

IMO 2015/2

Problem solving ad alta voce

darkcrystal

Sommario

Questo è (quasi parola per parola) il mio flusso di coscienza nel tentativo di risolvere l'IMO 2015/2. Circa tre quarti di quanto segue sono stati scritti di getto, per cui ci sono parecchi tentativi che non portano da nessuna parte (ma che al momento ritenevo potessero essere sensati). L'ultima sezione – il caso a, b, c dispari – è meno “onesta”, nel senso che l'idea che si usa mi è venuta in mente appena ho letto il problema, quindi tutto quello che vedete qui sono i dettagli di come concludere utilizzando quell'approccio, e non ci sono molti tentativi a vuoto.

1 Testo

Determinare tutte le terne (a, b, c) di interi positivi tali che

$$ab - c, bc - a, ca - b$$

siano tutti potenze di 2.

2 Reminder

Ricordo che $v_2(n)$, la valutazione 2-adica di un intero n , è il più grande intero k tale che 2^k divide n ; in altre parole, si ha $2^{v_2(n)} | n$ ma $2^{v_2(n)+1} \nmid n$. In ancora altre parole, è l'esponente del primo 2 nella fattorizzazione di n . La valutazione gode delle seguenti proprietà fondamentali:

- Se $v_2(a) > v_2(b)$, allora $v_2(a + b) = v_2(b)$
- Se $v_2(a) = v_2(b)$, allora $v_2(a + b) \geq v_2(a)$ (e in realtà anche $v_2(a + b) \geq v_2(a) + 1$)

3 IMO 2015/2

Intanto ci sono soluzioni? Sì, $(2, 2, 2)$. Ok, quindi non devo cercare di dimostrare che non ce ne sono. Così ad occhio direi che ci sarà solo un numero finito di soluzioni, ma non si sa mai... attenzione ad eventuali famiglie infinite.

Poi: ci saranno come minimo questioni di parità, perché se una potenza di 2 è dispari allora è uguale a 1, quindi il problema sarà più semplice se almeno uno tra $ab - c, bc - a, ca - b$ è dispari. Ora questo succede quando a, b, c non sono tutti e tre pari o tutti e tre dispari, quindi cerchiamo di fare i casi in cui c'è un dispari o ci sono due dispari. Allora, diciamo wlog a dispari... a proposito, questa è una seccatura: le tre espressioni $ab - c, bc - a, ca - b$ sono cicliche in a, b, c ma non sembrano simmetriche... cosa succede se tengo fisso a e scambio b, c ? Dunque, $bc - a$ resta fisso, e $ab - c, ca - b$ si scambiano: quindi in realtà la faccenda è simmetrica! L'insieme $\{ab - c, bc - a, ca - b\}$ dipende solo dall'insieme

$\{a, b, c\}$, e non dall'ordine di a, b, c . Benissimo. Quindi, dicevamo, cosa succede se ci sono dei dispari? Se ci sono esattamente due dispari, diciamo a e b , allora $ca - b$ e $bc - a$ sono entrambi dispari, quindi sono entrambi uguali a 1:

$$\begin{cases} ca - b = 1 \\ bc - a = 1 \end{cases}$$

Beh, facendo la differenza membro a membro trovo $c(a-b) + (a-b) = 0$, cioè $(c+1)(a-b) = 0$, cioè $a = b$. Ma allora $1 = ca - b = a(c-1)$, da cui $a = 1$ e $c = 2$, che non funziona. Ok, questo era facile. Cosa succede se uno solo tra a, b, c è dispari? Diciamo che sia c . Allora $ab - c = 1$, cioè $c = ab - 1$. Beh, il problema adesso è a sole due incognite, scriviamolo con due incognite. Voglio che $ab - (ab-1), b(ab-1) - a, (ab-1)a - b$ siano tutte potenze di 2. La prima condizione non dice niente, quindi siamo arrivati al problema seguente:

$$\begin{cases} a^2b - a - b = 2^m \\ ab^2 - a - b = 2^n \end{cases}$$

Boh? Ci saranno soluzioni? Intanto mi piacerebbe capire chi è più grande tra m e n . Abbiamo $m \geq n$ esattamente quando $a \geq b$, e $m = n$ se e solo se $a = b$. Ah, vediamo se questo caso stupido ha soluzioni: se metto $m = n$, cioè $a = b$, ottengo che $a^3 - 2a$ dev'essere una potenza di 2, quindi a e $a^2 - 2$ sono potenze di 2. Ma aspetta un attimo, se a è pari a^2 è divisibile per 4, quindi $a^2 - 2$ è 2 modulo 4, ma è anche una potenza di 2, quindi $a^2 - 2 = 2$, da cui $a = 2$, $b = 2$ e $c = ab - 1 = 3$, che funziona. Uffa, quindi ci sono soluzioni, non posso dimostrare che questo caso conduce ad un assurdo. Però il caso $m = n$ l'abbiamo fatto, si può provare a dimostrare che è l'unico caso che funziona¹. Diciamo tanto per fissare le idee $m > n$, cioè $a > b$. Quindi $2^m \geq 2 \cdot 2^n$, cioè $a^2b - a - b \geq 2(ab^2 - a - b)$. Che schifo, non si semplifica niente. Riesco a capire chi è n in funzione di a e b ? Per dire, se a, b e ab^2 hanno tutti valutazione 2-adica diversa, allora la valutazione 2-adica di $ab^2 - a - b$ è il minimo tra quelle di a, b e ab^2 . Ah, ma aspetta: sicuramente la valutazione di ab^2 è diversa da quella di a e da quella di b (perché è strettamente più grande), quindi se a, b hanno valutazioni diverse otteniamo che la valutazione di $ab^2 - a - b$ è il minimo tra la valutazione di a e quella di b . Ma questo sarebbe bellissimo, perché la stessa cosa è vera per $a^2b - a - b$ (visto che $v_2(a^2b) > v_2(a), v_2(b)$), quindi avremmo $v_2(a^2b - a - b) = v_2(ab^2 - a - b)$, quindi $m = n$ e avremmo finito. D'accordo, allora il problema è difficile solo se a e b hanno la stessa valutazione 2-adica. Cosa succede se scriviamo tutto esplicitamente? Se scrivo $a = d_1 2^k, b = d_2 2^k$ con d_1, d_2 dispari le condizioni diventano

$$\begin{cases} d_1^2 d_2 \cdot 2^{3k} - (d_1 + d_2) 2^k = 2^m \\ d_1 d_2^2 \cdot 2^{3k} - (d_1 + d_2) 2^k = 2^n \end{cases} \quad (1)$$

Boh, mi sa che si stia solo complicando... però certo, fare la differenza membro a membro mi tenta un sacco. Cosa succede?

$$d_1 d_2 (d_1 - d_2) \cdot 2^{3k} = 2^m - 2^n = 2^n (2^{m-n} - 1), \quad (2)$$

e visto che $d_1 - d_2$ è pari confrontando le valutazioni 2-adiche ottengo $n \geq 3k + 1$. Questo però vuol dire che $d_1 + d_2$ è divisibile per una potenza di 2 piuttosto grande: se prendo la seconda equazione modulo 2^{3k} ottengo $d_1 d_2^2 \cdot 2^{3k} - (d_1 + d_2) 2^k \equiv 2^n \pmod{2^{3k}}$, cioè $d_1 + d_2 \equiv 0 \pmod{2^{2k}}$. Questa strada mi sta scocciando, se non arrivo presto da qualche parte lascio perdere. Comunque, ho ottenuto $d_1 \equiv -d_2 \pmod{2^{2k}}$, quindi $d_1 - d_2 \equiv -2d_2 \pmod{2^{2k}}$; siccome $2k \geq 2$, questo vuol dire in particolare $d_1 - d_2 \equiv 2 \pmod{4}$, ovvero

¹a posteriori ho scoperto che questo è falso, ma a questo punto della soluzione credevo in questo claim, e ho provato a dimostrarlo... questa convinzione sballata può essere la fonte di parte delle difficoltà che seguono.

$v_2(d_1 - d_2) = 1$. Posso inserire questa informazione in (2) per scoprire che in effetti $n = 3k + 1$. Mi sembra che non stiamo andando da nessuna parte: ricominciamo da (1). Ah: ma ho appena scoperto un sacco di cose su $d_1 + d_2$, forse voglio far apparire $d_1 + d_2$ piuttosto che $d_1 - d_2$. Cosa succede se *sommo* le due equazioni membro a membro?

$$d_1 d_2 (d_1 + d_2) 2^{3k} - (d_1 + d_2) 2^{k+1} = 2^n (2^{m-n} + 1)$$

Bah, niente di troppo interessante, ma se non altro so calcolare la valutazione 2-adica di entrambi i membri: in effetti $v_2(d_1 d_2 (d_1 + d_2) 2^{3k})$ è chiaramente maggiore di $v_2((d_1 + d_2) 2^{k+1})$, quindi $v_2(LHS) = v_2((d_1 + d_2) 2^{k+1})$, mentre $v_2(RHS) = n = 3k + 1$, per cui $v_2(d_1 + d_2) = 2k$. Ok, ultimo tentativo in questa direzione: $d_1 + d_2 = d \cdot 2^{2k}$ con d dispari. Cosa ci dice?

$$d_1 d_2 d \cdot 2^{5k} - d \cdot 2^{3k+1} = 2^{3k+1} (2^{m-n} + 1)$$

$$d(d_1 d_2 \cdot 2^{2k-1} - 1) = 2^{m-n} + 1$$

No, non mi sembra che porti da nessuna parte. Lasciamo perdere questa strada. Dunque, in ogni buon problema di teoria dei numeri c'è una parte di divisibilità e una parte di disuguaglianze: che disuguaglianze posso scrivere? Ah, ma certo! Se a, b sono del tipo $2^k d_1, 2^k d_2$, allora ab^2 tenderà ad essere parecchio grosso rispetto a 2^{3k} , ma d'altro canto $ab^2 - a - b = 2^n = 2^{3k+1}$, e questo ci dirà che d_1, d_2 sono piccoli... proviamo.

$$2^{3k+1} = ab^2 - a - b = d_1 d_2^2 2^{3k} - (d_1 + d_2) 2^k$$

$$2 + (d_1 + d_2) 2^{-2k} \geq d_1 d_2^2 \quad (3)$$

Ok, questo è veramente improbabile che succeda... allora, il caso $d_1 = d_2 = 1$ dice che $a = b$ (infatti $d_1 = d_2 = 1$ implica che a, b sono entrambi potenze di 2, e siccome hanno la stessa valutazione 2-adica devono essere uguali), e questo porta ad $m = n$ e sappiamo concludere. Altrimenti fammi scrivere una qualunque disuguaglianza cretina, per dire²:

$$2 + \frac{d_1 + d_2}{4} \geq 2 + (d_1 + d_2) 2^{-2k} \geq d_1 d_2^2 \geq d_2 (d_1 + d_2 - 1) \geq d_1 + d_2 - 1,$$

cioè $3 \geq \frac{3}{4}(d_1 + d_2)$, cioè $d_1 + d_2 \leq 4$. Siccome $d_1 + d_2$ è pari e abbiamo già fatto il caso $d_1 = d_2 = 1$, resta solo il caso $d_1 = 3, d_2 = 1$ (quello simmetrico, $d_2 = 3$ e $d_1 = 1$, non funziona, perché la disuguaglianza (3) non è rispettata). Quindi le mie incognite diventano $a = 2^k, b = 3 \cdot 2^k, c = 3 \cdot 2^{2k} - 1$, e la condizione è che le tre quantità

$$ab - c = 1, \quad bc - a = 9 \cdot 2^{3k} - 2^{k+2}, \quad ca - b = 3 \cdot 2^{3k} - 2^{k+2}$$

siano tutte potenze di 2. Da qui ci saranno infiniti modi diversi di concludere, ma il primo che vedo è che la seconda di queste espressioni si fattorizza come

$$2^{k+2} (9 \cdot 2^{2k-2} - 1),$$

e questa deve essere una potenza di 2. Ma il termine nella seconda parentesi è dispari e diverso da 1 non appena $k \geq 2$, quindi l'unica possibilità è $k = 1$. Questo conduce ad $(a, b, c) = (2, 6, 11)$, che effettivamente funziona. E finalmente questo caso è finito!

Ok, questo ci lascia con i casi che avrei pensato essere più difficili: a, b, c tutti dispari o tutti pari. Il caso tutti pari però non potrà essere molto diverso da quello che abbiamo appena visto: quello che ho imparato è che devo usare il fatto che $v_2(ab - c) = k$ implica

²qui ho esteso la catena di disuguaglianze a sinistra e a destra finché non si sono semplificate abbastanza da avere una forma bella

$ab - c = 2^k$. Ora, se a, b, c sono tutti pari è facile controllare la valutazione di $ab - c$: diciamo che a sia il numero di valutazione 2-adica massima tra a, b e c . Allora io dico che

$$v_2(ab - c) = v_2(c), \quad v_2(ca - b) = v_2(b) :$$

infatti $v_2(ab) = v_2(a) + v_2(b) \geq v_2(a) + 1 > v_2(c)$ e similmente $v_2(ca) > v_2(b)$. Ma questo mi farà vincere, perché vuol dire $ab - c$ è una potenza di 2 con valutazione 2-adica minore o uguale a quella di c , ovvero $ab - c | c$. Allora similmente $ca - b | b$, cioè $ab - c \leq c$ e $ca - b \leq b$... Ok, ho ottenuto

$$\begin{cases} ab \leq 2c \\ ca \leq 2b \end{cases} \Rightarrow \begin{cases} b \leq \frac{2c}{a} \\ \frac{ca}{2} \leq b \leq \frac{2c}{a} \end{cases} \Rightarrow a^2 \leq 4 \Rightarrow a = 2$$

dove nell'ultima implicazione ho usato che a è positivo e pari. Ma d'altro canto a era quello di valutazione 2-adica massima: allora a, b, c sono tutti pari e nessuno è divisibile per 4, per cui $ab - c, bc - a, ca - b$ sono tutti pari e nessuno è divisibile per 4, per cui (siccome l'unica potenza di 2 pari e non divisibile per 4 è proprio 2) devo avere $ab - c = bc - a = ca - b = 2$. Da qui spero si troverà $a = b = c = 2$... ah guarda, dal sistema di sopra (sostituendo $a = 2$) scopro $b \leq c$ e $c \leq b$, quindi $b = c$, e da qui si finisce immediatamente. E siamo rimasti con il caso a, b, c tutti dispari.

Mi sembra che qui non ci sia proprio speranza di controllare $v_2(ab - c)$, perché siccome a, b, c sono tutti dispari può succedere il peggio, quindi bisogna farsi venire in mente qualcosa di più furbo... Allora, un'idea (standard) che non ho ancora avuto il tempo di provare è dire che date due qualunque potenze di 2 la più piccola divide la più grande. Siccome abbiamo già detto che la situazione è simmetrica, diciamo $ab - c \leq bc - a \leq ca - b$, cosicché $ab - c | bc - a | ca - b$.

Ora qui si potrà giocherellare un sacco con queste divisibilità: per esempio, dalla prima posso ricavare

$$ab - c | b(bc - a) + (ab - c) = b^2c - c = c(b^2 - 1)$$

e siccome $ab - c$ è una potenza di 2 mentre c è dispari ne ricavo $ab - c | b^2 - 1$. Allo stesso modo troverò $ab - c | a^2 - 1$ e $bc - a | c^2 - 1$. Dunque, queste divisibilità sono interessantissime, perché dicono (per esempio) che a meno che $a = 1$ si deve avere a relativamente grosso rispetto a $ab - c$... che succede se uno tra a, b, c è uguale a 1? Diciamo $a = 1$. Le tre cose che devono essere potenze di 2 sono

$$b - c, bc - 1, c - b$$

e questo è chiaramente assurdo, perché tra $b - c$ e $c - b$ almeno uno dovrà essere non-positivo. Ok, quindi a, b, c sono tutti diversi da 1. Ma, calma: la divisibilità vuol dire che b e c sono entrambi radici quadrate di 1 modulo $ab - c$. Ora sappiamo tutti³ che le radici quadrate di 1 modulo 2^{k+1} sono ± 1 e $2^k \pm 1$, quindi (siccome $b \neq 1, c \neq 1$) abbiamo per forza⁴ $b, c \geq \frac{ab - c}{2} - 1$ e similmente $c \geq \frac{bc - a}{2} - 1$. Scriviamo tutto per esteso e vediamo che cosa se ne può cavare:

$$\begin{cases} 2b + c + 2 \geq ab \\ 2c + c + 2 \geq ab \\ 2c + a + 2 \geq bc \end{cases}$$

Le prime due disuguaglianze sembrano dire che c è grande... se voglio una contraddizione sarà meglio far vedere che c è anche piccolo, cosa che potrebbe seguire dalla terza disuguaglianza se la riscrivo nella forma $c \leq \frac{a+2}{b-2}$ (notare che $b - 2 > 0$, quindi non ho fatto

³se non lo sapete, fate l'esercizio!

⁴convincetevi per bene di questa disuguaglianza

pastrocchi con i segni). E ora ci saremo, perché la seconda disuguaglianza, d'altra parte, dice $c \geq \frac{ab-2}{3}$. Il modo più veloce di concludere, ora, mi sembra dire che se $b \geq 5$ allora abbiamo

$$c \leq \frac{a+2}{b-2} \leq \frac{a+2}{3} < a \text{ e } c \geq \frac{ab-2}{3} > a,$$

contraddizione. Quindi (siccome b è dispari, diverso da 1, e minore o uguale a 3) dobbiamo avere $b = 3$. E ora abbiamo 2 incognite sole, il problema sarà pur finito... Sostituendo $b = 3$ nel nostro sistema di disuguaglianze troviamo

$$\begin{cases} c + 8 \geq 3a \\ 3c + 2 \geq 3a \\ a + 2 \geq c \end{cases}$$

e la seconda disuguaglianza fornisce $c \geq a$, mentre la terza fornisce $c \leq a + 2$. Siccome a e c hanno la stessa parità, abbiamo $a = c$ oppure $a = c - 2$. Il caso $a = c$ è idiota, perché $ab - c = a(b - 1)$ dev'essere una potenza di 2, quindi a deve essere una potenza di 2 che è anche dispari, quindi $a = c = 1$ che non funziona. Resta il caso $a = c - 2$, e le tre quantità che devono essere potenze di 2 sono

$$2c - 6, 2c + 2, c(c - 2) - 3.$$

Le prime due sono potenze di 2 che distano 8, quindi la più piccola è 8 e l'altra è 16. Questo implica $c = 7$, da cui infine l'ultima soluzione $(3, 5, 7)$.