Appunti di Algebra e Geometria.

Roberto Catenacci
Università del Piemonte Orientale "A.Avogadro"

August 20, 2002

Abstract

Questi appunti sono riassunti informali delle lezioni dei corsi di algebra e geometria per gli studenti del Corso di Laurea in Informatica. I files (in formato pdf) si trovano all'indirizzo:
www.mfn.unipmn.it/~catenacc/geo/appunti.html

Completano i corsi le raccolte di esercizi di esame risolti pubblicate all'indirizzo: **www.mfn.unipmn.it/~catenacc/geo/geoinf.html**

CENNI SULLE PROGRESSIONI, LE SERIE, LE RELAZIONI DI RICORRENZA E I NUMERI DECIMALI.

Una **progressione (o successione)** è un insieme **infinito** di numeri reali $P = \{a_n \text{ con } n = 1, 2, ...\} = \{a_1, a_2, ...\}$. La somma dei primi n termini della progressione si indica con $S_n = a_1 + a_2 + ... + a_n = \sum_{i=1}^{n} a_i$. Quando consideriamo "tutti" i termini della progressione, cioè quando facciamo tendere $n \to \infty$ si usa scrivere formalmente $S = S_\infty = \sum_{i=1}^{\infty} a_i$. S è detta somma della **serie** associata alla progressione. Ci sono casi di progressioni per cui la serie **converge** cioè S **è un numero finito**. Negli altri casi S non esiste oppure è $= \pm\infty$.

Si dice **progressione aritmetica** una progressione in cui $a_{n+1} = a_n + d$ con d uguale ad un numero fisso detto *ragione aritmetica* della progressione (in altri termini si ha: $a_1 = a, a_2 = a + d, a_3 = a + 2d, a_n = a + (n-1)d$).

ESEMPIO:

$1, 2, 3, 4, ...$ si ha $a = 1$ e $d = 1$

$20, 18, 16, 14, ...$ si ha $a = 20$ e $d = -2$

$-3, -3. - 3, ...$ si ha $a = -3$ e $d = 0$.

Per una progressione aritmetica si ha

$$S_n = a + (a + d) + (a + 2d) + ... + (a + (n-1)d) \text{ e anche:}$$
$$S_n = (a + (n-1)d) + (a + (n-2)d) + .. + (a + d) + a$$

Sommando le due righe **uguali** si ottiene:

$$S_n = \frac{1}{2}n(2a + (n-1)d$$

ESEMPIO:

$13 + 10 + 7 + ...$ fino a $n = 12$. Si ha: $a = 13, d = -3, n = 12$ per cui la somma è $S_{12} = \frac{1}{2}12(26 - 33) = -42$

Si dice **progressione geometrica** una progressione in cui $a_{n+1} = a_n d$ con d uguale ad un numero fisso detto *ragione geometrica* della progressione (in altri termini si ha: $a_1 = a, a_2 = ad, a_3 = ad^2, a_n = ad^{n-1}$).

ESEMPIO:

$2, 4, 8, 16....$ si ha $a = 2$ e $d = 2$

$1, \frac{1}{2}, \frac{1}{4}...$ si ha $a = 1$ e $d = \frac{1}{2}$

$-3, -3. - 3, ...$ si ha $a = -3$ e $d = 1$.

Per una progressione geometrica si ha:

$$S_n = a + ad + ad^2 + ... + ad^{(n-1)}$$
$$dS_n = ad + ad^2 + ... + ad^n$$

Sottraendo le due righe si ottiene:

$$S_n = \frac{a(1-d^n)}{1-d}$$

ESEMPIO: $1 + \frac{1}{2} + \frac{1}{4}$...fino a $n = 12$ si ha $a = 1$ e $d = \frac{1}{2}$, e $n = 12$ per cui:

$$S_{12} = \frac{(1-(\frac{1}{2})^{12})}{1-\frac{1}{2}} = \frac{4095}{2048}$$

.

Se $|d| < 1$ allora $d^n \to 0$ quando $n \to \infty$ (infatti se $|d| < 1$, prendendo n sufficientemente grande possiamo rendere d^n arbitrariamente piccolo) e quindi la serie associata ad una progressione geometrica **converge**:

$$S = S_\infty = \frac{a}{1-d}$$

ESEMPIO: $48 + 12 + 3 + \frac{3}{4} + ...$ si ha: $a = 48$, $d = \frac{1}{4} < 1$ per cui **la somma infinita** è 64.

Si dice **progressione di Fibonacci** una progressione in cui ogni termine (a partire dal terzo) è la somma dei due termini precedenti: $a_n = a_{n-2} + a_{n-1}$ per $n = 3, 4, 5, ...$ mentre per $n = 1, 2$ si pone $a_1 = a_2 = a$ (in altri termini si ha: $a_1 = a, a_2 = a, a_3 = 2a, a_3 = 3a, a_4 = 5a, ...$).

ESEMPIO:

I **numeri di Fibonacci** si ottengono ponendo $a = 1$; si ottiene: $1, 1, 2, 3, 5, 8, 13, 21, ...$questi numeri hanno proprietà affascinanti e intervengono in moltissimi campi della matematica e della biologia come sarà mostrato a lezione.

Se si considerano i rapporti tra i numeri di Fibonacci, $\frac{1}{1}, \frac{1}{2}, \frac{2}{3}, \frac{3}{5}, \frac{5}{8}, ...$ si nota che sono tutti ≤ 1 e > 0.

Sia $R_n = a_{n-1}/a_n$ l'n-esimo rapporto, e sia $R = R_\infty$ il limite dei rapporti (che esiste per l'osservazione precedente). Siccome $a_n = a_{n-2} + a_{n-1}$, dividendo per a_{n-1} si ottiene:

$$\frac{a_n}{a_{n-1}} = \frac{a_{n-2}}{a_{n-1}} + 1$$

cioè

$$1/R_n = R_{n-1} + 1$$

e, passando al limite, $1/R = R + 1$ cioè $R^2 + R - 1 = 0$, le cui soluzioni sono: $\left\{R = \frac{1}{2}\sqrt{5} - \frac{1}{2}\right\}, \left\{R = -\frac{1}{2} - \frac{1}{2}\sqrt{5}\right\}$. Si ottiene quindi, scartando la impossibile soluzione negativa,

$$R = \frac{1}{2}\sqrt{5} - \frac{1}{2} = 0.61803....$$

Questo numero è detto **sezione aurea** e rappresenta il modo di dividere un segmento di lunghezza unitaria in una parte **media proporzionale** tra l'intero segmento e la parte restante: $1 : R = R : (1 - R)$. Questo rapporto gioca un ruolo fondamentale nella storia dell'arte ed era già conosciuto dai greci. Altre osservazioni sui numeri di Fibonacci e la sezione aurea saranno esposte a lezione.

La relazione che definisce la progressione di Fibonacci è un esempio di relazione di ricorrenza**.** In generale una **relazione di ricorrenza lineare di ordine** k è una espressione della forma:

$$a_k u_{n+k} + a_{k-1} u_{n+k-1} + ... + a_1 u_{n+1} + a_0 u_n = f(n)$$

Dove a_i è un numero reale per $i = 0, 1.....k$, $a_k \neq 0$ e $f(n)$ è una funzione reale del numero intero n. Quando $f(n) = 0$ la relazione è detta **omogenea**, altrimenti è detta **inomogenea**.

Consideriamo la relazione $u_{n+1} - 2u_n = 0$. E' una relazione di ricorrenza lineare omogenea di **ordine** 1. Se supponiamo $u_0 = 1$, otteniamo $u_1 = 2$, $u_2 = 2^2$... è facile mostrare che $u_n = 2^n$. Si noti che per risolverla è necessario un valore iniziale. La più generale relazione di questo tipo si scrive:

$$a u_{n+1} + b u_n = 0$$

La cui soluzione è, ovviamente, $u_n = \alpha^n A$ dove $\alpha = -b/a$ e $A = u_0$.

Studiamo ora le relazioni lineari e omogenee di **ordine** 2 la cui forma generale è:

$$a u_{n+2} + b u_{n+1} + c u_n = 0$$

Non consideriamo la soluzione banale $u_n = 0$ per tutti gli n. Supponiamo (seguendo l'insegnamento del caso precedente) che la soluzione cercata sia della forma $u_n = \alpha^n A$ con $A \neq 0$ Allora deve essere:

$$a\alpha^{n+2} A + b\alpha^{n+1} A + c\alpha^n A = 0$$

Quindi si ottiene (dividendo per un u_n diverso da zero, che esiste per ipotesi) $a\alpha^2 + b\alpha + c = 0$. Ciò significa che α deve essere soluzione della seguente equazione di secondo grado, detta **equazione ausiliaria**:

$$ax^2 + bx + c = 0$$

Rimandiamo lo continuazione dello studio delle relazioni di ordine 2 a dopo aver trattato in maggior dettaglio le equazioni di secondo grado e i numeri complessi, e limitiamoci a esaminare il caso della relazione di Fibonacci: $a_n = a_{n-2} + a_{n-1}$ $(n \geq 2)$ che riscriviamo:

$$u_{n+2} - u_{n+1} - u_n = 0 \text{ per } n \geq 0 \text{ con } u_0 = 1 \text{ e } u_1 = 1$$

L'equazione ausiliaria è $x^2 - x - 1 = 0$, le cui soluzioni sono:

$$\left\{\alpha = \frac{1}{2}\sqrt{5} + \frac{1}{2}\right\}, \left\{\beta = \frac{1}{2} - \frac{1}{2}\sqrt{5}\right\}$$

Se supponiamo $u_0 = 1$ e $u_1 = 1$ (servono due condizioni iniziali) allora la soluzione generale è:

$$u_n = A\alpha^n + B\beta^n$$

Con A e B determinati dalle condizioni:

$$u_0 = 1 = A + B$$
$$u_1 = 1 = A\alpha + B\beta$$

Che, risolte, danno:

$$B = \tfrac{\beta-1}{\beta-\alpha} = \tfrac{-\alpha}{\beta-\alpha}$$
$$A = \tfrac{1-\alpha}{\beta-\alpha} = \tfrac{\beta}{\beta-\alpha}$$

Concludendo, nel caso dei numeri di Fibonacci, si ha:

$$u_n = \frac{\beta^{n+1} - \alpha^{n+1}}{\beta - \alpha}$$

Notare il risultato "apparentemente sorprendente":

$\dfrac{\left(\frac{1}{2}\sqrt{5} + \frac{1}{2}\right)^{n+1} - \left(-\frac{1}{2}\sqrt{5} + \frac{1}{2}\right)^{n+1}}{\sqrt{5}}$ è un numero **intero** per ogni n.

OSSERVAZIONI SUI NUMERI DECIMALI.

I **numeri decimali** si dividono in **terminanti** (se possono essere scritti esattamente con un numero finito di cifre significative) e **non terminanti**, che a loro volta possono essere **periodici** e **non perodici**, questi ultimi sono detti anche **irrazionali (**i primi due tipi, i terminanti e i periodici, sono detti anche **razionali)**. Esempi di numeri irrazionali sono $\sqrt{2}, \sqrt{3}, \pi, R$. Una frazione del tipo $\frac{1}{n}$ ha una espansione decimale terminante se e solo se gli unici fattori primi di n sono 2 e 5. Lo stesso vale per frazioni irriducibili di tipo $\frac{m}{n}$. Si usa indicare il periodo di un decimale periodico con una linea: $\frac{1}{9} = 0.111111.... = 0.\bar{1}$ Questo numero può essere scritto $\frac{1}{10} + \left(\frac{1}{10}\right)^2 + \left(\frac{1}{10}\right)^3 + ...$ Questa è una **progressione geometrica** di primo termine $\frac{1}{10}$ e ragione $\frac{1}{10}$ per cui, come deve essere, la sua somma infinita è proprio $\frac{1}{10}\left(\frac{1}{1-\frac{1}{10}}\right) = \frac{1}{9}$. Questo schema di calcolo è utile per trovare una frazione che rappresenti un

dato decimale periodico. Consideriamo $\frac{1}{9} = 0.\overline{1}$, $\frac{1}{99} = 0.\overline{01}$, $\frac{1}{999} = 0.\overline{001}$, ... allora, ad esempio:

$$0.\overline{234} = 234 \times 0.\overline{001} = \frac{234}{999} = \frac{26}{111}$$

E' vero anche il viceversa: ogni frazione rappresenta un decimale terminante o periodico, infatti basta considerare le frazioni del tipo $\frac{1}{n}$ già visto sopra. Cosa si può dire circa la **lunghezza del periodo** di un numero periodico? Ad esempio $\frac{1}{7} = 0.\overline{142857}$ ha lunghezza 6. In generale, se consideriamo $\frac{1}{n}$ con n **primo** la lunghezza del periodo è sempre un divisore di $n-1$, mentre se n **non è primo,** è un divisore di $q-1$ dove q è un fattore primo di n. *C'è un teorema che dice: la lunghezza del periodo di* $\frac{1}{n}$ *è il più piccolo* k *per cui* $10^m(10^k-1)$ *è divisibile per* n (m è scelto opportunamente per ottenere dalla divisione numeri maggiori di 1). Ad esempio, $\frac{1}{19}$ ha periodo 18, **ma come facciamo a trovarlo con un display da meno di 18 cifre?**

Ecco un **algoritmo** per trovare periodi arbitrariamente lunghi con display da k cifre:

Consideriamo $\frac{m}{n}$ con $m < n$.

Passo 1: poniamo $r_1 = m, i = 1$ e scriviamo il numero 0.

Passo 2: calcoliamo $r_i/n = 0.abcdefgh$ fino alla k-esima cifra decimale e scriviamo $abcdefgh$ dopo il *numero fin qui ottenuto.*

Passo 3: calcoliamo $r_i - n \times 0.abcdefgh = r_{i+1} \times 10^{-k}$

Passo 4: se $ik \geq n-1$ il periodo è il *numero ottenuto*, altrimenti $i \to i+1$ e si va al passo 2.

Esempio: $\frac{1}{19}$ con un display da 6 cifre:

$1/19 = 0.052631$, *il numero fin qui ottenuto è* 0.052631
$1 - 19 \times 0.052631 = 11 \times 10^{-6}$
$11/19 = 0.578947$, *il numero fin qui ottenuto è* 0.052631578947
$11 - 19 \times 0.578947 = 7 \times 10^{-6}$
$7/19 = 0.368421$, *il numero fin qui ottenuto è* 0.052631578947368421
$ik = 18 \geq 18$ quindi $1/19 = 0.\overline{052631578947368421}$

Esempio: $\frac{1}{23} = 0.\overline{0434782608695652173913}$

SOMME NOTEVOLI E DIMOSTRAZIONI PER INDUZIONE.

Trattando le serie appaiono spesso alcune notevoli formule di calcolo:

$$\sum_{i=1}^{n} i = 1 + 2 + 3 + ... + n = \frac{n(n+1)}{2}$$

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

$$\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}$$

Per dimostrare formule di questo tipo riguardo i numeri interi, e altre che vedremo in seguito, si usa un potente mezzo di dimostrazione, detto **prova per induzione.**

Sia $P(n)$ una affermazione riguardo il numero n, questa affermazione **è vera per tutti gli interi positivi** se:

1) $P(1)$ è vera.

2) $P(k)$ vera implica $P(k+1)$ vera.

Infatti se $P(1)$ è vera, il punto 2) implica che è vera $P(2)$; ancora lo stesso punto implica che $P(3)$ è vera e così via.

Osservazioni utili:

Il punto 1) può essere sostituito da : $P(a)$ è vera per un certo numero intero a; in questo caso $P(n)$ risulta **vera per tutti gli interi** $\geq a$.

Il punto 2) può essere sostituito da 2) bis : $P(k)$ vera per tutti i $k < m$ implica $P(m)$ vera.

Ad esempio sia $P(n)$ l'affermazione che $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$. Allora $P(1)$ è l'affermazione, ovviamente vera, che $\sum_{i=1}^{1} i = 1 = \frac{1(1+1)}{2}$. Occorre ora provare che $P(k) \Rightarrow P(k+1)$.

Se assumiamo vera $P(k)$ si ha:

$$\sum_{i=1}^{k} i = \frac{k(k+1)}{2} \Longrightarrow \sum_{i=1}^{k} i + (k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{(k+1)(k+2)}{2}$$

ma

$$\sum_{i=1}^{k} i + (k+1) = \sum_{i=1}^{k+1} i$$

per cui,

$$\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}$$

che è proprio l'affermazione $P(k+1)$ e quindi la formula $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ risulta vera per tutti gli n.

ALTRI ESEMPI DI INDUZIONE

a) Sia $P(n)$ l'affermazione che **dati** a **e** b **interi, e** n **un intero** > 0, **allora** $a - b$ **divide** $a^n - b^n$.

Ovviamente $P(1)$ è vera; ora osserviamo che:

$$a^{k+1} - b^{k+1} = a^k(a - b) + b(a^k - b^k)$$

Per cui **se** $P(k)$ è vera, e cioè $a-b$ divide a^k-b^k, è immediato osservare che **allora** $a-b$ divide anche $a^{k+1}-b^{k+1}$(infatti, in virtù della formula precedente, questo termine è la somma di due termini ciascuno dei quali è divisibile per $a - b$). Ne risulta che $P(n)$ è sempre vera.

b) Sia $P(n)$ l'affermazione che **dati** a **e** b **interi, e** n **un intero dispari** > 0, **allora** $a + b$ **divide** $a^n + b^n$.

(Questa affermazione riguarda solo gli interi dispari, e non tutti gli interi positivi; il metodo di induzione va così modificato:

Sia $P(n)$ una affermazione riguardo il numero **dispari** n, questa affermazione **è vera per tutti gli interi dispari** se:

1) $P(1)$ è vera.

2) bis $P(k)$ vera per tutti i k dispari $< n$ implica $P(n)$ vera.

Infatti se $P(1)$ è vera, il punto 2) bis implica che è vera $P(3)$; ancora lo stesso punto implica che $P(5)$ è vera e così via).

Ovviamente $P(1)$ è vera; ora osserviamo che:

$$a^n + b^n = a^{n-1}(a + b) - b(a^{n-1} - b^{kn-1})$$

Se n è dispari, allora $n - 1 = 2m$ e quindi

$$a^n + b^n = a^{n-1}(a + b) + b(a^{n-1} - b^{n-1}) = a^{n-1}(a + b) + b(a^m + b^m)(a^m - b^m)$$

Se ora m è **dispari** abbiamo finito, perchè $m < n$ e quindi $a^m + b^m$ per ipotesi è divisibile per $a + b$. Se invece m è **pari**, si ottiene $m = 2r$ e quindi:

$$a^n + b^n = a^{n-1}(a + b) + b(a^m + b^m)(a^r + b^r)(a^r - b^r)$$

Se ora r è **dispari** abbiamo finito, perchè $r < m < n$ e quindi $a^r + b^r$ per ipotesi è divisibile per $a + b$. Se invece r è **pari**, si ottiene $r = 2l$ e si procede nello stesso modo. Osservando che $l < r < m < n$ si vede che il procedimento si deve arrestare a un numero dispari (nel peggiore dei casi 1) perchè n è un numero positivo e il piu piccolo numero positivo è 1. Esempio $3^{27} + 2^{27} = 7625\,731\,702\,715$

c) **Se** $2^n + 1$ **è primo, allora** n **è una potenza di due.**

Infatti n deve essere pari, altrimenti (per il punto b) $2^n + 1$ sarebbe divisibile per $2 + 1 = 3$. Quindi $n = 2k$, $k < n$, e anche k deve essere pari (per lo stesso motivo di prima $2^n + 1 = 2^{2k} + 1 = 4^k + 1$ sarebbe divisibile per $4 + 1 = 5$, quindi $k = 2r$ con $r < k < n$. Il ragionamento termina come prima con 1 e quindi $n = 2 \times 2 \times 2 \times ..... \times 2 \times 1$

Notate che il viceversa non è vero: $2^5 = 32$ e $2^{32} + 1 = 641 \times 6700\,417$

RICHIAMI SUI NUMERI COMPLESSI E I POLINOMI.

Equazioni quadratiche.

Una equazione quadratica in x è una equazione della forma: $ax^2+bx+c=0$ dove a, b, c sono numeri reali e $a \neq 0$. Non è difficile risolverla; quando $\Delta = b^2 - 4ac \geq 0$ (la stessa formula vale anche se $\Delta < 0$, ma ne parleremo dopo) si ha:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Ci sono due tipi di equazioni quadratiche; quelle che hanno soluzioni *razionali* (ovvero che si possono scrivere nella forma m/n con m e n numeri interi relativi e $n \neq 0$) e quelle le cui soluzioni sono *irrazionali.* Le soluzioni sono razionali quando Δ è il quadrato di un numero razionale. Esempi di numeri irrazionali sono $\sqrt{2}, \sqrt{3}, \pi$.

Dimostriamo che $\sqrt{2}$ è irrazionale. Supponiamo che sia razionale; allora $\sqrt{2} = m/n$, *con m e n senza fattori comuni*; elevando al quadrato si ha: $m^2 = 2n^2$. Questo significa che m^2 è un numero pari e quindi anche m lo è (questa ultima osservazione deriva dal fatto che il quadrato di un numero dispari è un numero dispari, infatti $(2k+1)^2 = 4k^2 + 4k + 1$; ora usiamo anche il seguente fatto: se la proposizione A implica la proposizione B, allora la proposizione non-B implica la proposizione non-A. (m dispari implica m^2 dispari allora m^2 non-dispari cioè pari implica m non-dispari cioè pari)). Allora $m = 2k$ e quindi $4k^2 = 2n^2$ cioè $n^2 = 2k^2$ così n^2 è pari e anche n lo è. Allora sia m che n sono numeri pari e quindi hanno in comune almeno il fattore 2.

Questa è una contraddizione perchè abbiamo supposto che *m e n siano senza fattori comuni.* La contraddizione si risolve *solo negando l'assunto* che $\sqrt{2}$ sia razionale.

Il ragionamento precedente è un esempio di **dimostrazione per assurdo**, il metodo consiste nell'assumere falsa la proposizione che si vuole dimostrare e cercare di ottenere una contraddizione.

La formula risolutiva delle equazioni di secondo grado data sopra implica che una tale equazione ha, al più, due soluzioni. Se $\Delta = b^2 - 4ac = 0$ l'equazione ha una sola soluzione *(meglio dire due soluzioni coincidenti)*, se $\Delta = b^2 - 4ac > 0$ l'equazione ha due soluzioni distinte. Se $\Delta = b^2 - 4ac < 0$ l'equazione non ha soluzioni reali; introducendo i **numeri complessi** si possono estrarre le radici quadrate dei numeri negativi e si ripristina la simmetria: una equazione di grado *due* ha sempre *due* soluzioni.

Due equazioni $a_1x^2 + b_1x + c_1 = 0$ e $a_2x^2 + b_2x + c_2 = 0$ hanno le stesse soluzioni se e solo se sono proporzionali, cioè se esiste una costante $k \neq 0$ tale che $a_1/a_2 = b_1/b_2 = c_1/c_2 = k$.

Questa osservazione è utile perchè ci consente di scrivere subito, senza risolvere l'equazione la somma e il prodotto delle sue soluzioni: siano α e β le soluzioni dell'equazione $ax^2+bx+c = 0$. Anche l'equazione $a(x-\alpha)(x-\beta) = 0 = ax^2-(\alpha+\beta)x+\alpha\beta$ ha ovviamente le stesse soluzioni quindi, confrontando con l'equazione originaria, si trova: $\alpha + \beta = -b/a$ e $\alpha\beta = c/a$.

Esempio: data l'equazione $8x^2 - 9x + 2 = 0$ trovare una equazione che abbia come soluzioni i quadrati delle soluzioni dell'equazione data. Siano α e β le soluzioni: si ha $\alpha + \beta = -9/8$ e $\alpha\beta = 1/4$. Notiamo che $(\alpha^2 + \beta^2) = (\alpha + \beta)^2 - 2\alpha\beta = 49/16$ e $\alpha^2\beta^2 = 1/16$. Quindi l'equazione richiesta è $x^2 - (\alpha^2 + \beta^2)x + \alpha^2\beta^2 = x^2 - 49/16x + 1/16 = 0$.

Questo metodo funziona per trovare equazioni le cui radici siano **funzioni simmetriche** (una funzione f di α e β è simmetrica se $f(\alpha, \beta) = f(\beta, \alpha)$) delle radici dell'equazione data; infatti **tutte** le funzioni simmetriche si possono scrivere in funzione delle due funzioni simmetriche elementari $f_1(\alpha, \beta) = \alpha + \beta$ e $f_2(\alpha, \beta) = \alpha\beta$.

Esempio: $\alpha^3 + \beta^3 = 3(\alpha + \beta)^3 - 3\alpha\beta(\alpha + \beta)$.

NUMERI COMPLESSI

Per introdurre i numeri complessi si parte di solito dal fatto che l'equazione $x^2 + 1 = 0$ non ha soluzioni. Si *inventa* allora una soluzione dell'equazione data e la si chiama i. Si tratta poi i come un normale numero a cui si applicano le solite regole di calcolo e allora si ottiene $i^2 = -1$. Si scrivono poi tutti i simboli del tipo $a + ib$ con a e b numeri reali e si postulano per essi le usuali regole di calcolo: ecco i **numeri complessi**.

Un modo più *convincente* per introdurre i numeri complessi è quello di farli discendere direttamente dalle coppie di numeri reali.

Indichiamo con $\mathbb{R}$ il campo dei numeri reali con le solite operazioni e con $\mathbb{C}$ il campo dei numeri complessi.

Un **numero complesso** è una coppia ordinata di numeri reali $(a, b) \in \mathbb{R} \times \mathbb{R}$, cioè

$$\mathbb{C} = \{(a, b) : a, b \in \mathbb{R}\}.$$

Definiamo $\forall\, (a, b)\,, (c, d) \in \mathbb{C}$ le seguenti operazioni :

$i)$ **somma**: $(a, b) + (c, d) = (a + b, c + d)$;

ii) **prodotto**: $(a,b)\cdot(c,d)=(ac-bd,ad+bc)$.

Viene naturale identificare $a\in\mathbb{R}$ con la coppia $(a,0)\in\mathbb{C}$, cioè ogni numero reale può essere pensato come numero complesso $\Rightarrow\mathbb{C}$ è un "ampliamento" di $\mathbb{R}$, cioè $\mathbb{R}\subset\mathbb{C}$.

L'elemento $(0,1)\in\mathbb{C}$, si denota con i ed è detto **unità immaginaria**. Si ha

$$i^2=i\cdot i=(0,1)\cdot(0,1)=(-1,0)=-1.$$

Prendiamo $(a,b)\in\mathbb{C}$:

$$(a,b)=(a,0)+(0,b)=(a,0)+(0,1)\cdot(b,0)=a+ib,$$

cioè ogni numero complesso può essere scritto nella forma $a+ib$, detta **forma algebrica**. a è chiamata **parte reale**, ib è la **parte immaginaria**. Le operazioni tra numeri complessi scritti in forma algebrica si eseguono con le regole del calcolo letterale:

$$\begin{gathered}(a+ib)+(c+id)=a+ib+c+id=(a+c)+i(b+d);\\ (a+ib)\cdot(c+id)=ac+iad+ibc+i^2bd=ac+iad+ibc-bd\\ =(ac-bd)+i(ad+bc).\end{gathered}$$

Dato $z=a+ib$, si definisce il numero **complesso coniugato**

$$\overline{z}=a-ib.$$

Per semplificare una frazione con un complesso a denominatore, si può moltiplicare numeratore e denominatore per il coniugato del numero, osservando che $(a+ib)\cdot(a-ib)=a^2-iab+iab-i^2b=a^2+b^2$.

Rappresentazione geometrica dei numeri complessi

Fissiamo nel piano un sistema di riferimento cartesiano Oxy. Un numero complesso (a,b) può essere pensato come punto del piano π (**piano complesso**): a rappresenta l'ascissa e b l'ordinata.

OSSERVAZIONI.

1) Se $z \in \mathbb{R} \Rightarrow z = (a, 0) \Rightarrow z$ sta sull'asse x (detto **asse reale**).

2) Se $z = ib$, cioè z è immaginario puro $\Rightarrow z = (0, b)$ sta sull'asse y (detto **asse immaginario**).

3) La moltiplicazione per i equivale quindi a una rotazione di $90°$ in senso antiorario.

Forma trigonometrica di un numero complesso. Sia $z = a + ib$ un numero complesso e sia P la sua immagine sul piano π. Associamo a z due "coordinate polari" (ρ, θ):

1) $\rho = \sqrt{a^2 + b^2}$ è detto **modulo** di z ed è la lunghezza del segmento che congiunge l'origine con il punto P;

2) θ è detto **anomalia** o **argomento** di z, è l'angolo tra ρ e il semiasse positivo delle x ed **è individuato a meno di multipli di 2π.**

Dalla trigonometria si ha che

$$a = \rho \cos\theta \qquad b = \rho \sin\theta$$

$$\cos\theta = \frac{a}{\rho} = \frac{a}{\sqrt{a^2 + b^2}} \qquad \sin\theta = \frac{b}{\rho} = \frac{b}{\sqrt{a^2 + b^2}}.$$

Dalle formule precedenti si ottiene:

$$\boxed{a + ib = \rho\,(\cos\theta + i \sin\theta)},$$

detta **forma trigonometrica** del numero complesso $a + ib$.

Due numeri complessi non nulli $z_1 = \rho_1(\cos\theta_1 + i \sin\theta_1)$ e $z_2 = \rho_2(\cos\theta_2 + i \sin\theta_2)$ sono uguali se $\rho_1 = \rho_2$ e $\theta_1 = \theta_2 + 2k\pi$, con k intero.

Teorema. Dati $z_1, z_2 \in \mathbb{C}$, il loro prodotto è

$$z_1 \cdot z_2 = \rho_1 \rho_2 \left[\cos(\theta_1 + \theta_2) + i \sin(\theta_1 + \theta_2)\right].$$

Tale regola vale anche per un numero qualsiasi di fattori. Se i fattori sono uguali, si ha la **formula di De Moivre**:

$$\left[\rho\,(\cos\theta + i \sin\theta)\right]^n = \rho^n\,(\cos n\theta + i \sin n\theta)\,, \quad n \in \mathbb{N}.$$

Esempio: $(1+i)^{14} = (\sqrt{2}(\cos\pi/4 + i\sin\pi/4))^{14} = 128(\cos(-\pi/2) + i\sin(-\pi/2)) = -128i$, infatti $14\pi/4 = 7\pi/2 = 4\pi - \pi/2$ (provate solo a pensare di dover fare il calcolo senza la formula di De Moivre per capirne l'importanza !).

Se si conviene di porre

$$[\rho(\cos\theta + i\sin\theta)]^0 = 1, \text{ per } \rho \neq 0$$
$$[\rho(\cos\theta + i\sin\theta)]^{-n} = \frac{1}{[\rho(\cos\theta + i\sin\theta)]^n},$$

la formula di De Moivre vale per $n \in \mathbb{Z}$.

Radici n-esime dei numeri complessi. Sia $z \in \mathbb{C}$ e $n \in \mathbb{N}$. I numeri $w \in \mathbb{C}$ tali che $w^n = z$, si dicono **radici n-esime** di z.

Prendiamo $z = \rho(\cos\theta + i\sin\theta)$ e sia $w = r(\cos\varphi + i\sin\varphi)$ una radice n-esima di z. Si deve avere

$$w^n = z \Rightarrow r^n(\cos n\varphi + i\sin n\varphi) = \rho(\cos\theta + i\sin\theta)$$
$$\Rightarrow r^n = \rho \text{ e } n\varphi = \theta + 2k\pi,\ k \in \mathbb{Z}$$
$$\Rightarrow r = \sqrt[n]{\rho} \text{ (radice aritmetica) e } \varphi = \frac{\theta}{n} + \frac{2k\pi}{n},\ k \in \mathbb{Z}.$$

L'ultima formula dà infiniti valori per φ, ma solo n sono distinti ($k = 0, 1, ..., n-1$ poi si ripetono a meno di multipli di 2π).

Teorema. $z = \rho(\cos\theta + i\sin\theta)$ ammette n radici n-esime w distinte date dalla formula

$$(\sharp) \qquad \boxed{w = \sqrt[n]{z}^* = \sqrt[n]{\rho}\left[\cos\left(\frac{\theta}{n} + \frac{2k\pi}{n}\right) + i\sin\left(\frac{\theta}{n} + \frac{2k\pi}{n}\right)\right]},$$

nella quale si pone $k = 0, 1, 2, ..., n-1$.

(L'asterisco serve solo a distinguere la radice complessa da quella aritmetica).

Gli n numeri forniti da ($\sharp$), hanno lo stesso modulo $\sqrt[n]{\rho}$, quindi le loro immagini sul piano complesso stanno su una circonferenza di centro l'origine e raggio $\sqrt[n]{\rho}$.

Scegliamo $z = 1 = 1 + 0i = 1(\cos 0 + i\sin 0)$. Utilizzando ($\sharp$), troviamo le n **radici n-esime dell'unità**:

$$\epsilon_k = \sqrt[n]{1}^* = \sqrt[n]{1}\left[\cos\left(0+\frac{2k\pi}{n}\right)+i\sin\left(0+\frac{2k\pi}{n}\right)\right]$$
$$= \cos\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n}, \text{ con } k=0,1,2,...,n-1.$$

Le radici n-esime dell'unità si rappresentano geometricamente come vertici di un poligono regolare di n lati, inscritto in una circonferenza di raggio 1, con un vertice nel punto $(1,0)$.

Le radici n-esime dell'unità servono per calcolare le radici n-esime di qualsiasi numero: basta moltiplicare una qualsiasi radice complessa del numero per le radici n-esime dell'unità. Infatti sia ζ una qualunque radice n-esima di z, ponendo $\zeta_k = \zeta\epsilon_k$ si ottengono tutte le radici di z, infatti: $(\zeta_k)^n = (\zeta\epsilon_k)^n = \zeta^n\epsilon_k^n = z$

ESEMPI.
1) Calcolare le radici cubiche complesse di 8.
Scriviamo 8 in forma trigonometrica:

$$8 = 8+0i = 8(\cos 0 + i\sin 0).$$

$$w_k = \sqrt[3]{8}^* = \sqrt[3]{8}\left(\cos\frac{2k\pi}{3}+i\sin\frac{2k\pi}{3}\right),\ k=0,1,2.$$

Quindi

$w_0 = 2(\cos 0 + i\sin 0) = 2;$
$w_1 = 2\left(\cos\frac{2\pi}{3}+i\sin\frac{2\pi}{3}\right) = 2\left(-\frac{1}{2}+i\frac{\sqrt{3}}{2}\right) = -1+i\sqrt{3};$
$w_2 = 2\left(\cos\frac{4\pi}{3}+i\sin\frac{4\pi}{3}\right) = 2\left(-\frac{1}{2}-i\frac{\sqrt{3}}{2}\right) = -1-i\sqrt{3}.$

Le tre radici cubiche di 8 sono: 2, $-1+i\sqrt{3}$ e $-1+i\sqrt{3}$.

2) Calcolare le radici quarte di $-1+i\sqrt{3}$.
Si ha:

$$\rho = \sqrt{1+3} = 2,\ \cos\theta = -\frac{1}{2} \text{ e } \sin\theta = \frac{\sqrt{3}}{2} \Rightarrow \theta = \frac{2\pi}{3}$$
$$\Rightarrow -1+i\sqrt{3} = 2\left(\cos\frac{2\pi}{3}+i\sin\frac{2\pi}{3}\right).$$

Applicando la ($\sharp$) con $k = 0, 1, 2, 3$, si ha

$$w_k = \sqrt[4]{-1 + i\sqrt{3}}^* = \sqrt[4]{2}\left[\cos\left(\frac{\pi}{6} + \frac{k\pi}{2}\right) + i\sin\left(\frac{\pi}{6} + \frac{k\pi}{2}\right)\right].$$

$$\begin{aligned}
w_0 &= \sqrt[4]{2}\left[\cos\frac{\pi}{6} + i\sin\frac{\pi}{6}\right] = \sqrt[4]{2}\left(\frac{\sqrt{3}}{2} + i\frac{1}{2}\right) = \frac{\sqrt[4]{2}}{2}\left(\sqrt{3} + i\right);\\
w_1 &= \sqrt[4]{2}\left[\cos\left(\frac{\pi}{6} + \frac{\pi}{2}\right) + i\sin\left(\frac{\pi}{6} + \frac{\pi}{2}\right)\right] = \sqrt[4]{2}\left(\cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}\right)\\
&= \sqrt[4]{2}\left(-\frac{1}{2} + i\frac{\sqrt{3};}{2}\right) = \frac{\sqrt[4]{2}}{2}\left(-1 + i\sqrt{3}\right);\\
w_2 &= \sqrt[4]{2}\left[\cos\left(\frac{\pi}{6} + \pi\right) + i\sin\left(\frac{\pi}{6} + \pi\right)\right] = \sqrt[4]{2}\left(\cos\frac{7\pi}{6} + i\sin\frac{7\pi}{6}\right)\\
&= \sqrt[4]{2}\left(-\frac{\sqrt{3}}{2} - i\frac{1}{2}\right) = \frac{\sqrt[4]{2}}{2}\left(-\sqrt{3} - i\right);\\
w_3 &= \sqrt[4]{2}\left[\cos\left(\frac{\pi}{6} + \frac{3\pi}{2}\right) + i\sin\left(\frac{\pi}{6} + \frac{3\pi}{2}\right)\right] = \sqrt[4]{2}\left(\cos\frac{5\pi}{3} + i\sin\frac{5\pi}{3}\right)\\
&= \sqrt[4]{2}\left(\frac{1}{2} - i\frac{\sqrt{3};}{2}\right) = \frac{\sqrt[4]{2}}{2}\left(1 - i\sqrt{3}\right).
\end{aligned}$$

3) Calcolare le radici seste dell'unità.
Si ha:

$$\epsilon_k = \sqrt[6]{1}^* = \cos\frac{2k\pi}{6} + i\sin\frac{2k\pi}{6}, \text{ con } k = 0, 1, 2, 3, 4, 5.$$

Quindi

$$\begin{aligned}
\epsilon_0 &= \cos 0 + i\sin 0 = 1;\\
\epsilon_1 &= \cos\frac{\pi}{3} + i\sin\frac{\pi}{3} = \frac{1}{2} + i\frac{\sqrt{3}}{2};\\
\epsilon_2 &= \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2};\\
\epsilon_3 &= \cos\pi + i\sin\pi = -1;\\
\epsilon_4 &= \cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3} = -\frac{1}{2} - i\frac{\sqrt{3}}{2};\\
\epsilon_5 &= \cos\frac{5\pi}{3} + i\sin\frac{5\pi}{3} = \frac{1}{2} - i\frac{\sqrt{3}}{2}.
\end{aligned}$$

Le sei radici trovate sono i vertici di un esagono regolare.

<u>Formula di Eulero</u>. Consideriamo la funzione esponenziale di variabile complessa $f(z) = e^z$, $z \in \mathbb{C}$.
Valgono le consuete proprietà delle potenze:

$$e^z \cdot e^w = e^{z+w}; \qquad e^z : e^w = e^{z-w}; \qquad (e^z)^n = e^{nz},$$

con $z, w \in \mathbb{C}$, $n \in \mathbb{Z}$.
Se $z = x + iy$, con $x, y \in \mathbb{R}$, si pone

$$e^z = e^{x+iy} = e^x \cdot e^{iy} = e^x (\cos y + i \sin y).$$

Quindi è

$$\boxed{e^{iy} = (\cos y + i \sin y)}.$$

Quest'ultima è la **formula di Eulero**.
Si ha

$$e^{2\pi i} = \cos 2\pi + i \sin 2\pi = 1 + 0i = 1$$

e

$$e^{z+2\pi i} = e^z \cdot e^{2\pi i} = e^z,$$

cioè l'esponenziale e^z è periodica di periodo $2\pi i$.
Inoltre

$$e^{-iy} = \cos(-y) + i \sin(-y) = \cos y - i \sin y.$$

Esempio.
$i = 0 + 1i = \cos \dfrac{\pi}{2} + i \sin \dfrac{\pi}{2} = e^{\frac{\pi}{2} i}$;
$-1 = -1 + 0i = \cos \pi + i \sin \pi = e^{\pi}$.

POLINOMI

Un **polinomio** nella variabile x è un'espressione

$$P(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n$$

con $a_0, a_1, ..., a_n \in \mathbb{R}$ (o $\mathbb{C}$), detti **coefficienti** del polinomio e $n \in \mathbb{N}$, detto **grado** del polinomio: $n = \deg P(x)$. Se $a_n = 1$, il polinomio è detto **monico**. L'insieme dei polinomi in x su $\mathbb{R}$ (o $\mathbb{C}$) è denotato con $\mathbb{R}[x]$ (o $\mathbb{C}[x]$). Il **polinomio nullo** è il polinomio con tutti i coefficienti uguali a 0. Un **polinomio costante** è il polinomio nullo oppure un polinomio di grado 0.

Due polinomi in x sono uguali se hanno uguali i coefficienti delle potenze di x corrispondenti. I polinomi si sommano e si moltiplicano secondo le regole note del calcolo letterale.

Algoritmo della divisione. Dati due polinomi $A(x)$, $B(x) \in \mathbb{R}[x]$, sono determinati in modo unico i polinomi $Q(x)$ (**quoziente**) e $R(x)$ (**resto**) in $\mathbb{R}[x]$, tali che

$$A(x) = B(x)Q(x) + R(x)$$

con $R(x) = 0$ oppure $\deg R(x) < \deg B(x)$.
Se $\deg A(x) = n$, $\deg B(x) = m$:
i) se $m \leqslant n \Rightarrow \deg Q(x) = n - m$ e $\deg R(x) < m$;
ii) se $m > n \Rightarrow \deg Q(x) = 0$ e $R(x) = A(x)$.

Se nel polinomio $A(x) \in \mathbb{R}[x]$, x è sostituita da un $c \in \mathbb{R}$, il risultato è un elemento di $\mathbb{R}$ (e lo stesso vale se invece di $\mathbb{R}$ lavoriamo in $\mathbb{C}$).

Esempio.
$A(x) = x^3 - 2x^2 + 2 \in \mathbb{R}[x]$
$A(3) = 27 - 18 + 2 = 11 \in \mathbb{R}$.

Teorema del resto. Siano $A(x) \in \mathbb{R}[x]$ e $B(x) = x - c$, con $c \in \mathbb{R}$. Il resto della divisione di $A(x)$ per $B(x)$ è $A(c)$.

Infatti $A(x) = (x - c)Q(x) + R(x)$ e ponendo $x = c$ si ottiene $A(c) = R(c) = R(x)$ perchè il grado del resto deve essere, in questo caso, zero (il

grado del resto è minore del grado del polinomio divisore) e quindi $R(x)$ è un polinomio costante.

ESEMPIO.
$A(x) = x^3 - 2x^2 + 2$, $B(x) = x - 3$.
$R(x) = A(3) = 11$.
Il risultato si può facilmente verificare eseguendo la divisione tra i due polinomi.

Dati $A(x), B(x) \in \mathbb{R}[x]$ con $B(x) \neq 0$, diciamo che $A(x)$ è **divisibile** per $B(x)$ se $A(x) = B(x)Q(x)$, cioè se il resto della divisione è 0.
$c \in \mathbb{R}$ si dice **radice** (o **zero**) di un polinomio $A(x) \in \mathbb{R}[x]$ se $A(c) = 0$.

Teorema di Ruffini. Se $A(x) \in \mathbb{R}[x]$ e $c \in \mathbb{R}$, allora c è radice di $A(x) \Leftrightarrow A(x)$ è divisibile per $x - c$.

Teorema fondamentale dell'algebra. Ogni polinomio $P(x) \in \mathbb{C}[x]$ di grado $n \geqslant 1$, ha sempre n radici in $\mathbb{C}$.
Se il polinomio è monico e le radici sono $x_1, ..., x_n$ allora possiamo scomporre il polinomio nella forma

$$P(x) = (x - x_1)(x - x_2)...(x - x_n).$$

Se una radice compare k volte nella scomposizione, diciamo che ha **molteplicità algebrica** k. In questo caso essa è radice non solo del polinomio, ma anche delle sue derivate fino all'ordine $k - 1$.

RELAZIONI DI RICORRENZA LINEARI OMOGENEE DI ORDINE 2

Possiamo ora concludere il discorso sulle relazioni di ricorrenza di ordine due. Ricordiamo che una relazione del tipo che stiamo studiando è:

$$au_{n+2} + bu_{n+1} + cu_n = 0$$

Non consideriamo la soluzione banale $u_n = 0$ per tutti gli n. Supponiamo che la soluzione cercata sia della forma $u_n = \alpha^n A$ con $A \neq 0$ Allora deve essere:

$$a\alpha^{n+2}A + b\alpha^{n+1}A + c\alpha^n A = 0$$

Quindi si ottiene (dividendo per un $u_n = \alpha^n A$ diverso da zero, che esiste per ipotesi) $a\alpha^2 + b\alpha + c = 0$. Ciò significa che α deve essere soluzione della seguente equazione di secondo grado, detta **equazione ausiliaria**:

$$ax^2 + bx + c = 0$$

Ci sono ora tre casi, distinti in base al tipo di radici della equazione ausiliaria:

a) l'equazione ha **due radici reali e distinte** α e β : è immediato verificare che la soluzione è:

$$u_n = A\alpha^n + B\beta^n$$

con A e B determinati dalle condizioni: $u_0 = A + B$ e $u_1 = A\alpha + B\beta$

b) l'equazione ha **due radici reali e coincidenti** $\alpha = \beta = -b/2a$: la soluzione è:

$$u_n = (A + Bn)\alpha^n$$

con A e B determinati dalle condizioni: $u_0 = A$ e $u_1 = A\alpha + B\alpha$.

Infatti già sappiamo che $A\alpha^n$ è una soluzione; sostituendo $Bn\alpha^n$ nella relazione $au_{n+2} + bu_{n+1} + cu_n$ si ottiene:

$$aB(n+2)\alpha^{n+2} + bB(n+1)\alpha^{n+1} + cBn = \alpha^n(Bn(a\alpha^2 + b\alpha + c) + B(2a\alpha + b))$$

Ma $a\alpha^2 + b\alpha + c = 0$ e $2a\alpha + b = 0$ perchè α è radice di molteplicità 2 e quindi $\Delta = b^2 - 4ac = 0$. Avendo mostrato che $A\alpha^n$ e $Bn\alpha^n$ sono soluzioni, anche la loro somma lo è.

c) l'equazione ha **due radici complesse coniugate** α e $\bar{\alpha}$: è immediato verificare che la soluzione è

$$u_n = A\alpha^n + B\bar{\alpha}^n$$

Siccome per ipotesi u_n è un numero **reale** per ogni n, segue che B **deve essere il complesso coniugato di** A. Inoltre, posto $\alpha = re^{i\theta}$, si ha $\alpha^n = r^n e^{in\theta}$ e $\bar{\alpha}^n = r^n e^{-in\theta}$ per cui (ricordando che $e^{in\theta} = \cos n\theta + i \sin n\theta$)

$$u_n = r^n(C \cos n\theta + D \sin n\theta)$$

Dove $C = A + B$ e $D = i(A - B)$ sono **due numeri reali determinati dalle condizioni:**

$$u_0 = C \text{ e } u_1 = r(C\cos\theta + D\sin\theta)$$

ESEMPIO: la relazione da risolvere sia:

$$u_{n+2} - 2u_{n+1} + 2u_n = 0 \text{ con } u_0 = 1, u_1 = 2$$

Le radici dell'equazione ausiliaria sono:

$$\alpha = 1 + i = \sqrt{2}e^{i\pi/4} \text{ e } \bar{\alpha} = 1 - i = \sqrt{2}e^{-i\pi/4}$$

La soluzione generale è:

$$u_n = \sqrt{2}^n(C\cos n\pi/4 + D\sin n\pi/4)$$

Le condizioni $u_0 = 1, u_1 = 2$ danno $C = 1$ e $2 = \sqrt{2}(C\cos\pi/4 + D\sin\pi/4)$ ovvero $C = D = 1$ perchè $\cos\pi/4 = \sin\pi/4 = 1/\sqrt{2}$. La soluzione della nostra relazione è quindi:

$$u_n = \sqrt{2}^n(\cos n\pi/4 + \sin n\pi/4)$$

IL PIANO COME SPAZIO VETTORIALE.

Con $\mathbb{R}^2$ indichiamo l'insieme delle coppie (a, b) di numeri reali. Si può definire la somma $(+)$ tra coppie:

$$(a, b) + (c, d) = (a + c, b + d)$$

e il prodotto $(\cdot)$ di un numero reale α per una coppia (a, b):

$$\alpha\,(a, b) = (\alpha a, \alpha b).$$

Con $\mathbb{R}^n$ (o $\mathbb{C}^n$) indichiamo l'insieme delle n-uple $(a_1, a_2, ..., a_n)$ di numeri reali (o complessi). In analogia con il caso di $\mathbb{R}^2$, si definiscono una somma e un prodotto per un numero reale (o complesso).

Le proprietà di queste operazioni serviranno come traccia per definire, più astrattamente, la nozione di **spazio vettoriale.**

Calcolo combinatorio

Il calcolo combinatorio consiste nello sviluppo di nozioni e tecniche per contare i possibili ordinamenti di un insieme e le possibili scelte di sottoinsiemi di un insieme. Ha numerosi collegamenti con diversi settori della matematica, come l'algebra, la geometria, il calcolo delle probabilità. Quello che è importante non è tanto applicare meccanicamente ai problemi le nozioni e le tecniche apprese, ma usarle (o, anche, non usarle se non è il caso) come strumenti per modellizzare, per individuare le proprietà o le rappresentazioni che ne consentono la soluzione.

Esempio II.0.1

Di 3 urne la I contiene i numeri {1, 2, 3, 4, 5}, la II i numeri {11, 12, 13, 14, 15, 16}, la III i numeri {20, 21}. Quante sono le possibili sequenze composte da un numero della I urna, uno della II e uno della III? Evidentemente vi sono 5 scelte per la prima urna. Per la II urna vi sono 6 scelte per ciascuna delle 5 precedenti, per la III urna 2 scelte per ognuna delle 30 precedenti. Ciascuna scelta è indipendente dalle altre, quindi le possibili sequenze sono $5 \cdot 6 \cdot 2 = 60$.

Esempio II.0.2

Nella stessa situazione dell'esempio II.0.1, devo scegliere un numero a caso da una qualsiasi delle urne. Quante sono le scelte possibili? In questo caso la distribuzione dei numeri nelle urne è indifferente. Le scelte possibili saranno $5+6+2 = 13$. Questa formula vale perché non vi sono numeri che compaiono più volte (nella stessa urna o in urne diverse).

Adesso vediamo alcuni esempi di situazioni abbastanza frequenti in combinatoria, interessanti perché mettono bene in mostra alcune tecniche e alcuni modelli interpretativi.

II.1. Permutazioni

Le permutazioni di n elementi sono i possibili ordinamenti di un insieme di n elementi distinti.

Esempio II.1.1

4 atleti (A, B, C, D) partecipano a una gara per la quale non sono ammesse classificazioni alla pari. Quante sono le classifiche finali teoricamente possibili?

Possiamo ragionare come segue: al I posto potrebbe piazzarsi uno qualunque dei 4 atleti. Ciascuna di queste scelte dà origine a classifiche diverse. Per il II posto, per ciascuna delle scelte precedenti, rimangono 3 scelte possibili (una per ognuno degli atleti che non si sono classificati al I posto). Fino al II posto, le classifiche distinte possibili sono 12. Per il III posto rimangono 2 possibilità, che danno origine a 24 classifiche distinte. Per il IV posto rimane una sola possibilità. Quindi il numero delle classifiche possibili è 24.

Abbiamo trovato che le permutazioni di un insieme di 4 elementi sono 24, cioè $4 \cdot 3 \cdot 2 \cdot 1$; questo numero si può anche rappresentare con $4!$ e viene chiamato il fattoriale di 4 (vedi scheda 4).

Possiamo generalizzare il risultato dell'esempio e affermare che il numero delle permutazioni di un insieme finito di n elementi è $P_n = n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1 = n!$. Questo risultato dipende soltanto dal numero degli elementi distinti e non da altre proprietà.

Esempio II.1.2

Supponete di avere 5 cartellini, su ciascuno dei quali è riportata una cifra numerica, nel modo che segue: $\boxed{1}$, $\boxed{2}$, $\boxed{3}$, $\boxed{4}$, $\boxed{5}$. Quanti numeri distinti di cinque cifre potete rappresentare usando i 5 cartellini? In questo caso la situazione è analoga all'esempio 1: vi sono 5 possibilità per la I cifra, 4 per la seconda, ecc., in totale le permutazioni dei cartellini sono $5!$, e ciascuna permutazione dà origine a un numero diverso.

Esempio II.1.3

Supponete di avere 5 cartellini, su ciascuno dei quali è riportata una cifra numerica, nel modo che segue: $\boxed{1}$, $\boxed{2}$, $\boxed{3}$, $\boxed{4}$, $\boxed{4}$. Quanti numeri distinti di cinque cifre potete rappresentare usando i 5 cartellini?

Attenzione! Le permutazioni dei 5 cartellini sono sempre $5!$, ma non danno origine ad altrettanti numeri distinti. Infatti per ogni permutazione, se si scambiano fra loro i due cartellini con la cifra 4 si ottiene il medesimo numero. In altre parole, ogni numero è generato da due diverse permutazioni dei cartellini. Quindi i numeri distinti che si possono ottenere sono $\frac{5!}{2}$.

Esercizi

II.1.1 Quanti sono i numeri distinti di 3 cifre che si possono formare (in base dieci) con $\boxed{5}$, $\boxed{6}$, $\boxed{6}$?

II.1.2 Idem, ma con $\boxed{6}$, $\boxed{6}$, $\boxed{6}$.

II.1.3 Quanti sono i numeri distinti di 4 cifre che si possono formare (in base dieci) con $\boxed{5}$, $\boxed{6}$, $\boxed{6}$, $\boxed{6}$?

II.1.4 Idem, ma con $\boxed{5}$, $\boxed{5}$, $\boxed{6}$, $\boxed{6}$.

II.2. Disposizioni semplici

Una generalizzazione dell'idea di permutazione è data eliminando il vincolo per cui il numero degli elementi n è pari al numero dei posti k e considerando situazioni in cui $k \le n$. Una *disposizione semplice* (cioè, senza ripetizioni) *di n elementi k a k* è una sequenza ordinata di k elementi presi da un insieme di n elementi $(k \le n)$, senza ripetizioni.

Esempio II.2.1

A una finale di atletica partecipano 8 concorrenti. I primi 3 classificati, nell'ordine, salgono sul podio. Quante sono tutte le possibili composizioni del podio?

Il ragionamento non è molto diverso da quelli precedenti: ci sono 8 possibilità per il I posto, 7 per il II, 6 per il III, quindi in totale $8 \cdot 7 \cdot 6 = \frac{8!}{(8-3)!} = 336$ possibilità. Va osservato che in casi come questo l'ordine in cui gli atleti si dispongono sul podio è rilevante, mentre non è rilevante quello che accade a partire dal quarto posto. Abbiamo calcolato il numero delle disposizioni semplici di 8 elementi 3 a 3, che viene solitamente indicato con $D_{8,3}$. Più in generale, il numero delle disposizioni di n elementi k a k $(k \le n)$ è dato da: $D_{n,k} = n \cdot (n-1) \cdot \ldots \cdot (n-k+1) = \frac{n!}{(n-k)!}$.

Esercizi

II.2.1 In relazione all'esempio 1, supponete di sapere chi sono i primi 3 classificati ma di non sapere in che ordine. Quante sono le possibili composizioni del podio in questo caso?

II.2.2 Sempre in relazione all'esempio 1, supponete che 3 concorrenti (su 8) vengano squalificati e alla gara partecipino solo 5 atleti. Quante sono le possibili composizioni del podio in questo caso?

II.2.3 Uno studente ha frequentato 4 corsi e decide di sostenere 3 esami nella prossima sessione. Non ha ancora deciso quali esami sostenere e in che ordine. Fra quante possibilità può scegliere? Che cosa cambierebbe se decidesse di sostenere 4 esami?

II.2.4 Supponete di avere cinque cartellini, su ciascuno dei quali è riportata una cifra, nel modo che segue: $\boxed{1}$, $\boxed{2}$, $\boxed{3}$, $\boxed{4}$, $\boxed{5}$. Quanti numeri distinti di quattro cifre potete rappresentare usando 4 cartellini per volta?

II.3. Combinazioni semplici

Una ulteriore generalizzazione è ottenuta se non si tiene conto dell'ordine. Una *combinazione semplice di n elementi k a k* è una scelta di k elementi presi da un insieme di n elementi $(k \le n)$, senza ripetizioni, in situazione in cui l'ordine in cui vengono scelti gli elementi non è rilevante.

Esempio II.3.1

A una gara di atletica partecipano 8 concorrenti. I primi 3 classificati sono ammessi a una gara successiva, indipendentemente dal loro piazzamento. Quante sono le 'terne' di qualificati possibili?

Possiamo ragionare come segue. Alcune terne che nell'esempio precedente erano distinte adesso sono equivalenti; più precisamente, a ogni terna di qualificati corrispondono 6 (cioè, 3!) configurazioni del podio: gli ordini di arrivo che qualificano A, B, C sono tanti quante le loro permutazioni, e cioè ABC, ACB, BAC, BCA, CAB, CBA. Quindi possiamo prima calcolare quante sono le disposizioni semplici di 8 elementi 3 a 3 (come nell'esempio II.2.1), poi dividendo per 6 troviamo il numero delle combinazioni. Abbiamo calcolato il numero delle combinazioni semplici di 8 elementi 3 a 3, e abbiamo usato la formula $C_{8,3} = \frac{8!}{(8-3)!3!}$. Più in generale, il numero delle combinazioni semplici di n elementi k a k $(k \le n)$ è dato dalla formula $C_{n,k} = \frac{D_{n,k}}{k!} = \frac{n!}{(n-k)!k!}$. L'espressione $\frac{n!}{(n-k)!k!}$ viene chiamata anche *coefficiente binomiale*, si può abbreviare con $\binom{n}{k}$ e si legge: "n su k". Nella scheda 5 viene spiegato il perché di questa denominazione.

Esercizi

II.3.1. Il concorso del 'Totogol' consiste nel pronosticare le 8 partite di calcio in cui si segna il maggior numero di reti, scelte in un insieme di 30, con criteri opportuni per risolvere i casi di ex-aequo. Non è richiesto di specificare alcun ordine fra le 8 partite. Quante sono le possibili combinazioni che si potrebbero verificare in ogni concorso?

II.3.2. Una società sportiva organizza un torneo giovanile di calcio, che prevede 16 partite e intende organizzare una gara a premi sul tipo del 'Totogol'. Verranno premiati tutti coloro che indovinano le 6 partite in cui si segna il maggior numero di reti. Quante schedine sarebbe necessario giocare per avere la certezza di vincere un premio?

II.3.3. Nella situazione precedente, come modifichereste il numero delle partite da indovinare in modo da rendere la gara più facile possibile? E per renderla più difficile possibile?

II.3.4. Un insieme contiene 10 elementi. Quanti sono i suoi sottoinsiemi che contengono esattamente 4 elementi? E quelli che ne contengono 2? E quelli che ne contengono …?

II.4. Disposizioni con ripetizione

Nella definizione di disposizione semplice si richiedeva che non vi fossero ripetizioni e che $k \leq n$. Se si rinuncia a qusti vincoli si ottiene la definizione di disposizione con ripetizioni. Una *disposizione con ripetizioni di n elementi k a k* è una sequenza ordinata di *k* elementi presi da un insieme di *n* elementi, con la possibilità di ripetizioni.

Esempio II.4.1

2 tennisti, A e B, disputano una serie di 8 partite. Supponiamo di scrivere un elenco in cui per ognuna delle 8 partite viene riportato il nome del vincitore. Quanti sono gli elenchi possibili.

In questo caso occorre contare tutte le sequenze ordinate di 8 simboli, composte con i simboli A e B. Per ciascuna partita il vincitore può essere A oppure B, senza vincoli. Quindi le sequenze possibili sono $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^8$. Quindi le disposizioni con ripetizione di 2 elementi 8 a 8 sono 2^8. In generale le disposizioni con ripetizione di *n* elementi *k* a *k* sono n^k.

Esercizi

II.4.1. Quante sono le possibili colonne vincenti al Totocalcio?

II.4.2. Ogni mattina il professore della I ora segna nel registro, accanto ai nomi degli alunni, disposti in ordine alfabetico, il simbolo P (presente) o A (assente). Sapendo che gli alunni sono 20, quante sono le sequenze di simboli teoricamente possibili ogni mattina?

II.4.3. Considerate l'insieme {1, 2, 3, 4, 5, 6}. Quanti sono i suoi sottoinsiemi? (Questo problema può essere risolto con ragionamenti diversi: provate a individuarne un paio.)

Il problema dei compleanni:

Consideriamo le disposizioni con ripetizione di *n* elementi *k* a *k* che sono n^k: alcune di esse (le disposizioni semplici che sono $\frac{n!}{(n-k)!}$), non presentano ripetizioni. Possiamo concludere che la probabilità che **non** ci siano ripetizioni è $p=n!/(n-k)!\ n^k$. Ovviamente $1-p$ è, invece, la probabilità che ci siano ripetizioni. Questa formula fornisce risultati abbastanza sorprendenti.

Quale è la probabilità che su cinquanta studenti due di essi festeggino il compleanno lo stesso giorno? Applicando la formula con n=365 e k=50 si ottiene circa 99% !

Problemi vari

PII.1. Quanti sono, in base dieci, i numeri di tre cifre, senza cifre ripetute, compresi tra 200 e 400 ?

PII.2. Quanti sono, in base dieci, i numeri di tre cifre in cui non compare la cifra 0?

PII.3. Un esame scritto consiste di 3 domande. Si sa che i candidati sono 30, che la domanda 1 ha avuto 20 risposte corrette, che la domanda 2 ha avuto 20 risposte corrette e la domanda 3 ha avuto 15 risposte corrette. Come potrebbe variare il numero dei candidati che hanno risposto correttamente a tutte le 3 domande?

PII.4. E' dato l'insieme di lettere dell'alfabeto italiano A:= {a, b, c, d, e}.

a. Quanti sono i sottoinsiemi di A che non contengono consonanti?
b. Quanti sono i sottoinsiemi B di A tali che $a \in B$ ma $b \notin B$?
c. Quanti sono i sottoinsiemi di A contenenti al più 3 elementi?

PII.5. Supponete di disporre dei 6 cartellini raffigurati di seguito, su ognuno dei quali è stampato un numero.

$\boxed{1}$ $\boxed{2}$ $\boxed{3}$ $\boxed{4}$ $\boxed{4}$ $\boxed{4}$

a. Quanti numeri distinti (di 6 cifre in base dieci) si possono comporre usando tutti i 6 cartellini?
b. Quanti numeri distinti (di 5 cifre in base dieci) si possono comporre usando 5 a scelta dei 6 cartellini?

P.II.6. Supponete di avere i cinque cartellini rappresentati di seguito, su ognuno dei quali è stampata una cifra numerica: $\boxed{0}$, $\boxed{1}$, $\boxed{2}$, $\boxed{2}$, $\boxed{3}$ e di affiancarli per comporre numeri telefonici di cinque cifre (rappresentati in base dieci). Un numero telefonico non può iniziare con 0.

a. Quanti numeri telefonici distinti potete ottenere affiancando i cinque cartellini?
b. Quanti numeri telefonici distinti (di 5 cifre) potete ottenere se disponete inoltre di un sesto cartellino $\boxed{4}$?

P.II.7. E' dato il seguente insieme di numeri interi A:= {4, 11, 761, 22, 7, 80}.

a. Quanti sono i sottoinsiemi di A che non contengono numeri pari?
b. Quanti sono i sottoinsiemi B di A i cui elementi sono dispari oppure divisibili per 4?
c. Quanti sono i sottoinsiemi di A contenenti al più 4 elementi?

P.II.8. Considerate gli insiemi A:= {0, 1, 2, 3, 4}, B:= {0, 1, 2, 3, 4, 5} con l'ordinamento usuale. Quante sono le funzioni f: A→A che verificano la condizione "$x<y \Rightarrow f(x)<f(y)$".

PII.9. Considerate l'insieme I_5:= {1, 2, 3, 4, 5} con le usuali relazioni d'ordine sui numeri naturali.

a. Quante sono le funzioni f: $I_5 \to I_5$ tali che, dati m, n, se $m<n$, allora $f(m)<f(n)$?
b. Quante sono le funzioni iniettive f: $I_5 \to I_5$ tali che $f(3)<f(2)<f(1)$?

P.II.10. Considerate l'insieme I_4:= {1, 2, 3, 4} con le usuali relazioni d'ordine sui numeri naturali.

a. Quante sono le funzioni f: $I_4 \to I_4$ tali che, dati m, n, se $m<n$, allora $f(m)<f(n)$?
b. Quante sono le funzioni iniettive f: $I_4 \to I_4$ tali che $f(3)<f(2)$?
c. Se dalla domanda b. si elimina la condizione di iniettività, il numero richiesto aumenta, diminuisce o rimane costante?

Scheda 4

IL FATTORIALE

Dato un numero naturale n, il fattoriale di n, in formula $n!$, è il prodotto di tutti i numeri naturali da 1 a n.
Quindi $n! = 1\cdot 2\cdot 3\cdot \ldots \cdot(n-2)\cdot(n-1)\cdot n$. Il fattoriale di 0 vale 1 per convenzione.
È possibile definire il fattoriale induttivamente, nel modo che segue:

$$\begin{cases} 0! = 1 \\ (n+1)! = (n+1)n! \end{cases}$$

Esercizi

S4.1. Calcolate $n!$ per $n=0$, $n=1$, $n=2$, $n=3$, $n=4$, $n=5$, $n=6$.

S4.2. Provate (come?) che per ogni numero naturale n e per ogni numero naturale k, $n!\bullet(n+k)!$.

S4.3. Stabilite se è vero che $\frac{6!}{3!} = 3!$.

S4.4. Dato un qualunque numero naturale m, calcolate $\frac{m!}{(m-2)!}$.

S4.5. Stabilite se è vero che per ogni numero naturale n e ogni numero naturale k tale che $0<k\bullet m$, vale:

$$m\cdot(m-1)\cdot(m-2)\cdot\ldots\cdot(m-k+1) = \frac{m!}{(m-k)!}$$

Scheda 5

IL COEFFICIENTE BINOMIALE

Dati i numeri naturali n, k (k•n) si definisce: $\binom{n}{k} = \frac{n!}{(n-k)!k!}$

Il coefficiente binomiale trae il suo nome dallo sviluppo delle potenze dei binomi. Vale infatti la formula:

$$(a+b)^n = \sum_{i=0}^{n}\binom{n}{i}a^{n-i}b^i$$

Lo sviluppo di $(a+b)^n$ è dato dalla somma di 2^n monomi ciascuno dei quali è della forma $a^{n-i}b^i$. Se $i=0$ c'è un solo monomio di quella forma, e il coefficiente è 1. Se $i=1$, ci sono n monomi di quella forma (tutti quelli ottenuti moltiplicando un solo fattore b per $n-1$ fattori a).
Quindi il numero di monomi simili a un monomio della forma $a^{n-i}b^i$ è pari al numero delle combinazioni semplici di n elementi i a i.

Esercizi

S.5.1. Calcolate $\binom{4}{k}$ per tutti i valori interi di k compresi fra 0 e 4.

S.5.2. Provate che per ogni n naturale, $\binom{n}{0} = \binom{n}{n} = 1$.

S.5.3. Provate che per ogni n naturale, $\binom{n}{1} = \binom{n}{n-1} = n$.

S.5.4. Provate che per ogni n e ogni k naturali tali che $k\bullet n$, $\binom{n}{k} = \binom{n}{n-k}$.

S.5.5. Provate che per ogni n e ogni k naturali tali che $k\bullet n$, $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$.

1. Aritmetica Modulare e Applicazioni

Le parti precedute dal simbolo ► (adattate dal sistema di aiuto in linea del programma Scientific Workplace) si riferiscono alle procedure da seguire per svolgere i conti e fanno parte solo della versione "interattiva" della lezione.

1.1. Equazioni diofantine

Le *equazioni Diofantine* più semplici sono equazioni della forma $ax + by = c$ dove a, b e c sono *numeri interi*. Si cercano soluzioni in cui x e y sono anch'essi *numeri interi*. Una condizione necessaria e sufficiente per la sua risolubilità in numeri interi è che c sia divisibile per il *Massimo Comun Divisore di* a e b . La necessità della condizione è ovvia, un esempio chiarisce il metodo di risoluzione (e, con esso, la sufficienza).

Esempio: $122x+184y = 42$ è risolubile perchè 42 è divisibile per $\gcd(122, 184) = 2$. Dividendo si ottiene $61x + 92y = 21$. Si osservi che, se si conosce una soluzione particolare di $61x + 92y = 1$, allora moltiplicando la soluzione per 21 si trova una soluzione particolare dell'equazione originale. Per trovare una soluzione particolare basta impostare *l'algoritmo euclideo* delle divisioni successive fino a ottenere come resto finale il $\gcd(61, 92) = 1$.

$\frac{92}{61} = 1 + \frac{31}{61}$, $\frac{61}{31} = 1 + \frac{30}{31}$, $\frac{31}{30} = 1 + \frac{1}{30}$

Allora si ottiene, partendo dalla prima, e scrivendo via via tutti i resti in funzione dei numeri di partenza:

$31 = 92 - 61$, $30 = 61 - 92 + 61$, $1 = 92 - 61 - 61 - 61 + 92$

Cioè:

$61 \times (-3) + 92 \times 2 = 1$

Allora una soluzione particolare dell'equazione è $x = 21 \times (-3) = -63$ e $y = 21 \times 2 = 42$. Ovviamente la soluzione generale si trova sommando alla soluzione particolare tutte le *soluzioni intere* di $61x + 92y = 0$ ($x = -92k$, $y = 61k$ con k intero arbitrario). In definitiva si ottiene che tutte le soluzioni intere di: $122x + 184y = 42$ sono date da:

$x = -63 - 92k$ e $y = 42 + 61k$.

L'opzione Integer nel submenu Solve trova le soluzioni intere di equazioni e sistemi.

► Solve + Integer

$$122x + 184y = 42, \text{ Solution is : } \{x = -63 - 92N_1, y = 42 + 61N_1\},$$

L'intero k usato prima è rimpiazzato, dal programma, da N_1.

▶ Solve + Integer

$$\begin{matrix} 3x + 2y = 5 \\ 3x - z = 1 \end{matrix}, \text{ Solution is : } \{x = 5 - 2N_1, y = -5 + 3N_1, z = -6N_1 + 14\}$$

Infatti: $3x + 2y = 3(5 - 2N_1) + 2(-5 + 3N_1) = 5$ e $3x - z = 3(5 - 2N_1) - (-6N_1 + 14) = 1$.

1.2. Congruenze, resti e la funzione "mod(n)".

Due numeri interi a e b sono *congruenti modulo* m quando $a - b$ è un multiplo di m, in questo caso si scrive: $a \equiv b \pmod{m}$. Ad esempio, $15 \equiv 33 \pmod{9}$, infatti $15 - 33 = -18$ che è multiplo of 9.

Dati due interi a e m, la *funzione modulo* è data da: $a \bmod m = b$ se e solo se $a \equiv b \pmod{m}$ e $0 \leq b \leq m - 1$; quindi, $a \bmod m$ è il più *piccolo resto non negativo* della divisione di a per m.

▶ Per calcolare la funzione mod

1. Selezionare l'espressione $a \bmod b$.
2. Selezionare Evaluate.

▶ Evaluate

$$23 \bmod 14 = 9 \text{ mentre invece } (-23) \bmod 14 = 5$$

Infatti: $23 = 1 \times 14 + 9$, mentre, se vogliamo un resto positivo, $-23 = -2 \times 14 + 5$

Se a è positivo, si può trovare il valore di a modulo m applicando Expand al quoziente $\frac{a}{m}$.

▶ Expand

$$\frac{23}{14} = 1\frac{9}{14}$$

(in questa notazione, il primo numero è la parte intera del risultato)

Siccome $1\frac{9}{14} = 1 + \frac{9}{14}$,la moltiplicazione di $\frac{23}{14} = 1 + \frac{9}{14}$ per 14 dimostra che $23 \bmod 14 = 9$.

1.3. Tavole di somma e moltiplicazione Modulo m

Ogni intero a, usando la funzione $\bmod m$, si può trasformare in un intero appartenente all'insieme $\mathbf{Z}_m = \{0, 1, 2, \ldots, m-1\}$. Prendendo la "riduzione modulo m" della somma e della moltiplicazione tra numeri interi usuali si possono definire due nuove operazioni tra *"numeri modulo m"* cioè operazioni tra elementi dell'insieme $\mathbf{Z}_m$. L'importanza di queste operazioni risiede nel fatto che *il risultato di ambedue le operazioni resta all'interno dell'insieme Z_m* : le operazioni si dicono interne.

La somma è definita da: $(a \bmod m) + (b \bmod m) = (a + b) \bmod m$ e il prodotto da $(a \bmod m) \cdot (b \bmod m) = (a \times b) \bmod m$.

Esempi: $111 \bmod 6 = 3$, $459 \bmod 6 = 3$, $111 \times 459 = 50\,949$ e $111 + 459 = 570$.Si ottiene $50\,949 \bmod 6 = 3$ e $570 \bmod 6 = 0$ cioè $3 \cdot 3 = 3$ e $3 + 3 = 0$

Si noti che, ad esempio, $(2 \times 3) \bmod 6 = 0$ anche se $2 \bmod 6 = 2$ e $3 \bmod 6 = 3$ sono entrambi diversi da 0. Questo è vero in generale: se m non è un numero primo alcuni prodotti (quali?) danno come risultato 0 anche se ambedue i fattori sono, modulo m, diversi da 0.

▶ Per ottenere rapidamente la tabella di moltiplicazione modulo m (ad esempio con $m = 6$)

1. Definire la funzione $g(i, j) = (i - 1)(j - 1) \bmod 6$
2. Dal menu Matrices , selezionare Fill Matrix.
3. Selezionare Defined by Function.
4. Scrivere g nel campo Enter Function Name.
5. Selezionare 7 rows e 7 columns.
6. Selezionare OK.

1. Selezionare la matrice e infine Evaluate.

▶ Evaluate

0	0	0	0	0	0
0	1	2	3	4	5
0	2	4	0	2	4
0	3	0	3	0	3
0	4	2	0	4	2
0	5	4	3	2	1

► Per migliorare la leggibilità si può procedere così:

1) Fare una copia di questa matrice.

2) Dal menu Edit selezionare Insert Row(s)..., e aggiungere una nuova riga in alto.

3) Selezionare Insert Column(s)..., e aggiungere una nuova colonna a sinistra.

4) Riempire poi gli spazi vuoti come segue:

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Dalla tavola vediamo, ad esempio, che $2 \cdot 4 = 2$, $5 \cdot 2 = 4$ e $5 \cdot 5 = 1$ (Le linee orizzontali e verticali e il simbolo della moltiplicazione sono stati aggiunti per maggiore leggibilità)

Se p è primo, ad esempio 7, gli interi modulo p sono particolarmente importanti perchè nella tavola di moltiplicazione lo zero (0) appare solo come risultato di (0·qualche cosa) e in questa essenziale proprietà ricordano gli usuali numeri interi.

$\cdot$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

$+$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

1.4. Inversi Modulo m

Se $ab \bmod m = 1$, allora b è detto essere un *inverso* di a *modulo* m, si indica con $a^{-1} \bmod m$ il più piccolo resto positivo della divisione di b per m. L'inverso di a si può trovare applicando la definizione: $ab \bmod m = 1$ significa che $ab = km + 1$, con k intero, cioè si deve risolvere l'equazione diofantina (nelle incognite x e y):

$$ax - my = 1$$

E poi calcolare $b = x \bmod m$ .Spiegheremo dopo (vedi Teorema di Eulero) alcuni metodi più efficienti per trovare (quando esiste!) l'inverso modulo m di un numero.

Se m è un numero primo, ogni $a \neq 0 \bmod m$ possiede un inverso modulo m. Se m non è un numero primo, possiedono inverso modulo m solo i numeri a primi con m. (Nella tavola di moltiplicazione i "numeri modulo m" che possiedono inverso si riconoscono dal fatto che nella loro riga compare il numero uno)

$\gcd(24277, 54) = 1$ allora $24277^{-1} \bmod 54 = 7$

$\gcd(146524, 35) = 7$ allora $146524^{-1} \bmod 35$ non esiste anche se $146524 \bmod 35 = 14 \neq 0$.

▶ Evaluate

$5567^{-1} \bmod 7 = 4$

Infatti $5567 \times 4 \bmod 7 = 1$. Altre notazioni utilizzabili per gli inversi modulo m includono $1/a \bmod m$ e $\frac{1}{a} \bmod m$.

▶Evaluate

$1/23 \bmod 257 = 190$

$\frac{1}{5} \bmod 6 = 5$

La notazione $a/b \bmod m$ va interpretata come $(a \times (b^{-1} \bmod m)) \bmod m$; cioè, trovare l'inverso di b modulo m, moltiplicare il risultato per a, e poi ridurre il prodotto modulo m.

▶ Evaluate

$3/23 \bmod 257 = 56$ (infatti $(3 \times 190) \bmod 257 = 56$)

$\frac{2}{5} \bmod 6 = 4$

1.5. Equazioni Modulo m

Per risolvere una equazione della forma $ax \equiv b \pmod{m}$ si moltiplicano ambo i membri per $a^{-1} \bmod m$ e si ottiene $x = b/a \bmod m$.

Naturalmente questo si può fare se e solo se $a^{-1} \bmod m$ è diverso da 0.

Esempio: $17x \equiv 23 \pmod{127}$ ha, fra le sue soluzioni, $x = 91$, come illustrato dai seguenti passaggi:

- Evaluate

  $23/17 \bmod 127 = 91$

- Evaluate

  $17 \cdot 91 \bmod 127 = 23$

Notare che, siccome 91 è una soluzione di $17x \equiv 23 \pmod{127}$, tutte le altre soluzioni sono date da $91 + 127n$, dove n è un intero qualsiasi. Infatti, $x \equiv 91 \pmod{127}$ vuole dire proprio che $x = 91 + 127n$ per un qualche intero n.

1.6. Coppie di Congruenze lineari

Siccome le congruenze del tipo $ax \equiv b \pmod{m}$ si riducono a $x \equiv c \pmod{m}$, considereremo solo congruenze di questo tipo.

Esempio: sia da risolvere

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

Se i moduli m e n sono *primi fra loro* ($\gcd(m, n) = 1$) ,allora c'è una unica soluzione (modulo $m \times n$)

Consideriamo

$$\begin{aligned} x &\equiv 45 \pmod{237} \\ x &\equiv 19 \pmod{419} \end{aligned}$$

Si trova $\gcd(237, 419) = 1$, così 237 e 419 sono primi fra loro. la prima congruenza fornisce $x = 45 + 237k$ per qualche intero k. Sostituendo nella seconda,

$$45 + 237k = 19 + 419r$$

per un certo r. Questa equazione si può riscrivere $237k = (19 - 45) \bmod 419$, che ha come soluzione:

$$k = (19 - 45)/237 \bmod 419 = 60$$

Quindi,

$$x = 45 + 237 \times 60 = 14265$$

Infatti, $14265 \bmod 237 = 45$ e $14265 \bmod 419 = 19$.

La soluzione generale è data da:

$$x = 14265 + 237 \times 419s$$

Ovvero:

$$x \equiv 14265 \pmod{99303}$$

In generale, *se m e n sono primi fra loro*, le congruenze,

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

danno:

$$x = a + m\,[(b - a)/m \bmod n]$$

La soluzione completa è:

$$x = a + m\,[(b - a)/m \bmod n] + s \times m \times n$$

dove s è un intero arbitrario.

Si osservi che la formula precedente ci dice che, *se m e n sono numeri primi*, se $x \equiv 1 \pmod{m}$ e $x \equiv 1 \pmod{n}$ allora $x \equiv 1 \pmod{m \times n}$, infatti $x = 1 + s \times m \times n$. Questa osservazione sarà importante nel seguito.

1.7. Sistemi di Congruenze Lineari

Il cosiddetto *teorema cinese del resto* dice che, *se i moduli sono primi tra loro a coppie*, allora c'è un'unica soluzione modulo il prodotto di tutti i moduli.

$$\begin{aligned} x &\equiv 45 \pmod{237} \\ x &\equiv 19 \pmod{419} \\ x &\equiv 57 \pmod{523} \end{aligned}$$

Si verifica che $\gcd(237 \times 419, 523) = 1$; il sistema ha quindi soluzione. Le prime due congruenze (come visto sopra) sono rimpiazzate da $x \equiv 14265 \pmod{99303}$; quindi il sistema diventa:

$$\begin{aligned} x &\equiv 14265 \pmod{99303} \\ x &\equiv 57 \pmod{523} \end{aligned}$$

Come prima, $14265+99303k = 57+523r$. Così, $k = (57 - 14265)/99303 \bmod 523 = 134$; quindi $x = 14265 + 99303 \times 134 = 13320867$. Il sistema è quindi risolto da:

$$x \equiv 13320867 \pmod{51935469}$$

1.8. Aritmetica in altissima precisione

I sistemi moderni di computer algebra supportano calcoli con interi di milioni di cifre, come fanno?

Incominciamo a generare un po' di numeri primi fra loro a coppie:

$$(997, 999, 1000, 1001, 1003, 1007, 1009)$$

▶ Factor

$$\begin{bmatrix} 997 \\ 999 \\ 1000 \\ 1001 \\ 1003 \\ 1007 \\ 1009 \end{bmatrix} = \begin{bmatrix} 997 \\ 3^3 37 \\ 2^3 5^3 \\ 7 \times 11 \times 13 \\ 17 \times 59 \\ 19 \times 53 \\ 1009 \end{bmatrix}$$

Consideriamo i numeri 23890864094 e 1883289456. Rappresentiamoli "a pezzi" modulo i numeri trovati prima:

$$23890864094 \longleftrightarrow \begin{bmatrix} 23890864094 \bmod 997 & = 350 \\ 23890864094 \bmod 999 & = 872 \\ 23890864094 \bmod 1000 & = 94 \\ 23890864094 \bmod 1001 & = 97 \\ 23890864094 \bmod 1003 & = 879 \\ 23890864094 \bmod 1007 & = 564 \\ 23890864094 \bmod 1009 & = 218 \end{bmatrix}$$

$$1883289456 \longleftrightarrow \begin{bmatrix} 1883289456 \bmod 997 & = 324 \\ 1883289456 \bmod 999 & = 630 \\ 1883289456 \bmod 1000 & = 456 \\ 1883289456 \bmod 1001 & = 48 \\ 1883289456 \bmod 1003 & = 488 \\ 1883289456 \bmod 1007 & = 70 \\ 1883289456 \bmod 1009 & = 37 \end{bmatrix}$$

Thus, the product $23890864094 \cdot 1883289456$ is represented by the vector

$$\begin{bmatrix} 350 \cdot 324 \bmod 997 & = 739 \\ 872 \cdot 630 \bmod 999 & = 909 \\ 94 \cdot 456 \bmod 1000 & = 864 \\ 97 \cdot 48 \bmod 1001 & = 652 \\ 879 \cdot 488 \bmod 1003 & = 671 \\ 564 \cdot 70 \bmod 1007 & = 207 \\ 218 \cdot 37 \bmod 1009 & = 1003 \end{bmatrix}$$

Il prodotto $23890864094 \times 1883289456$ è ovviamente una soluzione del sistema:

$$\begin{aligned} x &\equiv 739 \pmod{997} \\ x &\equiv 909 \pmod{999} \\ x &\equiv 864 \pmod{1000} \\ x &\equiv 652 \pmod{1001} \\ x &\equiv 671 \pmod{1003} \\ x &\equiv 207 \pmod{1007} \\ x &\equiv 1003 \pmod{1009} \end{aligned}$$

Tutti i conti vengono quindi eseguiti "a pezzi" e poi ricostruiti solo alla fine.

1.9. Potenze Modulo m, Teoremi di Fermat e Eulero

▶ Per calcolare grandi potenze modulo m

Evaluate $a^n \bmod m$.

Define $a = 2789596378267275$, $n = 3848590389047349$, and $m = 2838490563537459$.

▶ Evaluate

$$a^n \bmod m = 26220\,18141\,09828$$

Il *piccolo teorema di Fermat* dice che, se p è primo e $0 < a < p$, allora

$$a^{p-1} \bmod p = 1$$

Eccone una dimostrazione elementare:
Il piccolo teorema di Fermat dice che, se p è primo e $0 < a < p$, (più in generale basta che $a \neq 0 \bmod p$) allora

$$a^{p-1} \bmod p = 1$$

Consideriamo l'insieme

$$Z_p^* = \{1, 2, ..., p-1\}$$

e l'insieme

$$M(a) = \{a \bmod p, 2a \bmod p, ..., (p-1)a \bmod p\}$$

Questi due insiemi coincidono: infatti se prendiamo un $m \in Z_p^*$, possiamo scriverlo come $(m \times a^{-1} \times a) \bmod p = (m \times a^{-1})a \bmod p$ e quindi $m \in M(a)$. Allora $Z_p^* \subseteq M(a)$ ma Z_p^* ha $p-1$ elementi distinti e non può essere quindi un sottoinsieme proprio di un insieme con al più $p-1$ elementi distinti; deve quindi coincidere con $M(a)$. Questo significa che

$$1 \times 2 \times ... \times (p-1) \bmod p = a \times 2a \times ... \times (p-1)a \bmod p.$$

Raccogliendo otteniamo: $(p-1)! \bmod p = a^{p-1} \times (p-1)! \bmod p$. Essendo $(p-1)! \bmod p \neq 0$, perchè $(p-1)!$ non contiene p come fattore, otteniamo la tesi.

Il teorema di Fermat fornisce un metodo per trovare $a^{-1} \bmod p$: siccome $a^p \bmod n = 1$, si ottiene subito che:

$$a^{-1} \bmod p = a^{p-2} \bmod p$$

Esempio: $p = 17$, $11^{16} \bmod 17 = 1$ e $11^{15} \bmod 17 = 14$ per cui $11^{-1} \bmod 17 = 14$

Dal piccolo teorema di Fermat otteniamo un importante risultato: il teorema di Eulero.

Se $n = p \times r$ con p e r due numeri primi, poniamo $\varphi(n) = (p-1)(r-1)$ (questa è detta la *funzione di Eulero*).

Dal piccolo teorema di Fermat si ottiene che $a^p \bmod p = a \bmod p$ per cui: $a^{\varphi(n)} \bmod p = a^{(p-1)(r-1)} \bmod p = a^{p(r-1)} a^{1-r} \bmod p = a^{r-1} a^{1-r} \bmod p = 1$ e anche:

$a^{\varphi(n)} \bmod r = a^{r(p-1))} a^{1-p} \bmod r = a^{p-1} a^{1-p} \bmod r = 1$. Essendo contemporaneamente $a^{\varphi(n)} \bmod p = 1$ e $a^{\varphi(n)} \bmod r = 1$ (con r e p primi fra loro) si ottiene

$$a^{\varphi(n)} \bmod n = 1$$

Questo è un caso particolare del Teorema di Eulero (è un caso particolare perchè supponiamo che n sia prodotto di due primi).

Il teorema di Eulero (che qui non dimostriamo) dice che se a e n sono primi fra loro, allora:

$$a^{\varphi(n)} \bmod n = 1$$

(anche quando n non è prodotto di due numeri primi). Dove, in questo caso, $\varphi(n)$ è il numero dei numeri $m < n$ e tali che $gcd(m, n) = 1$.

Esempio: $n = 14$, $\varphi(n) = 6$, $11^6 \bmod 14 = 1$

Il teorema di Eulero fornisce un metodo per trovare $a^{-1} \bmod n$: siccome $a^{\varphi(n)} \bmod n = 1$, si ottiene subito che:

$$a^{-1} \bmod n = a^{\varphi(n)-1} \bmod n$$

Esempio: $n = 15$, $\varphi(n) = 8$, $11^8 \bmod 15 = 1$ e $11^7 \bmod 15 = 11$ per cui $11^{-1} \bmod 15 = 11$.

- Evaluate

  $2^{1008} \bmod 1009 = 1$ (Fermat)

$r = 8311$, $p = 2738\,497\,289\,527\,589\,233\,333\,433$, $\varphi(n) = 8310 \times 2738\,497\,289\,527\,589\,233\,333\,432 = 22\,756\,912\,475\,974\,266\,529\,000\,819\,920$ e $n = 22\,759\,650\,973\,263\,794\,118\,234\,161\,663$

per cui $2^{22\,756\,912\,475\,974\,266\,529\,000\,819\,920} \bmod (22\,759\,650\,973\,263\,794\,118\,234\,161\,663) = 1$ (Eulero)

2. Quadrati modulo p e residui di Gauss

Un caso molto interessante di potenza modulo n è il quadrato; supponiamo di voler risolvere il seguente problema:

Trovare i valori di x per cui $x^2 = 4$ $(mod 7)$ cioè risolvere, nel campo Z_7 dei numeri modulo 7, l'equazione $x^2 = 4$. Si ottengono due soluzioni, $x = 2$ e $x = -2 \bmod 7 = 5$. Se invece l'equazione fosse $x^2 = 2$ le soluzioni sarebbero $x = 3$ e $x = -3 \bmod 7 = 4$ infatti $9 \bmod 7 = 16 \bmod 7 = 2$. Ancora, l'equazione $x^2 = 5$ non ha soluzioni (andate a controllare sopra: nella tavola di moltiplicazione modulo 7 il numero 5 non appare sulla diagonale). Naturalmente non dovrebbe essere necessario scrivere tutta la tavola di moltiplicazione, basta ragionare un pò (aiutati da Fermat e Gauss). Limitiamoci al caso in cui n sia un numero primo diverso da 2. (Il caso $n = 2$ è semplicissimo e lasciato al lettore volonteroso, il caso di n generico è risolto con un sistema di congruenze quando si abbia chiaro cosa succede per i fattori primi di n; per non appesantire troppo il corso faremo solo qualche esempio nel caso generale).

Se l'equazione $x^2 = a \pmod p$ con p *primo dispari* e $a \neq 0 \bmod p$ ammette soluzioni, allora a si dice essere *un residuo di Gauss modulo p*. In questo caso le soluzioni sono sempre due, siano b e $-b$ (quest'ultimo, in realtà, è uguale, $\bmod p$, a $p - b$). Essendo gli elementi di Z_p esattamente $p - 1$ si nota subito che ci sono sempre $(p - 1)/2$ residui e $(p - 1)/2$ non residui (a ogni residuo si associa una coppia di elementi e di coppie ce ne sono $(p-1)/2$). Se *a è un residuo*, si ha $a = b^2$ per cui Fermat ci dice che $a^{(p-1)/2} = b^{p-1} = 1$. Se invece *$a$ non è un residuo*, osservando che (ancora per il teorema di Fermat):

$$(a^{(p-1)/2} + 1)(a^{(p-1)/2} - 1) = a^{p-1} - 1 = 0$$

Siccome p è primo, almeno uno dei fattori deve essere uguale a 0, e quindi non essendo a un residuo deve essere $a^{(p-1)/2} = -1 = p - 1$.

Abbiamo ottenuto il più semplice dei criteri di Gauss: per sapere se l'equazione $x^2 = a \pmod p$ ammette soluzioni, si calcola $a^{(p-1)/2}$; se vale 1 ci sono soluzioni, se vale $p - 1$, no.

Esempio: $347^{504} \bmod 1009 = 1$ quindi ci sono interi x per cui $x^2 = 347 \bmod 1009$. *(Trovarli è un'altra storia...provate con 777 e 232)*

Se poniamo la seguente definizione $[a/p] = a^{(p-1)/2} \bmod p$ allora, se a è un residuo modulo p, $[a/p] = 1$, mentre se non è un residuo, $[a/p] = -1$.

Ecco invece un "difficile" risultato di Gauss detto *legge di reciprocità:* se $p \neq$

q sono due primi (diversi da 2).

$$[p/q] \times [q/p] = (-1)^{(p-1)/2 \times (q-1)/2}$$

Esempio: siano $p = 7$, $q = 1009$. Siccome $(p-1)/2 \times (q-1)/2 = 504 \times 3$ è un numero pari e p e q due primi dispari, $[7/1009] \times [1009/7] = 1$, cioè $7^{504} \bmod 1009 = 1009^3 \bmod 7$; adesso riflettiamo. E' facilissimo **calcolare** che $1009 \bmod 7 = 1$ per cui è immediato **dimostrare** ad esempio che $7^{5040000} \bmod 1009 = 1$ (siete obbligati a calcolarlo su un'isola deserta e potete scegliere tra un libro di algebra o una calcolatrice... attenzione, le batterie prima o poi si esauriscono...)

Altre utili regole di calcolo per i simboli $[a/p]$ sono: (a e b sono interi, p è un primo dispari e p non divide $a \times b$)

$$\begin{aligned}
[a \times b/p] &= [a/p] \times [b/p] \\
\left[a^2/p\right] &= [a/p] \times [a/p] = 1 \\
[2/p] &= (-1)^{(p^2-1)/8} \\
[-1/p] &= [p-1/p] = (-1)^{(p-1)/2}
\end{aligned}$$

Esempio: 18 è un quadrato perfetto modulo 97 ? Calcoliamo così: $[18/97] = [2/97] \times [9/97] = (-1)^{(97 \times 97-1)/8} \times [9/97] = 1$ (perchè 9 è un quadrato). Quindi 18 è un quadrato modulo 97, infatti $42^2 \bmod 97 = 18$. (siamo sulla solita isola...)

La teoria dei residui consente anche di risolvere problemi del tipo:

dimostrare che, per tutti gli interi m, esiste un intero n tale che $n^2 + am^2$ è divisibile per il.numero primo p

Ragioniamo così: se esiste una soluzione di $x^2 = -a \bmod p = (p-a) \bmod p$ posso porre $n = xm$ e quindi ottenere:

$$n^2 + am^2 = x^2m^2 + am^2 = (p - a + a)m^2 = pm^2 = 0 \bmod p$$

Analogamente se avessi da studiare $n^2 - am^2$ cercherei una soluzione di $x^2 = a \bmod p$ per ottenere

$$n^2 + am^2 = x^2m^2 - am^2 = (a - a)m^2 = 0 \bmod p$$

3. Test di primalità

I residui sono uno strumento utile per cercare criteri per verificare se un numero n è primo (sperabilmente un pò più veloci della ricerca di divisori primi fino a $\sqrt{n}$).

Sia q un numero dispari e x un intero positivo minore di q e primo con q. **Se q è primo** già sappiamo che se si calcola $x^{(p-1)/2}$ si ottiene $[x/q]$. Il simbolo $[x/q]$ può essere generalizzato al caso in cui q sia dispari ma non sia primo. Definiamo $[[x/q]]$ essere uguale a $[x/q]$ se q è primo e inoltre imponiamo la proprietà $[[x/q]] \times [[x/q']] = [[x/qq']]$. Si può dimostrare che per $[[x/q]]$ valgono tutte le regole di calcolo valide per $[x/q]$. Allora possiamo dire che se per un numero x come sopra si ha $x^{(q-1)/2} \neq [[x/q]]$ allora q **non può essere primo!** Naturalmente non si può barare, in matematica le difficoltà buttate dalla finestra rientrano sempre dalla porta: si deve riuscire a calcolare in qualche modo $[[x/q]]$ dalle sue proprietà (ovviamente senza sapere i suoi fattori primi!)

Esempio (molto banale): $q = 15$ sia $x = 13$ allora $13^7 \bmod 15 = 7$ mentre (notare che $13 \bmod 15 = -2$)

$$[[13/15]] = [[-1/15]] \times [[2/15]] = (-1)^7 \times (-1)^{(15^2-1)/8} = -1$$

Infatti, come verifica: $15 = 3 \times 5$ per cui:

$$[[13/15]] = [-2/3] \times [-2/5] = [-1/3] \times [2/3] \times [-1/5] \times [2/5] = -1$$

4. Numeri primi molto grandi

► La funzione di Maple *nextprime(x)* - rappresentata dal simbolo $p(x)$ - fornisce, per ogni numero x (ragionevolmente grande), il più piccolo numero primo più grande di x. La funzione *isprime(x)* - rappresentata dal simbolo $q(x)$ - determina se x è primo oppure no.

► Evaluate

$p(4) = 5$
$p(500) = 503$
$p(8298) = 8311$
$p\,(2738497289527589233333334) = 2738\,497\,289\,527\,589\,233\,333\,433$
$p(10^{45}) = 1000\,000\,000\,000\,000\,000\,000\,000\,000\,000\,000\,000\,000\,009$

► Evaluate

$q\,(2738497289527589233333337) = false$
$q(1000\,000\,000\,000\,000\,000\,000\,000\,000\,000\,000\,000\,000\,009) = true$
Infatti:

▶ Factor

$$2738497289527589233333337 = 79 \times 34\,664\,522\,652\,247\,964\,978\,903$$

5. Il sistema di crittografia di Rivest-Shamir-Adleman (RSA)

Il sistema di crittografia a chiave pubblica di Rivest-Shamir-Adleman (RSA) (è quello con cui è implementato il protocollo SSL, avete presente il lucchetto chiuso che appare quando visitate una pagina Web protetta?) è basato direttamente sul Teorema di Eulero.

Supponiamo che Alice voglia mandare a Bob il numero segreto del suo cellulare $x = 333123456$

Bob genera due numeri primi:

$$q = p(20934) = 20939$$

e

$$r = p\,(259384) = 259387.$$

Poi calcola

$$\begin{aligned} n &= q \times r \\ &= 20939 \times 259387 \\ &= 5431304\,393 \end{aligned}$$

$$\begin{aligned} \varphi(n) &= (q-1) \times (r-1) \\ &= 20938 \times 259386 \\ &= 5431\,024\,068 \end{aligned}$$

A questo punto genera la sua *chiave pubblica* (e, n) dove e è un intero relativamente primo con $\varphi(n)$: ad esempio $e = 1009$ (infatti $\gcd(1009, 5431024068) = 1$) e la sua *chiave privata* (d, n) dove $d = e^{-1} \bmod \varphi(n)$.

$d = 1009^{-1} \bmod 5431\,024\,068 = 4925\,061\,469$.

Sia $x = 333123456$ il testo in chiaro da trasmettere. Messaggi più lunghi di n non sono ammessi per cui bisogna, eventualmente, spezzare il testo in chiaro in frammenti adeguati.

Alice usa la chiave pubblica di Bob per cifrare il messaggio secondo il seguente algoritmo: $y = x^e \bmod n$,

e ottiene $y = 333123456^{1009} \bmod 5431304\,393 = 4978\,962\,229$.

Spedisce a Bob il numero y e *Bob applica la sua chiave privata per riottenere il messaggio in chiaro*:

$$x = y^d \bmod n = 4978\,962\,229^{4925\,061\,469} \bmod 5431304\,393 = 333\,123\,456.$$

Questo metodo funziona per due motivi.

a) se $x^e = y \bmod n$ e $d = e^{-1} \bmod \varphi(n)$, allora $y = x^e + kn$ e $de = 1 - h\varphi(n)$, con h e k numeri interi. Ma allora

$$(x^e + kn)^d = x \cdot (x^{\varphi(n)})^{-h} + m$$

con m un numero intero multiplo di n e, *per il teorema di Eulero*, $x^{\varphi(n)} \bmod n = 1$. Cioè $y^d \bmod n = x$ come si voleva.

b) per ottenere il testo in chiaro non basta avere e,n e y; se non si conoscono q e r l'impresa di invertire la formula di Alice cioè calcolare x da y è quasi disperata perchè la fattorizzazione di numeri molto grandi richiede moltissimo tempo di calcolo.

Ricapitoliamo (in realtà semplificando un po'): ogni sito Web protetto ha un suo numero n (molto grande, non come i nostri esempi) e la corrispondente $\varphi(n)$; quando ci si collega il nostro browser riceve la chiave pubblica del sito, codifica i messaggi e li spedisce. Il sito usa la sua chiave privata per leggere i messaggi ed eseguire le operazioni richieste.

5.1. Esempi di calcolo.

$q = p(444444444444) = 444\,444\,444\,461$

$r = p(555555555555) = 555\,555\,555\,559$

$n = q \times r = 444\,444\,444\,461 \times 555\,555\,555\,559 = 246\,913\,580\,257\,641\,975\,308\,699$

$\varphi(n) = (q-1) \times (r-1) = 555\,555\,555\,558 \times 444\,444\,444\,460 = 246\,913\,580\,256\,641\,975\,308\,680$

$\gcd(777177713, 246\,913\,580\,256\,641\,975\,308\,680) = 1$allora $e = 777177713$ è la chiave pubblica di Bob.

Alice ha il messaggio $x = 12345$, lo codifica $y = 12345^{777177713} \bmod 246\,913\,580\,257\,641\,975\,308\,699 = 102\,530\,308\,001\,854\,922\,814\,302$

Bob usa la sua chiave privata $d = 777177713^{-1} \bmod 246\,913\,580\,256\,641\,975\,308\,680 = 51\,004\,698\,350\,603\,138\,793\,977$ e decodifica il messaggio:

$102\,530\,308\,001\,854\,922\,814\,302^{51\,004\,698\,350\,603\,138\,793\,977} \bmod 246\,913\,580\,257\,641\,975\,308\,699 =$

$12\,345$

$p(123456789987654321) = r = 123\,456\,789\,987\,654\,353$

$p(987654321123456789) = s = 987\,654\,321\,123\,456\,823$

$n = 123\,456\,789\,987\,654\,353 \times 987\,654\,321\,123\,456\,823 = 121\,932\,632\,103\,337\,941\,464\,563\,328\,643\,500\,519$

$\varphi(n) = (r-1)(s-1) = 121\,932\,632\,103\,337\,940\,353\,452\,217\,532\,389\,344$

$\gcd(67777777777771, 121\,932\,632\,103\,337\,940\,353\,452\,217\,532\,389\,344) = 1$

messaggio :8888888888 $y = 8888888888^{67777777777771} \bmod 121\,932\,632\,103\,337\,941\,464\,563\,328\,643\,500\,519 = 78\,687\,260\,944\,075\,815\,618\,371\,573\,626\,229\,331$

$d = 67777777777771^{-1} \bmod 121\,932\,632\,103\,337\,940\,353\,452\,217\,532\,389\,344 = 2604\,717\,670\,245\,025\,077\,664\,852\,739\,463\,811$

$78\,687\,260\,944\,075\,815\,618\,371\,573\,626\,229\,331^{2604\,717\,670\,245\,025\,077\,664\,852\,739\,463\,811} \bmod 121\,932\,632\,103\,337\,941\,464\,563\,328\,643\,500\,519 = 8888\,888\,888$

Esercizi su divisibilità, primi ed equazioni diofantine

1. È vero che per ogni numero intero m vale quanto segue: se si divide m^2 per 4 si ottiene 0 oppure 1 come resto?

2. È vero che se si divide un qualunque numero primo maggiore di 6 per 6 si ottiene sempre come resto 1 oppure 5?

3. Determinate per quali valori interi di a hanno soluzioni intere le seguenti equazioni: $2ax+y=a$; $4ax+2ay=a$; $4ax+2ay=a+1$; $2ax+4ay=4$; $2ax+4y=a$;

4. Provate che la retta di equazione $2x-2y+1=0$ non passa per nessun punto del piano con entrambe le coordinate intere.

5. Stabilite se la retta di equazione $y=\frac{3}{2}x+1$ passa per punti del piano che abbiano entrambe le coordinate intere. In caso affermativo determinarne qualcuno.

6. Determinate, se ne esistono, alcuni valori di a (a intero) per cui siano contemporaneamente verificate: $a \bmod 11 = 2$ e $a \bmod 5 = 1$.

7. Determinate, se ne esistono, alcuni valori di a (a intero) per cui siano contemporaneamente verificate: $a \bmod 16 = 3$ e $a \bmod 8 = 2$.

8. Determinate tutti i numeri interi dispari a tali che $a \bmod 3 = 1$.

9. Dimostrare che se $p > 3$ è un numero primo, allora $p^2 - 1$ è divisibile per 24.

10. Tre scimmiette rubano un carico di banane e le nascondono in un loro deposito. La prima scimmietta vuole mettere al sicuro la sua parte di banane e si reca nottetempo da sola al deposito e asporta un terzo delle banane (dopo averne mangiata 1 perché il numero originario di banane non era divisibile per 3). La seconda scimmietta fa lo stesso con le banane rimanenti: ne mangia 1 e asporta un terzo delle rimanenti; lo stesso fa la terza. Al mattino le tre scimmie si recano insieme al deposito e prendono ciascuna un terzo delle banane rimaste (che sono in numero multiplo di 3). Quante potevano essere le banane all'inizio?

11. Il giorno di San Baudolino viene organizzata una sfilata in costume per le vie di Alessandria. I partecipanti si dispongono in file da 7 ma si accorgono che in questo modo uno di loro rimane da solo in una fila.

Provano allora a disporsi in file da cinque, ma ancora rimane una fila con una persona sola, e la stessa cosa succede quando provano a disporsi in file da tre e due. Sapendo inoltre che i partecipanti sono meno di 300, quanti ne resterebbero da soli se si disponessero in file da 4 ?

12. Il giorno di San Gaudenzio viene organizzata una sfilata in costume per le vie di Novara. I partecipanti si dispongono in file da dieci ma si accorgono che in questo modo uno di loro rimane da solo in una fila. Provano allora a disporsi in file da nove, ma ancora rimane una fila con una persona sola, e la stessa cosa succede quando provano a disporsi in file da otto, sette, sei, cinque, quattro, tre e due. Dire quanti erano i partecipanti alla sfilata sapendo che erano meno di 5000.

13. Il primo gennaio 2002 Ilaria va a fare la sua prima spesa in Euro. Dopo un'ora si accorge di aver già speso metà dei suoi soldi, e di essere rimasta con tanti centesimi quanti erano gli Euro che aveva all'inizio e con un numero di Euro pari alla metà dei centesimi che aveva all'inizio. Quanto ha speso Ilaria? (supponiamo ovviamente che il numero di centesimi iniziali sia minore di 100)

Esercizi su congruenze, teorema di Fermat e residui di Gauss

1. Trovate, se ne esistono, tutte le soluzioni di $2x = 5 \bmod 6$, di $2x = 0 \bmod 4$, di $3x = 4 \bmod 5$.

2. Provate che per ogni a, b, c interi, il numero $b^2 - 4ac$ è congruo (modulo 4) a 0 oppure a 1.

3. Provate che se $MCD(x, 6) = 1$, allora $x^2 \bmod 24 = 1$

4. Provate che se, dati gli interi a, b e il naturale n, vale $a = nb$, allora $MCD(a, n) = MCD(b, n)$.

5. Rappresentate con tabelle opportune somma, reciproco e prodotto in Z_4.

6. Determinare tutti gli elementi invertibili di $\mathbb{Z}_{12}$ e calcolarne gli inversi.

7. Provate che se a, b sono invertibili in $\mathbb{Z}_{n,}$ allora anche $a \times b$ è invertibile in Z_n.

8. Dimostrare che n^5 e n hanno la stessa cifra finale (quella delle unità).

9. Dimostrare che se 7 non divide n, necessariamente divide $n^{12} - 1$.

10. Dimostrare che, per ogni intero n, $n^{13} - n$ è divisibile per $2, 3, 5, 7$, e 13.

11. Dimostrare che $n^9 + 2n^7 + 3n^3 + 4n$ è sempre divisibile per 5.

12. Dimostrare che se n non è divisibile per 13 allora n^6 diviso 13 ha resto 1 oppure 12.

13. Dimostrare che se n non è divisibile per 23 allora n^{11} diviso per 23 ha resto 1 oppure 22.

14. Enunciare e dimostrare il risultato generale di cui gli esercizi 12 e 13 sono casi particolari.

15. Dimostrare che esistono e trovare le due soluzioni (positive e minori di 11) dell'equazione $x^2 = 5 \bmod 11$

16. Dimostrare che, per tutti gli interi m, esiste un intero n tale che $n^2 - 5m^2$ è divisibile per 11

17. Dimostrare che, per tutti gli interi m, esiste un intero n tale che $n^2 + 627m^2$ è divisibile per 17

18. Dimostrare che se n e m sono interi primi fra loro allora nessun numero della forma $n^2 + 5m^2$ è multiplo di 11.

19. Dimostrare che, per ogni primo p, si ha: $(p-1)! = (p-1) \bmod p$

20. Dimostrare che l'equazione $x^2 + 4x - 1 = 0$ è risolubile modulo 11 e trovare le soluzioni positive e minori di 11.

21. Dimostrare che l'equazione $x^2 + 4x + 5 = 0$ non è risolubile modulo 7.

22. Dimostrare che se n non è divisibile per 17 allora $(n^8 - 16) \bmod 17 = 0$ oppure $= 2$

23. Dimostrare che $n^5/5 + n^3/3 + 7n/15$ è un intero per ogni n.

24. Dimostrare che $n^{13} - n$ è divisibile per 2730 qualsiasi sia l'intero n.