

Block Notes Matematico

PARI/GP e le equazioni

ing. Rosario Turco

Abstract

In questo articolo ci si sofferma su esempi semplici per sull'utilizzo di PARI/GP per la risoluzione di alcuni tipi di equazioni.

PARI/GP è free e si presta facilmente a rapide verifiche, a lavorare con valori elevati di interi o numeri primi, sia alla programmazione di script per la risoluzione di problemi più complessi. E' naturale che per elaborazioni delicate di numeri elevati e test di primalità, essendo un linguaggio interpretato, ha minori prestazioni rispetto a quelli compilati e ottimizzati per l'architettura hardware a disposizione (AMD, INTEL, SPARC, etc). Spesso verificata la logica di un programma con PARI/GP è possibile riscrivere lo stesso con librerie GMP per ottenere elevate prestazioni. Inoltre PARI/GP fornisce una serie di librerie grafiche.

Risoluzione di Equazioni col Modulo (Congruenze lineari)

Supponiamo di avere la funzione $f(x)=x^2-1$ e di voler sapere se esiste un valore di "a modulo" per cui $f(a) = x \text{ Mod } 147$, con $x=1,2,\dots$

Come si risolve l'equazione con l'aiuto di PARI/GP? Dovendo generalizzare, scriviamo:

```
%3 n = 147;
? f(x)=x^2-1;
%4 = (x)->x^2-1
? for(i=0,n-1,a=Mod(i,n);b=f(a); if(b==Mod(1,n),print(a,"t",b)););
? for(i=0,n-1,a=Mod(i,n);b=f(a); if(b==Mod(2,n),print(a,"t",b)););
? for(i=0,n-1,a=Mod(i,n);b=f(a); if(b==Mod(3,n),print(a,"t",b)););
Mod(2, 147)  Mod(3, 147)
Mod(47, 147)  Mod(3, 147)
Mod(100, 147)  Mod(3, 147)
Mod(145, 147)  Mod(3, 147)
```

Nell'esempio abbiamo variato nell'if il valore del Modulo ogni volta e si è visto che per $f(x)=3 \text{ mod } 147$ esistono 4 soluzioni modulo per una equazione di secondo grado. Se si continua a variare x si trovano anche altre due a $\text{Mod}(8,n)$ etc.

Esaminiamo, invece, una congruenza lineare del tipo:

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

Essa ammette soluzione sse $\gcd(a,n) \mid b$, che si legge dicendo che la congruenza ammette soluzione se e solo se il MCD(a,n) è un divisore di b. Se la condizione è rispettata una soluzione si può trovare facendo in modo per $ax=b+kn$ di variare il valore k in modo da ottenere che la parte destra della uguaglianza sia un multiplo della parte sinistra.

Provate con la funzionalità EqMod(a,b,n) presente nel software del sito www.gruppoeratostene.com

Ad esempio con le equazioni:

$$3x \equiv 7 \pmod{6} \text{ (non risolvibile)}$$

$$3x \equiv 12 \pmod{6} \text{ soluzione } x=6$$

$$9x \equiv 16 \pmod{2} \text{ soluzione } x=2$$

Risoluzioni di sistemi di congruenze lineari

Un sistema di congruenze lineari del tipo:

$$\begin{cases} x \equiv b_1 \pmod{n_1} \\ x \equiv b_2 \pmod{n_2} \\ \dots\dots\dots \\ x \equiv b_r \pmod{n_r} \end{cases}$$

per il *Teorema cinese del resto* ammette soluzioni se n_1, n_2, \dots, n_r a due a due sono coprimi. Nel seguito esaminiamo un sistema di sole due equazioni per semplicità, ad esempio:

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

$$4x \equiv 2 \pmod{7}$$

Il Teorema cinese del resto suggerisce subito che essendo $\text{MCD}(7,10)=1$ allora n_1 e n_2 sono coprimi per cui il sistema è risolvibile e che dobbiamo considerare $N=n_1*n_2=70$.

Se risolviamo ognuna secondo il metodo del paragrafo precedente troviamo che

$$x \equiv 7 \pmod{10}$$

$$x \equiv 4 \pmod{7}$$

Ora x deve soddisfare entrambe le congruenze. L'identità di Bezout(10,7)=[-2,3,1]; per cui la soluzione è:

$$x = 4*(-2)*10+7*3*7=67 \pmod{70}$$

Tenendo conto di come abbiamo risolto il tutto la funzionalità Sist2EqMOD(a,b,n1,c,d,n2) del software risolve un sistema di due congruenze lineari.

Equazioni lineari diofantee di primo grado

Vogliamo risolvere l'equazione diofantea di primo grado $ax+by=c$ (vedi [1]), ad esempio:

$$8x+5y=81$$

Sappiamo dalla teoria delle equazioni diofantee che essa è risolvibile se e solo se il $\gcd(a,b)$ divide c , ovvero c è un multiplo del $\gcd(a,b)$; il che significa che $\text{Mod}(c,\gcd(a,b))=0$.

? a=8;

? b=5;

? d=gcd(a,b)

%14 = 1

Quindi l'equazione che stiamo esaminando è risolvibile. Sempre dalla teoria sappiamo che tutte le possibili soluzioni sono del tipo:

$$X = cx_0 + bt$$

$$Y = cy_0 - at$$

con (x_0,y_0) soluzione particolare e $t \in \mathbb{Z}$.

L'*identità di Bezout* è una particolare soluzione della equazione diofantea $ax+by=c$; in particolare in PARI/GP `bezout(x,y)` fornisce un vettore $[a,b,d]$ dove $d = \gcd(x,y)$ e a,b sono i coefficienti dell'equazione diofantea:

? bezout(a,b)

%15 = [2, -3, 1]

Quindi le soluzioni sono del tipo:

$$(81*2+5*t, 81*(-3) -8*t)=(162+5*t,-243-8*t)$$

A questo punto possiamo scrivere uno script che risolve equazione diofantee di primo grado:

```
DiofPG(a,b,c) = local(); {  
  if( Mod(c,gcd(a,b))!=0, error("Equazione diofantea NON risolvibile!"));  
  v = bezout(a,b);  
  print("Equazione Diofantea primo grado risolvibile");  
  print("x = ",c*v[1],"+",b,"*t");  
  print("y = ",c*v[2],"-",a,"*t");  
  return;  
}
```


$$p_2 = a_2 * p_1 + p_0 = 1 * 2 + 1 = 3$$

$$q_2 = a_2 * q_1 + q_0 = 1 * 1 + 0 = 1$$

$$p_3 = a_3 * p_2 + p_1 = 1 * 3 + 2 = 5$$

$$q_3 = a_3 * q_2 + q_1 = 1 * 1 + 1 = 2$$

$$p_4 = a_4 * p_3 + p_2 = 1 * 5 + 3 = 8$$

$$q_4 = a_4 * q_3 + q_2 = 1 * 2 + 1 = 3$$

Da qui si vede subito che $8^2 - 7 * 3^2 = 64 - 63 = (-1)^4 = 1$ rappresenta difatti una soluzione.

Se n fosse stato dispari per trovare la soluzione occorre andare oltre con i quozienti parziali della `contfrac` fino a trovare un altro termine pari a $2 * a_1$ e fare le iterazioni fino al termine precedente a quest'ultimo (in questo modo ci si riconduce ad un quoziente parziale di indice pari di nuovo).

Qualche dritta su `contfrac`: per poter ottenere una sufficiente espansione della frazione continua con molti termini, specie se il primo termine $2 * a_1$ non basta e il numero da trattare è abbastanza grande, occorre fare almeno due cose: eseguire un comando `\p <numero>` dove numero deve essere grande abbastanza, da far contenere nell'espansione di `contfrac` anche il secondo $2 * a_1$ (il default di `\p` è di 28); ed eseguire un sufficiente comando `allocatemem` per dare allo stack sufficiente memoria per l'elaborazione (qua dipende dal vostro computer).

Provate a eseguire, col software disponibile sul sito, la funzionalità `DiofPell(x)`, con i seguenti valori: 7 con 4 cifre di espansione, 28 con 4 cifre di espansione, 37 con 1 cifra di espansione, 309 con 26 cifre di espansione, 408 con 1 cifra di espansione, 409 con 2 cifre di espansione, 410 con 1 cifra di espansione, 30001 con 284 cifre di espansione, 123456811 con 20006 cifre di espansione.

Negli esempi non dovrete agire su `\p` e `allocatemem` fino all'esempio 408. Da 409, in poi, il programma vi chiederà di agire su `\p` aumentandolo a 300 o più.

Poi se vi darà uno dei due errori seguenti:

```
? DiofPell(123456811)
```

```
Equazione di Pell x^2-dy^2=1 risolvibile
```

```
*** array index (0) out of allowed range [1-3].
```

L'errore di sopra richiede `\p 200000`; mentre l'errore successivo richiede l'esecuzione del comando preventivo `allocatemem(64*1024*1024)` su un PC con sufficiente RAM.

```
? DiofPell(123456811)
```

```
Equazione di Pell x^2-dy^2=1 risolvibile
```

```
*** contfrac: the PARI stack overflows !
```

```
current stack size: 4000000 (3.815 Mbytes)
```

```
[hint] you can increase GP stack with allocatemem()
```

Nell'ultimo esempio col valore 123456811, con $\backslash p$ 200000 e `allocatemem(64*1024*1024)`, si ottiene una risposta in 26 ms con un PC QUAD Aspire M5641 (multiprocessore a 4Gb di RAM). Digitare # prima di eseguire `DiofPell(x)` in modo da settare a on il timer ed esaminerete anche il tempo impiegato.

Sul sito www.gruppoeratostene.com, sezione Software, è disponibile software per PARI/GP per la risoluzione dell'equazione di Pell $x^2 - dy^2 = 1$. Il software, però, è solo un semplice esempio, più che altro per imparare l'utilizzo di PARI/GP; ma per lavorare con numeri maggiori ed evitare di dover allocare memoria per `contfrac`, non va usato `contfrac` e occorre ricavarsi i vari quozienti parziali in maniera alternativa con l'espansione della radice (vedi [3]) e l'*algoritmo di Euclide*. Questo vuol dire rinunciare ad una funzionalità built-in ottimizzata di PARI/GP e nel caso di numeri molto grandi occorre attendere del tempo maggiore. Un'alternativa, se si è alla ricerca di velocità per numeri molto grandi, è riscrivere però il programma con GMP.

Radici di una equazione di qualunque grado

Supponiamo una equazione $x^2 = 4$. In PARI/GP si considera il polinomio $f(x) = x^2 - 4$ ed effettuando:

```
? polroots(f(x))
```

```
%58 = [-2.000 + 0.E-9*I, 2.000 + 0.E-9*I]
```

```
? matsize(%)
```

```
%59 = 2
```

Si è usata una precisione solo a 9 cifre ($\backslash p$ 9). Le parti immaginarie hanno coefficiente 0, per cui le radici trovate sono due attese: (2, -2).

Vediamo con una equazione di terzo grado:

```
? f(x)=x^3+x^2+2*x+12
```

```
%1 = (x)->x^3+x^2+2*x+12
```

```
? polroots(f(x))
```

```
%2 = [-2.338740539822604285469035064 + 0.E-28*I, 0.6693702699113021427345175319 - 2.164003284319594726962806087*I,  
0.6693702699113021427345175319 + 2.164003284319594726962806087*I]
```

```
? matsize(%)
```

```
%59 = 3
```

Quindi tre radici, di cui una reale e due immaginarie. Ovviamente il numero di radici attese per il Teorema di Gauss sono pari al grado dell'equazione e lo conferma anche `matsize()`.

In realtà si può fare per qualsiasi grado dell'equazione. Il metodo di sopra trova tutte le radici; se volessimo, invece, trovare solo le radici in un intervallo e non su tutto l'intervallo di definizione della funzione, allora useremo il Metodo delle tangenti (vedi [6]) o il `solve` (vedi [7]).

Risoluzione di Sistemi di equazioni lineari

Un sistema di equazioni lineari è esprimibile in forma matriciale $Ax = c$. Se A è una matrice quadrata, il cui determinante è diverso da zero, allora il teorema di *Rouchè - Capelli* afferma che il sistema ha un'unica soluzione.

È possibile, in tal caso, usare il determinante e la *regola di Laplace o di Cramer* per la risoluzione, dove se $(x_1, x_2, x_3, \dots, x_n)$ sono le soluzioni da trovare, allora la generica soluzione è data da: $x_i = \frac{\det(A_i)}{\det(A)}$ (vedi [5])

Ad esempio il sistema: $ax + by = e$
 $cx + dy = f$ si può scrivere in modo matriciale nel seguente modo:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} e \\ f \end{pmatrix}$$

Le cui soluzioni sono:

$$x = \frac{\begin{vmatrix} e & b \\ f & d \end{vmatrix}}{\begin{vmatrix} a & b \\ c & d \end{vmatrix}} \quad e \quad y = \frac{\begin{vmatrix} a & e \\ b & f \end{vmatrix}}{\begin{vmatrix} a & b \\ c & d \end{vmatrix}}$$

Nel caso più generale avremo n soluzioni se n sono le equazioni, ma la regola di sopra si itera ugualmente mettendo il vettore (e, f) al posto della i -esima colonna della i -esima soluzione x_i . E con PARI/GP come lo risolviamo un sistema di equazioni? Supponiamo $a=2, b=3, c=4, d=5, e=6, f=7$

Chiamiamo con A il determinante a denominatore di x e y ; poi chiamiamo B il determinante a numeratore di x e C il determinante a numeratore di y ; per cui con PARI/GP si ottiene:

? A = [2,3;4,5]

%48 =

[2 3]

[4 5]

? B = [6,3;7,5]

%49 =

[6 3]

[7 5]

? C = [2,6;3,7]

%50 =

[2 6]

[3 7]

Per cui a questo punto è:

$$x = \frac{\det(B)}{\det(A)}$$

$$x = -9/2$$

$$y = \frac{\det(C)}{\det(A)}$$

$$y = 2$$

Riferimenti

[1] http://it.wikipedia.org/wiki/Equazione_diofantea_lineare

[2] T. Nagell, Introduction to Number Theory, Second Edition

[3] Cristiano Teodoro, Sulla risoluzione dell'equazione di Pell

[4] http://it.wikipedia.org/wiki/Equazione_di_Pell

[5] http://it.wikipedia.org/wiki/Regola_di_Cramer

[6] R. Turco - Analisi numeriche e simulazioni

[7] R. Turco, M. Colonnese - Aggirandosi tra i plot della zeta di Riemann