

PreIMO 2006 TdN

Andrea Fogari

17 settembre 2006

Qua c'è qualche traccia di soluzione per i primi 3 problemi del lavoro singolo di teoria dei numeri al preimo 2006.

Capitolo 1

PreIMO 2006

1.1 Teoria dei numeri, lavoro singolo

Problema 1 *Determinare il più piccolo intero positivo che non si può scrivere nella forma*

$$\frac{2^a - 2^b}{2^c - 2^d}$$

con a, b, c, d interi positivi.

Per chiarire un po' le idee, proviamo a scrivere le condizioni di a, b, c, d per cui la frazione sia valida. Il risultato deve essere positivo, quindi o entrambi (numeratore e denominatore) sono positivi, o negativi. Si fa presto ad accorgersi che si ottengono gli stessi numeri, quindi li possiamo tranquillamente supporre positivi. $a > b$ e $c > d$.

Con questa condizione possiamo raccogliere le potenze in questo modo:

$$\frac{2^b(2^{a-b} - 1)}{2^d(2^{c-d} - 1)}$$

Sappiamo anche che il risultato deve essere intero, quindi $b \geq d$ perchè il numeratore "contiene" (nella sua scomposizione in fattori primi) più due che il denominatore. E gli altri due fattori che troviamo sono dispari, quindi... otteniamo questo:

$$2^{b-d} \frac{2^{a-b} - 1}{2^{c-d} - 1}$$

E per vederci chiaro si fa qualche sostituzione, da segnare sul foglio perchè le soluzioni si dovranno dare in funzione di a, b, c, d .

$$k = b - d$$

$$n = a - b$$

$$m = c - d$$

$$2^k \frac{2^n - 1}{2^m - 1}$$

Così abbiamo ottenuto una formula più trattabile. È giunto il momento di sporcarsi le mani, cercando qualche soluzione. La prima parte (2^k) una qualsiasi

potenza di due, mentre la seconda parte potrebbe essere qualsiasi numero dispari. Quindi il problema è cercare le soluzioni dispari, da cui otterremo delle altre moltiplicandole per ogni potenza di 2 (k lo scegliamo noi). Proviamo a calcolare e fattorizzare qualche $2^x - 1$:

x	$2^x - 1$	scomposizione
1	1	1
2	3	3
3	7	7
4	15	$3 \cdot 5$
5	31	31
6	63	$3^2 \cdot 7$
7	127	127

Che numeri riesco ad ottenere? 1,3,7 li vedo subito. Ma anche 2,4,6,8, basta aumentare k da 0 a qualcosa. Il 5 ce la faccio? Sì, è $\frac{15}{3}$. Quindi anche 10. Manca il nove: perfetto, $\frac{63}{7}$. Abbiamo i numeri da 1 a 10. L'undici sembra un po' difficile da ottenere, invece. Sarà la soluzione? Tanto vale provare a dimostrare che: *11 non lo posso ottenere*.

Strada 1 Provo con i moduli. C'è da scrivere la congruenza e scegliere il modulo:

$$11(2^m - 1) \equiv 2^n - 1 \pmod{p}$$

Abbiamo le potenze di 2, quindi il modulo potrebbe essere una potenza di 2. Ma 2 è troppo generico. 11 è vicino a 12, un multiplo di 4... vediamo se funziona. Se $x \geq 2$ allora $2^x \equiv 0 \pmod{4}$. Supponiamo $m, n \geq 2$:

$$-1 \cdot -1 \equiv -1 \pmod{4}$$

Impossibile. Se $n = 1$, abbiamo già numeri troppo piccoli.

Strada 2 Come posso ottenere almeno un multiplo di 11 con $2^n - 1$? Il piccolo teorema di Fermat serve proprio a questo: $2^{11-1} - 1 = 1023 = 11 \cdot 31 \cdot 3$. Le altre possibilità sono i divisori di $\Phi(11) = 10$, ma si vede subito che con 2 o 5 non funziona. Ora, qual'è il problema? Che 1023 contiene anche i fattori 3 e 31. E non è un caso: $2^2 \equiv 1 \pmod{3}$ e $2^5 \equiv 1 \pmod{31}$, proprio 2 e 5 sono gli ordini moltiplicativi di 2 rispetto a 3 e 31.

Quindi: per ottenere 11 devo prendere un $2^n - 1$ multiplo di 11, quindi un $2^{10k} - 1$, e dividerlo per un multiplo di 3 e 31 (sempre della forma $2^k - 1$). Quando posso trovare un multiplo di 3 e 31? Si fa così: $MCM(\text{ord}_3 2, \text{ord}_{31} 2) = 10 = \text{ord}_{11} 2$. C'era da aspettarsela: ogni multiplo di 11 (di quella forma) è anche divisibile per 3 e 31, e viceversa. Quindi per liberarmi del 3 e 31 dovrei trovare un multiplo di 11^2 e dividerlo per un multiplo di 11, ma forse rischio di rimanere fregato anche questa volta.

Infatti, l'ordine moltiplicativo di 2 rispetto a 121 è ... NO! Ci stiamo perdendo nell'inutilità. Stiamo cercando fattori quando, invece, il problema è già quasi risolto. Infatti, cosa vogliamo trovare a questo punto? Due numeri a, b tali che $a = 2^n - 1, b = 2^m - 1, \frac{a}{b} = 11$. Ma se il loro rapporto è 11... la distanza tra m e n certamente non sarà superiore a 4. Ma per la faccenda del 3 e del 31 sappiamo che b non può essere 1, quindi essendo due numeri entrambi multipli di 11 ma diversi, $n - m$ è almeno 10. E fine.

Problema 2 *Determinare tutte le soluzioni positive dell'equazione*

$$3^x = 2^x y + 1.$$

Diamoci un'occhiata. A sinistra ho una potenza di 3. A destra invece ho una potenza di due, con lo stesso esponente. Però c'è quella y che serve a riequilibrare un po' il tutto. La y mi dice "importano i fattori, non la grandezza dei numeri!".

Poi c'è l'uno, che dovrebbe essere l'elemento "fastidioso". Spostandolo di là però è meno fastidioso: le differenze si scompongono più facilmente delle somme. Ottengo:

$$3^x - 1 = 2^x y$$

che si legge: 3 elevato alla x , decrementato di 1, contiene almeno x fattori 2". Infatti la y può essere pari nel caso avanzi qualche fattore 2. È giunta l'ora di compilare la tabella:

n	$3^n - 1$	fattori 2
1	2	1
2	8	3
3	26	1
4	80	4
5	242	1
...		
8	6560	5

Le uniche soluzioni sembrano essere per $x = 1, 2, 4$, poi la massima potenza di 2 che divide 3^n sembra non riuscire in alcun modo a crescere linearmente. Cerchiamo di dimostrare questo.

In che modo? Moduli? E che modulo? 2,4,8,16,...non basterebbe mai, perché niente vieta che per un certo n $3^n - 1$ sia divisibile per una potenza di 2 anche molto grande. Poi abbiamo a sinistra un $(3^x - 1)$, che sappiamo che si può scomporre, anche tante volte, a seconda di x . Però nella nostra dimostrazione dovremmo riuscire a generalizzare questo.

A questo punto si può fare un'osservazione sulla tabella: escono grandi potenze di 2 quando l'esponente del 3 contiene anche abbastanza fattori 2. Sarà il caso oppure è qualcosa di bello? Si spera nella seconda. Allora, come lo scrivo questo? È conveniente scrivere l'esponente del 3 in questo modo: $x = d \cdot 2^k$, con d dispari. Ora bisogna vedere se si riesce a scomporre in maniera carina $3^{d \cdot 2^k}$ e ad evidenziare tutti i fattori 2 che compaiono. Forse è la strada sbagliata, ma tanto vale provarci.

Ad esempio, se fosse $3^4 - 1$, si scomporrebbe in $(3^2 + 1)(3 + 1)(3 - 1)$ come differenza di quadrati. Sembra andare bene: prima però conviene riscrivere come $(3^d)^{2^k}$, così riusciamo a mettere bene in evidenza quante volte si riuscirà a scomporlo come differenza di quadrati. Otteniamo:

$$a = 3^d, a^{2^k} - 1 = (a^{2^{k-1}} + 1)(a^{2^{k-2}} + 1) \cdots (a + 1)(a - 1)$$

Contiamo quanti fattori sono divisibili per 2 e quante volte. I fattori del tipo $3^{pari} + 1$ sono congrui a 0 modulo 2 e a 2 modulo 4, quindi divisibili solo una volta per 2. Quanti sono? Da $a^{2^{k-1}} + 1$ ad $a^2 + 1$, quindi in totale $k - 1$

volte. I restanti fattori sono $(3^d + 1)$ e $(3^d - 1)$, il primo divisibile per 4 mentre il secondo solo per 2.

Abbiamo generalizzato in: *la massima potenza di 2 che divide 3^x ($x \geq 2$) è la massima potenza di 2 che divide x , più 2.*

Molto bello, forse in qualche modo si può estendere anche ad altri primi ma non ci interessa: l'esercizio è quasi risolto.

Problema 3 *Determinare tutte le soluzioni dell'equazione*

$$n^8 - p^2 = n^2 + p^5,$$

in cui n è un intero positivo e p è un primo.

Dice il Gobbino: spesso la risoluzione di un problema di questo tipo (equazione negli interi) si divide in due parti:

1. una disuguaglianza, in cui si confronta le grandezze che assume l'espressione e che possono assumere le variabili
2. una parte di teoria dei numeri, in cui si considerano i fattori (soprattutto primi) in cui si scompone l'espressione

Questo problema è un perfetto esempio di applicazione di entrambi i metodi. Per cominciare osserviamo che ci sono tante potenze e nessuna costante, quindi forse si scompone bene con formule tipo differenza di quadrati ecc. Per farlo spostiamo ogni variabile dalla sua parte dell'uguale, raccogliamo e spezziamo tutto. Si ottiene:

$$n^2(n-1)(n+1)(n^2-n+1)(n^2+n+1) = p^2(p+1)(p^2-p+1)$$

Prima di procedere vediamo chi deve essere il più piccolo. n ha gli esponenti più alti, quindi probabilmente sarà il più piccolo, escludendo i valori più bassi (forse). Anzi, tanto per farci comodo, escludiamo subito i valori più bassi di n :

1. $n = 1$ \rightarrow non ha soluzioni
2. $n = 2$ \rightarrow ... $LHS = 4 \cdot 7 \cdot 9$, quindi p^2 deve essere 9... anzi, in questo caso funziona! Una soluzione: $n = 2, p = 3$. Se ce ne sono altre, le troveremo.

Ora possiamo supporre $n \geq 3, p \geq 2$.

Come si fa a dimostrare che deve essere $n < p$? Per questo polinomio è abbastanza facile. Dobbiamo dire che:

$$\begin{aligned} p < n &\implies p^2 + p^5 < n^8 - n^2 \\ &\iff p^2(p^3 + 1) < n^2(n^6 - 1) \\ &\iff p^3 + 2 < n^6 \end{aligned}$$

ma questi due polinomi sono monotoni crescenti e il secondo è maggiore del primo almeno da 2 in poi, quindi è fatta. $n < p$ (sempre escludendo $n = 1$).

Torniamo ai fattori. E per comodità cerchiamo di togliere ancora qualche caso, in modo da supporre $(n, p) = 1$. Allora, non può essere che $p|n$ perchè p è maggiore. Se $n|p$? Humm... proviamo prima dal punto di vista dei fattori. Sarà $p = kn$, se in n^2 e p^2 semplifichiamo il fattore n , a destra resta un k^2 di troppo.

Dove lo possiamo trovare a sinistra? Da nessuna parte, perchè ogni fattore è della forma $an \pm 1$.

Ora si può supporre $MCD(n, p) = 1$. Andiamo a caccia di fattori... partendo da p^2 , che sembra il più semplice. Dove lo troviamo in LHS ? n^2 no, $n - 1$ neanche, supponiamo che non sia neanche $n + 1$. In tal caso p^2 deve trovarsi in $n^2 - n + 1$ o in $n^2 + n + 1$ - può trovarsi un p in tutti e due? No, basta considerare la differenza... se $p \neq 2$ (che comunque è stato escluso), $p \nmid 2n$. E allora p^2 si trova in uno solo dei due. Quale? A questo punto siamo un po' a corto di idee... proviamo a tornare in modalità disuguaglianza.

Magari si può escludere $n^2 - n + 1$ dimostrando che $p < n^2$. Se sostituisco, mi resta da dimostrare che $n^8 - n^2 < n^{10} + n^4$, e il membro a destra è chiaramente maggiore in ogni caso. Quindi infine abbiamo $n < p < n^2 < p^2$. Torniamo in modalità "fattori".

Sarebbe che $p^2 \mid n^2 + n + 1$. Cosa si può pensare di questo? Per grandi numeri, $n^2 + n + 1$ è vicino a n^2 , che è minore di p^2 ... anzi è molto vicino! Infatti $(n + 1)^2 = n^2 + 2n + 1$! Quindi si avrebbe che $n < p \leq n + 1$, quindi $p = n + 1$... ma abbiamo comunque supposto che p non divide $n + 1$.

Resta solo un caso, che abbiamo scartato prima: $p \mid n + 1$. Visto che $n < p$, questo implica che $p = n + 1$. Che si fa? Si sostituisce e si spera di finire entro breve l'esercizio.

$$n^2 \cdot p(n - 1)(n^2 + n + 1)(n^2 - n + 1) = p^2(p + 1)(p^2 - p + 1)$$

Taglio il p ... resta da cercare ancora un $p = n + 1$ nella parte a sinistra. Non è $n^2 = (p - 1)^2$. Non è neanche $(n - 1) = (p - 2)$. Non è $n^2 + n + 1 = p^2 - p + 1$ e se fosse $n^2 - n + 1 = p^2 - 3p + 3$? In questo caso $p = 3$, ma l'unica soluzione l'abbiamo già trovata.

Fatta! È stato faticoso ma (forse) abbiamo analizzato tutti i casi.

Problema 4 *Su una scacchiera infinita i numeri interi positivi sono scritti in ordine lungo una spirale: si parte da 1 e si procede allargandosi girando in senso antiorario, come nella figura di Cesenatico 2006.*

Chiamiamo "semiretta destra" della scacchiera l'insieme delle caselle formato da una casella C e da tutte le caselle che si trovano nella riga di C e a destra di C .

Determinare per quali numeri primi p esiste almeno una semiretta destra le cui caselle non contengono multipli di p .

Boh, qua avevo scritto qualcosa ma è tutto sbagliato :(