico **a** possano essere più di due.
Vediamo allora di esaminare l'insieme ϕ_q , al fine di trovare la legge generale che ci consenta di stabilire quante e quali sono le radici quadrate di ciascuno dei suoi residui quadratici.
Se, oltre a v, c'è qualche altra radice c di **a**, avremo le congruenze: $v^2 \equiv \mathbf{a}$ (mod. q) ; $c^2 \equiv \mathbf{a}$ (mod. q) e quindi: $c^2 \equiv v^2$ (mod. q)
Da quest'ultima congruenza otteniamo l'uguaglianza:

$$(c-v)(c+v)=tq \qquad <*>$$

Analizziamo con attenzione questa equazione al fine di ricavare tutte le radici quadrate di **a** in ϕ_q e quindi tutti gli elementi "doppi" di ϕ_q , relativi ad **a**.

Per c=v e per c = q-v , l'espressione <*> è sempre vera, perché valgono le rispettive uguaglianze: $0 \cdot 2v=0$; $(q-2v) \cdot q=tq$
E' importante osservare che per ciascuno di questi due valori i fattori primi di q si trovano o tutti in (c-v) o tutti in (c+v).
Quindi, per qualunque residuo quadratico **a**, le due soluzioni di <*> trovate sono sempre elementi "doppi" di ϕ_q:
$v^2 \equiv \mathbf{a}$ (mod. q) ; $(q-v)^2 \equiv \mathbf{a}$ (mod. q) ; $v \cdot (q-v)=vq-v^2 \equiv -\mathbf{a}$ (mod. q)

Ricerchiamo tutte le altre possibili radici quadrate di **a** in ϕ_q in base alle seguenti considerazioni.
Affinchè l'uguaglianza <*> sia valida per $c \neq v$ e per $c \neq q-v$, ci deve essere un altro valore $c \in \phi_q$ tale che:
- la differenza (c-v) e la somma (c+v) non siano elementi di ϕ_q: $(c-v) \notin \phi_q$; $(c+v) \notin \phi_q$
- in (c-v) ci siano solo alcuni divisori primi di q e, contemporaneamente, in (c+v) ci siano tutti gli altri divisori primi di q .
- la distanza tra (c-v) e (c+v) sia 2v: (c+v)-(c-v)=2v

* Dato il numero composto dispari q , scegliamo in ϕ_q il residuo quadratico $\mathbf{a} \equiv v^2$ (mod. q) , $v \in \phi_q$
Se 2v > q , si sceglierà, come radice quadrata di **a**, $v' = q-v$, in modo che sia sicuramente 2v' < q .
Scomponiamo in fattori primi il numero q: $q = g \cdot j \cdot \ldots \cdot k$
Raggruppiamo questi fattori primi, nessuno appartenente a ϕ_q , in due insiemi disgiunti:

$$\mathbf{A} = \{g , j , \ldots , h\} \quad ; \quad \mathbf{B} = \{e , f , \ldots , k\}$$

Sia: $\mathbf{w}=g \cdot j \cdot \ldots \cdot h$ e $\mathbf{y}=e \cdot f \cdot \ldots \cdot k$ (**w** e **y** sono coprimi e nessuno dei due appartiene a ϕ_q , mentre $\mathbf{w} \cdot \mathbf{y}=q$)
Se $\mathbf{w}<\mathbf{y}$ consideriamo l'insieme ϕ_y dei numeri maggiori di zero, minori di **y** e coprimi con **y**.
(Se **w** > **y** , invertiamo **w** con **y** e consideriamo l'insieme ϕ_w dei numeri maggiori di zero, minori di **w** e coprimi con **w**).
Se 2v > y , aumentiamo il valore di **y** elevando a potenza uno o più dei suoi fattori primi: $\mathbf{y} = e^n \cdot f \cdot \ldots \cdot k$
in modo tale che divenga: 2v < y . In questo caso, $\mathbf{w} \cdot \mathbf{y} = dq$, (d|q) .
Gli elementi: 1, 2, v, 2v appartengono sicuramente a ϕ_y , perché sono anche elementi di ϕ_q e sono minori di **y** ; mentre **w** e **y-w** sono elementi di ϕ_y perché coprimi con **y** e $0<\mathbf{w}<\mathbf{y}$.
Come abbiamo avuto occasione di vedere, l'insieme ϕ_y è tale che , fissato l'elemento $2v \in \phi_y$ come base, esiste, ed è unico, un altro elemento s dello stesso ϕ_y che determina la congruenza: $s \cdot \mathbf{w} \equiv 2v$ (mod. **y**), cioè: $s\mathbf{w}-2v=t\mathbf{y}$.
E' importante osservare che:
- s non ha alcun divisore primo di y, perché $s \in \phi_y$;
- t non ha alcun divisore primo di w, altrimenti v non potrebbe essere coprimo con q . (Si evince da: $s\mathbf{w}-2v=t\mathbf{y}$) .

La nostra attenzione va rivolta al numero $(s\mathbf{w}-v)=(t\mathbf{y}+v)$ ricavato dall'uguaglianza $s\mathbf{w}-2v=t\mathbf{y}$.

Esaminiamolo:
* (s**w**-v) è maggiore di zero e potrebbe appartenere a ϕ_q (accade quando sw-v < q) , ma, in ogni caso, è coprimo con q.
Infatti, tenendo conto che (s**w**-v)=(t**y**+v), se (s**w**-v) avesse un divisore primo g di q, g dovrebbe: o dividere sia **w** sia v, o dividere sia **y** sia v. Ma v, per ipotesi, non ha divisori di q , quindi, necessariamente: [(s**w**-v) , q] = 1
* (s**w**-v)-v=s**w**-2v=t**y** ; (s**w**-v)+v=s**w** .
* (s**w**-v)-v ≡ b-v (mod. q) ; (s**w**-v)+v ≡ b+v (mod. q)

Il numero b di queste congruenze è un elemento "doppio" di ϕ_q , perché ne ha i requisiti:
- $b \in \phi_q$
Infatti, ricordando che (s**w**-v) > 0 e [(s**w**-v) , q] = 1 , si ha:
* 0 < b < q , perché b è il minimo resto positivo della divisione di (sw-v) per q: (sw-v)=kq+b , k ≥ 0 ;
* (b , q) = 1 , b è coprimo con q , perché anche (sw-v) e q sono coprimi.
- (b-v) contiene tutti i fattori primi di q che sono contenuti in **y** e nessuno di quelli contenuti in **w**.
Infatti, dalla congruenza (s**w**-v)-v ≡ b-v (mod. q) , essendo s**w**-2v=t**y** , ne segue che t**y**=fq+(b-v), f ≥ 0 per cui:
* se d è un divisore di **y** , d deve essere divisore pure di (b-v), perché divide anche q. Quindi: $d\,|\,\mathbf{y} \Rightarrow d\,|\,(b-v)$
* se supponiamo invece che un divisore g di **w** divide (b-v) , poiché divide anche q , g dovrebbe dividere anche **y**, in contraddizione con le ipotesi fatte e abbiamo già escluso sopra che g possa dividere t. Quindi: $g\,|\,\mathbf{w} \Rightarrow g \nmid (b-v)$.
- (b+v) contiene tutti i fattori primi di q che sono contenuti in **w** e nessuno di quelli contenuti in **y**.
Infatti, dalla congruenza (s**w**-v)+v ≡ b+v (mod. q) , ne segue che s**w**=jq+(b+v), j ≥ 0 per cui:
* se f è un divisore di **w**, f deve essere divisore pure di (b+v), perché divide anche q. Quindi: $f\,|\,\mathbf{w} \Rightarrow f\,|\,(b+v)$
* se supponiamo invece che un divisore h di **y** divide (b+v), poiché divide anche q, h dovrebbe dividere pure **w**, in contraddizione con le ipotesi fatte e abbiamo già escluso sopra che h possa dividere s. Quindi: $h\,|\,\mathbf{y} \Rightarrow h \nmid (b+v)$.
- $(b-v) \cdot (b+v)=mq$, perché in (b-v) e in (b+v) ci sono tutti i divisori primi di q , alcuni in (b-v) e tutti gli altri in (b+v) .
- La distanza tra (b-v) e (b+v) è 2v.

Pertanto l'elemento b di ϕ_q è una radice quadrata del residuo quadratico **a** in ϕ_q :
$(b-v) \cdot (b+v) = b^2 - v^2 \Rightarrow b^2 \equiv a$ (mod. q)

Ci chiediamo ora se il numero **w'** ottenuto da una scelta diversa dei fattori primi di q, ci fa trovare una radice b' del residuo quadratico **a**, diversa da b.
Confrontiamo le congruenze: b ≡ (s**w**-v) (mod. q) ; b' ≡ (s'w'-v) (mod. q) , tenendo presente che q e v rimangono costanti.
Se b=b' ne segue che: s'w'-v ≡ sw-v (mod. q) e quindi: s'w'-sw = tq
Se d è un fattore primo di w' , ma non di w, quest'ultima uguaglianza è valida solo se d divide s, perché d divide anche q .
Ma s è l'elemento di ϕ_y che abbiamo usato sopra: sw = ty+2v .
Da questa ci accorgiamo che, ipotizzando che d divide s, dovremmo ammettere anche che d divide $2v \in \phi_q$.
Infatti, se d non è un fattore di **w** , per definizione è invece un fattore di **y**.
Data la contraddizione a cui si andrebbe incontro, siamo sicuri che la nuova radice b' di **a** è diversa dalla precedente: $b' \neq b$

Si deduce facilmente che la dimostrazione non cambia, se tra i fattori di q ci sono potenze di primi: ciascuna potenza di un numero primo va considerata una sola unità della scomposizione e trattata come se fosse un singolo numero primo.

Se $q=g^a \cdot j^b \cdot \ldots \cdot k^m$, le potenze dei fattori primi si devono distribuire in due insiemi disgiunti:

$$\mathbf{A} = \{g^a, j^b, \ldots, h^n\} \;;\; \mathbf{B} = \{e^d, f^g, \ldots, k^m\}$$
$$\mathbf{W} = g^a \cdot j^b \cdot \ldots \cdot h^n \;;\; \mathbf{Y} = e^d \cdot f^g \cdot \ldots \cdot k^m$$

Le procedure per trovare gli elementi "doppi" di ϕ_q sono le stesse di quelle descritte prima.

Avendo trovato un metodo per ricavare le radici quadrate del residuo quadratico **a** in ϕ_q e tenendo conto delle osservazioni fatte prima, dato che **W** è il prodotto di un qualsiasi raggruppamento di potenze di fattori primi di q e **Y** il corrispondente prodotto delle potenze rimanti, arriviamo alla conclusione che gli elementi "doppi" di ϕ_q sono tanti quante sono le possibilità di distribuire in due insiemi disgiunti una quantità di oggetti pari alla quantità dei fattori primi presenti nella scomposizione di q.

Il calcolo di tutte le combinazioni possibili di n oggetti, è sintetizzato dalla formula:

$$m = 2^n$$

Nel nostro caso: n è la quantità dei divisori primi di q , m è la quantità degli elementi doppi di ϕ_q .

Adesso possiamo calcolare con esattezza il valore di $\phi_q!$
Come già sappiamo, fissato un qualsiasi residuo quadratico $\mathbf{a} \in \phi_q$ come base, tutti gli elementi di ϕ_q si possono associare, alcuni in coppie **a**-simmetriche, tali che il prodotto di ciascuna di esse è $c_1 \cdot c_2 \equiv \mathbf{a}$ (mod. q) , e gli altri, quelli che hanno sé stessi come **a**-simmetrici, in coppie di forma (c ; q-c) , tali che il prodotto di ciascuna di queste è $c \cdot (q-c) \equiv -\mathbf{a}$ (mod. q) :

$$\phi_q! = (c_1 \cdot c_j) \cdot (c_2 \cdot c_t) \cdot \ldots \cdot [c_h \cdot (q - c_h)] \cdot \ldots \cdot [c_k \cdot (q - c_k)] \equiv a \cdot a \cdot \ldots \cdot (-a) \cdot \ldots \cdot (-a) \pmod{q}$$

Come si può notare dalla formula $m=2^n$, quando i divisori primi di q sono due o più di due, le coppie (c ; q-c) di elementi "doppi" di ϕ_q sono in numero <u>pari</u> , e più precisamente: $m/2 = 2^{n-1}$ (n è la quantità dei divisori primi di q) . Per cui:

$$[c_h \cdot (q - c_h)] \cdot \ldots \cdot [c_k \cdot (q - c_k)] \equiv (-a)^{2^{n-1}} \equiv a^{2^{n-1}} \pmod{q}, \; (n \geq 2 \text{, perché q è composto})$$

Di conseguenza il valore di $\phi_q!$, relativo a ciascuna base **a**, è dato dalla congruenza:

$$\phi_q! \equiv \mathbf{a}^{\phi(q)/2} \equiv 1 \pmod{q} \;,\; \mathbf{a} \in \phi_q \text{ residuo quadratico , q multiplo dispari}$$

Come abbiamo potuto constatare prima, questa stessa congruenza vale anche quando si sceglie **a**=1 e vale pure quando si sceglie **a** non-residuo quadratico, per cui, qualunque sia $a \in \phi_q$, si ha:

$$\mathbf{a}^{\phi(q)/2} \equiv \mathbf{1} \pmod{q} \;,\; \mathbf{a} \in \phi_q \;,\; \text{q multiplo dispari}$$

Solo se nella formula $m=2^n$ si pone n=1, il che accade quando q è numero primo, si forma una sola coppia (c ; q-c) a cui corrisponde la congruenza $c \cdot (q - c) \equiv -\mathbf{a}$ (mod. q). Questo evento determina le congruenze, già riscontrate in quella mia relazione che ho titolato «Da Wilson a Fermat» :

$$\mathbf{a}^{\phi(q)/2} \equiv -\phi_q! \equiv \mathbf{1} \pmod{q} \;,\; \mathbf{a} \in \phi_q \text{ residuo quadratico, diverso da 1, e q primo}$$
$$\mathbf{a}^{\phi(q)/2} \equiv \phi_q! \equiv -\mathbf{1} \pmod{q} \;,\; \mathbf{a} \in \phi_q \text{ non-residuo quadratico e q primo}$$

Per il calcolo della formula $m=2^n$, cliccare su "Combinazione ϕ"

Quanti sono i residui quadratici dell'insieme ϕ_q

Una immediata conseguenza del teorema v-v è questa:
dato il numero composto q, la quantità $r(\phi_q)$ dei residui quadratici presenti nell'insieme ϕ_q è:

$$\mathbf{r(\phi_q)} = \phi(q)/2^n \;,\; \text{n è la quantità dei fattori primi di q}$$

Ciò perché ogni residuo quadratico ha 2^n radici quadrate in ϕ_q .

Ad esempio, la quantità di residui quadratici dei numeri composti 91, 105, 1155, 539, 1547 sono:

$r(\phi_{91}) = 72/4 = 18$; $r(\phi_{105}) = 48/8 = 6$; $r(\phi_{1155}) = 480/16 = 30$; $r(\phi_{539}) = 420/4 = 105$; $r(\phi_{1547}) = 1152/8 = 144$

Esempi

* Sia q = 105 = 3•5•7 ; $\phi(105) = 48$; $r(\phi_{105}) = 6$
Stabiliamo quali sono gli elementi doppi di ϕ_{105} relativi al residuo quadratico **a**=16
Poiché 16 è un quadrato perfetto, una delle sue radici quadrate è subito individuata (v=4).
Esaminiamo l'espressione (c-4)(c+4)=mq per determinare le altre 7 radici.
(Il numero 105 è il prodotto di 3 fattori primi, per cui le radici quadrate di 16 in ϕ_{105} sono 2^3= 8)

<u>1ª combinazione</u>: poniamo nessun fattore primo di 105 in (c-4) e tutti in (c+4).
w=0 ; y=3•5•7 ; dis.=0 (La distanza è zero, perché i fattori primi di 105 sono tutti in c+4).
A questa distribuzione corrisponde l'uguaglianza c+4=105 , da cui ricaviamo il primo elemento doppio: c_1=105-4=101
Calcoliamo il secondo elemento doppio con una sottrazione: c_2=105-101=4
Per questi due elementi doppi di ϕ_{105} si ha: 4^2=16 ; 101^2= 97•105+16 ≡ 16 (mod. 105) ; $c_1 \cdot c_2$ = 4•101 ≡ 89 ≡ -16 (mod. 105)

<u>2ª combinazione</u>: poniamo un fattore primo di 105 in A ; gli altri due nell'insieme B .
1ª possibilità: w=3 ; y=5•7=35 ; dis.=2v=8
Esiste in ϕ_{35} un elemento s tale che 3•s ≡ 8 (mod. 35)
Per s=26, si ha: 3•26=2•35+8 da cui si ricava: 3•26-4=2•35+4 = 74
Ne segue così che c_3=74 è un altro elemento doppio di ϕ_{105} .
Infatti: 74-4=70 è multiplo di 35 e 74+4=78 è multiplo di 3 , mentre la loro distanza è di 8 unità.
Calcoliamo il quarto elemento doppio di ϕ_{105} con una sottrazione: c_4=105-74=31 .
Per questi elementi doppi di ϕ_{105} si ha: 74^2= 52•105+16 ≡ 16 (mod. 105) ; 31^2 ≡ 16 (mod. 105) ; 74•31≡-16 (mod. 105)

2ª possibilità: w=5 ; y=3•7=21 ; dis.=8
Esiste in ϕ_{21} un elemento t tale che 5•t ≡ 8 (mod. 21)
Per t=10 si ha: 5•10=2•21+8 , per cui altri due elementi doppi sono: c_5= 46 e c_6= 105-46=59

3ª possibilità: w=7 ; y=15 ; dis.=8
Esiste in ϕ_{15} un elemento k tale che 7•k ≡ 8 (mod. 15)
Per k=14 si ha: 7•14=6•15+8 , per cui altri due elementi doppi sono: c_7= 94 e c_8= 105-94=11
Queste 8 radici quadrate di 16 in ϕ_{105} sono gli otto elementi doppi di ϕ_{105} relativi al residuo quadratico 16 .
Moltiplichiamoli: $c_1 \cdot c_2 \cdot c_3 \cdot c_4 \cdot c_5 \cdot c_6 \cdot c_7 \cdot c_8$ = 4•101•74•31•46•59•94•11 ≡ $(-16)^4$ ≡ 16^4 ≡ 16 (mod. 105)
Si deduce quindi che: $16^{24} \equiv 1$ (mod. 105) Infatti: $16^{4 \cdot 6} \equiv 16^6 \equiv 1$ (mod. 105)

* Sia $q = 1155 = 3\cdot5\cdot7\cdot11$; $\phi(1155) = 480$; $r(\phi_{1155}) = 30$

Stabiliamo quali sono gli elementi doppi di ϕ_{1155} relativi a residuo quadratico **a**=214

Per tentativi si trova una radice quadrata di 214 in ϕ_{1155} : v=37

Le radici di 214 sono in tutto $2^4=16$, cerchiamoli tutti nella relazione: (c-37)(c+37)=214

<u>1ª combinazione</u>: poniamo nessun fattore primo di 1155 in (c-37) e tutti in (c+37).

w=0 ; y=3•5•7•11 =1155 ; dis.=0 I punti doppi corrispondenti sono: $c_1=37$; $c_2 = 1118$

<u>2ª combinazione</u>: poniamo un fattore primo in A ; gli altri tre nell'insieme B .

1ª possibilità: w=3 ; y=5•7•11=385 ; dis.=2v=74

3•s≡74 (mod. 385) ; per s=153 e t=1 , si ha: 3•153=385+74 ⇒ 3•153-37=385+37=422 Quindi: $c_3=422$; $c_4=1155-422=733$

2ª possibilità: w=5 ; y=3•7•11=231 ; dis.=74

per s=61 e t=1 si ha: 5•61=231+74 Quindi: $c_5=231+37=268$; $c_6=1155-268=887$

3ª possibilità: w=7 ; y=3•5•11=165 ; dis.=74

per s=152 e t=6 si ha: 7•152=165•6+74 Ne segue che: $c_7 = 7\cdot152-37=1027$; $c_8 = 1155-1027=128$

4ª possibilità: w=11 ; y=3•5•7=105 ; dis.=74

per s=64 e t=6 si ha: 64•11=6•105+74 Ne segue che: $c_9 = 6\cdot105+37=667$; $c_{10} = 1155-667=488$

<u>3ª combinazione</u>: poniamo due fattori primi di 1155 in A ; gli altri due nell'insieme B .

1ª possibilità: w=3•5=15 ; y=7•11=77 ; dis.=74

per s=46 e t=8 si ha: 46•15=8•77+74 Ne segue che: $c_{11} =8\cdot77+37=653$; $c_{12} =1155-653=502$

2ª possibilità: w=3•7=21 ; y=5•11=55 ; a= 214 ; $c_1=37$; dis.=74

In questo caso dis.74 > 55 , per cui è necessario aggiungere un altro fattore di 1155 a w oppure a y :

W=3•7^2=147 ; y=5•11=55 ; dis.=74 .

Dobbiamo risolvere l'equazione: s•55=t•147+74

per s=143 e t=53 si ha: 143•55=53•147+74 per cui: 143•55-37=53•147+37 = 7828

Ma 7828 non è un elemento di ϕ_{1155} , perché maggiore di 1155.

(143•55-37)-37=53•147=tW ; (143•55-37)+37= 143•55=sy per cui: 7828-37=tW ; 7828+37=sy

Passiamo alle congruenze: 7828 ≡ 898 (mod. 1155)

Il numero 898 di questa congruenza è una radice quadrata di 214 in ϕ_{1155}

Infatti:

- 898 e 1155 sono coprimi (898=2•449 ; 1155=3•5•7•11) e quindi $898 \in \phi_{1155}$
- 898-37=861=3•7•41 ; 898+37=935=5•11•17 , per cui:
  * (898-37) contiene tutti quei divisori di 1155 che sono contenuti in W, ma nessuno di quelli contenuti in y.
  * (898+37) contiene tutti quei divisori di 1155 che sono contenuti in y, ma nessuno di quelli contenuti in W.
- (898-37)•(898+37)=861•935=805035=697•1155
- (898-37)•(898+37)= $898^2 - 37^2 \equiv 0$ (mod. 1155) >> $898^2 \equiv 37^2$ (mod. 1155) ⇒ $898^2 \equiv 214$ (mod. 1155)

Ne segue che: $c_{13} = 898$; $c_{14} = 1155 - 898 = 257$

3ª possibilità: w=3•11=33 ; y=5•7=35 ; dis.=74

W=w•3=99 ; y=35 ; dis. 74 Dobbiamo risolvere l'equazione: s•35=t•99+74

per s=70 e t=24 si ha: 70•35=24•99+74 per cui: 70•35-37=2413 ; 2413 ≡ 103 (mod. 1155)

Ne segue che: $c_{15} = 103$; $c_{16} = 1155-103=1052$

Moltiplichiamo tutte le radici quadrate di 214 in ϕ_{1155} :

37•1118•422•733•268•887•1027•128•667•488•653•502•898•257•103•1052 = $214^8 \equiv 961$ (mod. 1155)

Si deduce quindi che: $214^{240} \equiv 1$ (mod. 1155) Infatti: $214^{8\cdot30} \equiv 961^{30} \equiv 1$ (mod. 1155)