Barbatrucchi per il problem-solving (problem solving senza problemi)

Federico Poloni

21 marzo 2004

Introduzione

XXX: to be written...

I Barbatrucchi sono ancora un work in progress, come noterete dalle frequenti note con "XXX" durante il testo. Sono graditissime segnalazioni di errori e/o omissioni, consigli, opinioni, anche solo incoraggiamenti ("ti prego, pol, trova la voglia di scrivere ancora qualche pezzo dei barabtrucchi"). In particolar modo, riguardo ai problemi inseriti: proposte di nuovi problemi o di modifiche a quelli presenti ("se usi come coefficiente numerico 37 invece di 27 è più facile/difficile/istruttivo"), eventuali soluzioni qui mancanti che io non ho avuto voglia di scrivere, eccetera.

A questo scopo, un paio di indirizzi e-mail che dovrebbero funzionare sono `fphtrentasette@ngi.it` e `f.polonitrentasette@sns.it` (rimuovete il numero 37 per ottenere gli indirizzi e-mail veri... cerco di evitare di pubblicarli "as is" su internet per evitare spam e scocciatori vari).

Capitolo 1

Polinomi

1.1 Fattorizzazione

Spesso la soluzione di un problema passa (in modo più o meno evidente) attraverso la fattorizzazione di un polinomio, o comunque attraverso lo "switching" tra le due forme alternative di scrittura del polinomio[1]:

$$a_n \prod_{i=1}^{n}(x_i - \alpha_i) \Longleftrightarrow \sum_{i=1}^{n} a_i x^i$$

↬*Sembra teoria dei numeri, ma...*

Molti problemi che coinvolgono numeri interi in realtà si risolvono scrivendo un polinomio a coefficienti interi e fattorizzando. Non è difficile accorgersi quando ci si trova di fronte un problema di questo tipo. L'unico fatto importante da tenere a mente per la "traduzione" è che

Fatto 1 *Se $p(x)$ è un polinomio a coefficienti interi, $p(a)$ è intero $\forall$ a intero*

↬*Ruffinare le informazioni*

Una delle prime domande da porsi davanti a un problema è: Quali sono le forme equivalenti per scrivere le ipotesi? Quali mi saranno più utili per risolvere il problema?

Nei problemi riguardanti i polinomi, il teorema di fattorizzazione (teorema di Ruffini) ci fornisce un mezzo utile per metabolizzare informazioni del tipo $p(37) = 91$, con 37 e 91 numeri casuali. In generale, $p(a) = b$ significa

$$p(x) = (x - a)q(x) + b$$

per qualche $q(x)$ tale che $\partial q = \partial p - 1$.[2]

Un problema classico su questi temi:

[1] Ricordiamo che il simbolo $\prod$ rappresenta la "produttoria", che si comporta esattamente nello stesso modo della sommatoria, solo rispetto all'operazione "per" invece che al "più". Sono entrambe notazioni precise, comode e compatte che sarebbe il caso di imparare a usare il più presto possibile.

[2] Qui ∂p è il grado di $p(x)$, nel senso usuale di "massimo esponente della x"

Problema 1 *Sia $p(x)$ un polinomio a coefficienti interi tale che $p(a_i) = 5$ per quattro valori distinti a_1, a_2, a_3, a_4. Allora non esiste nessun n intero tale che $p(n) = 16$*

Applichiamo da bravi bambini la regola appena imparata: l'ipotesi si traduce in

$$p(x) - 5 = (x - a_1)(x - a_2)(x - a_3)(x - a_4)q(x)$$

per un qualche q(x) a coefficienti interi. Perciò, $p(n) = 16$ implicherebbe

$$11 = p(n) - 5 = (n - a_1)(n - a_2)(n - a_3)(n - a_4)q(n)$$

e avremmo scritto 11 come prodotto dei cinque fattori a secondo membro. Però 11 è primo, e quindi fattori del tipo $n - a_i$ (che sono tutti distinti) possono assumere solo i valori:

- ± 1
- ± 11 (una volta sola, o compare $+11$ oppure -11).

Perciò non è possibile scrivere 11 come prodotto di 4 fattori distinti (più il fattore $q(x)$, che essendo intero può solo assumere uno dei valori qui sopra e non modifica la situazione) □

↬ *Valutazioni furbe*

Spesso si riescono a estrarre informazioni valutando il polinomio per un valore "particolare" dell'indeterminata...

Problema 2 *Semplificare l'espressione*

$$\frac{(x-a)(x-b)}{(c-a)(c-b)} + \frac{(x-b)(x-c)}{(a-b)(a-c)} + \frac{(x-c)(x-a)}{(b-c)(b-a)}$$

, per a, b, c distinti

L'idea da applicare è evidente: se chiamiamo $P(x)$ l'espressione, valutiamo e otteniamo $P(a) = P(b) = P(c) = 1$. Quindi, poiché si tratta di un polinomio di secondo grado che ha tre radici distinte, esso deve essere costantemente uguale a 1.

Abbiamo così ripassato un importante lemma:

Fatto 2 *Se due polinomi di grado $\leq n$ assumono lo stesso valore in $n+1$ punti distinti, allora sono uguali*

A questo affianchiamo un altro teorema di importanza vitale per la ricerca di radici:

Fatto 3 (Rational root theorem) *Se un polinomio $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$ ha una radice razionale $\frac{p}{q}$, allora $q \mid a_n$ e $p \mid a_0$*

↬*Complessificare semplifica*

Le tecniche di *root-shooting* del punto precedente possono funzionare anche con valori complessi: il più delle volte, radici n-esime dell'unità. Quando un polinomio è il "candidato ideale" per provare a giocherellarci con i numeri complessi? Quando tutti (o quasi) i suoi coefficienti sono ± 1. Esempio:

Problema 3 *Fattorizzare nei razionali*

$$x^5 + x^4 + 1$$

Un polinomio di quinto grado si può spezzare in diversi modi, l'unico vincolo è che la somma dei gradi dei fattori sia 5: per esempio, due fattori di grado 1 e uno di grado 3, oppure $4+1$, $2+2+1$... Il primo tentativo è provare a cercare le radici razionali: per il fatto 3, esse possono essere solo ± 1, ma si verifica sostituendo che nessuno dei due numeri è radice.

Per cui, proviamo a cercare un fattore in un altro modo: sia ω una radice cubica complessa dell'unità: quindi, $\omega^3 = 1$ e $\omega^2 + \omega + 1 = 0$. Allora, abbiamo

$$\omega^5 + \omega^4 + 1 = \omega^3 \cdot \omega^2 + \omega^3 \cdot \omega + 1 = \omega^2 + \omega + 1 = 0$$

Per cui entrambe le radici cubiche complesse dell'unità (ω e ω^2)sono soluzioni del polinomio: esso ha allora come fattore $(x-\omega)(x-\omega^2) = x^2 + x + 1$. L'altro fattore si trova con l'algoritmo di divisione per polinomi (ripassare, ripassare), ed è di grado 3. Ora, può questo fattore essere ulteriormente scomponibile? Se lo fosse, per il semplice calcolo dei gradi, un fattore dovrebbe avere grado 1: ma abbiamo visto sopra che il polinomio di partenza non aveva radici razionali.□

↬*Quadrati ovunque*

Un fatterello che vale la pena di ricordare:

Fatto 4 (Identità di Sophie Germain) *La somma $a^4 + 4b^4$ si può fattorizzare negli interi*

Si dimostra aggiungendo e sottraendo $4a^2b^2$ in modo da riuscire a fattorizzare l'espressione come differenza di due quadrati:

$$a^4 + 4a^2b^2 + 4b^4 - 4a^2b^2 = (a^2 + 2b^2)^2 - (2ab)^2 = (a^2 + 2ab + 2b^2)(a^2 - 2ab + 2b^2)$$

In generale, lo scopo di questa sezione è quello di ricordare che si possono applicare tecniche come quella qui utilizzata per la fattorizzazione.

↬*Trucchi per ricordare le identità algebriche*

La madre di tutte le identità algebriche è

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \ldots + ab^{n-2} + b^{n-1}) \qquad (1.1)$$

che è semplicemente una generalizzazione della classica $a^2-b^2=(a-b)(a+b)$ Vale forse la pena di ricordarla direttamente nella forma "somma della serie geometrica":

$$1+x+x^2+\ldots+x^{n-1}+x^n=\frac{1-x^{n+1}}{1-x} \tag{1.2}$$

La (1.1), se n è dispari, ponendo $b\mapsto -b$, diventa

$$a^n+b^n=(a+b)(a^{n-1}-a^{n-2}b+a^{n-3}b^2+\ldots-ab^{n-2}+b^{n-1}$$

questa è la più semplice di quella serie di identità che dicono che

$x+y$	$\mid x^n+y^n$	$\Leftrightarrow$ n dispari
$x+y$	$\mid x^n-y^n$	$\Leftrightarrow$ n pari
$x-y$	$\mid x^n+y^n$	mai (salvo casi banali: $x=0$, $y=0$)
$x-y$	$\mid x^n-y^n$	sempre

Che, viste così, appaiono parecchio rognose da ricordare. In realtà sono abbastanza semplici se si fanno ragionamenti di questo tipo: (per la prima, ad esempio): devo dividere per $x+y$, quindi suppongo $x=-y$. Allora, $x^n+y^n=x^n+(-x)^n$ vale 0 se n è dispari e $2y^n$ se n è pari. Solo nel primo caso ho ottenuto 0, quindi la divisibilità c'è solo nel primo caso[3].

Altra identità importante a un certo livello è questa:

$$(a^2+b^2)(c^2+d^2)=(ac-bd)^2+(ad+bc)^2 \tag{1.3}$$

che esprime in formule il seguente fatto: *Se due numeri si possono scrivere come somma di due quadrati, allora anche il loro prodotto si può scrivere come somma di due quadrati.* Cattiva, vero? Invece si ricorda in questo modo: se $w=a+bi$ e $z=c+di$ sono due numeri complessi, allora

$$|w|\,|z|=|wz| \tag{1.4}$$

dove $|w|$ è il modulo di w (cioè a^2+b^2) e il prodotto a destra è il normale prodotto tra numeri complessi[4].

Problema 4 *Dimostrare che, dato un polinomio $f(x)$ a coefficienti reali, i seguenti due fatti sono equivalenti:*

[3] Già, ma come si formalizza? Ecco qui: prendiamo il seguente polinomio in x: x^n+y^n (con y costante). Esso è divisibile per $x+y$ se e solo se ponendo $x=-y$ il polinomio si annulla (è il buon vecchio teorema di Ruffini), quindi basta sostituire $y\mapsto -x\ldots$

[4] Un paio di note. Se avete già sentito parlare dei quaternioni e magari ricordate la regola per farne il prodotto, bene, la stessa identità riletta come se w e z fossero quaternioni fornisce un'identità per scomporre in somme di 4 quadrati il prodotto di due numeri che sono somma di 4 quadrati.

Poi, se invece avete già visto la scrittura in forma vettoriale della disuguaglianza di Cauchy-Schwarz, le due vi possono sembrare contraddittorie: CS dice che

$$w\cdot z\leq |v|\,|w|$$

Occhio al prodotto però! Il prodotto che compare in questa formula è il prodotto scalare tra vettori (cioè, $(a,b)\cdot(c,d)=ac+bd$, che restituisce un numero reale), mentre il prodotto della 1.4 è il prodotto tra complessi (cioè $(a+bi)(c+di)=ac-bd+(ad+bc)i$, che restituisce un numero complesso).

1. *$f(x) \geq 0$ per ogni x reale*
2. *f si scrive nella forma $p(x)^2 + q(x)^2$, dove p e q sono polinomi (a coefficienti reali) e $\partial p > \partial q$*

XXX: da scrivere!

↬*Scaletta per fattorizzare polinomi*

- Cercare soluzioni banali (0, 1, -1, porre $x = a$, $x = y \ldots$) e poi ruffinare
- Se il polinomio è a coefficienti interi: cercare zeri razionali con il *rational root theorem*; cercare una fattorizzazione negli interi[5]; provare il criterio di Eisenstein per vedere se per caso è irriducibile (vedi qui sotto)
- Cercare di applicare un'identità algebrica (es. scriverlo come differenza di due quadrati), eventualmente aggiungendo e sottraendo termini o facendo raccoglimenti furbi
- Cercare zeri complessi semplici (ad es. radici dell'unità)
- Il polinomio è quadratico (=di secondo grado) in una delle sue variabili? Allora posso scomporlo utilizzando la formula esplicita per le soluzioni
- Il polinomio è simmetrico? Allora posso provare a scriverlo come funzione dei polinomi simmetrici elementari e vedere se salta fuori qualcosa di illuminante
- Se siamo sui reali: usare il teorema di esistenza degli zeri (se un polinomio assume un valore positivo in a e uno negativo in b, allora esiste almeno una radice reale compresa tra a e b)
- XXX: altre idee?

Infine, un criterio per sapere quando un polinomio *non* si fattorizza:

Fatto 5 (Criterio di Eisenstein) *Sia $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$ un polinomio monico a coefficienti interi. Se esiste un primo p tale che $p \mid a_i$ per $i = 0 \ldots n-1$ e $p^2 \not| a_0$, allora il polinomio è irriducibile sugli interi (e quindi anche sui razionali).*

La dimostrazione è breve e interessante perché usa con profitto tecniche avanzate di algebra: supponiamo per assurdo che il polinomio si fattorizzi sugli interi come $f(x) = g(x) \cdot h(x)$. Ora, leggiamo la precedente uguaglianza come una congruenza modulo p: per le ipotesi fatte $f(x) \equiv x^n$, ma il teorema di Ruffini e la fattorizzazione unica di polinomi sono fatti che valgono anche sugli interi modulo p, quindi la fattorizzazione trovata dev'essere del tipo

$$x^n \equiv x^k \cdot x^{n-k}$$

Quindi $g(x) \equiv x^k \mod p$ e $h(x) \equiv x^{n-k} \mod p$: in particolare allora p divide i due termini noti di $g(x)$ e $h(x)$; quindi il termine noto di f (che è il prodotto di questi due termini noti) deve essere divisibile per p^2, che è assurdo perché è in contrasto con l'ipotesi. □

1.2 Polinomi simmetrici

Notazione

Si chiamano simmetrici quei polinomi in più variabili che rimangono formalmente uguali se si scambiano tra loro in qualunque modo le variabili. Ad esempio,

$$f(a,b,c) = a^3b + a^3c + b^3c + b^3a + c^3a + c^3b$$

è simmetrico. È utilissima con i polinomi simmetrici (specialmente nelle disuguaglianze) la notazione di "sommatoria simmetrica" [Kedlaya]: ad esempio, il polinomio qui sopra si scrive come

$$\sum_{\text{sym}} a^3b$$

dove il *sym* significa "somma tutte le espressioni che si ottengono permutando le variabili" (il fatto che le variabili siano tre qui è sottointeso, non capita spesso di dover cambiare numero di variabili all'interno dello stesso problema).

A volte si pone che la somma sia su *tutte* le permutazioni anche quando questo genera dei termini doppi: per esempio, in tre variabili

$$\sum_{\text{sym}} x^3 = 2x^3 + 2y^3 + 2z^3$$

dove si hanno, per esempio, due x^3 perché il primo corrisponde alla permutazione $(x,y,z) \mapsto (x,y,z)$ mentre il secondo alla $(x,y,z) \mapsto (x,z,y)$. Entrambe le notazioni (porre $\sum_{\text{sym}} x^3 = x^3 + y^3 + z^3$ oppure $2(x^3 + y^3 + z^3)$), cioè utlizzare il concetto ingenuo di e tutte le espressioni simmetriche oppure sommare su tutte le permutazioni) hanno i loro vantaggi e svantaggi. La prima è più intuitiva; la seconda è utile solo se ci si è già molto impratichiti, in tal caso rende più semplici i conti che si possono fare manipolando direttamente l'espressione sotto $\sum_{\text{sym}}$ senza svolgere (con le opportune regole di calcolo, che qui non enunceremo). Su [Kedlaya] è usata la seconda.

La "sommatoria ciclica" fa quasi la stessa cosa, solo che invece di sommare su tutte le permutazioni si somma solo su quelle "di tipo shift", cioè $a \mapsto b, b \mapsto c, c \mapsto d \ldots y \mapsto z, z \mapsto a$ iterato un po' di volte. Quindi, in quattro variabili, si ha

$$\sum_{\text{cyclic}} a^3b = a^3b + b^3c + c^3d + d^3a$$

Notate che, in n variabili, le $\sum_{\text{cyclic}}$ hanno n termini, le $\sum_{\text{sym}}$ ne hanno $n!$, se si adotta la seconda convenzione.

Talvolta torna comodo avere una notazione anche per le funzioni simmetriche elementari, in questo testo porremo in quattro variabili per esempio,

$$\begin{aligned}\sigma_1 &= a+b+c+d\\ \sigma_2 &= ab+ac+ad+bc+bd+cd\\ \sigma_3 &= abc+abd+acd+bcd\\ \sigma_4 &= abcd\end{aligned}$$

e l'ovvia estensione per un numero qualsiasi di variabili.

↬*Se si chiamano simmetrici, un motivo ci sarà*

Calcolando prodotti con i polinomi simmetrici, la cosa buona è che si devono calcolare solo pochi coefficienti. Vogliamo calcolare per esempio, in 4 variabili,

$$(a^2b+a^2c+a^2d+b^2a+b^2c+b^2d+c^2a+c^2b+c^2d+d^2a+d^2b+d^2c)(a+b+c+d)$$

(esercizio: verificare che entrambi i termini sono simmetrici!). Il conto può accorciarsi notevolmente se si nota che tipo di polinomi simmetrici dovranno comparire nel prodotto: ci si convince velocemente che potranno solo comparire termini del tipo a^3b, o a^2b^2, o a^2bc. Perciò il prodotto si scrive come

$$A(a^3b+a^3c+\ldots)+B(a^2b^2+a^2c^2+\ldots)+C(a^2bc+a^2bd+\ldots)$$

e a questo punto si trovano A, B e C cercando manualmente il coefficiente di uno solo dei termini di quel tipo: per esempio, a^3b si può ottenere solo moltiplicando a^2b per a, quindi ha coefficiente 1. D'altra parte, a^2b^2 si ottiene sia come $a^2b\cdot b$ che come $ab^2\cdot a$, quindi ha coefficiente 2. Il prodotto risulta quindi:

$$(a^3b+a^3c+\ldots)+2(a^2b^2+a^2c^2+\ldots)+(a^2bc+a^2bd+\ldots)$$

↬*Un'utile verifica*

Per controllare il risultato possiamo provare a contare il numero di termini nei due lati dell'uguaglianza: a sinistra sono $12\cdot 4=48$; a destra sono $12+2\cdot 12+12=48$. Questo equivale chiaramente a porre tutti i termini uguali a 1. Ulteriori verifiche si possono fare ponendo alcuni termini uguali a 1 e gli altri a 0.

↬*La scomposizione ovvia*

Fatto 6 *Ogni polinomio simmetrico si scrive come un polinomio in funzione dei σ_i introdotti al paragrafo precedente.*

Ad esempio, dato un qualsiasi polinomio simmetrico in tre variabili, diciamo

$$x_1^3+x_2^3+x_3^3+x_1x_2x_3$$

possiamo scomporlo (dopo un po' di conti) come

$$\sigma_1^3-3\sigma_2\sigma_1-2\sigma_2$$

Questo tipo di scomposizione è potente già in due variabili: per esempio permette di risolvere sistemi di equazioni del tipo

$$\begin{cases} x^2 + y^2 = 5 \\ x^3 + y^3 = 10 \end{cases}$$

in modo semplice: riscriviamo infatti come ($\sigma_1 = x + y$, $\sigma_2 = xy$)

$$\begin{cases} \sigma_1^2 - 2\sigma_2 = 5 \\ \sigma_1^3 - 3\sigma_2\sigma_1 = 10 \end{cases}$$

XXX: finire i conti (sostituire con una + semplice?)

1.3 L'anello dei polinomi

I polinomi sono un *anello euclideo*, cioè hanno molte delle proprietà dei numeri interi, e questo parallelismo ci permette di vedere meglio diversi teoremi e applicazioni. Ad esempio, consideriamo gli enunciati dei teoremi di divisione con resto:

- Per ogni a, b interi, esistono (unici) q, r interi t.c. $a = qb + r$ e $0 \leq r < b$

- Per ogni $f(x), g(x)$, esistono unici $q(x), r(x)$ polinomi t.c. $f(x) = q(x)g(x) + r(x)$ e $\partial(r) < \partial(g)$ oppure[6] $r(x) = 0$

È chiaro il parallelismo tra i due enunciati; è chiaro anche che la funzione grado prende il ruolo del valore assoluto per gli interi. Possiamo andare oltre ed estendere il parallelismo:

- Il *massimo comun divisore* tra due polinomi è definito come il polinomio di grado massimo che divide (senza resto) entrambi. Chiaramente, il MCD tra due polinomi è tutt'altro che unico: per come è definita la divisibilità il MCD tra $x^2 - 1$ e $x^3 + 10x^2 - 7x - 4$ è $x - 1$, ma anche $2x - 2$ o $1 - x$ vanno bene: il MCD è *unico a meno di moltiplicazione per costanti* (questo è l'equivalente algebrico del fatto che sugli interi l'MCD è definito a meno del segno: cioè l'MCD tra 27 e 336 è 3 oppure -3, anche se di solito si sottintende di scegliere il valore positivo).

- Possiamo applicare l'algoritmo di Euclide per il MCD così com'è scritto anche ai polinomi, tutto funziona allo stesso modo perché usiamo solo le proprietà delle operazioni e l'enunciato del teorema di divisione ricordato sopra.

- Se avete visto la semplice dimostrazione del teorema di Bézout[7] che usa l'algoritmo di Euclide e "inverte i passaggi", bene, la stessa dimnostrazione funziona pari pari anche con i polinomi: possiamo quindi enunciare il

[6] Ricordiamo che il grado di 0 non è definito (diffidate di chi vi dice che sia -1 o ∞, mente!)

[7] Teorema di Bézout: dati due interi a, b, esistono r e s interi t.c. $ar + bs = MCD(a, b)$, spesso usato nel caso in cui $MCD(a, b) = 1$

Fatto 7 (Teorema di Bézout (per i polinomi)) *Se $f(x), g(x)$ sono due polinomi senza fattori comuni, allora esistono $r(x), s(x)$ polinomi t.c.*

$$fr + gs = 1$$

(qui, come faremo anche più avanti per semplicità di notazione e per evidenziare il parallelismo con gli interi, abbiamo omesso di indicare esplicitamente la dipendenza dalla variabile).

↬*Congruenze modulo polinomi*

Bene, abbiamo fatto la divisibilità, cosa ci vieta ora di fare anche congruenze modulo polinomi? Le congruenze si possono definire nel modo ovvio:

$$a(x) \equiv b(x) \mod c(x) \iff c(x) \mid b(x) - a(x)$$

Esse ci torneranno comode principalmente per calcolare resti, insieme ai noti principi che ci permettono di sostituire termini equivalenti in una congruenza (principi di sostituzione):

Fatto 8 *se $a \equiv a'$, $b \equiv b'$, allora*

$$\begin{aligned} a + b &\equiv a' + b' \\ ab &\equiv a'b' \end{aligned}$$

In questo modo possiamo ricontrollare le equazioni 1.3: ad esempio

$$x + y \mid x^n + y^n \Leftrightarrow \text{n dispari}$$

si reinterpreta nel linguaggio delle congruenze: se facciamo congruenze modulo $x + y$, $y \equiv -x$, quindi per il principio di sostituzione (se n dispari)

$$x^n \equiv (-x)^n \equiv -y^n \iff x + y \mid x^n + y^n$$

Se invece n è pari, otteniamo

$$x^n + y^n \equiv x^n + (-x)^n \equiv 2x^n$$

che non è mai nullo salvo casi banali. In questo modo si possono velocizzare conti di divisibilità e divisioni tra polinomi. XXX:esempio!

Ora, un problema interessante:

Problema 5 *Il polinomio $p(x)$ dà resto 4 quando viene diviso per $x - 5$,resto -3 quando viene diviso per $x + 5$ e resto 1 quando viene diviso per x. Che resto dà quando viene diviso per $x^3 - 25x$?*

Possiamo risolvere questo problema esplicitamente ponendo

$$p(x) = [a(x - 5) + b][c(x + 5) + d][ex + f]$$

e imponendo le varie relazioni tra i coefficienti (XXX: credo!), ma c'è un metodo che usa i risultati di questo capitolo e ci permette di visualizzare molto più efficacemente la situazione.

L'avete intuito? Proviamo a scrivere il problema in questa forma

$$\begin{cases} p \equiv 4 & \mod x-5 \\ p \equiv -3 & \mod x+5 \\ p \equiv 1 & \mod x \end{cases}$$

Esatto, è proprio la situazione del Teorema Cinese del Resto fatto sui polinomi (infatti notiamo che $x-5$, $x+5$ e x non hanno fattori in comune). Possiamo applicare l'algoritmo di soluzione del TCR anche ai polinomi, visto che non usiamo nessun fatto che non abbiamo "reinterpretato" in termini di polinomi (a proposito, breve esercizio teorico: dimostrare che si possono trovare inversi moltiplicativi modulo m anche tra i polinomi).

$\looparrowright$A che servono le congruenze con i polinomi? Ci si risolvono i problemi?

Raramente le congruenze modulo polinomi sono qualcosa che consente di risolvere un problema *tout court*; le abbiamo introdotte qui soprattutto perché sono un utile strumento per velocizzare i conti con i polinomi e ridurre gli errori di calcolo (dividere polinomi con l'algoritmo "long" è sempre fastidioso!). Inoltre sono un argomento interessante e non-standard che (speriamo!) getterà luce su due diversi argomenti della matematica olimpica collegandoli tra loro.

1.4 Topics in algebra

Nei paragrafi precedenti siamo stati un po' vaghi: polinomi sì, ma con quali coefficienti? In alcuni punti si usano coefficienti reali, in altri complessi, alcuni teoremi funzionano solo quando i coefficienti sono interi o razionali.

In realtà, le principali proprietà dei polinomi sono indipendenti da queste differenze perché dipendono solo dal fatto che i coefficienti siano scelti in un *campo*, cioè, (intuitivamente): un insieme in cui sono definite le quattro operazioni (in particolare serve che la divisione sia sempre possibile, tranne che per 0) e in cui esse hanno le classiche proprietà algebriche (associatività, commutatività, distributività...). I seguenti insiemi in particolare sono campi (e quindi possiamo "farci i polinomi"):

- $\mathbb{Q}$(i numeri razionali)
- $\mathbb{R}$(i numeri reali)
- $\mathbb{C}$(i numeri complessi)
- $\mathbb{Z}_p$ (gli interi modulo un numero primo p, con la relazione di congruenza $a \equiv b$ in luogo della normale uguaglianza)

È evidente dal procedimento che l'algoritmo di divisione tra polinomi funziona senza problemi in tutti questi contesti[8]; quindi funzionano anche tutte le proprietà che da esso derivano, per esempio: un polinomio di grado n ha al più n

[8] nel caso degli interi $\mod p$ "dividere" significa "moltiplicare per l'inverso": ad esempio negli interi $\mod 11$ abbiamo $5/3 = 5 \cdot 4$, perché 4 è l'inverso di 3

radici, oppure: se due polinomi di grado $\leq k$ assumono lo stesso valore su $k+1$ valori diversi della x allora hanno tutti i coefficienti uguali[9]. L'unica cosa a cui bisogna fare particolare attenzione è che in $\mathbb{F}_p$ i valori ammissibili sono p, quindi non ha senso dire che "due polinomi coincidono in $p+1$ punti".

↬Riassunto delle proprietà dei polinomi e dei campi in cui valgono

"Funzionano bene" in tutti i campi elencati sopra:

- Grado e suo "buon comportamento" rispetto alla somma e al prodotto
- Algoritmo di divisione tra polinomi e teorema di Ruffini
- Un polinomio di grado n ha al più n radici; se due polinomi di grado $\leq k$ assumono lo stesso valore su $k+1$ valori diversi della x allora hanno tutti i coefficienti uguali (si dimostrano con Ruffini)
- Identità algebriche e fattorizzazioni notevoli
- MCD e congruenze
- Un polinomio p ha dei "fattori multipli" (con esponente > 1) sse $\mathrm{mcd}(p, p') \neq 1$ (p' è la "derivata" del polinomio calcolata con le regole di derivazione dei polinomi).
- XXX: che altro c'è?

Non sono invece veri in generale (o comunque richiedono più attenzione):

- esistenza di radici (l'esistenza di radici in $\mathbb{C}$ e $\mathbb{R}$ è "speciale", su $\mathbb{Q}$ esistono polinomi di grado molto alto che non si fattorizzano; inoltre su)
- in $\mathbb{Z}_p$ non funzionano cose che richiedono disuguaglianze, positività o radici quadrate (ad esempio, la formula di soluzione delle equazioni di secondo grado)[10]
- teoremi di analisi (ad esempio, l'esistenza del minimo)
- in $\mathbb{Z}_p$ non vale il fatto che se $p(x) = q(x)$ per ogni x, allora p e q hanno i coefficienti uguali (principio di identità dei polinomi): ad esempio, $x^p - x$ e 0 assumono lo stesso valore in ogni punto

↬Un problema che vale un corso di algebra

Problema 6 *Dimostrare che per ogni primo p se k non è multiplo di $p-1$ allora*

$$1^k + 2^k + \ldots + (p-1)^k \equiv 0 \mod p$$

[9] Provate a riguardare la dimostrazione di queste proprietà e controllare che in effetti funzionano per tutti i campi che abbiamo preso in esame

[10] in realtà le radici quadrate si riescono ad "aggiustare" utilizzando la teoria dei residui quadratici, argomento che per ora non tratteremo

Una soluzione che fa un brillante uso delle conoscenze di algebra enunciate sopra. Completiamo aggiungendo il termine mancante p^k per rendere più simmetrica la formula:

$$1^k + 2^k + \ldots + (p-1)^k + p^k \equiv 0 \mod p$$

Ora, ci accorgiamo che il termine di sinistra mantiene invariato il suo valore anche se aggiungiamo 1 a tutti i numeri e partiamo da 2:

$$2^k + 3^k + \ldots + p^k + (p+1)^k \equiv 0 \mod p$$

In generale, possiamo aggiungere un qualunque intero x[11]: possiamo inglobare queste informazioni in un polinomio dicendo che

$$x^k + (x+1)^k + \ldots + (x+p-1)^k$$

ha valore costante per qualunque x in $\mathbb{Z}_p$, e chiamiamo d questo valore costante (dopo avere visto un po' di soluzioni che utilizzano questa tecnica, dovrebbe diventare un "barbatrucco standard" quello di inglobare le ipotesi in un opportuno polinomio). Ora, possiamo applicare una proprietà dei polinomi che resta vera anche in $\mathbb{Z}_p$, quella che dice che *un polinomio di grado $\leq n$ ha al più n radici.* In questo caso sappiamo che

$$f(x) := x^k + (x+1)^k + \ldots + (x+p-1)^k - d$$

vale 0 per tutti gli x da 0 a $p-1$ (quindi tutti i p elementi di $\mathbb{Z}_p$); allora se $k < p$ possiamo concludere che f è il polinomio nullo (se così non fosse avrebbe "troppe radici" per la proprietà appena enunciata).

Quindi sappiamo che i suoi coefficienti devono essere tutti $\equiv 0$, cioè multipli di p. Questa è un'informazione che ci torna utile? La prima idea è di provare a scrivere esplicitamente il suo termine noto, che dovrebbe assomigliare molto all'espressione che stiamo cercando di valutare: esso è $f(0)$, cioè

$$0^k + 1^k + \ldots + (p-1)^k - d \equiv 0$$

Siamo stati sfortunati: non abbiamo ricavato nulla di nuovo, già sapevamo che $1^k + \ldots + (p-1)^k = d$. Proviamo invece a considerare il termine di grado 1: si ricava essere, svolgendo le potenze di binomio:

$$k(0^{k-1} + 1^{k-1} + \ldots + (p-1)^{k-1}) \equiv 0$$

[11] o ancora più in generale possiamo considerare qualunque *sistema completo di residui modulo p*, cioè un insieme di interi che abbraccia una e una sola volta tutte le classi di resto mod p. Valgono questi teoremi, utili quando si considerano i sistemi completi di residui:

1. Se $a_1 \ldots a_p$ è un sistema completo di residui, lo è anche $a_1 + m, \ldots a_p + m$ per ogni m intero
2. Se $a_1 \ldots a_p$ è un sistema completo di residui, lo è anche $m \cdot a_1, \ldots m \cdot a_p$ per ogni m intero che non sia multiplo di p.

Notare che una dimostrazione classica del piccolo teorema di Fermat (quella riportata anche su *Che cos'è la matematica*) utilizza in modo essenziale la seconda proprietà

In questo caso, se $k \not\equiv 0 \mod p$, abbiamo che

$$1^{k-1} + \ldots + (p-1)^{k-1} \equiv 0$$

Magnifico: esattamente quello che cercavamo, solo con $k-1$ al posto di k. Per cui ci basta prendere $k+1$ invece di k nel ragionamento precedente e otterremo la tesi.

Ora, un piccolo riesame della soluzione, per controllare per quali k abbiamo effettivamente dimostrato la tesi: abbiamo supposto lungo la dimostrazione di avere

- $k < p$
- $k \not\equiv 0 \mod p$ (che è automaticamente soddisfatta se vale la precedente)

Poiché abbiamo poi sostituito $k+1$ al posto di k, abbiamo effettivamente dimostrato la tesi per tutti i $k \leq p-2$. Ma questi sono tutti i valori che ci servono: infatti la tesi esclude esplicitamente $k = p-1$, e per $k \geq p$ possiamo applicare il piccolo teorema di Fermat e ridurre tutti gli esponenti finché non cadono nel range $[0 \ldots p-1]$. □

Esercizio: riformalizzare la dimostrazione precedente per renderla una dimostrazione "da gara" (dite, avrete mica pensato che scritta così andasse bene in una gara, spero!)

↬*Polinomi a coefficienti interi e razionali*