

Congruenze

L'aritmetica dell'orologio

Dipartimento di Informatica

Olimpiadi della Matematica

31 marzo 2006

Tutti sanno benissimo che se mettiamo

Tutti sanno benissimo che se mettiamo
quarantaquattro gatti in fila per sei

Tutti sanno benissimo che se mettiamo
quarantaquattro gatti in fila per sei
ne restano fuori due

Tutti sanno benissimo che se mettiamo
quarantaquattro gatti in fila per sei
ne restano fuori due

Più in generale, supponiamo di dover dividere una certa quantità di cose fra più persone

I quaranta ladroni della famosa favola di Alì Babà si ritrovano nella loro caverna (“Apriți, Sesamo”) e si siedono per dividersi il bottino

I quaranta ladroni della famosa favola di Alì Babà si ritrovano nella loro caverna (“Apriți, Sesamo”) e si siedono per dividersi il bottino

Sono ladroni modernizzati e il bottino consiste in un sacco pieno di banconote da 100 Euro

I quaranta ladroni della famosa favola di Alì Babà si ritrovano nella loro caverna (“Apriți, Sesamo”) e si siedono per dividersi il bottino

Sono ladroni modernizzati e il bottino consiste in un sacco pieno di banconote da 100 Euro

Come fanno a dividersi in parti uguali il bottino senza dover contare tutte le banconote?

I quaranta ladroni della famosa favola di Alì Babà si ritrovano nella loro caverna (“Apriți, Sesamo”) e si siedono per dividersi il bottino

Sono ladroni modernizzati e il bottino consiste in un sacco pieno di banconote da 100 Euro

Come fanno a dividersi in parti uguali il bottino senza dover contare tutte le banconote?

Fra l'altro, sono sì ladroni moderni,

I quaranta ladroni della famosa favola di Alì Babà si ritrovano nella loro caverna (“Apri, Sesamo”) e si siedono per dividersi il bottino

Sono ladroni modernizzati e il bottino consiste in un sacco pieno di banconote da 100 Euro

Come fanno a dividersi in parti uguali il bottino senza dover contare tutte le banconote?

Fra l'altro, sono sì ladroni moderni, ma ignorano l'aritmetica e non sanno eseguire le divisioni con due cifre e la divisione va fatta in 41 parti, perché il capo conta per due

Per sistemare la cosa dal punto di vista matematico, chiamiamo a il numero di cose da dividere e b il numero di persone tra cui eseguire la divisione

Per sistemare la cosa dal punto di vista matematico, chiamiamo a il numero di cose da dividere e b il numero di persone tra cui eseguire la divisione
Naturalmente $b > 0$, altrimenti non c'è niente da fare

Per sistemare la cosa dal punto di vista matematico, chiamiamo a il numero di cose da dividere e b il numero di persone tra cui eseguire la divisione. Naturalmente $b > 0$, altrimenti non c'è niente da fare. Il metodo trovato prima ci permette di dire che esistono due numeri q e r tali che

$$a = bq + r$$

$$r < b$$

Per sistemare la cosa dal punto di vista matematico, chiamiamo a il numero di cose da dividere e b il numero di persone tra cui eseguire la divisione. Naturalmente $b > 0$, altrimenti non c'è niente da fare. Il metodo trovato prima ci permette di dire che esistono due numeri q e r tali che

$$a = bq + r \qquad r < b$$

Il *quoziente* q è la quantità che va a ciascuno,

Per sistemare la cosa dal punto di vista matematico, chiamiamo a il numero di cose da dividere e b il numero di persone tra cui eseguire la divisione. Naturalmente $b > 0$, altrimenti non c'è niente da fare. Il metodo trovato prima ci permette di dire che esistono due numeri q e r tali che

$$a = bq + r \qquad r < b$$

Il *quoziente* q è la quantità che va a ciascuno, il *resto* r è quanto rimane e non può essere diviso.

Unicità del quoziente e del resto

Possiamo immaginare altri metodi per eseguire la divisione del bottino; chi ci dice che il quoziente e il resto siano invariabilmente gli stessi?

Unicità del quoziente e del resto

Possiamo immaginare altri metodi per eseguire la divisione del bottino; chi ci dice che il quoziente e il resto siano invariabilmente gli stessi?

Lo *dimostriamo*

Unicità del quoziente e del resto

Possiamo immaginare altri metodi per eseguire la divisione del bottino; chi ci dice che il quoziente e il resto siano invariabilmente gli stessi?

Lo *dimostriamo*

Il metodo A dà il quoziente q e il resto r :

$$a = bq + r$$

$$r < b$$

Unicità del quoziente e del resto

Possiamo immaginare altri metodi per eseguire la divisione del bottino; chi ci dice che il quoziente e il resto siano invariabilmente gli stessi?

Lo *dimostriamo*

Il metodo A dà il quoziente q e il resto r :

$$a = bq + r \qquad r < b$$

Il metodo B dà il quoziente q' e il resto r' :

$$a = bq' + r' \qquad r' < b$$

Unicità del quoziente e del resto

Possiamo immaginare altri metodi per eseguire la divisione del bottino; chi ci dice che il quoziente e il resto siano invariabilmente gli stessi?

Lo *dimostriamo*

Il metodo A dà il quoziente q e il resto r :

$$a = bq + r \qquad r < b$$

Il metodo B dà il quoziente q' e il resto r' :

$$a = bq' + r' \qquad r' < b$$

Supponiamo, per assurdo, che i due resti siano diversi e che il metodo A dia il resto maggiore

Unicità del quoziente e del resto

Possiamo immaginare altri metodi per eseguire la divisione del bottino; chi ci dice che il quoziente e il resto siano invariabilmente gli stessi?

Lo *dimostriamo*

Il metodo A dà il quoziente q e il resto r :

$$a = bq + r \qquad r < b$$

Il metodo B dà il quoziente q' e il resto r' :

$$a = bq' + r' \qquad r' < b$$

Supponiamo, per assurdo, che i due resti siano diversi e che il metodo A dia il resto maggiore

$$r' < r$$

Unicità del quoziente e del resto

Abbiamo, dalle ipotesi precedenti

$$a = bq + r = bq' + r'$$

$$r' < r < b$$

Unicità del quoziente e del resto

Abbiamo, dalle ipotesi precedenti

$$a = bq + r = bq' + r'$$

$$r' < r < b$$

Possiamo scrivere allora

$$r - r' = b(q' - q) > 0$$

Unicità del quoziente e del resto

Abbiamo, dalle ipotesi precedenti

$$a = bq + r = bq' + r'$$

$$r' < r < b$$

Possiamo scrivere allora

$$r - r' = b(q' - q) > 0$$

Quindi $q' - q > 0$ e perciò $b(q' - q) \geq b$

Unicità del quoziente e del resto

Abbiamo, dalle ipotesi precedenti

$$a = bq + r = bq' + r' \qquad r' < r < b$$

Possiamo scrivere allora

$$r - r' = b(q' - q) > 0$$

Quindi $q' - q > 0$ e perciò $b(q' - q) \geq b$

Ma $r - r' < r$

Unicità del quoziente e del resto

Abbiamo, dalle ipotesi precedenti

$$a = bq + r = bq' + r'$$

$$r' < r < b$$

Possiamo scrivere allora

$$r - r' = b(q' - q) > 0$$

Quindi $q' - q > 0$ e perciò $b(q' - q) \geq b$

Ma $r - r' < r < b$



Unicità del quoziente e del resto

Abbiamo, dalle ipotesi precedenti

$$a = bq + r = bq' + r'$$

$$r' < r < b$$

Possiamo scrivere allora

$$r - r' = b(q' - q) > 0$$

Quindi $q' - q > 0$ e perciò $b(q' - q) \geq b$

Ma $r - r' < r < b$



Quindi deve essere $r = r'$

Unicità del quoziente e del resto

Abbiamo allora dimostrato che il metodo A e il metodo B danno lo stesso resto

Unicità del quoziente e del resto

Abbiamo allora dimostrato che il metodo A e il metodo B danno lo stesso resto

$$a = bq + r = bq' + r$$

Unicità del quoziente e del resto

Abbiamo allora dimostrato che il metodo A e il metodo B danno lo stesso resto

$$a = bq + r = bq' + r$$

Quindi possiamo scrivere

$$bq = bq'$$

e dunque, siccome $b > 0$,

Unicità del quoziente e del resto

Abbiamo allora dimostrato che il metodo A e il metodo B danno lo stesso resto

$$a = bq + r = bq' + r$$

Quindi possiamo scrivere

$$bq = bq'$$

e dunque, siccome $b > 0$,

$$q = q'$$

Unicità del quoziente e del resto

Abbiamo allora dimostrato che il metodo A e il metodo B danno lo stesso resto

$$a = bq + r = bq' + r$$

Quindi possiamo scrivere

$$bq = bq'$$

e dunque, siccome $b > 0$,

$$q = q'$$

Il metodo A e il metodo B *danno lo stesso risultato* di quoziente e resto

Possiamo allora definire una nuova operazione:

$$a \% b \quad (a \bmod b)$$

Possiamo allora definire una nuova operazione:

$$a \% b \quad (a \bmod b)$$

è il resto della divisione di a per b . Come per la divisione, c'è la restrizione che $b > 0$.

Possiamo allora definire una nuova operazione:

$$a \% b \quad (a \bmod b)$$

è il resto della divisione di a per b . Come per la divisione, c'è la restrizione che $b > 0$.

Il risultato di $a \% b$ è sempre un numero naturale *minore di b* .

Possiamo allora definire una nuova operazione:

$$a \% b \quad (a \bmod b)$$

è il resto della divisione di a per b . Come per la divisione, c'è la restrizione che $b > 0$.

Il risultato di $a \% b$ è sempre un numero naturale *minore di* b .
Come facciamo se vogliamo usare anche numeri interi negativi?

Diremo che r è il resto della divisione di a per b se

$$a = bq + r$$

Diremo che r è il resto della divisione di a per b se

$$a = bq + r \quad \text{e} \quad 0 \leq r < |b|$$

Diremo che r è il resto della divisione di a per b se

$$a = bq + r \quad \text{e} \quad 0 \leq r < |b|$$

Come determiniamo r e q ?

Resto e numeri interi

Diremo che r è il resto della divisione di a per b se

$$a = bq + r \quad \text{e} \quad 0 \leq r < |b|$$

Come determiniamo r e q ? Non come prima, se a o b sono negativi.

Diremo che r è il resto della divisione di a per b se

$$a = bq + r \quad \text{e} \quad 0 \leq r < |b|$$

Come determiniamo r e q ? Non come prima, se a o b sono negativi.

Facciamo prima il caso di $b > 0$ e $a < 0$: invece che sottrarre b più e più volte, sommiamo, fino a che troviamo il resto.

Diremo che r è il resto della divisione di a per b se

$$a = bq + r \quad \text{e} \quad 0 \leq r < |b|$$

Come determiniamo r e q ? Non come prima, se a o b sono negativi.

Facciamo prima il caso di $b > 0$ e $a < 0$: invece che sottrarre b più e più volte, sommiamo, fino a che troviamo il resto.

Se invece $b < 0$ e a è qualunque, vediamo subito da che parte andare e sommiamo o sottraiamo.

Diremo che r è il resto della divisione di a per b se

$$a = bq + r \quad \text{e} \quad 0 \leq r < |b|$$

Come determiniamo r e q ? Non come prima, se a o b sono negativi.

Facciamo prima il caso di $b > 0$ e $a < 0$: invece che sottrarre b più e più volte, sommiamo, fino a che troviamo il resto.

Se invece $b < 0$ e a è qualunque, vediamo subito da che parte andare e sommiamo o sottraiamo.

La stessa dimostrazione di prima fa vedere che resto e quoziente sono unici.

Dividiamo -44 per 6 :

Dividiamo -44 per 6 :

$$-44 + 6 = -38$$

Dividiamo -44 per 6 :

$$-44 + 6 = -38 \quad -38 + 6 = -32$$

Resto e numeri interi — Esempi

Dividiamo -44 per 6 :

$$-44 + 6 = -38 \quad -38 + 6 = -32 \quad -32 + 6 = -26$$

Resto e numeri interi — Esempi

Dividiamo -44 per 6 :

$$-44 + 6 = -38 \quad -38 + 6 = -32 \quad -32 + 6 = -26$$

$$-26 + 6 = -20$$

Dividiamo -44 per 6 :

$$\begin{array}{l} -44 + 6 = -38 \quad -38 + 6 = -32 \quad -32 + 6 = -26 \\ -26 + 6 = -20 \quad -20 + 6 = -14 \end{array}$$

Dividiamo -44 per 6 :

$$\begin{array}{lll} -44 + 6 = -38 & -38 + 6 = -32 & -32 + 6 = -26 \\ -26 + 6 = -20 & -20 + 6 = -14 & -14 + 6 = -8 \end{array}$$

Dividiamo -44 per 6 :

$$-44 + 6 = -38 \quad -38 + 6 = -32 \quad -32 + 6 = -26$$

$$-26 + 6 = -20 \quad -20 + 6 = -14 \quad -14 + 6 = -8$$

$$-8 + 6 = -2$$

Resto e numeri interi — Esempi

Dividiamo -44 per 6 :

$$-44 + 6 = -38 \quad -38 + 6 = -32 \quad -32 + 6 = -26$$

$$-26 + 6 = -20 \quad -20 + 6 = -14 \quad -14 + 6 = -8$$

$$-8 + 6 = -2 \quad -2 + 6 = 4$$

Resto e numeri interi — Esempi

Dividiamo -44 per 6 :

$$-44 + 6 = -38 \quad -38 + 6 = -32 \quad -32 + 6 = -26$$

$$-26 + 6 = -20 \quad -20 + 6 = -14 \quad -14 + 6 = -8$$

$$-8 + 6 = -2 \quad -2 + 6 = 4$$

Dividiamo -44 per -15 :

Dividiamo -44 per 6 :

$$-44 + 6 = -38 \quad -38 + 6 = -32 \quad -32 + 6 = -26$$

$$-26 + 6 = -20 \quad -20 + 6 = -14 \quad -14 + 6 = -8$$

$$-8 + 6 = -2 \quad -2 + 6 = 4$$

Dividiamo -44 per -15 :

$$-44 - (-15) = -29$$

Dividiamo -44 per 6 :

$$-44 + 6 = -38 \quad -38 + 6 = -32 \quad -32 + 6 = -26$$

$$-26 + 6 = -20 \quad -20 + 6 = -14 \quad -14 + 6 = -8$$

$$-8 + 6 = -2 \quad -2 + 6 = 4$$

Dividiamo -44 per -15 :

$$-44 - (-15) = -29 \quad -29 - (-15) = -14$$

Dividiamo -44 per 6 :

$$-44 + 6 = -38 \quad -38 + 6 = -32 \quad -32 + 6 = -26$$

$$-26 + 6 = -20 \quad -20 + 6 = -14 \quad -14 + 6 = -8$$

$$-8 + 6 = -2 \quad -2 + 6 = 4$$

Dividiamo -44 per -15 :

$$-44 - (-15) = -29 \quad -29 - (-15) = -14$$

$$-14 - (-15) = 1$$

Dividiamo -44 per 6 :

$$-44 + 6 = -38 \quad -38 + 6 = -32 \quad -32 + 6 = -26$$

$$-26 + 6 = -20 \quad -20 + 6 = -14 \quad -14 + 6 = -8$$

$$-8 + 6 = -2 \quad -2 + 6 = 4$$

Dividiamo -44 per -15 :

$$-44 - (-15) = -29 \quad -29 - (-15) = -14$$

$$-14 - (-15) = 1$$

Dividiamo 44 per -13 :

Dividiamo -44 per 6 :

$$-44 + 6 = -38 \quad -38 + 6 = -32 \quad -32 + 6 = -26$$

$$-26 + 6 = -20 \quad -20 + 6 = -14 \quad -14 + 6 = -8$$

$$-8 + 6 = -2 \quad -2 + 6 = 4$$

Dividiamo -44 per -15 :

$$-44 - (-15) = -29 \quad -29 - (-15) = -14$$

$$-14 - (-15) = 1$$

Dividiamo 44 per -13 :

$$44 + (-13) = 31$$

Dividiamo -44 per 6 :

$$-44 + 6 = -38 \quad -38 + 6 = -32 \quad -32 + 6 = -26$$

$$-26 + 6 = -20 \quad -20 + 6 = -14 \quad -14 + 6 = -8$$

$$-8 + 6 = -2 \quad -2 + 6 = 4$$

Dividiamo -44 per -15 :

$$-44 - (-15) = -29 \quad -29 - (-15) = -14$$

$$-14 - (-15) = 1$$

Dividiamo 44 per -13 :

$$44 + (-13) = 31 \quad 31 + (-13) = 18$$

Dividiamo -44 per 6 :

$$-44 + 6 = -38 \quad -38 + 6 = -32 \quad -32 + 6 = -26$$

$$-26 + 6 = -20 \quad -20 + 6 = -14 \quad -14 + 6 = -8$$

$$-8 + 6 = -2 \quad -2 + 6 = 4$$

Dividiamo -44 per -15 :

$$-44 - (-15) = -29 \quad -29 - (-15) = -14$$

$$-14 - (-15) = 1$$

Dividiamo 44 per -13 :

$$44 + (-13) = 31 \quad 31 + (-13) = 18 \quad 18 + (-13) = 5$$

Qual è la regola pratica?

Divisione nella realtà di tutti i giorni

Divisione nella realtà di tutti i giorni

Che cos'hanno in comune tutti i lunedì?

Che cos'hanno in comune tutti i mezzogiorno?

Divisione nella realtà di tutti i giorni

Che cos'hanno in comune tutti i lunedì?

Che cos'hanno in comune tutti i mezzogiorno?

Se passano 72 ore da adesso, che ore saranno?

Divisione nella realtà di tutti i giorni

Che cos'hanno in comune tutti i lunedì?

Che cos'hanno in comune tutti i mezzogiorno?

Se passano 72 ore da adesso, che ore saranno?

Non teniamo conto della riforma del calendario e basiamoci sull'usanza moderna di contare i giorni della settimana a partire dal lunedì.

Divisione nella realtà di tutti i giorni

Che cos'hanno in comune tutti i lunedì?

Che cos'hanno in comune tutti i mezzogiorno?

Se passano 72 ore da adesso, che ore saranno?

Non teniamo conto della riforma del calendario e basiamoci sull'usanza moderna di contare i giorni della settimana a partire dal lunedì.

Assumiamo che il giorno 1 gennaio dell'anno 1 sia stato di lunedì e numeriamo tutti i giorni.

Che cos'hanno in comune tutti i lunedì?

Divisione nella realtà di tutti i giorni

Che cos'hanno in comune tutti i lunedì?

Che cos'hanno in comune tutti i mezzogiorno?

Se passano 72 ore da adesso, che ore saranno?

Non teniamo conto della riforma del calendario e basiamoci sull'usanza moderna di contare i giorni della settimana a partire dal lunedì.

Assumiamo che il giorno 1 gennaio dell'anno 1 sia stato di lunedì e numeriamo tutti i giorni.

Che cos'hanno in comune tutti i lunedì?

Che il numero del giorno diviso per 7 dà resto 1

Fissiamo un intero $n > 0$

Fissiamo un intero $n > 0$

Diciamo che gli interi a e b sono *congruenti modulo n* se

$$a \% n = b \% n$$

cioè se la divisione di a e b per n dà lo stesso resto

Fissiamo un intero $n > 0$

Diciamo che gli interi a e b sono *congruenti modulo n* se

$$a \% n = b \% n$$

cioè se la divisione di a e b per n dà lo stesso resto

Scriveremo, in questo caso

$$a \equiv b \pmod{n}$$

oppure

$$a \equiv_n b$$

C'è un altro modo di esprimere la relazione $a \equiv b \pmod{n}$?

C'è un altro modo di esprimere la relazione $a \equiv b \pmod{n}$?

Prendiamo due numeri a e b tali che $a \equiv b \pmod{n}$

C'è un altro modo di esprimere la relazione $a \equiv b \pmod{n}$?

Prendiamo due numeri a e b tali che $a \equiv b \pmod{n}$

Allora $a = nx + r$ e $b = ny + r$, quindi

C'è un altro modo di esprimere la relazione $a \equiv b \pmod{n}$?

Prendiamo due numeri a e b tali che $a \equiv b \pmod{n}$

Allora $a = nx + r$ e $b = ny + r$, quindi

$$a - b = (nx + r) - (ny + r) =$$

C'è un altro modo di esprimere la relazione $a \equiv b \pmod{n}$?

Prendiamo due numeri a e b tali che $a \equiv b \pmod{n}$

Allora $a = nx + r$ e $b = ny + r$, quindi

$$a - b = (nx + r) - (ny + r) = nx + r - ny - r =$$

C'è un altro modo di esprimere la relazione $a \equiv b \pmod{n}$?

Prendiamo due numeri a e b tali che $a \equiv b \pmod{n}$

Allora $a = nx + r$ e $b = ny + r$, quindi

$$a - b = (nx + r) - (ny + r) = nx + r - ny - r = n(x - y)$$

C'è un altro modo di esprimere la relazione $a \equiv b \pmod{n}$?

Prendiamo due numeri a e b tali che $a \equiv b \pmod{n}$

Allora $a = nx + r$ e $b = ny + r$, quindi

$$a - b = (nx + r) - (ny + r) = nx + r - ny - r = n(x - y)$$

cioè $a - b$ è **un multiplo di n**

Supponiamo adesso che $a - b$ sia un multiplo di n :

$$a - b = nk$$

che si può scrivere anche $a = nk + b$

Supponiamo adesso che $a - b$ sia un multiplo di n :

$$a - b = nk$$

che si può scrivere anche $a = nk + b$

Possiamo eseguire la divisione di b per n :

$$b = nq + r$$

Supponiamo adesso che $a - b$ sia un multiplo di n :

$$a - b = nk$$

che si può scrivere anche $a = nk + b$

Possiamo eseguire la divisione di b per n :

$$b = nq + r$$

Ma allora

$$a = nk + b =$$

Supponiamo adesso che $a - b$ sia un multiplo di n :

$$a - b = nk$$

che si può scrivere anche $a = nk + b$

Possiamo eseguire la divisione di b per n :

$$b = nq + r$$

Ma allora

$$a = nk + b = nk + nq + r =$$

Supponiamo adesso che $a - b$ sia un multiplo di n :

$$a - b = nk$$

che si può scrivere anche $a = nk + b$

Possiamo eseguire la divisione di b per n :

$$b = nq + r$$

Ma allora

$$a = nk + b = nk + nq + r = n(k + q) + r$$

e quindi

Supponiamo adesso che $a - b$ sia un multiplo di n :

$$a - b = nk$$

che si può scrivere anche $a = nk + b$

Possiamo eseguire la divisione di b per n :

$$b = nq + r$$

Ma allora

$$a = nk + b = nk + nq + r = n(k + q) + r$$

e quindi

$$r = b \% n =$$

Supponiamo adesso che $a - b$ sia un multiplo di n :

$$a - b = nk$$

che si può scrivere anche $a = nk + b$

Possiamo eseguire la divisione di b per n :

$$b = nq + r$$

Ma allora

$$a = nk + b = nk + nq + r = n(k + q) + r$$

e quindi

$$r = b \% n = a \% n$$

cioè

$$a \equiv b \pmod{n}$$

Congruenze e operazioni

Supponiamo che $a \equiv b \pmod{n}$ e che $c \equiv d \pmod{n}$

Congruenze e operazioni

Supponiamo che $a \equiv b \pmod{n}$ e che $c \equiv d \pmod{n}$

Allora $a - b = nx$ e $c - d = ny$; dunque

Congruenze e operazioni

Supponiamo che $a \equiv b \pmod{n}$ e che $c \equiv d \pmod{n}$

Allora $a - b = nx$ e $c - d = ny$; dunque

$$(a - b) + (c - d) = nx + ny$$

Congruenze e operazioni

Supponiamo che $a \equiv b \pmod{n}$ e che $c \equiv d \pmod{n}$

Allora $a - b = nx$ e $c - d = ny$; dunque

$$(a - b) + (c - d) = nx + ny$$

che si può scrivere anche

$$(a + c) - (b + d) = n(x + y)$$

Congruenze e operazioni

Supponiamo che $a \equiv b \pmod{n}$ e che $c \equiv d \pmod{n}$

Allora $a - b = nx$ e $c - d = ny$; dunque

$$(a - b) + (c - d) = nx + ny$$

che si può scrivere anche

$$(a + c) - (b + d) = n(x + y)$$

$$\begin{array}{r} a \equiv b \pmod{n} \\ c \equiv d \pmod{n} \\ \hline (a + c) \equiv (b + d) \pmod{n} \end{array}$$

Congruenze e operazioni

Supponiamo che $a \equiv b \pmod{n}$ e che $c \equiv d \pmod{n}$

Allora $a - b = nx$ e $c - d = ny$; dunque

$$(a - b) + (c - d) = nx + ny$$

che si può scrivere anche

$$(a + c) - (b + d) = n(x + y)$$

$$\begin{array}{r} a \equiv b \pmod{n} \\ c \equiv d \pmod{n} \\ \hline (a + c) \equiv (b + d) \pmod{n} \end{array}$$

Le congruenze possono essere sommate come le uguaglianze

Supponiamo di nuovo che $a \equiv b \pmod{n}$ e che $c \equiv d \pmod{n}$

Supponiamo di nuovo che $a \equiv b \pmod{n}$ e che $c \equiv d \pmod{n}$

Possiamo moltiplicare le congruenze come le uguaglianze?

Cioè, è vero che $ac \equiv bd \pmod{n}$?

Congruenze e operazioni

Supponiamo di nuovo che $a \equiv b \pmod{n}$ e che $c \equiv d \pmod{n}$

Possiamo moltiplicare le congruenze come le uguaglianze?

Cioè, è vero che $ac \equiv bd \pmod{n}$?

$$44 \equiv 2 \pmod{6} \quad 28 \equiv 4 \pmod{6}$$

Supponiamo di nuovo che $a \equiv b \pmod{n}$ e che $c \equiv d \pmod{n}$

Possiamo moltiplicare le congruenze come le uguaglianze?

Cioè, è vero che $ac \equiv bd \pmod{n}$?

$$44 \equiv 2 \pmod{6} \quad 28 \equiv 4 \pmod{6}$$

$$44 \cdot 28 = 1232 \quad 1232 = 205 \cdot 6 + 2$$

Supponiamo di nuovo che $a \equiv b \pmod{n}$ e che $c \equiv d \pmod{n}$

Possiamo moltiplicare le congruenze come le uguaglianze?

Cioè, è vero che $ac \equiv bd \pmod{n}$?

$$44 \equiv 2 \pmod{6} \quad 28 \equiv 4 \pmod{6}$$

$$44 \cdot 28 = 1232 \quad 1232 = 205 \cdot 6 + 2$$

$$2 \cdot 4 = 8 \quad 8 = 1 \cdot 6 + 2$$

Supponiamo di nuovo che $a \equiv b \pmod{n}$ e che $c \equiv d \pmod{n}$

Possiamo moltiplicare le congruenze come le uguaglianze?

Cioè, è vero che $ac \equiv bd \pmod{n}$?

$$44 \equiv 2 \pmod{6} \quad 28 \equiv 4 \pmod{6}$$

$$44 \cdot 28 = 1232 \quad 1232 = 205 \cdot 6 + 2$$

$$2 \cdot 4 = 8 \quad 8 = 1 \cdot 6 + 2$$

Quindi $44 \cdot 28 \equiv 2 \cdot 4 \pmod{6}$

Supponiamo di nuovo che $a \equiv b \pmod{n}$ e che $c \equiv d \pmod{n}$

Possiamo moltiplicare le congruenze come le uguaglianze?

Cioè, è vero che $ac \equiv bd \pmod{n}$?

$$44 \equiv 2 \pmod{6} \quad 28 \equiv 4 \pmod{6}$$

$$44 \cdot 28 = 1232 \quad 1232 = 205 \cdot 6 + 2$$

$$2 \cdot 4 = 8 \quad 8 = 1 \cdot 6 + 2$$

Quindi $44 \cdot 28 \equiv 2 \cdot 4 \pmod{6}$

È un caso?

Supponiamo di nuovo che $a \equiv b \pmod{n}$ e che $c \equiv d \pmod{n}$

Possiamo moltiplicare le congruenze come le uguaglianze?

Cioè, è vero che $ac \equiv bd \pmod{n}$?

$$44 \equiv 2 \pmod{6} \quad 28 \equiv 4 \pmod{6}$$

$$44 \cdot 28 = 1232 \quad 1232 = 205 \cdot 6 + 2$$

$$2 \cdot 4 = 8 \quad 8 = 1 \cdot 6 + 2$$

Quindi $44 \cdot 28 \equiv 2 \cdot 4 \pmod{6}$

È un caso? **NO**

Congruenze e operazioni

Supponiamo che $a \equiv b \pmod{n}$ e che $c \equiv d \pmod{n}$

Congruenze e operazioni

Supponiamo che $a \equiv b \pmod{n}$ e che $c \equiv d \pmod{n}$

Per vedere se $ac \equiv bd \pmod{n}$, che dobbiamo fare?

Congruenze e operazioni

Supponiamo che $a \equiv b \pmod{n}$ e che $c \equiv d \pmod{n}$

Per vedere se $ac \equiv bd \pmod{n}$, che dobbiamo fare?

Con la divisione c'è poca speranza, proviamo a vedere se la differenza è un multiplo di n :

Congruenze e operazioni

Supponiamo che $a \equiv b \pmod{n}$ e che $c \equiv d \pmod{n}$

Per vedere se $ac \equiv bd \pmod{n}$, che dobbiamo fare?

Con la divisione c'è poca speranza, proviamo a vedere se la differenza è un multiplo di n :

$$ac - bd = ?$$

Congruenze e operazioni

Supponiamo che $a \equiv b \pmod{n}$ e che $c \equiv d \pmod{n}$

Per vedere se $ac \equiv bd \pmod{n}$, che dobbiamo fare?

Con la divisione c'è poca speranza, proviamo a vedere se la differenza è un multiplo di n :

$$ac - bd = ?$$

Noi sappiamo solo che $a - b = nx$, $c - d = ny$.

Congruenze e operazioni

Supponiamo che $a \equiv b \pmod{n}$ e che $c \equiv d \pmod{n}$

Per vedere se $ac \equiv bd \pmod{n}$, che dobbiamo fare?

Con la divisione c'è poca speranza, proviamo a vedere se la differenza è un multiplo di n :

$$ac - bd = ?$$

Noi sappiamo solo che $a - b = nx$, $c - d = ny$.

Se non c'è niente da raccogliere, ce lo mettiamo!

Congruenze e operazioni

Supponiamo che $a \equiv b \pmod{n}$ e che $c \equiv d \pmod{n}$

Per vedere se $ac \equiv bd \pmod{n}$, che dobbiamo fare?

Con la divisione c'è poca speranza, proviamo a vedere se la differenza è un multiplo di n :

$$ac - bd = ?$$

Noi sappiamo solo che $a - b = nx$, $c - d = ny$.

Se non c'è niente da raccogliere, ce lo mettiamo!

$$ac - bd =$$

Congruenze e operazioni

Supponiamo che $a \equiv b \pmod{n}$ e che $c \equiv d \pmod{n}$

Per vedere se $ac \equiv bd \pmod{n}$, che dobbiamo fare?

Con la divisione c'è poca speranza, proviamo a vedere se la differenza è un multiplo di n :

$$ac - bd = ?$$

Noi sappiamo solo che $a - b = nx$, $c - d = ny$.

Se non c'è niente da raccogliere, ce lo mettiamo!

$$ac - bd = ac - bc$$

Congruenze e operazioni

Supponiamo che $a \equiv b \pmod{n}$ e che $c \equiv d \pmod{n}$

Per vedere se $ac \equiv bd \pmod{n}$, che dobbiamo fare?

Con la divisione c'è poca speranza, proviamo a vedere se la differenza è un multiplo di n :

$$ac - bd = ?$$

Noi sappiamo solo che $a - b = nx$, $c - d = ny$.

Se non c'è niente da raccogliere, ce lo mettiamo!

$$ac - bd = ac - bc + bc - bd$$

Congruenze e operazioni

- $a - b = nx$
- $c - d = ny$
- $ac - bd = ac - bc + bc - bd$

Congruenze e operazioni

- $a - b = nx$
 - $c - d = ny$
 - $ac - bd = ac - bc + bc - bd$
- $$ac - bd = (a - b)c + (c - d)b =$$

Congruenze e operazioni

- $a - b = nx$
- $c - d = ny$
- $ac - bd = ac - bc + bc - bd$

$$ac - bd = (a - b)c + (c - d)b = (nx)c + (ny)b =$$

Congruenze e operazioni

- $a - b = nx$
- $c - d = ny$
- $ac - bd = ac - bc + bc - bd$

$$ac - bd = (a - b)c + (c - d)b = (nx)c + (ny)b = n(xc + yb)$$

- $a - b = nx$
- $c - d = ny$
- $ac - bd = ac - bc + bc - bd$

$$ac - bd = (a - b)c + (c - d)b = (nx)c + (ny)b = n(xc + yb)$$

Le congruenze si possono moltiplicare come le uguaglianze!

$$\begin{array}{r} a \equiv b \pmod{n} \\ c \equiv d \pmod{n} \\ \hline ac \equiv bd \pmod{n} \end{array}$$

Una conseguenza

Prendiamo un numero, per esempio 8574, che vuol dire

$$4 + 7 \cdot 10 + 5 \cdot 10^2 + 8 \cdot 10^3$$

Una conseguenza

Prendiamo un numero, per esempio 8574, che vuol dire

$$4 + 7 \cdot 10 + 5 \cdot 10^2 + 8 \cdot 10^3$$

Ora, $4 \equiv 1 \pmod{3}$, $7 \equiv 1 \pmod{3}$, $5 \equiv 2 \pmod{3}$,
 $8 \equiv 2 \pmod{3}$, $10 \equiv 1 \pmod{3}$, $100 \equiv 1 \pmod{3}$,
 $1000 \equiv 1 \pmod{3}$

Una conseguenza

Prendiamo un numero, per esempio 8574, che vuol dire

$$4 + 7 \cdot 10 + 5 \cdot 10^2 + 8 \cdot 10^3$$

Ora, $4 \equiv 1 \pmod{3}$, $7 \equiv 1 \pmod{3}$, $5 \equiv 2 \pmod{3}$,
 $8 \equiv 2 \pmod{3}$, $10 \equiv 1 \pmod{3}$, $100 \equiv 1 \pmod{3}$,
 $1000 \equiv 1 \pmod{3}$

$$\begin{array}{cccccc} 4 & 7 & 10 & 5 & 10^2 & 8 & 10^3 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 8574 \equiv (1 & + & 1 & \cdot & 1 & + & 2 & \cdot & 1 & + & 2 & \cdot & 1 &) \pmod{3} \end{array}$$

Una conseguenza

Prendiamo un numero, per esempio 8574, che vuol dire

$$4 + 7 \cdot 10 + 5 \cdot 10^2 + 8 \cdot 10^3$$

Ora, $4 \equiv 1 \pmod{3}$, $7 \equiv 1 \pmod{3}$, $5 \equiv 2 \pmod{3}$,
 $8 \equiv 2 \pmod{3}$, $10 \equiv 1 \pmod{3}$, $100 \equiv 1 \pmod{3}$,
 $1000 \equiv 1 \pmod{3}$

$$\begin{array}{cccccc} 4 & 7 & 10 & 5 & 10^2 & 8 & 10^3 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 8574 \equiv (1 & + & 1 & \cdot & 1 & + & 2 & \cdot & 1 & + & 2 & \cdot & 1 &) \pmod{3} \end{array}$$

$$8574 \equiv (1 + 1 + 2 + 2) \pmod{3}$$

Una conseguenza

Prendiamo un numero, per esempio 8574, che vuol dire

$$4 + 7 \cdot 10 + 5 \cdot 10^2 + 8 \cdot 10^3$$

Ora, $4 \equiv 1 \pmod{3}$, $7 \equiv 1 \pmod{3}$, $5 \equiv 2 \pmod{3}$,
 $8 \equiv 2 \pmod{3}$, $10 \equiv 1 \pmod{3}$, $100 \equiv 1 \pmod{3}$,
 $1000 \equiv 1 \pmod{3}$

$$\begin{array}{cccccc} 4 & 7 & 10 & 5 & 10^2 & 8 & 10^3 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 8574 \equiv (1 & + & 1 & \cdot & 1 & + & 2 & \cdot & 1 & + & 2 & \cdot & 1 &) \pmod{3} \end{array}$$

$$8574 \equiv (1 + 1 + 2 + 2) \pmod{3}$$

$$8574 \equiv 6 \equiv 0 \pmod{3}$$

Proviamo in un altro modo, forse più familiare:

$$8574 \equiv (4 + 7 \cdot \underset{\downarrow}{10} + 5 \cdot \underset{\downarrow}{10^2} + 8 \cdot \underset{\downarrow}{10^3}) \pmod{3}$$

Proviamo in un altro modo, forse più familiare:

$$8574 \equiv (4 + 7 \cdot \underset{\downarrow}{10} + 5 \cdot \underset{\downarrow}{10^2} + 8 \cdot \underset{\downarrow}{10^3}) \pmod{3}$$

$$8574 \equiv (4 + 7 + 5 + 8) \equiv 24 \equiv (2 + 4) \equiv 6 \equiv 0 \pmod{3}$$

$$1 \equiv 1 \pmod{3}$$

$$10 \equiv 1 \pmod{3}$$

$$10^2 \equiv 1 \cdot 10 \equiv 1 \pmod{3}$$

...

Il criterio di divisibilità per 3 si basa su questo.

$$1 \equiv 1 \pmod{3}$$

$$10 \equiv 1 \pmod{3}$$

$$10^2 \equiv 1 \cdot 10 \equiv 1 \pmod{3}$$

...

Il criterio di divisibilità per 3 si basa su questo.

E il criterio di divisibilità per 2?

$$1 \equiv 1 \pmod{3}$$

$$10 \equiv 1 \pmod{3}$$

$$10^2 \equiv 1 \cdot 10 \equiv 1 \pmod{3}$$

...

Il criterio di divisibilità per 3 si basa su questo.

E il criterio di divisibilità per 2?

$$1 \equiv 1 \pmod{2}$$

$$10 \equiv 0 \pmod{2}$$

$$10^{k+1} \equiv 10^k \cdot 10 \equiv 0 \pmod{2}$$

$$1 \equiv 1 \pmod{3}$$

$$10 \equiv 1 \pmod{3}$$

$$10^2 \equiv 1 \cdot 10 \equiv 1 \pmod{3}$$

...

Il criterio di divisibilità per 3 si basa su questo.

E il criterio di divisibilità per 2?

$$1 \equiv 1 \pmod{2}$$

$$10 \equiv 0 \pmod{2}$$

$$10^{k+1} \equiv 10^k \cdot 10 \equiv 0 \pmod{2}$$

Divisibilità per 4

$$1 \equiv 1 \pmod{4}$$

$$10 \equiv 2 \pmod{4}$$

$$10^k \equiv 0 \pmod{4} \text{ se } k > 1$$

Divisibilità per 4

$$1 \equiv 1 \pmod{4}$$

$$10 \equiv 2 \pmod{4}$$

$$10^k \equiv 0 \pmod{4} \text{ se } k > 1$$

Un numero $a_n a_{n-1} \dots a_2 a_1 a_0$ è divisibile per 4
se e solo se $a_0 + 2a_1$ è divisibile per 4
se e solo se $a_1 a_0 = a_0 + 10a_1$ è divisibile per 4

$$1 \equiv 1 \pmod{4}$$

$$10 \equiv 2 \pmod{4}$$

$$10^k \equiv 0 \pmod{4} \text{ se } k > 1$$

Un numero $a_n a_{n-1} \dots a_2 a_1 a_0$ è divisibile per 4

se e solo se $a_0 + 2a_1$ è divisibile per 4

se e solo se $a_1 a_0 = a_0 + 10a_1$ è divisibile per 4

Provate a giustificare allo stesso modo i criteri di divisibilità per 5, 11, 25.

Divisibilità per 4

$$1 \equiv 1 \pmod{4}$$

$$10 \equiv 2 \pmod{4}$$

$$10^k \equiv 0 \pmod{4} \text{ se } k > 1$$

Un numero $a_n a_{n-1} \dots a_2 a_1 a_0$ è divisibile per 4

se e solo se $a_0 + 2a_1$ è divisibile per 4

se e solo se $a_1 a_0 = a_0 + 10a_1$ è divisibile per 4

Provate a giustificare allo stesso modo i criteri di divisibilità per 5, 11, 25.

Ne sapreste trovare uno per 7?

Quali sono i numeri congruenti a zero modulo 5?

Quali sono i numeri congruenti a zero modulo 5?

$$\{\dots, -15, -10, -5, 0, 5, 10, 15, \dots\} = [0]_5$$

Quali sono i numeri congruenti a zero modulo 5?

$$\{\dots, -15, -10, -5, 0, 5, 10, 15, \dots\} = [0]_5$$

Quali sono i numeri congruenti a uno modulo 5?

Quali sono i numeri congruenti a zero modulo 5?

$$\{\dots, -15, -10, -5, 0, 5, 10, 15, \dots\} = [0]_5$$

Quali sono i numeri congruenti a uno modulo 5?

$$\{\dots, -14, -9, -4, 1, 6, 11, 16, \dots\} = [1]_5$$

Quali sono i numeri congruenti a zero modulo 5?

$$\{\dots, -15, -10, -5, 0, 5, 10, 15, \dots\} = [0]_5$$

Quali sono i numeri congruenti a uno modulo 5?

$$\{\dots, -14, -9, -4, 1, 6, 11, 16, \dots\} = [1]_5$$

Quali sono i numeri congruenti a due modulo 5?

Quali sono i numeri congruenti a zero modulo 5?

$$\{\dots, -15, -10, -5, 0, 5, 10, 15, \dots\} = [0]_5$$

Quali sono i numeri congruenti a uno modulo 5?

$$\{\dots, -14, -9, -4, 1, 6, 11, 16, \dots\} = [1]_5$$

Quali sono i numeri congruenti a due modulo 5?

$$\{\dots, -13, -8, -3, 2, 7, 12, 17, \dots\} = [2]_5$$

Quali sono i numeri congruenti a zero modulo 5?

$$\{\dots, -15, -10, -5, 0, 5, 10, 15, \dots\} = [0]_5$$

Quali sono i numeri congruenti a uno modulo 5?

$$\{\dots, -14, -9, -4, 1, 6, 11, 16, \dots\} = [1]_5$$

Quali sono i numeri congruenti a due modulo 5?

$$\{\dots, -13, -8, -3, 2, 7, 12, 17, \dots\} = [2]_5$$

Quali sono i numeri congruenti a tre modulo 5?

Quali sono i numeri congruenti a zero modulo 5?

$$\{\dots, -15, -10, -5, 0, 5, 10, 15, \dots\} = [0]_5$$

Quali sono i numeri congruenti a uno modulo 5?

$$\{\dots, -14, -9, -4, 1, 6, 11, 16, \dots\} = [1]_5$$

Quali sono i numeri congruenti a due modulo 5?

$$\{\dots, -13, -8, -3, 2, 7, 12, 17, \dots\} = [2]_5$$

Quali sono i numeri congruenti a tre modulo 5?

$$\{\dots, -12, -7, -2, 3, 8, 13, 18, \dots\} = [3]_5$$

Quali sono i numeri congruenti a zero modulo 5?

$$\{\dots, -15, -10, -5, 0, 5, 10, 15, \dots\} = [0]_5$$

Quali sono i numeri congruenti a uno modulo 5?

$$\{\dots, -14, -9, -4, 1, 6, 11, 16, \dots\} = [1]_5$$

Quali sono i numeri congruenti a due modulo 5?

$$\{\dots, -13, -8, -3, 2, 7, 12, 17, \dots\} = [2]_5$$

Quali sono i numeri congruenti a tre modulo 5?

$$\{\dots, -12, -7, -2, 3, 8, 13, 18, \dots\} = [3]_5$$

Quali sono i numeri congruenti a quattro modulo 5?

Quali sono i numeri congruenti a zero modulo 5?

$$\{\dots, -15, -10, -5, 0, 5, 10, 15, \dots\} = [0]_5$$

Quali sono i numeri congruenti a uno modulo 5?

$$\{\dots, -14, -9, -4, 1, 6, 11, 16, \dots\} = [1]_5$$

Quali sono i numeri congruenti a due modulo 5?

$$\{\dots, -13, -8, -3, 2, 7, 12, 17, \dots\} = [2]_5$$

Quali sono i numeri congruenti a tre modulo 5?

$$\{\dots, -12, -7, -2, 3, 8, 13, 18, \dots\} = [3]_5$$

Quali sono i numeri congruenti a quattro modulo 5?

$$\{\dots, -11, -6, -1, 4, 9, 14, 19, \dots\} = [4]_5$$

Dato $n > 0$ ogni numero intero sta in una e una sola classe resto e possiamo identificare ogni classe resto con uno dei numeri

$$0, 1, \dots, n - 2, n - 1$$

e questi insiemi sono proprio n .

Dato $n > 0$ ogni numero intero sta in una e una sola classe resto e possiamo identificare ogni classe resto con uno dei numeri

$$0, 1, \dots, n - 2, n - 1$$

e questi insiemi sono proprio n .

Ma una classe resto è individuata da uno qualunque dei suoi elementi: i numeri interi congruenti a 3 modulo 5 sono esattamente gli stessi che sono congruenti a 8 modulo 5 (e così via per tutti gli altri)

Siccome si possono sommare e moltiplicare le congruenze come le si fa con le uguaglianze, possiamo anche sommare e moltiplicare le classi resto:

$$[7]_{11} + [6]_{11} = [13]_{11} = [2]_{11}$$

Siccome si possono sommare e moltiplicare le congruenze come le si fa con le uguaglianze, possiamo anche sommare e moltiplicare le classi resto:

$$[7]_{11} + [6]_{11} = [13]_{11} = [2]_{11}$$

Infatti dire che $[a]_n = [b]_n$ è lo stesso che dire $a \equiv b \pmod{n}$

Siccome si possono sommare e moltiplicare le congruenze come le si fa con le uguaglianze, possiamo anche sommare e moltiplicare le classi resto:

$$[7]_{11} + [6]_{11} = [13]_{11} = [2]_{11}$$

Infatti dire che $[a]_n = [b]_n$ è lo stesso che dire $a \equiv b \pmod{n}$

Attenzione!

Siccome si possono sommare e moltiplicare le congruenze come le si fa con le uguaglianze, possiamo anche sommare e moltiplicare le classi resto:

$$[7]_{11} + [6]_{11} = [13]_{11} = [2]_{11}$$

Infatti dire che $[a]_n = [b]_n$ è lo stesso che dire $a \equiv b \pmod{n}$

Attenzione!

L'aritmetica con le classi resto può essere strana

Siccome si possono sommare e moltiplicare le congruenze come le si fa con le uguaglianze, possiamo anche sommare e moltiplicare le classi resto:

$$[7]_{11} + [6]_{11} = [13]_{11} = [2]_{11}$$

Infatti dire che $[a]_n = [b]_n$ è lo stesso che dire $a \equiv b \pmod{n}$

Attenzione!

L'aritmetica con le classi resto può essere strana

$$[2]_5 + [3]_5 = [0]_5$$

Siccome si possono sommare e moltiplicare le congruenze come le si fa con le uguaglianze, possiamo anche sommare e moltiplicare le classi resto:

$$[7]_{11} + [6]_{11} = [13]_{11} = [2]_{11}$$

Infatti dire che $[a]_n = [b]_n$ è lo stesso che dire $a \equiv b \pmod{n}$

Attenzione!

L'aritmetica con le classi resto può essere strana

$$[2]_5 + [3]_5 = [0]_5$$

$$[6]_{18} \cdot [3]_{18} = [0]_{18}$$

Siccome si possono sommare e moltiplicare le congruenze come le si fa con le uguaglianze, possiamo anche sommare e moltiplicare le classi resto:

$$[7]_{11} + [6]_{11} = [13]_{11} = [2]_{11}$$

Infatti dire che $[a]_n = [b]_n$ è lo stesso che dire $a \equiv b \pmod{n}$

Attenzione!

L'aritmetica con le classi resto può essere strana

$$[2]_5 + [3]_5 = [0]_5$$

$$[6]_{18} \cdot [3]_{18} = [0]_{18}$$

$$[7]_{18} \cdot [13]_{18} = [91]_{18} = [1]_{18}$$

Siccome si possono sommare e moltiplicare le congruenze come le si fa con le uguaglianze, possiamo anche sommare e moltiplicare le classi resto:

$$[7]_{11} + [6]_{11} = [13]_{11} = [2]_{11}$$

Infatti dire che $[a]_n = [b]_n$ è lo stesso che dire $a \equiv b \pmod{n}$

Attenzione!

L'aritmetica con le classi resto può essere strana

$$[2]_5 + [3]_5 = [0]_5$$

$$[6]_{18} \cdot [3]_{18} = [0]_{18}$$

$$[7]_{18} \cdot [13]_{18} = [91]_{18} = [1]_{18}$$