**Punto aperto dello studio dell’esistenza di coppie di spazi complementari basata sui trattini**

**Ipotesi:**

1. n1 ed n2 primi con n1 < n2 ;
2. n intero maggiore di 1

**Tesi:**

1. esistono due multipli di n1: n1\*h ed n1\*k (con h e k > 0) tali che n1\*h -1 ed n1\*k +1 non sono divisibili per n2
2. h+k deve essere uguale ad un n prefissato maggiore di 1

Dimostrazione della Tesi a)

Esistono infiniti h ed infiniti k tali che n1\*h -1 ed n1\*k +1 non siano divisibili per n2.

In ordine crescente di h e k, n1\*h -1 ed n1\*k +1 non sono divisibili per n2, in quanto minori di esso, per tutti gli h < e per tutti i k < .

Dimostriamo ora che per infiniti valori di h e k superiori ad h0 e a k0, n 1\*h -1 ed n1\*k +1 non sono divisibili per n2 e si possono scrivere:

1. n1\*h -1 = h’\* n2 +rh con 0 <rh <n2
2. n1\*k +1 = k’\* n2 +rk con0 <rk <n2

Infatti dalla 1) si vede che per ogni h Ꜫ N maggiore di e tale che [h\* n1]mod n2 sia diverso da 1, ponendo rh = [h\* n1]mod n2 – 1 (cioè ponendo [h\* n1] ed [rh+1] congrui con n2), esisterà sempre un h’ Ꜫ N che soddisfa la 1).

Analogamente dalla 2) si vede che per ogni k Ꜫ N e tale che [k\* n1]mod n2 sia diverso da -1, ponendo rk = [k\* n1]mod n2 + 1 (cioè [k\* n1] ed [rk-1] congrui con n2), esisterà sempre un k’ Ꜫ N che soddisfa la 2).

Le due condizioni: [h\* n1]mod n2 diverso da 1 e [k\* n1]mod n2  diverso da -1 valgono sempre per gli h e k minori rispettivamente di h0 e di k0, e per quelli superiori escludono la possibilità che rh o rk  possano essere uguali a 0.

Dimostrazione della Tesi b)

Dobbiamo ora dimostrare che tra gli infiniti h e k che soddisfano la Tesi a) ce ne sono anche alcuni che soddisfano la condizione h + k =n.

Abbiamo visto che, per soddisfare la Tesi A), [h\* n1]mod n2 deve essere diverso da 1 ed [k\* n1]mod n2  deve essere diverso da -1 e cioè devono essere rispettate le due condizioni:

1. [h\* n1]mod n2 ≠ 1
2. [k\* n1]mod n2 ≠ -1 ≠ n2 - 1

Se imponiamo ora la condizione che h + k = n, ne discendono due conseguenze:

1. che sia h che k (entrambi maggiori di 0, con n maggiore di 1 per ipotesi) appartengono all’intervallo [1, n-1]
2. che h e k sono complementari rispetto ad n per cui in aritmetica modulare tra i moduli n2 dei loro prodotti per n1 sussiste la seguente relazione:

 [k\*n1]mod n2 = [(n-h)\*n1]mod n2 = [n\*n1-h\*n1]mod n2 = [n\*n1]mod n2 --

[h\*n1]mod n2

con la conseguenza che anche [h\*n1]mod n2 e [k\*n1]mod n2 sono complementari rispetto a [n\*n1]mod n2 , per cui se n è un multiplo di n2 si avrà che [n\*n1]mod n2 = 0 = n2 ed il verificarsi o meno della condizione 3) implicherà anche quello della condizione 4); se invece n2 non divide n bisogna verificare il rispetto di entrambe le condizioni.

**Nel caso A) quindi che n2 divide n** per soddisfare la condizione 3), e come detto quindi anche quella 4), basta dimostrare che esiste almeno un hi tale che:

[\* n1]mod n2 ≠ 1 con Ꜫ {1,2, ……. n-1}

ora per ogni hi ed ogni hi+1 (con 1 < i <n-1) è possibile scrivere:

[\* n1]mod n2 = [hi \* n1 ± n1]mod n2 = [hi\* n1] mod n2 ± [n1]mod n2.

e questo vuol dire che se [\* n1]mod n2 = 1 non lo sarà [\* n1]mod n2 (o viceversa) essendo [n1]mod n2 = n1 ed n1 ≠ n2.

In conclusione e oppure e soddisfarranno le condizioni 3) e 4).

**Nel caso B) invece, in cui n2 non divide n**, dobbiamo verificare che entrambe le condizioni 3) e 4) siano verificate. Consideriamo allora due valori qualsiasi di h e k complementari rispetto ad n ed i moduli n2 dei loro prodotti per n1:

[hi\*n1]mod n2 e [kj\*n1]mod n2 con i, j Ꜫ {1,2, ……. n-1} e j = n – i

Ora per ogni hi, hi+1 e kj-1 (con 1 < i <n-1) è possibile considerare le seguenti relazioni:

 [hi\*n1]mod n2 = [hi+1\*n1]mod n2 – [n1]mod n2

[\* n1]mod n2 + [n1]mod n2 \* n1]mod n2

Se [hi\*n1]mod n2 = 1 si avrà che:

[hi+1\*n1]mod n2 = [hi\*n1]mod n2 + [n1]mod n2 ≠ 1

essendo [n1]mod n2 ≠ 0

d’altra parte avremo:

[kj-1\*n1]mod n2 = [kj\*n1]mod n2 – [n1]mod n2 = [n\*n1]mod n2 - [hi\*n1]mod n2 – [n1]mod n2 = [n1]mod n2 \* [n-1]mod n2 – 1

e quindi **se escludiamo che n2 divida (n-1)** risulterà[kj-1\*n1]mod n2 ≠ -1 con la conclusione che hi+1 e kj-1 soddisfarranno le condizioni 3) e 4).

Se invece [kj\*n1]mod n2 = -1 si avrà che:

[kj+1\*n1]mod n2 = [kj\*n1]mod n2 + [n1]mod n2 ≠ -1

essendo [n1]mod n2 ≠ 0

d’altra parte avremo:

[hi-1\*n1]mod n2 = [hi\*n1]mod n2 – [n1]mod n2 = [n\*n1]mod n2 - [kj\*n1]mod n2 – [n1]mod n2 = [n1]mod n2 \* [n-1]mod n2 + 1

e quindi **se escludiamo che n2 divida (n-1)** risulterà[hi-1\*n1]mod n2 ≠ 1 con la conclusione che hi-1 e kj+1 soddisfarranno le condizioni 3) e 4).

Se invece [hi\*n1]mod n2 ≠ 1 e [ki\*n1]mod n2 ≠ 1 saranno proprio hi e ki a soddisfare le condizioni 3) e 4).

**Nel caso C) infine che n2  non divide n ma divide n – 1** consideriamo sempre due valori qualsiasi di h e k complementari rispetto ad n ed i moduli n2 dei loro prodotti per n1:

[hi\*n1]mod n2 e [kj\*n1]mod n2 con i, j Ꜫ {1,2, ……. n-1} e j = n – i

Ora per ogni hi , hi+2 e kj-2 (con 2 < i <n-2) è possibile considerare le relazioni che seguono.

Se [hi\*n1]mod n2 = 1 si avrà che:

[hi+2\*n1]mod n2 = [hi\*n1]mod n2 + 2\*[n1]mod n2 ≠ 1

essendo [n1]mod n2 ≠ 0 e 2\*n1 ≠ n2

d’altra parte avremo:

[kj-1\*n1]mod n2 = [kj\*n1]mod n2 – [n1]mod n2 = [n\*n1]mod n2 - [hi\*n1]mod n2 – [n1]mod n2 = [n1]mod n2 \* [n-1]mod n2 – 1

[kj-2\*n1]mod n2 = [n1]mod n2 \* [n-1]mod n2 – 1 - [n1]mod n2 = [n1]mod n2 \* [n-2]mod n2 – 1 ≠ -1

essendo [n-2]mod n2  ≠ 0 in quanto n-2 non è divisibile per n2 essendolo già n-1 ed essendo [n1]mod n2 ≠ 0

In conclusione hi+2 e kj-2 soddisfarranno le condizioni 3) e 4).

Se invece [kj\*n1]mod n2 = -1 si avrà che:

[kj+2\*n1]mod n2 = [kj\*n1]mod n2 + 2\*[n1]mod n2 ≠ -1

essendo [n1]mod n2 ≠ 0 e 2\*n1 ≠ n2

d’altra parte avremo:

[hi-1\*n1]mod n2 = [hi\*n1]mod n2 – [n1]mod n2 = [n\*n1]mod n2 - [kj\*n1]mod n2 – [n1]mod n2 = [n1]mod n2 \* [n-1]mod n2 + 1

[hi-2\*n1]mod n2 = [n1]mod n2 \* [n-1]mod n2 + 1 - [n1]mod n2 = [n1]mod n2 \* [n-2]mod n2  + 1 ≠ 1

essendo [n-2]mod n2  ≠ 0 in quanto n-2 non è divisibile per n2 essendolo già n-1 ed essendo [n1]mod n2 ≠ 0

In conclusione hi-2 e kj+2 soddisfarranno le condizioni 3) e 4).

Se invece [hi\*n1]mod n2 ≠ 1 e [ki\*n1]mod n2 ≠ -1 saranno proprio hi e ki a soddisfare le condizioni 3) e 4).

Per n ≥ 5 la tesi del teorema è verificata per ognuno dei tre casi considerati di n: n2 divide n, n2 non divide né n né (n-1), n2 non divide n ma divide (n-1).

Invece per n=2 il teorema è verificato in quanto sia h che k sono uguali ad 1 e quindi minori rispettivamente di h0 e di k0; per n=3 il teorema è verificato in base al caso A) o a quello B) a seconda della divisibilità di n per n2; per n=4 infine il teorema è verificato in base al caso B).