**Tratto da quipo base 5**

**Il teorema cinese del resto**

**Dall'aritmetica modulare alla risoluzione dei sistemi modulari**

Consideriamo il seguente problema:

**Quante sono le cose?**Dato un certo numero di cose, si sa che:
- dividendolo per 3 dà come resto 2,
- dividendolo per 5 dà come resto 3,
- dividendolo per 7 dà come resto 2.
Qual è il numero?

Il problema, in altre parole, può essere espresso così:

**Quante sono le cose?**Dato un certo numero di cose
ne avanzano 2, se disposte a gruppi di 3
ne avanzano 3, se disposte a gruppi di 5
ne avanzano 2, se disposte a gruppi di 7
Quante sono le cose?

**Questo problema fu posto per la prima volta da Sun Tsu Suan-Ching (300 a. C.)**

Il **Teorema cinese del resto** è utile per risolvere problemi come questo, nei quali bisogna trovare un numero conoscendo i resti di alcune divisioni di quello stesso numero per numeri diversi.

Ma procediamo per gradi...

**Risoluzione del problema con una tabella**Proviamo dapprima a risolvere il problema con la forza bruta di una tabella.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Multipli di 3 + 2 | 2 | 5 | 8 | 11 | 14 | 17 | 20 | **23** | 26 |
| Multipli di 5 + 3 | 3 | 8 | 13 | 18 | **23** | 28 | 33 | 38 | 43 |
| Multipli di 7 + 2 | 2 | 9 | 16 | **23** | 30 | 37 | 44 | 51 | 58 |

E va bé, siamo stati fortunati. 23 è il più piccolo numero che soddisfa le condizioni date.
Se andassimo avanti troveremmo che anche 128, 233, ... sono soluzioni valide.
Anzi, le soluzioni sono infinite e si possono calcolare con la formula: x = 23 + 105u

**Risoluzione del problema con ragionamenti elementari ma un po' più raffinati**
La risoluzione sarà più lunga e laboriosa, ma fornirà una strategia generale.

**Quante sono le cose?**Dato un certo numero di cose, si sa che:
- dividendolo per 3 dà come resto 2,
- dividendolo per 5 dà come resto 3,
- dividendolo per 7 dà come resto 2.
Qual è il numero?

**Dividiamo questo problema in tre sottoproblemi** molto simili fra loro, le cui soluzioni addizionate daranno la soluzione del problema originale.

**Scholium: ma siamo sicuri che il problema ha una soluzione?
Le condizioni ce le dà il Teorema cinese del resto**

|  |  |
| --- | --- |
| **1° sottoproblema** | Trovare un numero che diviso per 3 dia resto 2 e che nello stesso tempo sia multiplo sia di 5 che di 7.5\*7 = 35, quindi il numero deve essere multiplo di 35.Toh! Guarda un po'! 35 = 33 + 2 perciò va già bene.**Primo numero = 35** |
| **2° sottoproblema** | Trovare un numero che diviso per 5 dia resto 3 e che nello stesso tempo sia multiplo sia di 3 che di 7.3\*7 = 21, quindi il numero deve essere multiplo di 21.In questo caso non siamo così fortunati, perciò recitiamo la **tabellina del 21** finché non troviamo un multiplo di 5 +2.21 - 42 - 63 - ...Wow! 63 va bene perché 63 = 60 + 3**Secondo numero = 63** **Scholium: come facciamo ad essere sicuri che tale numero esista?** |
| **3° sottoproblema** | Trovare un numero che diviso per 7 dia resto 2 e che nello stesso tempo sia multiplo sia di 5 che di 3.5\*3 = 15, quindi il numero deve essere multiplo di 15.Anche in questo caso recitiamo la **tabellina del 15**finché non troviamo un multiplo di 7 +2.15 - 30 - ...Che manna! 30 va bene!**Terzo numero = 30** **Scholium: non si può evitare di recitare la tabellina?** |

Ora addizioniamo i tre numeri e otteniamo un numero miracoloso, che risolve il problema.

**35 + 63 + 30 = 128**

Perché 128 è una soluzione del problema?
Perché soddisfa le tre condizioni del problema.
Infatti:

35 diviso per 3 dà come resto 2, mentre gli altri due numeri , 63, 30 sono multipli di 3 quindi addizionati a 35 non cambiano il resto della divisione.
**35 + 63 + 30 = 2 (mod 3)**

63 diviso per 5 dà come resto 3, mentre gli altri due numeri , 35, 30 sono multipli di 5 quindi addizionati a 63 non cambiano il resto della divisione.
**35 + 63 + 30 = 3 (mod 5)**

30 diviso per 7 dà come resto 2, mentre gli altri due numeri , 63, 35 sono multipli di 7 quindi addizionati a 30 non cambiano il resto della divisione.
**35 + 63 + 30 = 2 (mod 7)**

Il problema però, ha infinite soluzioni che si trovano aggiungendo o sottraendo a 128 i multipli di 3\*5\*7 = 105. Infatti 105, essendo multiplo di tutti i divisori, lascia invariati i resti delle divisioni.

La soluzione positiva più piccola è 128 - 105 = 23, perciò tutte le soluzioni possono essere espresse nella forma:

**x = 23 + k105**

Se ora vogliamo fare qualche passo avanti, dobbiamo studiare l'aritmetica modulare

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **L'Aritmetica modulare**I numeri di cui si parla nel seguito sono naturali.Per un piccolo approfondimento sugli interi relativi, vedi la pagina: [**Divisione, quoziente, resto**](http://utenti.quipo.it/base5/numeri/divquotresto.htm).**Definizione di congruenza modulo n**Due numeri a, b, sono detti uguali o congrui modulo n se e solo se n|(a-b)La scrittura **n|(a-b)** significa che n divide la differenza (a-b).Di solito a, b sono interi relativi mentre n è intero positivo.La congruenza modulo n si può esprimere così:**a = b (mod n)**ovvero, esiste un k intero per cui:**a - b = kna = kn + b****Esempi:**12 = 6 (mod 3), perché (12-6)/3 = 2 con resto 018 =/= 5 (mod 3), perché (18-5) non è divisibile per 318 = 23 (mod 5), perché (18-23)/5 = 1 con resto 045 = 3 (mod 7) perché 45/7 e 3/7 danno come resto 3, ovvero 45 = 7k + 3 (per un k intero)**Congruenza e resto delle divisioni**18 e 23 danno lo stesso resto se sono divisi per 5In generale tutti i numeri congrui modulo un certo numero n danno lo stesso resto se vengono divisi per n.La relazione di congruenza modulo n è una **relazione di equivalenza**, cioè gode delle proprietà simmetrica, riflessiva e transitiva.L'insieme di tutti i numeri congrui modulo n si chiama **classe di congruenza modulo n** e si denota con [a]n**Le classi di congruenza modulo n sono esattamente n**Siccome la divisione per n può dare esattamente n resti diversi, per ogni n esisteranno esattamente n insiemi [a]ndistinti**Esempio:**Esistono 5 insiemi distinti di numeri congrui modulo 5, [a]5[0]5 = {5, 10, 15, 20, ...}[1]5 = {6, 11, 16, 21, ...}[2]5 = {7, 12, 17, 22, ...}[3]5 = {8, 13, 18, 23, ...}[4]5 = {9, 14, 19, 24, ...}Per individuare una classe di congruenza conviene usare come **rappresentante**, il più piccolo dei suoi elementi, ciè l'effettivo resto della divisione.**Esempio:**[48]7 = [6]7 perché 6 è il resto della divisione 48/7**Come si trova il più piccolo degli elementi di una classe di congruenza?**Si deve calcolare il resto della divisione del numero dato per n**Esempio:**[453]6 = [3]6 perché 453/6 = 75,5; 75\*6 = 450; 453-450 = 3**Nota:**quando non c'é ambiguità si possono omettere le parentesi e i pedici e indicare una classe utilizzando soltanto un numerale. Inoltre si può indicare una classe utilizzando uno dei suoi rappresentanti.**Esistono infinite aritmetiche modulari, una per ogni modulo****Ogni singola aritmetica modulare è finita perché opera su un numero finito di elementi****Tra le classi di congruenza si possono definire le 3 operazioni: addizione, sottrazione, moltiplicazione****La divisione può essere definita solo in certi casi****Addizione di classi di congruenza**Si può dimostrare che se:a = b (mod n)c = d (mod n)allora(a+c) = (b+d) (mod n)Da ciò si ricava la regola:[a]n + [b]n = [a + b]n**Esempio:**[7]3 + [8]3 = [15]3 = [0]3**La tabella dell'addizione modulo 5**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **+** | **0** | **1** | **2** | **3** | **4** | **5** | **6** |
| **0** | 0 | 1 | 2 | 3 | 4 | 0 | 1 |
| **1** | 1 | 2 | 3 | 4 | 0 | 1 | 2 |
| **2** | 2 | 3 | 4 | 0 | 1 | 2 | 3 |
| **3** | 3 | 4 | 0 | 1 | 2 | 3 | 4 |
| **4** | 4 | 0 | 1 | 2 | 3 | 4 | 0 |
| **5** | 0 | 1 | 2 | 3 | 4 | 0 | 1 |
| **6** | 1 | 2 | 3 | 4 | 0 | 1 | 2 |

**Sottrazione di classi di congruenza**Analogamente si ricava la regola:[a]n - [b]n = [a - b]n**Esempio:**[17]3 - [6]3 = [11]3 = [2]3**La tabella della sottrazione modulo 5 (col-rig)**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **-** | **0** | **1** | **2** | **3** | **4** | **5** | **6** |
| **0** | 0 | 1 | 2 | 3 | 4 | 0 | 1 |
| **1** | 4 | 0 | 1 | 2 | 3 | 4 | 0 |
| **2** | 3 | 4 | 0 | 1 | 2 | 3 | 4 |
| **3** | 2 | 3 | 4 | 0 | 1 | 2 | 3 |
| **4** | 1 | 2 | 3 | 4 | 0 | 1 | 2 |
| **5** | 0 | 1 | 2 | 3 | 4 | 0 | 1 |
| **6** | 4 | 0 | 1 | 2 | 3 | 4 | 0 |

**Moltiplicazione di classi di congruenza**Si può dimostrare che se:a = b (mod n)c = d (mod n)allora(a×c) = (b×d) (mod n)Da ciò si ricava la regola:[a]n × [b]n = [a × b]n**Esempio:**[5]2 × [7]2 = [35]2 = [1]2**La tabella della moltiplicazione modulo 5**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **x** | **0** | **1** | **2** | **3** | **4** | **5** | **6** |
| **0** | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **1** | 0 | 1 | 2 | 3 | 4 | 0 | 1 |
| **2** | 0 | 2 | 4 | 1 | 3 | 0 | 2 |
| **3** | 0 | 3 | 1 | 4 | 2 | 0 | 3 |
| **4** | 0 | 4 | 3 | 2 | 1 | 0 | 4 |
| **5** | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **6** | 0 | 1 | 2 | 3 | 4 | 0 | 1 |

**Divisione di classi di congruenza**La divisione può essere definita univocamente solo nelle aritmetiche modulo n, numero primo.(da approfondire)**La tabella della divisione modulo 5 (col/rig)**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **:** | **0** | **1** | **2** | **3** | **4** | **5** | **6** |
| **0** |  |  |  |  |  |  |  |
| **1** | 0 | 1 | 2 | 3 | 4 | 0 | 1 |
| **2** | 0 | 3 | 1 | 4 | 2 | 0 | 3 |
| **3** | 0 | 2 | 4 | 1 | 3 | 0 | 2 |
| **4** | 0 | 4 | 3 | 2 | 1 | 0 | 4 |
| **5** | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **6** | 0 | 1 | 2 | 3 | 4 | 0 | 1 |

**Esempi:**Nell'aritmetica modulo 5,3/2 = 4 perché 4\*2 = 34/3 = 3 perché 3\*3 = 40/2 = 0 perché 0\*2 = 0Nell'aritmetica modulo 6,3/2 = ? non c'è nessun numero che moltiplicato per 2 dia 34/2 = ? 2\*2 = 4 e 5\*2 = 4 dunque esistono due possibili risultati |

Con questi nuovi strumenti possiamo tradurre il problema iniziale in un sistema di equazioni modulari (niente panico!)

**Quante sono le cose?**Dato un certo numero di cose, si sa che:
- dividendolo per 3 dà come resto 2,
- dividendolo per 5 dà come resto 3,
- dividendolo per 7 dà come resto 2.
Qual è il numero?

Chiamiamo x il numero cercato.

x = 2 (mod 3) perché x e 2 danno lo stesso resto se divisi per 3
x = 3 (mod 5)
x = 2 (mod 7)

La soluzione trovata può esser espressa così:

**x = 23 + k105**ovvero**x = 23 (mod 105)**

NOTA BENE: 3, 5, 7 sono primi fra loro e 105 è il loro mcm

Proviamo a risolvere un altro problema classico.

**Uova con resto**Una contadina porta delle uova al mercato. Sa che contandole a 2 a 2 ne avanzava 1, contandole a 3 a 3 ne avanzava 1, a 4 a 4 ne avanzava 1, a 5 a 5 ne avanzava 1, a 6 a 6 ne avanzava 1 e contandole a 7 a 7 aveva un numero esatto. Quante uova?
**RISPOSTA: 301, ovvero 301 più un multiplo di 420. Così Leonardo Pisano, pag. 281.**

x = 1 (mod 2)
x = 1 (mod 3)
x = 1 (mod 4)
x = 1 (mod 5)
x = 1 (mod 6)
x = 0 (mod 7)

In questo caso 2, 3, 4, 5, 6, 7 NON sono primi fra loro.
Una soluzione veloce è data dal seguente ragionamento: il numero più piccolo che dà resto 1 quando è diviso per 2, 3, 4, 5, 6 è mcm(2,3,4,5,6) + 1 = 60 + 1 = 61.
La soluzione generale delle prime 5 equazioni è **61 + k60 = 1 (mod 60)**La 6° equazione chiede di scegliere fra le soluzioni trovate, quelle divisibili per 7.
Recitiamo la tabellina del 7 (\*3, \*13, \*23, ...) fin che non troviamo un multiplo di 60 + 1.
**7\*43 = 60\*5 + 1 = 301**

Dunque la soluzione generale è:
**x = 301 + k(mcm(2,3,4,5,6,7) = 301 + k420**

**Utilizzando l'aritmetica modulare si può evitare la tabellina del 7 (o quasi)**Sostituisco la soluzione delle prime cinque equazioni nella settima equazione: **x = 61 + k60 = 0 (mod 7)
k60 = -61 (mod 7)
k = -61/60 = -5/4 = -3 = 4 (mod 7)**, perché la divisione (mod 7) è definita, essendo 7 un numero primo **x = 61 + 240 = 301**

Mi fuma il cervello!

|  |
| --- |
| **Le equazioni lineari modulo n**Nel seguito:MCD(a,b) significa Massimo Comun Divisore di a, b, si usa anche indicare (a,b)mcm(a,b) significa minimo comune multiplo di a, b, si usa anche indicare [a,b]Un'equazione lineare modulo n è un'uguaglianza del tipo:**ax = b (mod n)**dove x è l'incognita, numero intero.**La soluzione esiste se e solo se il MCD(a,n) divide b.**Inoltre l'equazione ha esattamente d soluzioni distinte (non congruenti mod n) con d = MCD(a,n)Per trovarla si effettuano i seguenti passi:- si calcola d = MCD(a,n)- si usa l'algoritmo di Euclide per determinare h e k in modo che: d = ha + kn- si determina un p tale che b = p\*dUna soluzione è x = phLe altre soluzioni si ottengono aggiungendo alla prima n/d, 2n/d, ... e così via.**Esempio:**14x = 26(mod 4)Verifico l'esistenza della soluzioneMCD(14,4) = 2, che divide 26, quindi la soluzione esiste, anzi, ne esistono due distinte.Trovo la soluzioneTrovo h, k tali che 2 = 14h + 4kh = 1; k = -3Ora trovo p tale che 26 = p\*2p = 13Quindi una soluzione è:ph = 13\*1 = 13La seconda soluzione è:13 + 2 = 15Verifica14\*13 = 26(mod 4)182 = 26(mod 4) = 2(mod 4)(182-26)/4 = 156/4 = 39 resto 0 (verificato)Altra verifica182/4 = 180 resto 226/4 = 6 resto 2Verifica14\*15 = 26(mod 4)210 = 2(mod 4)(210 - 2)/4 = 52 resto 0 (verificato)Inoltre13 =/= 15 (mod 4) |
| **Il teorema cinese del resto****Teorema**Il sistema di congruenze:**x = a (mod n)x = b (mod m)****ha soluzione se e solo se:MCD(m,n) divide (a-b)**ovvero se e solo se:a = b (mod MCD(n,m))ovvero se e solo se:a-b = k(MCD(m,n)**a = k(MCD(m,n) + b**Inoltre la soluzione, se c'è, è unica ed è del tipo:x = c (mod mcm(n,m))ovvero:**x = c+k\*mcm(n,m)** al variare di k intero**Esempio:**Dato un certo numero di arancene avanzano 6 , se disposte a gruppi di 7ne avanzano 5 , se disposte a gruppi di 9Quante sono le arance?x = 6 (mod 7)x = 5 (mod 9)MCD(7,9) = 1 divide (6-5), quindi la soluzione esiste.x = 7t + 6 = 5 (mod 9)7t = 5 (mod 9) - 6 = 8 (mod 9)Questo passaggio mi porta ad una unica equazione nell'incognita t alla quale applico la procedura vista sopra:7t = 8 (mod 9)MCD(7,9) = 11 = 7h +9k; h = 4; k = -38 = p\*1; p = 8t = ph = 32x = 7t + 6 = 230Siccome mcm(7,9) = 63, la soluzione è:x = 230 + 63k = 230 (mod 63) = 41 (mod 63) |

**Quante sono le cose?**Dato un certo numero di cose, si sa che:
- dividendolo per 3 dà come resto 2,
- dividendolo per 5 dà come resto 3,
- dividendolo per 7 dà come resto 2.
Qual è il numero?
**Sun Tsu Suan-Ching (300 a. C.)**

**Uova con resto**Una contadina porta delle uova al mercato. Sa che contandole a 2 a 2 ne avanzava 1, contandole a 3 a 3 ne avanzava 1, a 4 a 4 ne avanzava 1, a 5 a 5 ne avanzava 1, a 6 a 6 ne avanzava 1 e contandole a 7 a 7 aveva un numero esatto. Quante uova?
**RISPOSTA: 301, ovvero 301 più un multiplo di 420. Così Leonardo Pisano, pag. 281.**

**Le tre Grazie**Le tre Grazie portando pomi, ognuna lo stesso numero, incontrano le nove Muse, e con loro dividono i pomi, sicché tutte hanno lo stesso numero di pomi. Quanti erano i pomi?
RISPOSTA: 12 o un suo multiplo.
**Questo problema è estratto dall'Antologia greca; questo libro, dei tempi dell'imperatore Traiano, morto nell'anno 117, contiene in versi greci vari problemi, alcuni antichissimi.**

**Le nove Muse**Le nove Muse, portando ognuna lo stesso numero di corone, incontrano le tre Grazie e loro distribuiscono delle corone, e tutte ne hanno lo stesso numero. Quante corone?
**RISPOSTA: un multiplo di 9 e di 12, cioè di 36.. Dall'Antologia greca.**

**Tre interi**Tre interi X,Y,Z hanno la seguente proprieta':
X\*Y non e' divisibile per Z, difatti c'e' il resto di 1.
X\*Z non e' divisibile per Y, difatti c'e' il resto di 1.
Y\*Z non e' divisibile per X, difatti c'e' il resto di 1.

Non e' difficile trovare i 3 numeri.
Dimostrare che questa soluzione e' unica.

**Dal newsgroup it.hobby.enigmi ho trovato questo problema proposto da Dario Uri**

**Arance 1**
Dato un certo numero di arance
ne avanzano 2 , se disposte a gruppi di 5
ne avanzano 6 , se disposte a gruppi di 7
Quante sono le arance?

**Arance 2**Dato un certo numero di arance
ne avanzano 4 , se disposte a gruppi di 17
ne avanzano 8 , se disposte a gruppi di 11
Quante sono le arance?

**Arance 3**Dato un certo numero di arance
ne avanzano 8 , se disposte a gruppi di 26
ne avanzano 3 , se disposte a gruppi di 5
ne avanzano 3 , se disposte a gruppi di 11
Quante sono le arance?

**Arance 4**
Dato un certo numero di arance
ne avanzano 2 , se disposte a gruppi di 4
ne avanzano 4 , se disposte a gruppi di 13
ne avanzano 3 , se disposte a gruppi di 19
ne avanzano 2 , se disposte a gruppi di 9
Quante sono le arance?

**Sistema**Risolvere il sistema di congruenze
x = 8 modulo 11
x = 3 modulo 5
x = 4 modulo 13
x = 2 modulo 4