$\mathbb{Z}$-trucchi

Federico Poloni

29/7/2005

Non temere
Zeta reticoli on my mind
(Meganoidi, *Zeta Reticoli*)

Introduzione

(che non ho mai voglia di scrivere)

Questa è una dispensa "avanzata": non cerca di insegnarvi le cose base della teoria dei numeri (congruenze, teorema cinese), ma da per scontato che voi sappiate già quello che c'è scritto sul Gobbino e cerca di insegnarvi alcuni trucchi e "idee ricorrenti" che capitano nei problemi di NT. (o perlomeno, quei pochi che so io <smile>)

Cerca di essere un po' nello spirito della dispensa sui polinomi che ho già scritto (i "barbatrucchi"), anche se ho l'impressione che mi sia uscita peggio e che non prepari veramente ai problemi difficili ma serva solo a tagliare le gambe a tante possibili "problemi facili". Ho cercato di mantenere i ghirigori prima dei trucchi e il tono un po' alla "dieci comandamenti", che spero non troverete fastidioso.

Mi rendo conto che gli altri testi "per le olimpiadi" che ho scritto avrebbero bisogno di un'aggiustatina (per esempio quella sulle equazioni funzionali necessiterebbe di un "cappello" veramente introduttivo su come si risolvono e non si risolvono le e.f. e di una nutrita sezione di esercizi); però visto che le dispense in italiano in giro scarseggiano preferisco usare il mio tempo per scriverne di nuove che per "limare" ulteriormente le vecchie.

Buona parte dei contenuti di queste dispense deriva, direttamente o indirettamente, dagli stage a cui ho assistito e partecipato, curati dal gruppo delle Olimpiadi di Matematica. A tutto il gruppo, e soprattutto al prof. Massimo Gobbino, una quantità più che numerabile di ringraziamenti.

Have fun, e se prendete un oro alle IMO mandatemi una cartolina.

Capitolo 1

Teoria dei numeri

1.1 Fatti ovvii

Questi saranno stupidi ma non potevo non metterceli:

- Almeno nel contesto delle Olimpiadi, $\mathbb{N}$ comprende lo zero, e si intende che zero non è un numero positivo (come recita il detto, *positive means positive*).
- Dicendo "numeri primi" solitamente si intende che siano positivi e non invertibili: quindi i primi più piccoli sono $2, 3, 5, 7, \ldots$.
- 0 è un multiplo di ogni numero. $\text{MCD}(0, n) = n$ per ogni $n \in \mathbb{Z}$[1].

1.2 Sporcarsi le mani

I problemi di teoria dei numeri di solito "prendono in prestito" molto dall'algebra o dalla combinatoria come strategie risolutive. Dell'algebra vedremo utilizzate soprattutto le fattorizzazioni notevoli; della combinatoria ricordiamo soprattutto che

$\looparrowright$ *Per risolvere i problemi bisogna "sporcarsi le mani"*

cioè fare alcune prove, verificare gli enunciati per i numeri più bassi e cercare di capire cosa succede. Preparatevi anche a fare un po' di conticini a mano, e siate pronti a lavorare tranquillamente anche con numeri a tre cifre. Come riscaldamento, vi propongo un noto "problema–scherzo" che può far sudare parecchie camicie se si prova ad affrontarlo subito *de visu* invece di applicare il suggerimento:

Esercizio: ("teorema di Grande Puffo sui numeri primi") Dimostrare che se p e $p^2 + 2$ sono primi, anche $p^3 + 2$ è primo.

[1] Se siete in vena di pignolerie: a patto di definire l'MCD nel modo giusto, vale anche $\text{MCD}(0, 0) = 0$.

Tutti o quasi i problemi che compaiono in questo testo sono corredati di soluzione perché sono intesi soprattutto come "esempi", però:

↬ *Provate a fare i problemi prima di leggere la soluzione!*

Seriamente, non siate pigri.

XXX: tra la parola soluzione e la vera soluzione c'è una spaziatura insana per non invogliare la gente a leggere la soluzione subito. C'è un metodo migliore e/o più carino tipograficamente per ottenere lo stesso risultato? Suggerimenti in proposito sono bene accetti.

Soluzione:

Proviamo a vedere cosa succede per i primi più bassi:

p	p^2+2	
2	6	non verifica l'ipotesi!
3	11	verifica le ipotesi: $p^3+2=29$ che è primo: ok
5	27	no!
7	51	no!
11	123	no!
13	171	no!

hmm... Anche andando avanti con le prove, sembra che le ipotesi funzionino solo per $p=3$. In più, succede sempre che $3 \mid p^2+2$. A questo punto è facile capire cosa succede: se $p \neq 3$, $p \equiv \pm 1 \mod 3$, e $p^2+2 \equiv 0 \mod 3$.

Il teorema allora è vero, ma le ipotesi sono verificate solo per $p=3$: il teorema sembra un fatto profondo sui numeri primi ma in realtà è un "imbroglio". Ma ce ne saremmo accorti così facilmente se invece di provare a fare due conti ci fossimo buttati subito a dimostrarlo "in astratto"?

1.3 Fattorizzare, fattorizzare, fattorizzare

Il primo e il più importante "trucco" in aritmetica è:

↬ *Fattorizzare tutto quello che capita sottomano*

Come nell'algebra, la soluzione di un problema di teoria dei numeri passa spesso per lo "switching" tra due forme alternative di rappresentare gli interi; solitamente questo avviene attraverso la fattorizzazione: si hanno due fattorizzazioni distinte dello stesso numero e le si vuole identificare. Vediamo qualche esempio.

Esercizio: (XXX:Febbraio 2001?) Trovare tutte le coppie di interi (x, y) per cui

$$y^3 = x^3 + 91$$

Soluzione:

L'idea qui è "raggruppare" in modo da avere il prodotto notevole $y^3 - x^3$:

$$(y - x)(y^2 + xy + x^2) = 91 = 13 \cdot 7$$

Ora, $(y - x)(y^2 + xy + x^2)$ è una scomposizione di 91 in due fattori interi: quindi abbiamo le otto possibilità $y - x = \pm 1, \pm 7, \pm 13, \pm 91$ ($\leadsto$ *mai dimenticare di considerare entrambi i segni* in casi come questo!). Quindi ci siamo ridotti a otto sistemi (che possiamo ridurre a quattro con qualche considerazione di simmetria) del tipo

$$\begin{cases} y - x = 1 \quad (-1, \pm 3, \pm 7, \pm 91) \\ y^2 + xy + x^2 = 91 \quad (-91, \pm 7, \pm 3, \pm 1) \end{cases}$$

che sappiamo risolvere[2]. Controlliamo quali hanno soluzioni intere e abbiamo finito.

Esercizio: (Steinhaus, 100 problemi...) Dimostrare che il numero $3^{105} + 4^{105}$ è divisibile per $7, 13, 49, 181, 379$.

Soluzione:

[2]Li sappiamo risolvere, vero? È un esercizio di algebra; in breve: poniamo $x \mapsto -x$ e ci riconduciamo a un sistema simmetrico in due incognite; sostituiamo con la somma e il prodotto di x e y: $s = x + y$,$t = xy$ e abbiamo $s = 1$,$s^2 - 3t = 91$ da cui ricaviamo $t = -30$; risolviamo l'equazione $\lambda^2 - s\lambda + t = 0$ che ci dà le possibili scelte di x e y.

Usiamo di nuovo la fattorizzazione notevole $x+y \mid x^{2n+1}+y^{2n+1}$:

$$7 = 3+4 \mid 3^{105}+4^{105}$$

$$7 \times 13 = 3^3+4^3 \mid (3^3)^{35}+(4^3)^{35}$$

e così via, lasciando nella "base" ogni volta un diverso fattore di 105.

In generale le "fattorizzazioni algebriche" del tipo $x^3+y^3 = (x+y)(x^2-xy+y^2)$ determinano delle "fattorizzazioni aritmetiche" quando coinvolgono solo polinomi a coefficienti interi. Tra i vari enunciati di algebra, il più utile solitamente è appunto la fattorizzazione notevole di $x^n \pm y^n$, che compare in tutte le salse (spesso anche con $y=1$).

Vi ricordo anche il *lemma di Gauss*: se un polinomio $f(x)$ a coefficienti interi si spezza[3] come $f(x) = g(x)h(x)$ con f e g polinomi a coefficienti *razionali*, allora (a meno di moltiplicare per una costante) g e h sono a coefficienti *interi*. Cioè: in un certo senso, tutte le scomposizioni a coefficienti razionali di un polinomio a coefficienti interi sono in realtà a coefficienti interi, dove con "in un certo senso" intendiamo questo: anche se il polinomio x^2-4 si può fattorizzare nel prodotto dei due polinomi a coefficienti razionali $3x-6$ e $\frac{x}{3}+\frac{2}{3}$, "moralmente" la sua scomposizione (e *ogni* sua scomposizione) è in polinomi a coefficienti interi, perché possiamo raccogliere un tre e scriverla nella forma $(x-2)(x+2)$.

Attenzione però: questo non implica che *ogni* polinomio a coefficienti interi si fattorizzi: esistono anche polinomi a coefficienti interi che non si possono proprio scomporre in due fattori a coefficienti razionali (non costanti), per esempio $x^{18}-37$.

Un altro "spezzone di esercizio" sul rapporto tra fattorizzazioni algebriche e numeri interi: è un esercizio difficile, non lo risolviamo completamente ma facciamo solo qualche osservazione.

Esercizio: (IMO 2002) (**)(XXX:ricontrollare testo) Trovare tutti gli interi $m, n \geq 3$ per cui il numero

$$\frac{a^m+a-1}{a^n+a^2-1}$$

è intero per infiniti valori interi della variabile a.

Soluzione:

[3] "si spezza" è un modo che piace agli algebristi per dire "si fattorizza", "si scompone".

Un ottimo modo per assicurarsi che il numero sia intero è che il denominatore divida esattamente (come polinomio) il numeratore, cioè $a^m+a-1 = g(a)(a^n+a^2-1)$ per un polinomio $g(a)$. g ha coefficienti razionali (perché la divisione tra polinomi si può fare con l'algoritmo "che insegnano a scuola" facendo solo operazioni razionali sui coefficienti), ma in realtà questi coefficienti sono interi per il lemma di Gauss. (in realtà in questo caso sono interi anche per un motivo più stupido, cioè che il divisore è un polinomio monico e quindi lungo algoritmo non dobbiamo mai fare divisioni). Quindi si avrebbe che il quoziente $g(a)$ è un polinomio a coefficienti interi in a e quindi è intero per *tutti* i valori di a.

E se i polinomi non si dividono esattamente? In questo caso, se poniamo $c(a) := a^m + a - 1$ e $d(a) := a^n + a^2 - 1$ abbiamo

$$c(a) = q(a)d(a) + r(a)$$

per opportuni polinomi a coefficienti interi (come sopra, segue dall'algoritmo di divisione che sono interi) $q(a)$ e $r(a)$, con $r(a)$ di grado minore di quello di $d(a)$. Quindi $c(a)/d(a) = q(a) + r(a)/d(a)$: perché questo quoziente sia intero dev'essere $r(a)/d(a)$ intero, ma $r(a)$ ha grado *minore* di $d(a)$, quindi per $|a|$ maggiore di un certo valore $|r(a)| < |d(a)|$[4] e il quoziente non può essere un numero intero (a meno che sia zero, ma se $r(a)$ è nullo per infiniti valori di a allora $r(a) = 0$).

Quindi abbiamo che se $c(a)/d(a)$ è intero per infiniti valori di a allora $d(a)$ deve dividere come polinomio $c(a)$, e quindi in particolare $c(a)/d(a)$ deve essere intero per *tutti* i valori di a.

Questo in particolare ci da un metodo semplice per verificare quali m e n vanno bene, almeno per i casi più bassi: calcoliamo i polinomi in $a = 2$ ($a = 0$ e $a = 1$ ci danno ben poche informazioni...) e controlliamo per quali scelte di m ed n $c(2)/d(2)$ risulta intero. In questo modo troviamo subito la soluzione $m = 5, n = 3$, che sembra essere l'unica (almeno per valori bassi di m e n).

Il lavoro che abbiamo fatto finora valeva due punti alle IMO, che per un problema 3 tutto sommato sono un bottino interessante. (XXX:controllare quest'affermazione chiedendo in giro.)

Esercizio: (Engel) Se $4^n + 2^n + 1$ è primo (per $n \in \mathbb{N}$), allora n è una potenza di 3.

Soluzione:

[4] XXX: Questo punto è chiaro o devo spiegarlo meglio? Devo fare una divagazione sul "comportamento per $x \to \infty$ dei polinomi?

(solo hint)

↬ *Se devi dimostrare che qualcosa non è primo, cerca una "fattorizzazione algebrica" (e ricordati di dimostrare che non è banale)*

Qui l'idea è quella di ricondurci a un problema di algebra e fattorizzare il polinomio $x^{2n} + x^n + 1$; già sappiamo dal testo che dobbiamo aspettarci che la nostra fattorizzazione "non funzionerà" (in qualche modo...) per n potenza di 3. Il resto al lettore.

1.4 Divisibilità e MCD

La proprietà più utilizzata nei problemi che coinvolgono divisibilità e MCD è quella di essere "invarianti per combinazioni lineari": cioè,

$$m \mid a, \quad m \mid b \Longrightarrow m \mid a+b, a-b, a+kb$$

e analogamente per l'MCD[5]:

$$(a, b) = (a + kb, b)$$

che è la proprietà che fa "funzionare" l'algoritmo di Euclide.

Qualche applicazione:

Esercizio: (Engel)

$$a - c \mid ab + cd \Leftrightarrow a - c \mid ad + bc$$

Soluzione:

Behold:

$$a - c \mid (a - c)(b - d) = (ab + cd) - (ad + bc)$$

[5]Con (a, b) si indica l'MCD, il massimo comun divisore, di a e b: è una di quelle notazioni che all'inizio danno i nervi perché sono facilmente fraintendibili ma alla lunga tornano comode. Talvolta si usa anche $[a, b]$ per il minimo comune multiplo, o i termini inglesi gcd(o gcf, *greatest common divisor/factor*) e lcm (*lowest common multiple* XXX: o era least? controllare...).

Esercizio: (Larson) a e b sono interi primi tra loro. Provare che

$$\text{MCD}(a^2 - ab + b^2, a + b) \leq 3$$

Soluzione:

$\text{MCD}(a^2-ab+b^2, a+b) = \text{MCD}(a^2-ab+b^2-(a+b)^2, a+b) = \text{MCD}(3ab, a+b)$

Ora, l'MCD è un divisore di $3ab$: ma poiché a e b sono primi tra loro, $\text{MCD}(a, a+b) = \text{MCD}(a, b) = 1$ e quindi i divisori di a sono da scartare; analogamente per quelli di b, quindi può rimanere solo un fattore 3. To sum up, l'MCD è 1 oppure 3.

Sapreste ora trovare tutti gli interi x, y primi tra loro e tali che $y^3 - x^3 = 10000$? (hint: dopo aver fattorizzato il polinomio come nel caso 91, per un lemma simile a quello appena visto i due fattori hanno MCD 1 o 3, quindi tutti i fattori 2 (e 5) devono stare "dalla stessa parte...")

Esercizio: (Larson) Provare che due numeri di Fibonacci consecutivi sono sempre primi tra loro.

Soluzione:

Applichiamo l'idea vista:

$$\text{MCD}(F_{n+2}, F_{n+1}) = \text{MCD}(F_n + F_{n+1}, F_{n+1}) = \text{MCD}(F_n, F_{n+1})$$

quindi se F_{n+2} e F_{n+1} hanno un fattore in comune ce l'ha anche F_n, e ripetendo il ragionamento $F_{n-1}, F_{n-2}, \ldots, F_1$. Ma $F_1 = 1$ non ha molti fattori da condividere.

Esercizio: (Larson) Se $T_1 = 2$ e $T_{n+1} = T_n^2 - T_n + 1$ per $n > 0$, provare che i T_k sono tutti primi tra loro.

Soluzione: XXX:questo non ho provato a risolverlo, il Larson lo mette come "punto b" di quello coi Fibonacci. Sembra carino.

Qualcosa di più impegnativo, ora, ma le idee sono le stesse:
Esercizio: (IMO '98,B1) Trovare tutte le coppie di interi positivi (a, b) tali che

$$ab^2 + b + 7 \mid a^2b + a + b$$

Soluzione:

Al solito, cerchiamo di fare "combinazioni lineari" che ci semplifichino l'espressione a destra. Inizialmente proviamo a sottrarre una volta il "divisore":

$$ab^2 + b + 7 \mid ab(a - b) + a - 7$$

Questo non sembra aiutarci molto, e ulteriori semplificazioni non portano a una "bella" espressione. Nessun segnale positivo, cerchiamo un'altra strada.

L'idea che ci torna comoda qui è che nel termine a destra del simbolo di "divide" possiamo sostituire tutte le volte che compare il termine ab^2 con $-b - 7$: ad esempio,

$$ab^2 + b + 7 \mid 5ab^3 + 2b + 37$$

$$\Updownarrow$$

$$ab^2 + b + 7 \mid 5b(-b - 7) + 2b + 37$$

Vi è chiaro perché questo funziona? Basta sommare un multiplo del divisore, $-5b(ab^2 + b + 7)$. Pensare alla divisibilità in questi termini spesso aiuta molto[6].

[6] Nei "barbatrucchi", compariva un metodo simile per controllare le divisibilità notevoli tra polinomi del tipo $x \pm y \mid x^n \pm y^n$: se il divisore è $x + y$, si sostituisce $x = -y$ a destra e si controlla se viene 0, se è $x - y$ si sostituisce $x = y$...

In questo caso non è immediatamente disponibile un termine ab^2, quindi lo "creiamo" moltiplicando per b:

$$\begin{aligned} ab^2 + b + 7 \mid b(a^2b + a + b) &= a^2b^2 + ab + b^2 \\ \mid a(-b - 7) + ab + b^2 &= b^2 - 7a \end{aligned}$$

Ora il termine di destra si è semplificato molto. In particolare, è piccolo rispetto al divisore: infatti, se $b^2 - 7a \geq 0$ abbiamo

$$ab^2 + b + 7 > b^2 > b^2 - 7a$$

e quindi la divisibilità è impossibile ($\not\rightarrow$ $a \mid b$ *implica* $|a| \leq |b|$); analogamente, se $b^2 - 7a < 0$,

$$ab^2 + b + 7 > ab^2 > 7a > 7a - b^2$$

non appena $b^2 > 7$. Quindi, a meno che $b \geq 2$, dev'essere $7a - b^2 = 0$, da cui facilmente $b = 7k$, $a = k^2$, che è una soluzione.

Ci restano quindi da controllare solo i casi $b = 1, b = 2$, che presumibilmente ci daranno qualche soluzione particolare: $b = 1$ fornisce

$$a + 8 \mid a^2 + a + 1$$

e di nuovo ricorriamo al trucco di rimpiazzare tutti gli a con -8 (notate come ci semplifica la vita?), ottenendo $a + 8 \mid (-8)^2 + (-8) + 1 = 57$. Poiché a dev'essere positivo, $a + 8$ è uno dei divisori di 57 che sono maggiori di 8, cioè 19 o 57, che ci danno $a = 11$ e $a = 49$. Il caso $b = 2$ si fa in modo analogo:

$$\begin{aligned} 4a + 9 \mid 2a^2 + a + 2 \\ \mid 16a^2 + 8a + 16 \\ \mid (-9)^2 + 2(-9) + 16 = 79 \end{aligned}$$

ma 79 non ha fattori della forma $4a + 9$ (per $a > 0$), quindi per $b = 2$ non abbiamo ulteriori soluzioni.

To sum up, le soluzioni sono $(k^2, 7k)$, $(11, 1)$ e $(49, 1)$.

Esercizio: (IMO '94, B1) Trovare tutte le coppie (m, n) di interi positivi per cui

$$\frac{n^3 + 1}{mn - 1}$$

è un intero.

Soluzione: A voi. È una versione un po' più difficile di quello prima.

1.5 Polinomi a coefficienti interi

↬ *Polinomi a coefficienti interi vuol dire* $a - b \mid p(a) - p(b)$

Appena leggete "sia $p(x)$ un polinomio a coefficienti interi", vi deve venire in mente di usare il fatto che per ogni a, b interi $a - b \mid p(a) - p(b)$. È la chiave in quasi tutti i problemi di questo tipo.
Esercizio: (dal forum) Sia $p(x)$ un polinomio a coefficienti interi e a, b due interi distinti tali che $p(a) = b$ e $p(b) = a$. Dimostrare che esiste al più un intero c tale che $p(c) = c$.

Soluzione:

Cominciamo a scrivere la nostra relazione di divisibilità per un po' delle "lettere" che compaiono nel problema: in particolare, abbiamo

$$c - a \mid p(c) - p(a) = c - b$$

$$c - b \mid p(c) - p(b) = c - a$$

quindi $c - b = \pm(c - a)$. (↬ *Non dimenticarsi che ci può essere anche il segno meno!*)

Allora, visto che $a \neq b$, ci deve essere il segno meno e $c = \frac{a+b}{2}$: ma allora c è univocamente determinato, e quindi può esistere solo quel possibile valore di c. Quindi esiste al più un c per cui $p(c) = c$ (domanda: ma non abbiamo dimostrato che in questo caso vale *sempre* $p(c) = c$ per $c = \frac{a+b}{2}$? No, in effetti abbiamo *supposto* che esistesse un c siffatto. D'altra parte non è neppure detto che $c = \frac{a+b}{2}$ sia intero.)

Esercizio: Sia $p(\cdot)$ un polinomio a coefficienti interi tale che esistano $n > 0, x$ interi per cui $p(p(p(\dots p(x) \dots))) =: p^{(n)}(x) = x$ Provare che $p^{(2)}(x) =: p(p(x)) = x$

Soluzione:

Qui con un po' di esperienza dovrebbe essere chiaro cosa dobbiamo fare:

$$p(x) - x \mid p^{(2)}(x) - p(x) \mid \cdots \mid p^{(n+1)}(x) - p^{(n)}(x) = p(x) - p(x)$$

Quindi nessuno dei "divide" può essere un "divide strettamente" (↬ *Spesso il simbolo di "divide" si comporta un po' come il simbolo di "minore o uguale". In effetti si ha anche* $a \mid b \Rightarrow |a| \leq |b|$). Allora abbiamo

$$p(x) - x = \pm(p^{(2)}(x) - p(x)) = \cdots = \pm(p^{(n+1)}(x) - p^{(n)}(x)).$$

Ora dobbiamo "mettere a posto" i segni, che è la parte non standard (leggi *difficile*) del problema. Facciamo queste osservazioni:

1. Se c'è un segno meno dopo il primo uguale, abbiamo vinto.

2. Analogamente, se c'è un "cambio di segno" da qualche parte, per esempio $p^{(4)}(x) - p^{(3)}(x) = -(p^{(5)})(x) - p^{(4)}(x))$, abbiamo $p^{(3)}(x) = p^{(5)}(x)$: ma anche questo ci basta per concludere, perché basta applicare $n-3$ volte p a entrambi i lati e otteniamo $p^{(n)}(x) = p^{(n+2)}(x)$, cioè $x = p^{(2)}(x)$. (qui c'è sotto un'idea di algebra, simile a come capita per le congruenze: dobbiamo "invertire" p per riuscire a eliminare $p^{(3)}$ dall'inizio di entrambi i membri: ma visto che $p^{(n)}(x) = x$, l'"inverso" di p è $p^{(n-1)} \dots$)

3. Ci resta da scartare il caso in cui tutti i segni sono dei più. In questo caso facciamo una prova con dei valori a caso (ad esempio, $x = 0$, $p(x) = 1$ e ci accorgiamo subito che $x, p(x), p^{(2)}(x), \dots$ sono una successione monotona (crescente o decrescente), quindi non possiamo mai ritrovare x a un certo punto della successione.

E abbiamo finito.

1.6 Idee per le diofantee

Si chiama diofantea una qualunque equazione che coinvolga solo numeri interi: per esempio: trovare tutti gli interi $n > 0$,x,p, con p primo, per cui valga

$$2^n = x^2 + p^3 + 37$$

(l'ho scritta a caso per fare un "catalogo" dei termini che possono comparire, non vi consiglio di provare a risolverla)

↬ *solution-shooting*

Cercare "a caso" soluzioni alle diofantee, provando con i valori più bassi, può dare molti indizi sul metodo risolutivo da usare. In particolare, possiamo distinguere quattro categorie di equazioni:

1. equazioni senza soluzioni
2. equazioni con solo la soluzione banale "tutto uguale a zero" (o un suo stretto parente)
3. equazioni con solo "qualche" soluzione con i numeri bassi.
4. equazioni con un numero infinito di soluzioni parametrizzate in una forma "bella" (qualcosa del tipo $x = 5^k, y = 1$)

Ognuna di queste soluzioni ha un suo metodo risolutivo principale che è, solitamente, il primo da tentare: rispettivamente,

1. passare alla congruenza che si ottiene trasformando l'$=$ in un $\equiv$, per un modulo opportuno, e cercare di dimostrare che è non ammette soluzioni. Se non funziona, cambiare modulo e riprovare.
2. Sicuramente la discesa infinita. Se no, vedi il punto successivo
3. Sono le più difficili. Prima, trovare qualche vincolo con un uso "furbo" delle congruenze, scegliendo i moduli in modo tale da ritagliare nella dimostrazione un "buco" per far rientrare le soluzioni trovate. Poi, fattorizzare & identificare (magari confrontando le potenze di un primo nei vari termini).
4. Le equazioni di questo tipo di solito non sono eccessivamente difficili, il modo in cui si trovano le soluzioni "costruttivamente" spesso funziona già da dimostrazione. Altrimenti, stesse idee del punto sopra.

↬ *Capire quando usare la discesa infinita*

Come avete visto llo schemino sopra, la discesa infinita è un'arma specializzata: funziona in un solo tipo di problemi, però in quel tipo è solitamente il metodo migliore. È utile imparare a usarla e a formalizzarla nel modo migliore (non "divido infinite volte", ma "sia k la più grande potenza di "..." che divide "...")

Esercizio: (Larson) Trovare gli interi x, y, z tali che

$$x^2 + y^2 + z^2 = 2xyz$$

Soluzione:

Lavoriamo modulo 4: vediamo (controllare...) che l'unica combinazione possibile è $x^2 \equiv y^2 \equiv z^2 \equiv 0$. Allora x, y, z sono pari e possiamo dividere tutto per 2: otteniamo

$$x'^2 + y'^2 + z'^2 = 4x'y'z'.$$

Ora abbiamo un 4 al posto del 2 ma il ragionamento appena fatto funziona ancora: quindi possiamo dividere di nuovo tutto per 2, ottenendo un 8 al posto del 4, e così via. Poiché x, y e z sono divisibili per potenze arbitrariamente grandi di 2, devono essere nulli.

In una soluzione "da gara", può essere più pulito formalizzare la soluzione così: *sia k il più grande intero tale che 2^k divide sia x che y che z*, e siano x', y', z' i risultati di questa divisione. In particolare, almeno uno di questi è dispari. Allora dall'equazione di partenza si ha

$$x'^2 + y'^2 + z'^2 = 2^{k+1}x'y'z'$$

che è impossibile modulo 4 (argomentare dettagliatamente).

Esercizio: (Cesenatico 2004) Risolvere negli interi:

1. $x^2 + y^2 = 2005^{2004}$
2. $x^2 + y^2 = 2004^{2005}$

Soluzione: Al lettore.

Un'altra osservazione importante:

↬ *Va bene sporcarsi le mani, ma provare moduli a caso è male*

Cioè: provare bovinamente le congruenze modulo 11, 13, 17, 19 e 23 in tutte le equazioni diofantee che ci troviamo di fronte è solo fatica sprecata. Spesso il modulo giusto da usare (che solitamente è abbastanza basso...) ci viene dettato dalla forma stessa del problema. Presentiamo qualche euristica:

- Se c'è un "numero fisso", ad esempio 35 in $x^3 = 2^n + 35$, conviene provare moduli che lo annullino (in questo caso 5 e 7)
- Se c'è un "numero fisso" elevato a una qualche potenza, ad esempio 3 in $x^2 + y^2 = 3^n$, conviene provare moduli rispetto ai quali le potenze assumono solo un numero basso di valori: ad esempio per 3 succede con 8, 13, 121. (come si trovano questi valori? Sono i divisori di $3^k - 1$ per $k = 2, 3, \ldots$: difatti se $m \mid 3^k - 1$, allora $3^k \equiv 1 \mod m$). Oltre ovviamente ai moduli che annullano il termine, come 3 e 9 in questo caso. Se invece prendiamo un primo p tale che 3 sia un generatore modulo p, è chiaro che non faremo molta strada perché 3^k può assumere tutti i valori possibili modulo p.

- Se c'è un k per cui compaiono molte potenze k-esime (ad esempio 5 in $a^5 + 2b^5 = 37$), conviene provare moduli m tali che le potenze k-esime assumono solo "pochi" valori modulo m: in particolare i primi per cui $k \mid p-1$ o comunque $\mathrm{MCD}(k, p-1)$ è alto[7].

- Nel caso dei quadrati ($k = 2$), i residui quadratici sono sempre metà delle classi resto $\mod p$, quindi il criterio precedente non ci dice nulla. L'esperienza dice che di solito funzionano i moduli più bassi: 3, 4 (oppure direttamente 8. 2 di solito è inutile), talvolta 5. $\looparrowright$ *Conviene ricordarsi a memoria quali sono i residui quadratici per questi moduli.*

Qualche esercizio di esempio:
Esercizio: (Bulgaria e giornalino XXX:quale?) Trovare tutte le coppie di primi p e q tali che $p^2 + 3pq + q^2$ risulti:

1. un quadrato perfetto

2. una potenza di 5

Soluzione:

La prima idea che ci viene in mente è che potremmo provare a raccogliere un quadrato perfetto da quella forma quadratica, qualcosa del tipo $(p+q)^2 + pq$. Così da sola (fare i primi tentativi...) non sembra portare a nulla, ma teniamo a mente quest'idea e cerchiamo di ricavare qualche informazione dalle congruenze.

1. Dopo alcune prove ricaviamo la soluzione $(3, 7)$, che sembra essere l'unica. Gli "indizi" sono: quadrate, un 3 nel testo e uno nell'unica soluzione: proviamo allora a "far sparire" il termine misto lavorando modulo 3: $p^2 + q^2 \equiv a^2 \mod 3$. Ora, se p e q sono primi diversi da 3, $p \equiv \pm 1 \mod 3$ e quindi $p^2 \equiv 1$: avremmo allora $a^2 \equiv 1 + 1 = 2$, ma 2 non è un residuo quadratico. *Bingo*, ci resta solo da sistemare il caso $p = 3$: abbiamo $q^2 + 9q + 9 = a^2$. Ora, ritorniamo all'idea di raccogliere

[7] Vale il seguente teoremino, che si dimostra facilmente con i generatori: se p è primo, le potenze k-esime possono assumere tutti i valori possibili modulo p quando $(k, p-1) = 1$; invece assumono solo $p - 1/d$ valori ripetuti ognuno d volte quando $d := (k, p-1) > 1$

un quadrato: l'espressione è uguale a $(q+3)^2+3q$, quindi viene "subito dopo" un quadrato, ma tra $(q+3)^2$ e il quadrato successivo sta una distanza dell'ordine di q: difatti abbiamo $(q+3)^2 < q^2+9q+9 < (q+5)^2$, quindi dev'essere $q^2+9q+9 = (q+4)^2 = q^2+8q+16$, da cui ricaviamo $q = 7$.

2. Per questo punto i primi moduli che ci vengono in mente sono 3, 4 (così $5^k \equiv 1$) e 5. Il 3 è già stato usato nel primo punto, quindi difficilmente funzionerà ancora. In più, possiamo far saltare fuori un altro 5 raccogliendo un quadrato perfetto, così:

$$p^2+3pq+q^2 = (p-q)^2+5pq$$

Un altro fattore 5 è un "segnale positivo" sembra proprio quello che cerchiamo, quindi continuiamo in questa direzione e proviamo a lavorare modulo 5:

$$(p-q)^2+5pq = 5^k$$

Se p e q sono diversi da 5, il secondo termine contiene solo un fattore 5, mentre gli altri (se $k > 1$) ne contengono almeno due (un quadrato perfetto deve avere tutti i fattori "doppi" nella sua fattorizzazione...), assurdo. Quindi uno tra p e q deve essere 5, e da qui concludiamo velocemente.

Un semplice esempio di "diofantea con poche soluzioni" in cui troviamo il modulo giusto per "girare attorno" alla soluzione e poi fattorizziamo:
Esercizio: Trovare tutti gli interi m, n che soddisfano

$$5^m = 2^n+1$$

Soluzione:

È immediata la soluzione $5 = 1+4$, che congetturiamo essere l'unica. Ora, vogliamo un modulo che "ritagli fuori" questa soluzione: ad esempio 25, oppure 8: difatti, se abbiamo una soluzione diversa da quella trovata, il membro di sinistra è $\equiv 0$ modulo 25 e quello di destra è $\equiv 0+1$ modulo 8: quindi riusciamo a trovare delle conclusioni che valgono in tutti i casi

tranne che nella nostra soluzione particolare. 25 ci dice che perché valga la congruenza $2^n + 1 \equiv 0$ dev'essere $n = 20k + 10$, e analogamente 8 ci dice che dobbiamo avere $m = 2h$.

La seconda informazione in particolare ci è utile perché permette di fattorizzare:

$$2^n = (5^h + 1)(5^h - 1)$$

Quindi $5^h + 1$ e $5^h - 1$ devono essere entrambe potenze di 2: ma questo è impossibile, perché sono due numeri che distano di 2 l'uno dall'altro.

Il modo in cui abbiamo concluso la dimostrazione è un'idea ricorrente: dopo aver fattorizzato una differenza di quadrati in quel modo, guardiamo come possono distribuirsi i suoi fattori.

Visto che si parla di 2 e 5, ricordiamo due fatti notevoli che legano tra loro questi numeri:

- 2 è un generatore modulo 5^k per tutti i k.
- 2^k non ha un generatore per $k > 2$, come ricorderete, ma 5 si avvicina molto ad esserlo: difatti il suo ordine è sempre 2^{k-2}, che è il massimo ordine possibile ($\varphi(2^k) = 2^{k-1}$, che non è raggiunto da nessun numero perché non c'è generatore).

Questo esercizio in realtà è un caso particolare di questa diofantea mortalmente lunga da risolvere:

Esercizio: (Bulgaria e giornalino XXX:quale?) (**) Trovare tutte le quaterne di interi positivi (x, y, z, t) tali che

$$1 + 5^x = 2^y + 2^z 5^t$$

Soluzione: Buona fortuna...

1.6.1 Estrarre tutte le informazioni

...dalla divisibilità e dai moduli. Sempre fare tutte le sostituzioni che si possono fare per "ridurre" le incognite:

Esercizio: (forum, fonte "vera" ignota) Trovare tutte le soluzioni intere di

$$3x^2 - 2y^2 = 1998$$

Soluzione:

Usiamo ripetutamente questo fatto: $\looparrowright$ *se sappiamo che d divide tutti i termini di una somma tranne uno (ad esempio due tra x, y e z in $x+y=z$), allora divide anche l'ultimo* . Per il fatto, x è multiplo di 2, allora scriviamo $x = 2x_1$; allo stesso modo y è multiplo di 3, quindi scriviamo $y = 2y_1$ (notare la scelta delle variabili per evitare che le lettere in gioco diventino troppe). Sostituisco e semplifico, ottengo

$$2x_1^2 - 3y_1^2 = 333.$$

Di nuovo, x_1 è multiplo di 3, pongo $x_1 = 3x_2$ e risostituisco:

$$6x_2^2 - y_1^2 = 111.$$

Di nuovo, y_1 è multiplo di 3, pongo $y_1 = 3y_2$:

$$2x_2^2 - 3y_2^2 = 37.$$

Ora ci si rende conto che le sostituzioni di questo tipo sono finite, bisogna continuare con un altro metodo. Al lettore, questa dovrebbe essere abbastanza facile (ricordate le euristiche che abbiamo già visto...).

Analogamente, su un esercizio che abbiamo già risolto:
Esercizio: Solve

$$5^m = 2^n + 1.$$

Soluzione:

Lavoriamo modulo 5: dev'essere $n \equiv 2 \mod 4$. Lavoriamo modulo 8 (una volta scartate le soluzioni con $n \leq 2$): dev'essere m pari. Allora conviene cambiare variabili subito in modo da avere

$$5^{2m_1} = 4 \times 16^{n_1} + 1$$

Questa sostituzione è "favorevole" perché ora ci si rende conto subito che possiamo fattorizzare in almeno due modi diversi come differenza di quadrati. Eventualmente possiamo andare oltre, provando moduli come 25 e 16...

XXX:vvv questo va spostato

Esercizio: (preIMO 2005, da una sessione di esercizi) Trovare tutte le potenze di 2 tali che "aggiungendo" una prima cifra decimale alla sua sinistra si ottiene un'altra potenza di 2.

Soluzione:

La prima "ricerca manuale" di radici ci dà $2,32$ e $4,64$. Più avanti, sembra difficile che ci siano altre soluzioni.

Qui la chiave dell'esercizio è trovare il modo corretto di "inscatolare" le informazioni: si ha

$$2^n = 2^m + k10^h$$

dove chiamiamo k la cifra aggiunta, e abbiamo $\log_{10} 2^n = \log_{10} 2^m + 1 = h$.

Dividiamo il "pezzo pari" e il "pezzo dispari":

$$\begin{cases} 2^m = k_1 2^h \\ 2^{n-m} - 1 = k_2 5^h \end{cases}$$

dove k_1 e k_2 sono il "pezzo pari" e il "pezzo dispari" di una cifra da 0 a 9, quindi $k_1 = 2, 4, 8$ e $k_2 = 1, 3, 5, 7, 9$ (con alcuni casi che si escludono a vicenda).

In più c'è la "strana" informazione che $\log_{10} 2^n = \log_{10} 2^m + 1 = h$.

XXXX

1.6.2 La parte "disuguaglianzosa" delle diofantee

XXXX:servono esempi buoni. PreIMO 2005: trovare tutte le potenze di 2 che restano potenze di 2 se si leva la prima cifra in base 10, in realtà si fa meglio senza disuguaglianze, quindi non va bene.

1.7 Modi strani di usare le congruenze

1.7.1 sistemi completi di residui

Un sistema completo di residui modulo m è un insieme di m valori che assumono, uno a testa, tutti gli m possibili valori modulo m. Ad esempio,

$15, 73, -10$ è un sistema completo di residui modulo 3. I due lemmini base sono:

- Ai sistemi completi di residui possiamo sommare un intero a piacere: se $a_1, a_2, \ldots, a_m$ è un sistema completo di residui, lo è anche $a_1 + k, a_2 + k, \ldots, a_m + k$. Dimostrazione: ci basta verificare che siano tutti distinti modulo m: ma se $m \mid (a_i + k) - (a_j + k)$, allora $m \mid a_i - a_j$, impossibile perché gli a_i erano un sistema completo di residui (e quindi tutti distinti modulo m).
- Possiamo moltiplicare i sistemi completi per un intero primo con m: se $a_1, a_2, \ldots, a_m$ è un sistema completo di residui e $\mathrm{MCD}(k, m) = 1$, allora $ka_1, ka_2, \ldots, ka_m$ è un sistema completo di residui. Dimostrazione: è analoga, se $m \mid ka_i - ka_j$, visto che m e k sono coprimi, $m \mid a_i - a_j$, impossibile per ipotesi.

Probabilmente conoscerete già questa dimostrazione del piccolo teorema di Fermat:
Esercizio: (well-known) Se p è primo e a non è multiplo di p,

$$a^{p-1} \equiv 1 \mod p$$

Soluzione: I numeri $0, 1, 2, \ldots, p-1$ sono un sistema completo di residui modulo p. Per il lemma visto sopra, anche $0, a, 2a, \ldots, (p-1)a$ sono un sistema completo di residui. Se moltiplichiamo tra loro (modulo p) tutti i residui del primo sistema completo tranne lo 0 otteniamo $(p-1)!$: ma questo risultato è il prodotto di tutti i residui non nulli, e quindi è indipendente dal sistema di residui scelto: allora,

$$1 \cdot 2 \cdot \cdots \cdot p-1 \equiv a \cdot 2a \cdot \cdots \cdot (p-1)a$$
$$(p-1)! \equiv a^{p-1}(p-1)!$$

Dall'ultima uguaglianza possiamo semplificare $(p-1)!$ (perché è primo con p) e otteniamo $a^{p-1} \equiv 1$[8].

Questo problema l'avevo già risolto nei "barbatrucchi" con una soluzione più algebrica, ma questa è più semplice:
Esercizio: Provare che se p è primo e $p - 1 \not| a$ (XXX:come diavolo si fa il "non divide" in tex? su qualche giornalino vecchio c'era...), allora

$$1^a + 2^a + 3^a + \cdots + (p-1)^a \equiv 0 \mod p$$

[8]la dimostrazione si adatta facilmente al teorema della funzione φ di Eulero, se consideriamo l'insieme delle sole classi di resto che sono coprime con il modulo.

Soluzione:

Avete riconosciuto che la somma è su un sistema completo di residui modulo p, vero? In particolare, possiamo prendere come sistema completo quello che si ottiene moltiplicando tutto per un certo k:

$$1^a+2^a+\cdots+(p-1)^a \equiv k^a+(2k)^a+\cdots+((p-1)k)^a = k^a(1^a+2^a+\cdots+(p-1)^a)$$

Ora, se $1^a+2^a+\cdots+(p-1)^a$ fosse diverso da zero, potremmo semplificarlo e ottenere $1 = k^a$: ma possiamo scegliere k in modo che questa uguaglianza non valga, ad esempio prendendo per k un generatore modulo p (in modo che $k^a \equiv 1$ sse $p-1 \mid a$). Quindi dev'essere per forza $a^1+2^a+\cdots+(p-1)^a \equiv 0$.

1.7.2 frazioni e radici nell'aritmetica modulare

Nell'aritmetica modulare modulo un primo possiamo usare tranquillamente le frazioni: se definiamo $\frac{1}{a}$ come l'inverso moltiplicativo di a modulo p (e $\frac{b}{a}$=ba^{-1}), allora valgono tutte le normali proprietà delle frazioni, inclusa la possibilità di fare somme e prodotti, moltiplicare numeratore e denominatore per una quantità diversa da 0 (modulo p, ovviamente!), eccetera. Provate voi stessi a verificare qualche identità con un modulo basso, per esempio 7:

$$\frac{1}{4}+\frac{1}{12}=\frac{1}{3}$$
$$\frac{1}{2}\cdot\frac{1}{3}=\frac{1}{6}$$

e così via. Questo ci permette per esempio di usare anche nell'aritmetica modulare alcune comode formule algebriche: ad esempio

$$1^2+2^2+\cdots+a^2 \equiv \frac{a(a+1)(2a+1)}{6} \mod 7$$

e in generale in tutti i primi diversi da 2 e da 3 (per cui "il denominatore diventa 0" e quindi la frazione non ha significato).

In più, abbiamo l'utile formula $\frac{1}{a} = a^{-1} = a^{p-2}$, che non ha un corrispondente nelle frazioni "vere".

Se si fa sufficiente attenzione, si possono anche usare frazioni con moduli non primi, a patto di mettere a denominatore solo numeri coprimi con il modulo.

Esercizio: (IMO 2005, B1) Trovare tutti gli interi positivi che sono coprimi con tutti i termini della successione

$$a_n = 2^n + 3^n + 6^n - 1$$

Soluzione:

Appena "decifriamo" il testo, ci accorgiamo che dobbiamo cercare quei primi (e potenze di primi) che non dividono nessuno dei termini della successione. Controllando i termini più bassi, notiamo subito che 2, 3 e 5 non vanno bene. 7 funziona? Per scoprirlo facciamo una "tabella dei resti" modulo 7 ($\leadsto$ *bisogna "sporcarsi le mani"!*):

n	2^n	3^n	6^n	$2^n + 3^n + 6^n - 1$
0	1	1	1	2
1	2	3	-1	3
2	4	2	1	-1
3	1	-1	-1	-2
4	2	-3	1	-1
5	4	-2	-1	0
6	1	-1	1	2

Che sfortuna, proprio l'ultimo valore "non va bene": infatti, se la successione non fosse stata multipla di 7 per $0, 1, 2, \ldots, 5$, allora per la periodicità delle potenze modulo 7 lo sarebbe stata per tutti gli n. Questo ultimo valore è un caso? No: se facciamo la tabella analoga modulo 11 (verificare, prego) di nuovo l'unico valore che "salta" è l'ultimo, cioè $p - 2$. Questo ci suggerisce di provare a dimostrare che

$$2^{p-2} + 3^{p-2} + 6^{p-2} - 1 \equiv 0 \mod p$$

per tutti i primi p. Questi "$p - 2$" per il piccolo teorema di Fermat sono gli inversi di 2, 3 e 6, quindi dobbiamo dimostrare che

$$2^{-1} + 3^{-1} + 6^{-1} \equiv 1 \mod p$$

che, se introduciamo le frazioni, diventa veramente ovvio:

$$\frac{1}{2}+\frac{1}{3}+\frac{1}{6}=1\equiv 1 \mod p$$

Questo ragionamento, tutto sommato semplice, ci dice che per tutti i primi diversi da 2 e 3 (attenzione, per 2 e 3 le frazioni non si possono usare perché annulliamo un denominatore!) il termine a_{p-2} è multiplo di p. 2 e 3 li abbiamo già "sistemati" con i primi termini della successione, quindi abbiamo finito.

Sul foglio risposte scriveremo quindi che l'unico intero positivo che è coprimo con tutti i termini della successione è 1. (ve ne eravate dimenticati, del povero 1 che non ha fattori primi?).

Allo stesso modo delle frazioni, talvolta possiamo usare le radici: visto che nei calcoli algebrici l'unica proprietà del simbolo $\sqrt{2}$ che usiamo è che $(\sqrt{2})^2=2$, se troviamo un numero che modulo p "fa lo stesso lavoro", possiamo "battezzarlo" $\sqrt{2}$. Per esempio, $\sqrt{2}=3 \mod 7$, perché $3^2\equiv 2$. Notiamo che, come nel caso reale, le radici quadrate di un numero sono due, ossia 3 e il suo opposto $-3=4$ modulo 7. Possiamo fare lo stesso "lavoro" per tutti i moduli che sono residui quadratici nel nostro modulo.

Questo ci permette, per esempio, di risolvere equazioni quadratiche:

$$ax^2+bx+c\equiv 0 \mod p$$

si risolve con la stessa formula del caso reale,

$$x_{12}=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$$

in tutti i moduli primi diversi da 2 (a non è mai zero modulo p, se no l'equazione diventa di primo grado...), se abbiamo l'accortezza di trovare una "radice quadrata modulo p" nel modo descritto sopra. Notare che qui (e in tutti i calcoli di questo tipo) non conta quale delle due radici quadrate $+3$ e -3 scegliamo perché $+\sqrt{a}$ e $-\sqrt{a}$ compaiono sempre "accoppiati" nei calcoli. Ad esempio, risolviamo

$$x^2-4x+2\equiv 0 \mod 7:$$

$$x_{12}=2\pm\sqrt{4-2}=2\pm 3;\quad x_1=-1,\ x_2=5$$

perché, come abbiamo visto sopra, $\sqrt{2}=3$, nell'aritmetica modulo 7.

Oltre alle equazioni di secondo grado, questo torna molto comodo quando applichiamo le tecniche per "svolgere ricorrenze" modulo p: per esempio, i Fibonacci modulo 31 assumono un aspetto particolarmente semplice: poiché $\sqrt{5}=6$, $\frac{1}{\sqrt{5}}=\frac{1}{6}=26$ e $2^{-1}=16$,

$$F_n=\frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n-\left(\frac{1-\sqrt{5}}{2}\right)\right]=26\cdot([(1+6)\cdot 16]^n-[(1-6)\cdot 16]^n)$$

XXX:c'era un problema che si fa con questo trucco sul fascicolo degli stage senior, riportarlo.

1.7.3 Approfondimento: estensioni "complex-like" dei campi finiti

Visto che si parla di radici quadrate modulo p... questo per il problem–solving non dovrebbe servire, ma potreste trovarlo interessante. (XXX:di nuovo, come con i barbatrucchi, sono finito con pesanti divagazioni nell'*undergraduate algebra*. Damn.)

Per i primi per i quali -1 è un residuo quadratico (quali sono? Dovreste saperlo...), il simbolo $\sqrt{-1}$ è ben definito e tutto "funziona bene": per esempio, $\sqrt{-1} = \pm 2 \mod 5$, e possiamo usare tranquillamente questo valore nei calcoli. Il "ruolo" che nei reali ha $\sqrt{-1}$ qui ce l'hanno le radici dei non residui quadratici: $\sqrt{2}$, modulo 5, non si può proprio fare, esattamente come nei reali non si può fare $\sqrt{-1}$. Dovreste sapere che i non residui quadratici sono "la metà meno uno" dei possibili resti modulo p, quindi il problema di come gestirli si dovrebbe verificare abbastanza spesso (in realtà no, perché nei problemi "di tipo olimpico" di solito si cerca di evitare questo caso).

La risposta è: si fa esattamente nello stesso modo che nei reali, si "aggiungono" artificialmente le radici che mancano. Per esempio, modulo 13, come abbiamo visto $\sqrt{-1}$ non ci dà problemi, ma $\sqrt{5}$ sì. In questo caso, possiamo "chiamare" $i = \sqrt{-5}$ e fare i calcoli "lasciando espressa la i" proprio come si fa con i complessi, facendo solo la sostituzione $i^2 \mapsto -5$. Notiamo che (come nei reali) una volta aggiunta una "unità immaginaria" riusciamo a fare *tutte* le radici, quindi anche $\sqrt{6}$ e $\sqrt{7}$ per esempio, perché se 5 e 6 sono non residui quadratici allora differiscono per un quadrato: $\sqrt{6} = \sqrt{(6 \cdot 5^{-1})5}$, e $6 \cdot 5^{-1} \equiv 6 \cdot 8 \equiv 9$ che è un quadrato perfetto (succede sempre: sono le proprietà dei residui quadratici, non residuo per non residuo uguale residuo) e possiamo portarlo fuori dalla radice.

Allora, se cerchiamo di esprimere la sequenza di Fibonacci modulo 13 come somma di due esponenziali (con la "formula di Binet modulo p", come abbiamo fatto per 31), avremo dei termini "complessi", cioè che contengono il simbolo che abbiamo battezzato i. Però, potete verificare che quando andiamo a eseguire i calcoli e calcolare il termine n-esimo tutte le i spariscono, esattamente come nella formula di Binet (reale) "spariscono" tutte le radici di cinque. (XXX:fare i contazzi e riportarli come esempio. Se me li fa qualcuno e me li spedisce per posta mi fa un favore, non ho proprio voglia <smile>)

In questo modo tutti i polinomi di secondo grado hanno due radici negli interi modulo p "complessificati". Potreste allora chiedervi se è vero o no che tutti i polinomi hanno un numero di radici pari al grado (cioè "si fattorizzano completamente" come prodotto di polinomi di grado 1), come succede con i numeri complessi "ordinari". La risposta è no, come potete verificare

facilmente con un qualunque polinomio di terzo grado.Per dotare tutti i polinomi di una soluzione (cioè, ottenere la cosiddetta *chiusura algebrica* degli interi modulo p) bisogna fare molta più strada... To be continued nei corsi di algebra dell'università, se farete Matematica.

1.8 Teorema cinese

XXX:TODO

1.9 Rappresentazioni in base b

XXX: mi servono esempi "belli" Il problema di Josephus non è considerato bello, almeno secondo me.

.1 Qualche problema IMO sparso

Esercizio: (IMO '96, B1) I numeri $15a + 16b$ e $16a - 15b$ (con a e b interi positivi) sono quadrati perfetti positivi. Qual è il minimo valore che può assumere il più piccolo dei due?

Soluzione:

Elenco le "idee standard" in successione: se vi siete fermati a metà esercizio, potete guardare le prime idee che servono e poi continuare (e chiedermi: come mai non mi è venuta quell'idea?).

Prima osservazione: è strano che chiedano solo il minimo dei due numeri; minimo che tra l'altro può essere uno qualunque dei due (sembrerebbe quello a destra, ma se a è molto più grande di b è più piccolo quello di sinistra). Forse questo minimo ritornerà nel futuro.

Qui la prima idea che vi dovrebbe venire in mente è quella di fattorizzare la differenza di quadrati:

$$(m + n)(m - n) = m^2 - n^2 = 31b - a$$

che sfortunatamente non ci sembra portare a molto (non si fattorizza bene...). La seconda è ricavare a e b in funzione di m^2 e n^2:

$$(15^2+16^2)a = 15m^2 + 16n^2 (16^2+15^2)b = 15n^2 - 16m^2$$

in cui ci capita lo strano fattore $15^2 + 16^2 = 481 = 13 \cdot 37$, che entra anche nel determinante dei due "sistemi lineari" che danno m^2, n^2 e a, b. Anche questa idea però sembra abbastanza sterile, non ci porta ad altre manipolazioni algebriche efficaci. Ci serve un altro modo di combinare le due equazioni per ricavarne qualcosa di utile.

L'idea successiva è che il modo in cui sono combinati 15 e 16 con a e b ricorda un po' la moltiplicazione tra complessi, o la formula di Eulero per scrivere un prodotto di somme di due quadrati come somma di due quadrati. Qualche tentativo di manipolazione anche verso questa direzione: scrivere qualcosa come $(16 + 15i)(a - ib)$, per esempio. La prossima idea è prendere il *modulo* di questi numeri complessi: se facciamo

$$(15a + 16b)^2 + (16a - 15b)^2,$$

allora i termini misti spariscono: difatti, l'espressione diventa

$$(15^2 + 16^2)a^2 + (15^2 + 16^2)b^2 = m^4 + n^4.$$

(viene naturale provare anche il tentativo parallelo di fare $m^4 - n^4$ per far sparire i termini a^2 e b^2, che qui non riportiamo). Bingo: possiamo raccogliere quel $15^2 + 16^2 = 481$, il che è un segnale positivo perché l'espressione comincia a fattorizzarsi. Abbiamo allora

$$m^4 + n^4 = 13 \cdot 37(a^2 + b^2),$$

che è indubbiamente un'espressione incoraggiante. Continuiamo su questo versante. L'espressione ricorda un po' quella delle discese infinite del tipo $x^2 + y^2 = 4 \cdot qualcosa$: se riuscissimo a dimostrare per esempio che $13 \cdot 37 \mid m, n$, sarebbe un notevole passo avanti. Partiamo dal 13: facciamo i residui quartici modulo 13 (che sono solo tre, altro segnale positivo) e controlliamo che effettivamente quando $13 \mid m^2 + n^2$ allora $13 \mid m, n$. Ripetiamo lo stesso calcolo per 37 (anche lui ha "pochi" residui quartici, segnale positivo) e abbiamo che anche $37 \mid m, n$ [9].

Abbiamo trovato due fattori "grossi", 13 e 37, in m e n. Vediamo dall'espressione di a e b in funzione di m e n che abbiamo ricavato prima che

[9] In effetti il calcolo dei residui quartici modulo 37 è un contazzo notevole. Possiamo velocizzare tutto facendo un discorso più sofisticato: se x e $-x$ sono residui quartici, allora anche -1 lo è (perché $x^{-}1$ è la quarta potenza dell'inverso della radice quarta di x, e quindi $-x \cdot x^{-1}$ è un prodotto di quarte potenze). Ma, sia modulo 13 che modulo 37, -1 non è un residuo quartico: difatti, se g è un generatore, $-1 = g^{(p-1)/2}$ e sia per $p = 13$ che $p = 37$ l'esponente di g non è multiplo di 4. Quindi -1 non è una quarta potenza né mod 13 né mod 37. Esercizio: capire bene perché funziona il ragionamento e scriverlo bene...

questo implica che sia a che b sono multipli di $13 \cdot 37$. A questo punto potremmo quasi pensare che il lavoro sia finito e che basta trovare effettivamente un caso in cui m o n valga proprio $(13 \cdot 37)^2$ per dimostrare che questo è il minimo.

Trovare un esempio però non sembra del tutto banale: a e b devono contenere i fattori 13 e 37 (una volta sola, perché chiaramente se a e b hanno un divisore comune che è un quadrato possiamo semplificarlo e ridurre il valore dell'espressione...). Però $a = b = 13 \cdot 37$ e cose simili non funzionano; scriviamo $a = 13 \cdot 37 \cdot \alpha$, $b = 13 \cdot 37 \cdot \beta$ e proviamo a buttare tutto nell'espressione...

Qui però ci possono tornare in aiuto le scritture come somma di due quadrati: proviamo a scrivere i nostri fattori come somme di quadrati e moltiplicare. Abbiamo $13 = 4+9$, $37 = 36+1$, questo ci permette di scrivere $13 \cdot 37$ come somma di due quadrati? Sì: avevamo $13 \cdot 37 = 15^2 + 16^2$, cosa che sappiamo già e che nei primi tentativi non ci portava a nulla. Però, notiamo che possiamo "accoppiare" i termini nella formula di Eulero anche in un altro modo[10], e questo ci dà $481 = 20^2 + 9^2$. Questo ci porta a qualcosa? Sì: difatti, a noi servivano un α e un β bassi tali che $481 \mid \alpha^2 + \beta^2$, e se prendiamo $\alpha = 20$, $\beta = 9$ siamo a posto. $a = 13 \cdot 37 \cdot 20$ e $b = 13 \cdot 37 \cdot 9$ in effetti ci danno $m = n = 13 \times 37$, e abbiamo vinto (abbiamo dimostrato che $13 \times 37 \mid m, n$, quindi il minimo è almeno 13×37).

[Remark: questo è il metodo che ho usato io, almeno. Arrivato al punto di dover trovare un esempio, se avessi posto $m = 481x$, $n = 481y$ invece che $a = 481\alpha$, $b = 481\beta$ come fa la soluzione riportata da Kalva avrei finito prima (provate...). Sfortunatamente ho fatto la scelta sbagliata delle incognite, le due scelte sembravano equivalenti ma una si è poi rivelata migliore.]

XXX:fare la bibliografia.

[10] È un caso particolare del seguente risultato interessante: il numero di possibili rappresentazioni di un numero N come somma di due quadrati di interi (quindi contando come distinte anche le scelte di segno e lo scambiare le variabili) è uguale a $4(d_1 - d_3)$, dove d_1 e d_3 sono il numero di divisori di N congrui rispettivamente a uno e a tre modulo 4.