Capitolo 5

Aritmetica modulare

5.1 Diamo ... i numeri

Per cominciare cosa disse nel 1891 il matematico Peano[1]

"I primi numeri che si presentano, e con cui si formano tutti gli altri, sono gli interi e positivi. E la prima questione è: possiamo noi definire l'unità, il numero, la somma di due numeri?

La definizione comune di numero, che è l'Euclidea, «numero è l'aggregato di più unità», può servire come schiarimento, ma non è soddisfacente come definizione.

Invero un bambino, a pochi anni usa le parole uno, due, tre, ecc.; in seguito adopera la parola numero; solo molto più tardi nel suo dizionario comparisce la parola aggregato. E nello stesso ordine, come insegna la filologia, ci sono presentate nello sviluppo delle lingue ariane.

Quindi, dal lato pratico la questione parmi risoluta; ossia,

non conviene in un insegnamento dare alcuna definizione di numero, essendo questa idea chiarissima agli allievi, e ogni definizione non avendo che l'effetto di confonderIa.

E di questa opinione è pure la maggior parte degli autori.

Dal lato teorico, per decidere la questione della definizione [del concetto di numero], occorre sia detto prima di quali idee ci possiamo servire. Qui si suppongono note le sole idee rappresentate dai segni $\cap\,(e)$, $\cup\,(o)$, $-(non)$, *ecc.*

[...] E allora il numero non si può definire, poiché è evidente che comunque si combinino fra loro queste parole non si potrà mai avere una espressione equivalente a numero.

Però, se il numero non si può definire, si possono enunciare quelle proprietà da cui derivano come conseguenza tutte le innumerevoli e ben note proprietà dei numeri.

I concetti, adunque, che non definiamo sono quelli di numero, n, di unità, 1, e di successivo d'un numero a, che qui si indica per un istante con a+ . Questi concetti non si possono ottenere per deduzione; bisogna ottenerli per induzione (astrazione). Il successivo di a si è qui indicato con a+, invece che con a+1,

[1] Giuseppe Peano (1858-1932), matematico italiano, portò avanti le ricerche sulla aritmetizzazione della matematica, giungendo alla conclusione che tutta la matematica poteva essere ricondotta ai concetti e alle operazioni dell'aritmetica.

come d'uso; e ciò si è fatto per indicare con un segno solo, + , l'operazione fondamentale «successivo di».

Del resto [...], definita la somma a + b di due numeri, ne risulta che a+1 vale appunto a+, cioè il successivo di a, e così si ritorna alle solite notazioni.

Le proposizioni primitive, vale a dire le proposizioni esprimenti le più semplici proprietà dei numeri interi, da cui derivano tutte le altre, sono:

1. «L'unità è un numero».

2. «il segno + messo dopo un numero produce un numero».

3. «Se a e b sono due numeri, e se i loro successivi sono eguali, anche essi sono eguali».

4. «L'unità non segue alcun numero».

5. «Se s è una classe che contiene l'unità, e se la classe formata dai successivi di s è contenuta in s, allora ogni numero è contenuto nella classe s». [...]

La prop. 5 si può enunciare:

«Se s è una proprietà (dei numeri), e se l'unità ha questa proprietà, e se

tutte le volte che un numero ha questa proprietà, anche il successivo la possiede; allora ogni numero ha la proprietà s». [...]

Questa proprietà è comunemente chiamata la regola di induzione matematica. Essa è intuitiva, e non si può ridurre ad altre più semplici."

GIUSEPPE PEANO, Sul concetto di numero.

Archiviato (diciamo così) il problema dei numeri, facciamo tesoro di alcune idee lette nel brano e analizziamo le proprietà dei numeri naturali.

5.1.1 L'insieme $\mathbb{N}$

In $\mathbb{N}$ è definita una legge di composizione interna (operazione) definita dal simbolo $+$ con le seguenti proprietà:

$\forall a, b \in \mathbb{N}$ si ha che $a + b \in \mathbb{N}$

$\forall a, b \in \mathbb{N}$ si ha che $a + b = b + a$

$\forall a, b, c \in \mathbb{N}$ si ha che $(a + b) + c = a + (b + c)$

$$\exists 0 \in \mathbb{N} \forall a \in \mathbb{N} : a + 0 = a$$

In $\mathbb{N}$ è definita una legge di composizione interna (operazione) definita dal simbolo $\cdot$ (o meglio senza nessun simbolo) con le seguenti proprietà:

$\forall a, b \in \mathbb{N}$ si ha che $ab \in \mathbb{N}$

$\forall a, b \in \mathbb{N}$ si ha che $ab = ba$

$\forall a, b, c \in \mathbb{N}$ si ha che $(ab)c = a(bc)$

$\exists 1 \in \mathbb{N} \forall a \in \mathbb{N} : a \cdot 1 = a$ inoltre:
$\forall a, b, c \in \mathbb{N}\ a(b + c) = ab + ac$
Applicazioni: le espressioni

5.2 L'insieme $\mathbb{Z}$

Costruisco un nuovo insieme $\mathbb{Z}$ aggiungendo alle proprietà di sopra questa:

$$\forall a \in \mathbb{Z}\ \exists b = -a \in \mathbb{Z}\ :\ a + b = 0 \tag{5.1}$$

scrivi le proprietà di $\mathbb{Z}$

Attento all'idea: la proprietà 5.1 ci "costringe" a creare un nuovo insieme numerico!

5.2.1 Aritmetica in $\mathbb{Z}$

L'uguaglianza fra elementi di $\mathbb{Z}$ gode di "evidenti" proprietà:

$$\forall a \in \mathbb{Z} \quad a = a$$

$$\forall a, b \in \mathbb{Z} \quad se \quad a = b \rightarrow b = a$$

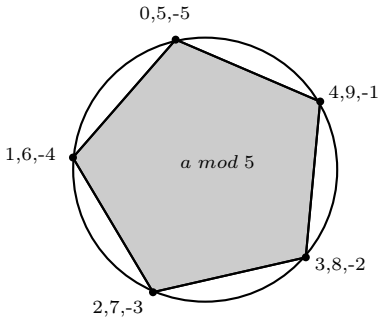
$$\forall a, b, c \in \mathbb{Z} \quad se \quad a = b \wedge b = c \rightarrow a = c$$

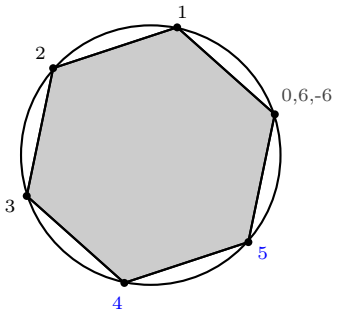
e inoltre se $x = x'$ e $y = y'$ si ha che $x + y = x' + y'$ e $xy = x'y'$

le congruenze

Definizione 32 (Congruenza)**.** Definiamo *congruenti* (mod d) due numeri di $\mathbb{Z}$ se restituiscono nella divisione con d lo stesso resto.

Ad esempio: 6 e 11 sono congrui modulo 5 infatti $6 = 5 \cdot 1 + 1$ e $11 = 5 \cdot 2 + 1$ in questo caso diremo $6 \equiv 11(\ mod\ 5)$
un modo facile per rappresentare le congruenze:





le proprietà dell'uguaglianza valgono anche per le congruenze:
$\forall a \in \mathbb{Z} \quad a \equiv a$ (mod d)
$\forall a, b \in \mathbb{Z} \quad se \quad a \equiv b \rightarrow b \equiv a$ (mod d)

$\forall a, b, c \in \mathbb{Z} \quad se \quad a \equiv b \wedge b \equiv c \rightarrow a \equiv c$ (mod d)
due numeri a, b sono congruenti (mod d) se e solo se $a = b + nd$ e d divide $a - b$
siano $a \equiv a'$ e $b \equiv b'$ allora:

$$a + b \equiv a' + b'$$

$ab \equiv a'b'$
infatti:
$a = a' + nd, b = b' + md$ quindi $a+b = a' + nd + b' + md = a' + b' + d(m+n) \rightarrow a + b \equiv a' + b'$
$a = a' + nd, b = b' + md$ quindi $ab = (a' + nd)(b' + md) = a'b' + mda' + b'nd + nmd = a'b' + d(ma + b'n + mn) \rightarrow ab \equiv a'b'$
Quanto sopra giustifica i criteri di divisibilità già studiati:

i) un numero è divisibile per 3 se la somma delle cifre è divisibile per 3:
sia $m \in \mathbb{Z}$ un numero di n cifre, m può essere scritto come:
$a_0 10^0 + a_1 10^2 + ... + a_n 10^n$ valutiamo le congruenze (mod 3) delle potenze di 10:

$$10 \ mod \quad 3 = 1 cio è \quad 10 \equiv 1 (mod\ 3)$$

$10^2 = 10 \cdot 10$ quindi applicando le proprietà si ha $10^2 \equiv 1 \cdot 1 \equiv 1$ pertanto:

$$a_0 10^0 + a_1 10^2 + ... + a_n 10^n \equiv a_0 \cdot 1 + a_1 \cdot 1 + ... + a_n \cdot 1$$

ii) un numero è divisibile per 11 se la differenza fra le cifre di posto pari meno quelle di posto dispari è divisibile per 11: infatti $10^1 \quad mod \quad 11 = -1$ e $10^2 \quad mod \quad 11 = 1$, applicando le proprietà si ha la regola.

Esercizio 2. Quanto vale il resto della divisione di $10(2007)^4$–$8(2007)^3$+$12(2007)^2$+ 721 per 669?

Soluzione. $2007\ mod\ 669 = 0$ quindi
$(10(2007)^4$–$8(2007)^3 + 12(2007)^2 + 721)\ mod\ 669$=
$=10(2007)^4\ mod\ 669 - 8(2007)^3\ mod\ 669 + 12(2007)^2\ mod\ 669 + 721\ mod\ 669$=
$0 + 0 + 0 + 721\ mod\ 669 = 52$ □

Esercizio 3. A quale numero tra 0 e 6 è congruo modulo 7 il prodotto:

$$11 \cdot 18 \cdot 2322 \cdot 13 \cdot 19$$

Soluzione. 11 mod 7=4; 18 mod 7=4; 2322 mod 7 =5; 13 mod 7=6; 19 mod 7=5, ma dato che: $6 \equiv -1$ e $5 \equiv -2$ si ha $4 \cdot 4 \cdot (-2) \cdot (-1) \cdot 5 = 160, 160\ mod\ 7 = 6$ □

Esercizio 4. A quale numero fra 0 e 4 è congrua modulo 5 la somma
$1 + 2 + 2^2 + 2^3 + ... + 2^{19}$?

Soluzione. $1\ mod\ 5 = 1$, $2\ mod\ 5 = 2$,
$2^2\ mod\ 5 = (2\ mod\ 5)(2\ mod\ 5) = 4, 2^3 \equiv 4 \cdot 2 \equiv 3\ 2^4 \equiv 3 \cdot 2 \equiv 1$
$2^5 \equiv 1 \cdot 2 \ldots$
la somma richiesta si può scrivere:
$(1 + 2 + 2^2 + 2^3) + (2^4 + 2^5 + 2^6 + 2^7) + ...2^{18} + 2^{19} \equiv (1 + 2 + 4 + 3) \cdot 4 + 1 + 2$
ma $(1 + 2 + 4 + 3) = 10 \equiv 0$ e quindi il resto è 3. □

Quanto vale il resto modulo 5 della somma $\sum_{k=0}^{2013} 2^k$

5.3 Algoritmo euclideo per il calcolo del massimo comun divisore

Osservazione preliminare: detti m ed n due numeri naturali ($\in \mathbb{N}$), tali che $m \geq n$, si può sempre scrivere $m = qn + r$ dove $q, r \in \mathbb{N}$; quindi un intero che divide m ed n divide anche r, pertanto gcd(m,n)=gcd(n,m mod n).

Il seguente programmino in java applica quando illustrato:

```
import javax.swing.*;
public class gcd {

public static void main(String[] args)
{
int m=0;
int n=0;
int r=0;
String datom = JOptionPane.showInputDialog(null, "Valore di m");
m=Integer.parseInt(datom);
String daton = JOptionPane.showInputDialog(null, "Valore di n");
n=Integer.parseInt(daton);
if(m<n)
{
int s=n;
n=m;
m=s;
}
do
{
r=m%n;
m=n;
n=r;
}while(r!=0);
String v="gcd("+datom+","+daton+")=";
System.out.print(v);
System.out.print(m);
}

}
```

Teorema 19 (di Bézout)**.** Siano $a, b \in \mathbb{Z}$, sia d massimo comune divisore di a e b.
Allora esistono $s, t \in \mathbb{Z}$ tali che:

$$sa + tb = d \tag{5.2}$$

Tale uguaglianza si dice identità di Bézout, I numeri s e t si dicono coefficienti di Bézout di a e b.

Dimostrazione. Se $a = 0$, allora b è un massimo comune divisore di a e b, e si può prendere $s = 0$, $t = 1$.

Supponiamo ora che a non sia nullo, sia $X = \{ax + by > 0 \quad a, \in \mathbb{Z} - \{0\}\}$. Allora X è un sottoinsieme di $\mathbb{N}$ Inoltre è diverso dal vuoto, infatti, se $a > 0$, allora $a1 + b0 = a \in X$, e se $a < 0$, allora $a(-1) + b0 = -a \in X$. Essendo X inferiormente limitato ammette minimo, sia m questo minimo. Presi $s, t \in \mathbb{Z}$ tali che $as + bt = m$, vogliamo provare che m è un massimo comune divisore (gcd) di a e b. Per provare che m divide a e b, utilizziamo il teorema di divisione euclidea. Siano q ed r il quoziente ed il resto della divisione di a per m. Allora $r < m$ e $r = a - mq = a - (as + bt)q = a(1 - sq) + b(-tq)$. Se fosse $r > 0$, allora si avrebbe $r \in X$, e quindi $m \leq r$, il che costituisce una contraddizione. Quindi $r = 0$, il che prova che m divide a. Analogamente si prova che m divide b.

Supponiamo ora che $e \in \mathbb{Z}$ sia tale che $e|a$ ed $e|b$. Allora, e divide as e bt e quindi, divide $as + bt = m$. Ciò prova che m soddisfa le condizioni ed è dunque un massimo comune divisore di a e b. □

5.4 Terne pitagoriche

Problema 1. Trovare tutte le terne di interi (i, j, n) tali che $n^2 = i^2 + j^2 \wedge gcd(i, j) = 1$.

Dimostrazione. Osservazione preliminare $(2n)^2 \equiv 0(\ mod\ 4)$ $(2m + 1)^2 \equiv 1(\ mod\ 4) \forall n, m \in \mathbb{N}$

Se i e j sono entrambi pari allora $i = 2k, j = 2h$ $gcd(i, j) \neq 1$

Se i e j sono entrambi dispari allora $i = 2k + 1, j = 2h + 1$ quindi $n^2 = 4k^2 + 4k + 1 + 4h^2 + 4h + 1=$

$4(k^2 + k + h^2 + h) + 2$ ma questo comporta che $n^2 \equiv 2(\ mod\ 4)$ non possibile data l'osservazione preliminare.

Si ricava che i e j sono uno pari e l'altro dispari, supponiamo, senza violare la generalità del problema, che i sia dispari :

$n - i$ è pari

$n + i$ è pari

allora $\exists p \in \mathbb{N} : p = \frac{n-i}{2}$ e anche $\exists q \in \mathbb{N} : q = \frac{n+i}{2}$

$$q + p = \frac{n + i}{2} + \frac{n - i}{2} = \frac{n + i + n - i}{2} = n$$

$$q - p = \frac{n + i}{2} - \frac{n - i}{2} = \frac{n + i - n + i}{2} = i$$

$$j^2 = n^2 - i^2 = (q+p)^2 - (q-p)^2 = q^2 + 2qp + p^2 - \left(p^2 - 2qp + p^2\right) = q^2 + 2qp + p^2 - p^2 + 2qp - p^2 = 4qp$$

dato che j è pari $\frac{j^2}{4} \in \mathbb{N}$ $\frac{j^2}{4} = \left(\frac{j}{2}\right)^2$ quindi qp è un quadrato perfetto, possiamo scrivere:

$p = x^2 m_1$ dove m_1 è il prodotto di tutti i fattori non ripetuti di p

$q = y^2 m_2$ dove m_2 è il prodotto di tutti i fattori non ripetuti di q

$pq = x^2 y^2 m_1 m_2$ ma dato che pq è un quadrato si dovrà avere $m_1 = m_2 = m$ ora per l'ipotesi $gcd(i, j) = 1$ si ha $m = 1$

una generica terna pitagorica (i, j, n) si può costruire partendo da due interi $x, y : gcd(x, y) = 1$ e calcolando $i = x^2 - y^2; j = 2xy; n = x^2 + y^2$ □

Qualche esempio in wxMaxima:

```
(%i8)  x:23;
(%o8)  23
(%i9)  y:8;
(%o9)  8
(%i10)  gcd(x,y);
(%o10)  1
(%i11)  n:x^2+y^2;
(%o11)  593
(%i12)  i:x^2-y^2;
(%o12)  465
(%i13)  j:2*x*y;
(%o13)  368
(%i14)  n^2-j^2-i^2;
(%o14)  0
(%i15)  gcd(i,j);
(%o15)  1
```

```
(%i16)  x:523;
(%o16)  523
(%i17)  y:256;
(%o17)  256
(%i18)  gcd(x,y);
(%o18)  1
(%i19)  n:x^2+y^2;
(%o19)  339065
(%i20)  i:x^2-y^2;
(%o20)  207993
(%i21)  j:2*x*y;
(%o21)  267776
(%i22)  n^2-j^2-i^2;
(%o22)  0
(%i23)  gcd(i,j);
(%o23)  1
```

- *cosa verificano le istruzioni (%i14) e (%i22)?*
- *sapresti fare qualche esempio in cui pur valendo* $gcd(x, y) = 1$ *non vale* $gcd(i, j) = 1$.
- *scelti* x *dispari e* y *pari sotto l'ipotesi* $gcd(x, y) = 1$ *vale sempre che* $gcd(i, j) = 1$*?*

Capitolo 6

Calcolo discreto

6.1 Calcolo discreto . . . ovvero matematica ricreativa

6.1.1 Permutazioni

I risultati che andremo via via a trovare saranno ricavati partendo da problemi «reali»

Problema 2. Quanti sono gli anagrammi (anche privi di senso) della parola *via*?

Dimostrazione. si possono facilmente elencare:

1: *aiv*

2: *avi*

3: *iav*

4: *iva*

5: *vai*

6: *via*

Sono 6, infatti il primo carattere può essere scelto in 3 modi (a,i,v) una volta fissato il primo carattere me ne restano due fra cui scegliere, quindi per ogni primo carattere due caratteri cioè $3 \cdot 2$ per l'ultimo carattere non c'è scelta. □

Proviamo a generalizzare il problema: se ho una parola come *sfera*, formata da 5 caratteri diversi, posso ragionare come in precedenza: in 5 modi scelgo il primo carattere per ogni scelta ho 4 possibilità per il secondo carattere, poi 3 per il terzo 2 per il quarto e 1 solo per quinto, ottengo $5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$

Definizione 33 (fattoriale di n)**.** Si definisce fattoriale di un $n \in \mathbb{N}$, $n!$ la funzione così definita:

$$\begin{aligned} 0! &= 1 \\ n! &= n \cdot ((n-1)!) \end{aligned} \tag{6.1}$$

Gli anagrammi di *sfera* son $5! = 120$.

In generale si può affermare che dati n oggetti distinti è possibile porli in $n!$ sequenze distinte, le sequenze così ottenute si chiamano permutazioni.

6.1.2 Permutazioni con ripetizione

Problema 3. Quanti sono gli anagrammi (anche privi di senso) della parola *aia*?

Dimostrazione. si possono facilmente elencare:

1: *aai*

2: *aia*

3: *aai*

4: *aia*

5: *iaa*

6: *iaa*

Come si osserva le permutazioni (3!) si ripetono a causa della presenza della doppia *a*, infatti le due *a* son indistinguibili e quando vengono permutate non si crea una nuova stringa, pertanto le stringhe diverse sono: $\frac{3!}{2!} = 3$ □

Mettiamo alla prova la tecnica introdotta utilizzando un esempio un po' più complesso: troviamo quanti sono gli anagrammi di *matta*; stando a quanto visto dovrebbero essere: $\frac{5!}{2! \cdot 2!} = 30$:

1: *aamtt*

2: *aatmt*

3: *aamtt*

4: *amatt*

5: *amtat*

6: *amtta*

7: *atamt*

8: *atatm*

9: *atmat*

10: *atmta*

11: *attam*

12: *attma*

13: *maatt*

14: *matat*

15: *matta*

16: *mtaat*

17: *mtata*

18: *mttaa*

19: *taamt*

20: *taatm*

21: *tamat*

22: *tamta*

23: *tatam*

24: *tatma*

25: *tmaat*

26: *tmata*

27: *tmtaa*

28: *ttaam*

29: *ttama*

30: *ttmaa*

Problema 4. Della parola *MATEMATICA* si costruiscono gli anagrammi e si elencano in ordine alfabetico: calcolare che posizione occupa la parola *MATEMATICA*.

Dimostrazione. Intanto osserviamo che l'elenco è formato da $\frac{10!}{3!\cdot 2!\cdot 2!} = 151200$ stringhe; quelle che iniziano per A sono $\frac{9!}{2!\cdot 2!\cdot 2!} = 45360$, quelle che iniziano per C sono $\frac{9!}{3!\cdot 2!\cdot 2!} = 15120$, quelle che iniziano per E sono $\frac{9!}{3!\cdot 2!\cdot 2!} = 15120$, quelle che iniziano per I sono $\frac{9!}{3!\cdot 2!\cdot 2!} = 15120$, la prima parola che inizia per M occupa il posto 90721 e sarà: $MAAACEIMTT$, ora le parole che iniziano per MAA sono $\frac{7!}{2!} = 2520$, quelle del tipo MAC sono $\frac{7!}{2!\cdot 2!} = 1260$, quelle MAE sono $\frac{7!}{2!\cdot 2!} = 1260$, quelle MAI sono $\frac{7!}{2!\cdot 2!\cdot 2!} = 1260$, quelle MAM sono $\frac{7!}{2!\cdot 2!\cdot 2!} = 1260$, la 98281 stringa è $MATAACEIM$, le stringhe che iniziano per $MATA$ sono $6! = 720$, quelle $MATC$ 360 la 99361 è $MATEAACIMT$, la 99601 stringa è $MATEMAACIT$, la 99672 è $MATEMATACI$, ci sono 12 parole la cui ottava lettera è A o C, si giunge così a $MATEMATIAC$ ancora un passo ed otteniamo **MATEMATICA** cioè la 99686 del nostro elenco. □

Problema 5. Quante parole di 5 lettere posso formare con le prime 5 *(A,B,C,D,E)* lettere dell'alfabeto?

Dimostrazione. Posso pensare alla parola formata da 5 caselle in ciascuna casella è possibile inserire una qualsiasi lettera quindi le parole sono $5^5 = 3125$ □

6.1.3 Una definizione di probabilità senza tanti «fronzoli»

Sia $\mathcal{F}$ l'insieme dei possibili risultati di un certo esperimento (lancio di un dado, estrazione di una carta etc.), definiamo i risultati eventi allora $\mathcal{F}$ è detto spazio degli eventi. Definiamo probabilità di un certo evento il numero dei modi in cui si può verificare diviso tutti i possibili risultati. Ad esempio nel caso del lancio di un dado (6 facce) gli eventi possibili sono: faccia che mostra un solo punto; faccia che mostra due punti ..., che sono in totale 6, se le evento richiesto è esce una faccia con un numero pari di punti, è evidente che questo si verifica in tre occasioni (esce la faccia che mostra due punti, oppure quattro oppure sei). Nel nostro caso la probabilità è data da $\frac{3}{6} = \frac{1}{2}$.

Nel lancio di due dadi voglio ottenere una coppia di sei (evento le due facce mostrano entrambe sei punti). I casi possibili sono 36, infatti per ogni faccia mostrata dal primo dado il secondo ne può mostrare altre sei. La probabilità nel nostro caso è: $\frac{1}{36} = \frac{1}{6} \cdot \frac{1}{6}$.

Accettiamo questa idea: se gli eventi sono indipendenti (cioè uno non condiziona l'altro) la probabilità si ottiene come prodotto delle probabilità.

Qualche esempio:

Problema 6. Qual è la probabilità che, formando un numero di sei cifre, utilizzando solo il 3, il 5 e il 7, si ottenga un numero in cui compaiono due 3, due 5 e due 7?

Dimostrazione. Calcoliamo i casi possibili, in ogni casella posso mettere uno qualsiasi dei tre numeri pertanto: 3^6; i casi favorevoli sono le sequenze tutte le sequenze di 6 cifre formate dalle 2-ripetizioni dei tre numeri: $\frac{6!}{2! \cdot 2! \cdot 2!} = 90$. La probabilità cercata è $\frac{90}{3^6} = \frac{10}{81} \simeq 0.1234568$ □

6.1.4 Disposizioni e combinazioni

Problema 7. Quante parole di tre lettere posso formare con i caratteri J, O, G, A, S, usando in ogni parola sempre lettere distinte.

Dimostrazione. La prima lettera può essere scelta fra uno qualsiasi dei 5 caratteri, per la seconda ho a disposizione 4 caratteri mentre solo 3 per la terza, in totale $5 \cdot 4 \cdot 3 = 60$ □

In generale se ho n oggetti distinti con cui riempire contenitori con k posti ho $n(n-1)(n-2)\dots(n-k+1)$ modi.

Definizione 34 (Disposizioni di n oggetti presi a k a k)**.** $D_{n,k} = n(n-1)(n-2)\dots(n-k+1)$ Le disposizioni sono il numero di k-uple ordinate che si possono formare con n elementi.

Problema 8. Quante sono le cinquine che si possono ottenere estraendo una dopo l'altra cinque pallina da un'urna contenente 90 palline numerate (da uno a novanta). ([1])

Dimostrazione. Il problema è simile al precedente solo che, in questo cosa, non mi interessa l'ordine in cui sono estratte le palline, quindi ogni permutazione di una cinquina è equivalente, pertanto: $\frac{D_{n,k}}{k!}$ è il numero cercato. □

In generale se ho n oggetti distinti con cui riempire contenitori con k posti ho $n(n-1)(n-2)\dots(n-k+1)$ modi.

Definizione 35 (Combinazione di n oggetti presi a k a k)**.**

$$C_{n,k} = \frac{n(n-1)(n-2)\dots(n-k+1)}{k!} \tag{6.2}$$

Le combinazioni sono il numero dei sottoinsiemi di k elementi che si possono formare con n elementi distinti.

La 6.2 può essere così modificata:

$$\begin{aligned} C_{n,k} = \binom{n}{k} &= \frac{n(n-1)(n-2)\dots(n-k+1)}{k!} \\ &= \frac{n(n-1)(n-2)\dots(n-k+1)}{k!}\frac{(n-k)!}{(n-k)!} \\ &= \frac{n!}{k!(n-k)!} \end{aligned} \tag{6.3}$$

Il simbolo $\binom{n}{k}$ si legge *n su k*

6.1.5 Il superEnalotto

Dal regolamento scopriamo ...

Art. 3 - Il concorso consiste nel pronosticare i primi numeri estratti nelle ruote del lotto di Bari, Firenze, Milano, Napoli, Palermo e Roma, indipendentemente dalla posizione dei sei pronostici rispetto all'ordine alfabetico delle ruote. Per ogni pronostico indovinato si consegue un punto; la somma dei punti (massimo sei) si prende a base per la determinazione dei vincitori, come previsto dall'art. 14. Per il conseguimento della vincita di seconda categoria il pronosticatore deve indovinare cinque dei sei numeri primi estratti nelle ruote del lotto di cui al primo comma del presente articolo e il numero primo estratto nella ruota di Venezia , denominato numero complementare . Se il primo estratto di una ruota sia un numero uguale al primo estratto di una ruota che in ordine alfabetico la precede, ai fini della determinazione dei numeri vincenti, viene preso in considerazione il secondo numero estratto; se anche il secondo estratto sia un numero uguale al primo estratto di altra ruota che precede , viene preso in considerazione il terzo numero estratto, e così via. La medesima procedura si applica anche nei confronti del numero complementare. Qualora non sia possibile determinare una combinazione vincente di prima categoria con punti 6 o di

[1] In sostanza il gioco del Lotto

seconda categoria, con punti 5 più il numero complementare, perché nelle sei ruote utili per l'individuazione del pronostico vengono estratti numeri uguali o per qualsiasi altro motivo, si applica la disposizione prevista al terzo comma dell'art. 14.

Art. 14 - Le giocate vincenti sono di norma di cinque categorie. Alla prima categoria appartengono quelle in cui i pronostici relativi ai primi numeri estratti nelle sei ruote indicate nel primo comma dell'art. 3 sono esatti; alla seconda categoria appartengono quelle in cui sono esatti cinque pronostici più il numero complementare (primo estratto nella ruota di Venezia), alla terza, alla quarta e alla quinta categoria le giocate rispettivamente con 5, 4 e 3 pronostici esatti.

...

Per ciascun concorso, in mancanza di:

a) vincite di prima categoria con punti 6, il relativo montepremi andrà a sommarsi con quello della medesima categoria del concorso successivo, fino al concorso nel quale saranno realizzate vincite con punti 6;

b) vincite di seconda categoria con punti 5 più il numero complementare, ...

analizziamo prima con attenzione l'evento $6 = \{indovino\ i\ 6\ numeri\}$ dal regolamento si coglie che non sempre si può formare la sestina, infatti:

BA ->10
FI -> 18
MI -> 84
NA -> 12
PA -> 90

se la cinquina estratta a Roma è 84, 12, 18, 90, 10 la sestina del superenalotto non si forma.

Calcoliamo ora la probabilità dell'evento $p6n = p\{non\ si\ forma\ lasestina\}$
$p6n = \frac{1}{\binom{90}{5}}$ una sola cinquina fra tutte le possibili!

Sia $p6v = p\{si\ realizza\ la\ sestina\} = 1 - p6n$

$$p6v = 1 - \frac{1}{\binom{90}{5}}$$

l'evento $6n = \{non\ si\ realizza\ lasestina\}$ e l'evento $6v = \{si\ realizza\ lasestina\}$ costituiscono l'insieme di tutte le possibili alternative: $6v \cup 6n = \Omega$

Per calcolare la probabilità di fare sei ($p6$) ho due alternative (eventi): $6v$ o $6n$, se si verifica $6n$ allora $p6 = 0$ se si verifica $6v$ calcolo la $p6$ in questo nuovo insieme, scrivo così: $p(6\,|6v\,)$ che si legge "probabilità dell'evento 6 SAPENDO CHE si è realizzato l'evento $6v$"

$$\begin{aligned} p6 &= p(6\,|6v\,) + p(6\,|6n\,) = p6v\ p(6 \cap 6v) + p6n\ p(6 \cap 6n) \\ &= \left(1 - \frac{1}{\binom{90}{5}}\right) \frac{1}{\binom{90}{6}} + \frac{1}{\binom{90}{5}} 0 \end{aligned}$$

per il 5 si ragiona in modo analogo:

$$p5 = p(5\,|6v\,) + p(5\,|6n\,) = p6v\ p(5 \cap 6v) + p6n\ p(5 \cap 6n)$$
$$= \left(1 - \frac{1}{\binom{90}{5}}\right) \frac{\binom{6}{5}\binom{84}{1}}{\binom{90}{6}} + \frac{1}{\binom{90}{5}} \frac{\binom{5}{5}\binom{85}{1}}{\binom{90}{6}}$$

... 4, 3

per il 5+1

se si realizza la sestina (evento 6v), allora la probabilità che il numero Jolly sia diverso dai sei già estratti è: $1 - \frac{\binom{6}{5}}{\binom{90}{5}}$ e quindi indovino il 5+1 se faccio 5 e se indovino il Jolly: probabilità:

$$\frac{\binom{6}{5}\binom{84}{1}}{\binom{90}{6}} \frac{1}{84}$$

se non si realizza la sestina (evento 6n), allora la probabilità che il numero Jolly sia diverso dai cinque già estratti è: $1 - \frac{1}{\binom{90}{5}}$ e quindi indovino il 5+1 se faccio 5 e se indovino il Jolly: probabilità:

$$\frac{\binom{5}{5}\binom{85}{1}}{\binom{90}{6}} \frac{1}{85}$$

quindi

$$p5p1 = \left(1 - \frac{1}{\binom{90}{5}}\right)\left(1 - \frac{\binom{6}{5}}{\binom{90}{5}}\right)\left(\frac{\binom{6}{5}\binom{84}{1}}{\binom{90}{6}} \frac{1}{84}\right) + \left(\frac{1}{\binom{90}{5}}\right)\left(1 - \frac{1}{\binom{90}{5}}\right)\left(\frac{\binom{5}{5}\binom{85}{1}}{\binom{90}{6}} \frac{1}{85}\right)$$

6.1.6 Combinazioni con ripetizione

Problema 9. In quanti modi posso ottenere 7 sommando 3 numeri interi non negativi ($x_1, x_2, x_3 \in \mathbb{N}$).

Dimostrazione. Pensiamo a 7 come 7 barrette $|, |, |, |, |, |, |$ che hanno la proprietà di aggregarsi, ad esempio $||||$ è 4. Il problema diventa contare i possibili "aggregati" di barrette sommati fra loro, come ad esempio $||| + || + ||$. Pertanto devo contare in quanti modi posso disporre le sette barrette nell'insieme sette $|$ e due $+$.

$$C^R_{n,k} = \binom{n-1+k}{k}$$

Nel nostro caso k sono le barrette e n le x_i. □

$C^R_{n,k}$ sono le combinazioni con ripetizione.

Problema 10. La nonna Maria va in drogheria per acquistare delle guarnizioni per i dolci. Il negozio vende: confetti, chicchi di caffè, candeline a 50 centesimi alla confezione e canditi a 2e alla confezione. La nonna ha speso 10e. Quanti sono i diversi tipi di spesa possibili?

Soluzione. Prendiamo come unità 50 centesimi, così il problema si può scrivere:

$$x_1 + x_2 + x_3 + 4x_4 = 20$$

Prendiamo il caso in cui la nonna acquisti una sola confezione di canditi, otteniamo: $x_1 + x_2 + x_3 = 16$, che ci permette di determinare che in questo caso le diverse spese sono: $C^R_{3,16} = \binom{18}{16} = 153$. Dette i il numero di confezioni acquistate, la soluzione generale è data da:

$$\sum_{i=0}^{5} \binom{20 - 4i + 3 - 1}{20 - 4i} = 536$$

□

Quanti modi diversi esistono per scegliere sei bottiglie di vino di tre qualità diverse?