Lezione 3 - Teoria dei Numeri

Problema 1 *Nel cortile esterno di Villa San Saverio vivono molti animali fantastici. Tra unicorni, ippogrifi, fisici, ed altre creature della cui esistenza il mondo non è a conoscenza, vi è un bizzarro branco di camaleonti. Essi possono avere la pelle di colore rosso, blu o verde; in questo momento, vi sono* 2017 *camaleonti blu,* 2016 *rossi e* 2015 *verdi. Ogni volta che esattamente due (non più) camaleonti di colore diverso si incontrano, la loro pelle muta e diventa del terzo colore possibile (come esempio, se un camaleonte blu e uno rosso si incontrano, diventano entrambi verdi); inoltre, questo è l'unico modo in cui essi cambiano colore. Sapendo che unicorni, ippogrifi, fisici e camaleonti non si riproducono, è possibile che, ad un certo punto, tutti i camaleonti siano dello stesso colore?*

Soluzione: Indichiamo con (R, V, B) il numero di camaleonti di ciascun colore presenti in cortile. Quando due camaleonti si incontrano, uno dei tre valori R, V, B aumenta di 2, mentre gli altri due diminuiscono di 1. Quindi, poiché $2 \equiv -1 \pmod 3$, possiamo affermare che, modulo 3, ad ogni incontro tra camaleonti, la terna (R, V, B) diventa $(R-1, V-1, B-1)$. Poiché la terna iniziale è $(2017, 2016, 2015) = (1, 0, 2)$ e ogni volta togliamo 1 a tutti e tre i valori, i resti modulo 3 di R, V, B saranno sempre distinti a due a due. Quindi, due di questi tre resti non potranno mai essere contemporaneamente uguali a zero, e da ciò possiamo dedurre che almeno due tra R, V, B saranno sempre diversi da zero. Quindi non è possibile che tutti i camaleonti siano dello stesso colore.

Problema 2 *Calcolare il massimo comune divisore di tutti gli interi della forma*

$$I_n = n^5 + 4n^4 - 49n^3 + 104n^2 - 60n,$$

con $n \geq 1$ *intero (ricordate che* 0 *è multiplo di qualsiasi intero).*

Soluzione: Raccogliendo un fattore n notiamo che

$$I_n = n(n^4 + 4n^3 - 49n^2 + 104n - 60)$$

Osserviamo ora che $I_1 = 0$. Quindi, per il Teorema di Ruffini, si ha che 1 è una radice del polinomio $n^4 + 4n^3 - 49n^2 + 104n - 60$. Utilizzando la regola di Ruffini scomponiamo il polinomio come

$$n^4 + 4n^3 - 49n^2 + 104n - 60 = (n-1)(n^3 + 5n^2 - 44n + 60).$$

Quindi $I_n = n(n-1)(n^3 + 5n^2 - 44n + 60)$, e calcolando I_2 otteniamo $I_2 = 2 \cdot 1 \cdot (8 + 5 \cdot 4 - 44 \cdot 2 + 60) = 0$: allora, sempre per il Teorema di Ruffini, 2 è una radice del polinomio $n^3 + 5n^2 - 44n + 60$, che posso scomporre come $n^3 + 5n^2 - 44n + 60 = (n-2)(n^2 + 7n + 30)$. Scomponendo anche il polinomio di secondo grado $n^2 + 7n + 30$ come $n^2 + 7n + 30 = (n-3)(n+10)$ otteniamo infine

$$I_n = n(n-1)(n-2)(n-3)(n+10).$$

Da questa formula si ricavano immediatamente $I_4 = 4 \cdot 3 \cdot 2 \cdot 1 \cdot 14$ e $I_5 = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 15$; osserviamo che I_4 e I_5 hanno in comune un fattore 4, un fattore 3, e un fattore 2. Sempre dalla formula per I_n, osserviamo che tra gli interi $n, (n-1), (n-2), (n-3)$, vi sono almeno un multiplo di 3 e due interi pari, di cui uno deve essere anche un multiplo di 4. Quindi il massimo comun divisore degli interi I_n è $4 \cdot 3 \cdot 2 = 24$.

Problema 3 *(Test di Ammissione SSC 2006-07)*
Provare che l'equazione $x^2 - 7y^2 = -1$ non ha soluzioni tra i numeri interi relativi.

Soluzione: Considerando l'equazione modulo 7, si deve avere $x^2 \equiv -1 \pmod 7$, il che è impossibile in quanto (si vede anche a mano) le potenze seconde modulo 7 possono fare solo $0, 1, 2, 4$.

Problema 4 *(Test di Ammissione SSC 2007-08)*
Sia $n > 5$ un numero della forma $2p$, con p numero primo. Determinare tutti i numeri naturali m tali che $m!$ è divisibile per n.

*(NOTA: Dato un numero naturale m, denotiamo con $m!$ il **fattoriale** di m, ottenuto moltiplicando tra loro tutti gli interi tra 1 e m.)*

Soluzione: Chiaramente, dato che $p > 2$, $n = 2p$ divide $p! = 1 \cdot 2 \cdot \ldots \cdot p$. Quindi, poiché per ogni $m \geq p$, per definizione di fattoriale $p! | m!$, si ha che $n = 2p$ divide $m!$ per ogni $m \geq p$.

D'altra parte, se $m < p$, il fattoriale $m!$ non contiene il fattore p: quindi in questo caso n non divide $m!$.

Problema 5 *Siano a,b numeri interi tali che* $2a+3b$ *è divisibile per* 11. *Si dimostri che* a^2-5b^2 *è divisibile per* 11.

Soluzione: Poiché $2a+3b$ è un multiplo di 11, allora anche $4a^2-9b^2 = (2a+3b)(2a-3b)$ è un multiplo di 11. Da questo segue che $4a^2-20b^2 = (4a^2-9b^2)-11b^2$ è un multiplo di 11, e quindi, che $a^2-5b^2 = \frac{4a^2-20b^2}{4}$ è un multiplo di 11.

Problema 6 *(Iran - Gara Nazionale 2001)*
Siano p *e* n *numeri naturali tali che* $n > p$, p *sia primo e* $1+np$ *sia un quadrato perfetto. Provare che il numero* $n+1$ *è la somma di* p *quadrati perfetti (non necessariamente distinti).*

Soluzione: Posto $1+np = a^2$, si ottiene $np = (a-1)(a+1)$, quindi possiamo distinguere due possibili casi: $p|a-1$ e $p|a+1$.
Se $p|a-1$ allora $a = kp+1$ e $1+np = (kp+1)^2$, e svolgendo i conti otteniamo $n = k^2p+2k$. Possiamo riscrivere in modo furbo questa equazione come

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

Se invece $p|a+1$ allora $a = kp-1$ e $1+np = (kp-1)^2$, da cui segue $n = k^2p-2k$, e procedendo come prima otteniamo

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

Poiché in entrambi i casi abbiamo scritto $n+1$ come somma di p quadrati perfetti, abbiamo finito.

Problema 7 *Dato* $n \in \mathbb{N}$, *dimostrare che esiste un suo multiplo che avrà come cifre tutte* 1 *e* 0 *(ad esempio, per* $n = 3$, 1011 *è divisibile per* 3 *e ha come cifre tutte* 1 *e* 0*).*

Soluzione: Consideriamo l'insieme di $n+1$ elementi formato dai numeri $1, 11, 111, \ldots$ fino al numero formato da $n+1$ cifre 1. Le classi di resto modulo n sono al più n: quindi, per il principio dei cassetti, vi sono due numeri in questo insieme che hanno lo stesso resto modulo n. La differenza di questi due numeri sarà quindi divisibile per n, e, siccome i due numeri sono formati da tutti 1, la loro differenza sarà formata solo da cifre 1 e 0.

Problema 8 *$a, b, c, d, e \in \mathbb{N}$ sono tali che $a^4 + b^4 + c^4 + d^4 = e^4$. Mostrare che tra i cinque numeri*

(a) almeno tre sono pari;

(b) almeno tre sono multipli di 5;

(c) almeno due sono multipli di 10.

Soluzione:

(a) Osserviamo che se un intero m è pari, allora $m^4 \equiv 0 \pmod{16}$, mentre, se $m = 2k + 1$ è dispari, allora

$$m^4 \equiv (2k+1)^4 \equiv 16k^4+32k^3+24k^2+8k+1 \equiv 8k(k+1)+1 \equiv 1 \pmod{16}$$

in quanto $k(k+1)$ è pari. Dunque, se consideriamo l'uguaglianza modulo 16, al secondo membro avremo 0 o 1, mentre (per lo stesso motivo) al primo membro vi sono tutti termini uguali a 0 o 1. Quindi al primo membro devono esserci almeno tre termini uguali a zero modulo 16, ovvero tre numeri pari.

(b) Sia m un intero. Per il Piccolo Teorema di Fermat, se m non è un multiplo di 5 si ha $m^4 \equiv 1 \pmod{5}$, mentre se 5 divide m chiaramente $m^4 \equiv 0 \pmod{5}$. Dunque, se consideriamo l'uguaglianza modulo 5, al secondo membro avremo 0 o 1, mentre (per lo stesso motivo) al primo membro vi sono tutti termini uguali a 0 o 1. Quindi al primo membro devono esserci almeno tre termini uguali a zero modulo 5, ovvero tre multipli di 5.

(c) Per i punti precedeti almeno tre dei quattro numeri del primo membro sono multipli di 2 e almeno tre sono multipli di 5: incrociando queste ipotesi si vede che almeno due devono essere multipli di 10.

Problema 9 *(Test di Ammissione SSC 2010-11)*
Dati sei interi positivi distinti, qual è il massimo numero di primi tra l'insieme delle somme di due di essi?

Soluzione: Poichè i numeri devono essere distinti, tra le somme delle coppie non ci può essere 2, che è l'unico numero primo pari. Per questo motivo, possiamo ottenere numeri primi tra queste somme solo sommando un numero pari ed un numero dispari. Pertanto, detto n il numero di numeri

pari scelti e detto k il numero di primi fra le somme delle coppie, si deve avere $k \leq n(6-n)$. Poiché n è compreso tra 0 e 6, il massimo valore di $n(6-n)$ è 9, che potremmo ottenere se $n = 3$. Ora, se riuscissimo ad esibire un esempio per cui risulta $k = 9$, avremo finito. Ad esempio una soluzione è data dall'insieme dei numeri $\{1, 4, 7, 9, 22, 52\}$, per cui l'insieme dei numeri primi tra le somme di due di essi è $\{5, 11, 13, 23, 29, 31, 53, 59, 61\}$.

Problema 10 *(Test di Ammissione SSC 2016-17)*
Si considerino 18 *numeri consecutivi* N, $N+1$, $\cdots$, $N+17$ *di al più tre cifre (dunque compresi fra 0 e 999). Si mostri che almeno uno di essi è divisibile per la somma delle sue cifre.*
Suggerimento: almeno uno dei numeri $N, N+1, \ldots, N+17$ *è divisibile per* 9.

Soluzione: Chiaramente tra i 9 numeri consecutivi $N, N+1, \ldots, N+8$, vi deve essere almeno un multiplo di 9; chiamiamo questo numero K. Dunque, la somma delle cifre di K è un multiplo di 9: poiché K ha tre cifre questa somma può essere 9 (e in tal caso abbiamo finito perché K è divisibile per 9), può essere 27, e allora il numero è necessariamente $K = 999 = 37 \cdot 27$ (dunque anche in questo caso abbiamo finito), o può essere 18. Supponiamo dunque che la somma delle cifre di K sia 18. Se K è pari, allora è divisibile sia per 2 sia per 9, e pertanto in tal caso abbiamo concluso. Se invece K è dispari, poiché $K \leq N + 8$, il numero $K + 9$ è ancora compreso tra N e $N + 17$; inoltre, questo numero è divisibile per 9 (perché K è divisibile per 9) e per 2 (poiché K è dispari), quindi è divisibile per 18: quindi anche in questo caso abbiamo trovato il numero cercato.

Problema 11 *(Test di ammissione SNS 2013-14)*
Trova tutti gli interi positivi n *tali che* $n^4 + n^3 + n^2 + n + 1$ *sia un quadrato perfetto.*

Soluzione: Sia $F_n = n^4 + n^3 + n^2 + n + 1$. Chiaramente, se riesco a posizionare F_n tra i quadrati di due numeri interi consecutivi, F_n non può essere un quadrato perfetto. Dividiamo il nostro problema in due casi:

1. **CASO 1**: Supponiamo che n sia pari, e cerchiamo un intero P_n tale che $P_n^2 < F_n < (P_n + 1)^2$.

   Osserviamo che

   $$\left(n^2 + \frac{n}{2}\right)^2 = n^4 + n^3 + \frac{1}{4}n^2 < F_n,$$

e inoltre

$$\left[\left(n^2+\frac{n}{2}\right)+1\right]^2 = n^4+n^3+\frac{9}{4}n^2+n+1 > F_n.$$

Quindi, posto $P_n = n^2+\frac{n}{2}$, si ha $P_n^2 < F_n < (P_n+1)^2$, e quindi F_n non è un quadrato perfetto.

2. **CASO 2**: Supponiamo che n sia dispari, e procediamo come nel caso precedente.

   Osserviamo che

$$\left(n^2+\frac{n-1}{2}\right)^2 = n^4+n^3-\frac{3}{4}n^2-\frac{n}{2}+\frac{1}{4} < F_n,$$

   e inoltre se $n>3$ si ha $n^2-2n-3>0$, ovvero che $\frac{5}{4}n^2+\frac{n}{2}+\frac{1}{4} > n^2+n+1$, da cui segue che

$$\left[\left(n^2+\frac{n-1}{2}\right)+1\right]^2 = n^4+n^3+\frac{5}{4}n^2+\frac{n}{2}+\frac{1}{4} > F_n.$$

   Quindi, assumendo $n>3$ e posto $P_n = \left(n^2+\frac{n-1}{2}\right)$, si ha $P_n^2 < F_n < (P_n+1)^2$, da cui segue che F_n non è un quadrato perfetto se $n>3$. Quindi, gli unici valori possibili sono $n=1$ e $n=3$. Per $n=1$ si ha $F_1=5$, che non è un quadrato perfetto, mentre per $n=3$ si ha $F_3 = 3^4+3^3+3^2+3+1 = 121 = 11^2$.

L'unica soluzione possibile è $n=3$.

Problema 12 *(IMO 1975, Problema 4)*

Sia $N = 4444^{4444}$ (scritto in notazione decimale), sia A la somma delle cifre di N, e sia B la somma delle cifre di A (scritto in notazione decimale). Trovare la somma delle cifre di B.

(Suggerimento: $4444^{4444} < 10000^{4444}$. Quante cifre ha 10000^{4444}?)

Soluzione: Sia C la somma delle cifre di B. Poiché $4444^{4444} < 10000^{4444}$, allora N ha meno di $4444 \cdot 4 < 20000$ cifre. Allora la somma delle cifre di N è minore di $9 \cdot 20000 = 180000$, ovvero $A < 180000$: quindi A ha al più 6 cifre, e quindi $B < 9 \cdot 6 = 54$. Allora B ha 2 cifre, e poiché la cifra delle decine di B è al più 5, si ha che la somma delle cifre di B può essere al più

$4 + 9 = 13$ (perché B non può essere 59). Inoltre, dal criterio di divisibilità per 9 si ha che un numero è pari alla somma delle sue cifre modulo 9, allora

$$N \equiv A \equiv B \equiv C \pmod 9.$$

Poiché $4444 \equiv 16 \equiv 7 \pmod 9$ e per il Piccolo Teorema di Fermat $7^6 \equiv 1 \pmod 9$, si ha (poiché $4444 = 6 \cdot 740 + 4$) che

$$4444^{4444} \equiv 7^{6 \cdot 740} \cdot 7^4 \equiv (7^6)^{740} \cdot 7^4 \equiv 7^4 \equiv 7 \pmod 9.$$

Quindi si ha $C \equiv 7 \pmod 9$ e $C \leq 13$: quindi si deve avere necessariamente $C = 7$.

Problema 13 *(Pan African MO 2013)*
Un intero positivo n è tale che $n(n + 2013)$ è un quadrato perfetto.

(a) Mostrare che n non può essere un numero primo.

(b) Trovare un valore di n tale che $n(n + 2013)$ sia un quadrato perfetto.

Soluzione:

(a) Se n fosse un primo allora, poichè $n(n + 2013)$ è un quadrato, si dovrebbe avere $n|n + 2013$, ovvero $n|2013$. Poiché $2013 = 3 \cdot 11 \cdot 61$, le uniche soluzioni possibili sono $n = 3, n = 11, n = 61$; tuttavia, si verifica immediatamente che per nessuno di questi valori $n(n + 2013)$ è un quadrato perfetto.

(b) Poniamo $k^2 = n(n + 2013)$. Moltiplicando per 4 entrambi i membri e sommando 2013^2 si ha $4n^2 + 2 \cdot 2013 \cdot 2n + 2013^2 = 4k^2 + 2013^2$, ovvero $(2n + 2013)^2 - 4k^2 = 2013^2$. Osserviamo ora che il primo membro è una differenza di quadrati, quindi otteniamo

$$(2n + 2013 - 2k)(2n + 2013 + 2k) = 2013^2.$$

Quindi $2n + 2013 - 2k$ e $2n + 2013 + 2k$ sono due fattori di 2013^2; quindi, se consideriamo tutte le possibili coppie a, b tali che $ab = 2013^2$ e $a \leq b$, ad ogni possibile coppia è possibile associare un sistema del tipo

$$\begin{cases} 2n + 2013 - 2k = a \\ 2n + 2013 + 2k = b \end{cases}$$

Risolvendo questo sistema si ricavano i valori di n e k (se sono interi,

ovvero se $b-a$ è un multiplo di 4). Come esempio, ponendo $a = \frac{2013}{3} = 671$ e $b = 2013 \cdot 3$, si ha

$$\begin{cases} n-k = -671 \\ n+k = 2013 \end{cases}$$

da cui otteniamo la soluzione $n = 671$, $k = 1342$.

Problema 14 *(Spagna - Gara Nazionale 2009)*
Trovare tutte le coppie di interi (x, y) *tali che* $x^2 - y^4 = 2009$.

Soluzione: Innanzitutto osserviamo che possiamo cercare solo le soluzioni non negative, in quanto per ogni coppia di interi (x, y) avremo che anche $(-x, y), (x, -y), (-x, -y)$ sono soluzioni.
Fattorizziamo l'equazione di partenza come $(x - y^2)(x + y^2) = 2009$. Ora, consideriamo tutte le possibili coppie a, b tali che $ab = 2009$ e $a < b$. Allora x e y saranno dati dalle soluzioni dei sistemi

$$\begin{cases} x - y^2 = a \\ x + y^2 = b \end{cases}$$

al variare delle possibili coppie di valori di a e b. Dal sistema precedente si vede che $\frac{b-a}{2} = y^2$ deve essere un quadrato perfetto. Quindi, considerando tutte le possibili coppie di valori a, b (sono solo 3), si verifica che questo accade solo se $a = 41$ e $b = 49$, in corrispondenza della quale si trovano le soluzioni $(x, y) = (45, 2), (-45, 2), (45, -2), (-45, -2)$.

Problema 15 *Sia* $p = 3k + 2$ *un numero primo. Provare che per ogni* a *compreso tra* 0 *e* $p - 1$ *esiste un intero* x *tale che si abbia* $x^3 \equiv a \pmod{p}$.

Soluzione:
Per il Piccolo Teorema di Fermat si ha $a^{3k+1} \equiv a^{p-1} \equiv 1 \pmod{p}$. Allora per ogni intero $N_\lambda = \lambda(3k+1) + 1$ si ha

$$a^{N_\lambda} \equiv a^{\lambda(3k+1)} \cdot a \equiv (a^{3k+1})^\lambda \cdot a \equiv 1 \cdot a \pmod{p}.$$

Scegliamo un intero della forma N_λ che sia anche un multiplo di 3; per esempio, $N_2 = 2(3k+1) + 1 = 3(2k+1)$. Per quanto visto, si ha $a^{N_2} \equiv a$

(mod p), e inoltre ovviamente $a^{N_2} \equiv (a^{2k+1})^3 \pmod{p}$. Quindi, se consideriamo un intero x tale che $x \equiv a^{2k+1} \pmod{p}$ (ricordiamo che a e k sono fissati), si ha

$$x^3 \equiv (a^{2k+1})^3 \equiv a^{6k+3} \equiv a^{N_2} \equiv a \pmod{p},$$

da cui si ottiene la tesi.

Problema 16 *(IMO 1991, Problema 2)*

Sia $n > 6$ e siano $a_1, a_2, \ldots, a_k$ tutti gli interi positivi d minori di n e tali che $MCD(n, d) = 1$. Se

$$a_2 - a_1 = a_3 - a_2 = \ldots = a_k - a_{k-1} > 0,$$

provare che n deve essere un numero primo, o una potenza di 2.

(Suggerimento: Sia $n = 4k + r$, con $r = 0, 1, 2, 3$. Sapreste trovare due interi d_1, d_2 abbastanza vicini tali che $MCD(n, d_1) = MCD(n, d_2) = 1$?)

Soluzione: Sia $n = 4k + r$, con $r = 0, 1, 2, 3$. Studiamo tre casi:

1. Se $r = 1$ o $r = 3$ (ovvero se n è dispari), allora $MCD(n, 1) = 1$ e $MCD(n, 2) = 1$, quindi $a_1 = 1$ e $a_2 = 2$. Quindi sfruttando la relazione si ha $a_i = i$ per ogni $i = 1, \ldots, k$. Ma poiché $MCD(n, n-1) = 1$, chiaramente $a_k = n - 1$, e quindi $k = n - 1$: quindi n non ha fattori in comune con $n - 1$ interi positivi minori di n, ovvero non ha fattori in comune con nessun intero minore di n: quindi n deve essere un numero primo.

2. Se $r = 2$, ovvero se $n = 4k + 2$, allora n è un multiplo di $2k + 1$. Osserviamo ora che

   $$MCD(2k + 3, 4k + 2) = MCD(2k + 3, 4k + 2 - 2k - 3) =$$
   $$= MCD(2k + 3, 2k - 1) = MCD(2k + 3, 4) = 1,$$

   in quanto $2k + 3$ è dispari, e che

   $$MCD(2k + 5, 4k + 2) = MCD(2k + 5, 4k + 2 - 2k - 5) =$$
   $$= MCD(2k + 5, 2k - 3) = MCD(2k + 5, 8) = 1,$$

   in quanto anche $2k + 5$ è dispari.

   Quindi $2k + 3 = a_i$ per qualche i, poiché chiaramente n ha un fattore 2 in comune con $2k + 4$, si ha $2k + 5 = a_{i+1}$. Allora $a_{i+1} - a_i = 2$, quindi per la relazione si deve avere $a_{i-1} = 2k + 3 - 2 = 2k + 1$, il che è impossibile in quanto $2k + 1$ è un fattore di $n = 4k + 2 = 2(2k + 1)$.

3. Se $r = 0$, ovvero $n = 4k$, allora

$$MCD(2k-1, 4k) = MCD(2k-1, 4k-2k+1) =$$

$$= MCD(2k-1, 2k+1) == MCD(2k-1, 2) = 1,$$

in quanto $2k-1$ è dispari, e similmente

$$MCD(2k+1, 4k) = MCD(2k+1, 4k-2k-1) =$$

$$= MCD(2k+1, 2k-1) = MCD(2k+1, 2) = 1,$$

in quanto $2k+1$ è dispari.

Allora, poiché $n = 4k$ ha un fattore $2k$ in comune con $2k$, si deve avere $2k-1 = a_i$ per qualche i, e $2k+1 = a_{i+1}$. Allora $a_{i+1} - a_i = 2$. Quindi, poiché $a_1 = 1$, si ha dalla relazione che $a_2 = a_1 + 2 = 3$, $a_3 = a_2 + 2 = 5$, e in genere $a_i = 2i - 1$. Poiché $a_k = n - 1$ in quanto $MCD(n, n-1) = 1$, si deve avere necessariamente che n è coprimo con tutti gli interi positivi dispari minori di n: quindi n contiene solo fattori 2, ovvero è una potenza di 2.

Problema 17 *(Test di Ammissione SSC 2013-14)*
Si determinino tutti i numeri primi p tali che il numero $p(2^{p-1} - 1)$ sia una potenza n^k (con $k > 1$) di un intero positivo n.

Soluzione: Se $p = 2$, l'espressione è uguale a 2, che non è una potenza; quindi possiamo supporre che p sia un primo dispari. Posto quindi $p = 2q+1$ si ha

$$p(2^{p-1} - 1) = p(2^{2q} - 1) = p(2^q + 1)(2^q - 1).$$

Poiché $(2^q + 1)$ e $(2^q - 1)$ sono due interi dispari consecutivi, essi non hanno fattori comuni; quindi, affinché il prodotto sia una potenza perfetta, almeno uno di essi deve essere una potenza perfetta, cioè deve essere $2^q + 1 = m^k$ oppure $2^q - 1 = m^k$, con m dispari.
Nel primo caso, se k è dispari si avrebbe

$$2^q = m^k - 1 = (m-1)(m^{k-1} + m^{k-2} + \cdots + 1)$$

ed essendo il fattore $m^{k-1} + m^{k-2} + \cdots + 1$ di 2^k un numero dispari, dovrebbe essere uguale a 1, il che è impossibile se $k > 1$. Il secondo caso con k dispari è analogo.
Supponiamo allora che k sia pari, uguale a $2s$, e sia $2^q - 1 = m^k = (m^s)^2$. Ogni

quadrato di un numero dispari ha resto 1 nella divisione per 4, quindi non può essere $q > 1$. Se $q = 1$ allora $p = 3$ e si ha in effetti che $3(22-1) = 9 = 3^2$, cioè $p = 3$ soddisfa l'espressione.
Sia ora sempre k pari, uguale a $2s$ e sia $2^q + 1 = m^k = (m^s)^2$, si ha allora

$$2^q = m^k - 1 = (m^s + 1)(m^s - 1).$$

Poiché due pari consecutivi possono avere in comune solo il fattore 2, l'unica possibilità che siano entrambe potenze di 2 è che siano i numeri 2 e 4, da cui $q = 3$, e in effetti segue che $p = 7$ soddisfa l'espressione, essendo $7(2^6 - 1) = 441 = (21)^2$.
In conclusione gli unici primi che soddisfano i requisiti richiesti sono 3 e 7.

Problema 18 *(Balkan Mathematical Olympiad 2009)*
Trovare le soluzioni intere positive dell'equazione $3^x + 5^y = z^2$

Soluzione: Poiché 3 non divide 5^y, chiaramente z non è un multiplo di 3. Facendo i conti, si verifica subito che per ogni intero m non multiplo di 3, $m^2 \equiv 1 \pmod 3$; dunque $5^y \equiv 1 \pmod 3$, da cui segue facilmente che y dev'essere pari.
Posto $y = 2a$, con a intero positivo, si ha $3^x + 5^{2a} = z^2$, ovvero $3^x = (z - 5^a)(z + 5^a)$. Poiché gli unici divisori di 3^x sono potenze di 3, segue che $3^m = z - 5^a$ e $3^n = z + 5^a$ per m, n interi non negativi tali che $m < n$ e $m + n = x$; quindi $3^n - 3^m = 2 \cdot 5^a$. Poiché $2 \cdot 5^a$ non è un multiplo di 3, segue che m e n non possono essere entrambi positivi, e poiché $m < n$, si deve avere necessariamente $m = 0$.
Sostituendo, otteniamo quindi $3^n = 2 \cdot 5^a + 1$. Considerando questa uguaglianza modulo 5 si ha $3^n \equiv 1 \pmod 5$, e quindi (calcolando le potenze di 3 modulo 5) osserviamo che n deve essere pari. D'altro canto, poiché $2 \cdot 5^a \equiv 2 \pmod 4$, si deve avere $3^n \equiv 3 \pmod 4$, quindi n dev'essere dispari: da ciò segue che l'equazione non ha soluzioni.

Problema 19 *Trovare tutte le soluzioni intere positive dell'equazione*

$$x^3 + y^3 + z^3 = 2017.$$

(Suggerimento: $13^3 = 2197$*)*

Soluzione: Notiamo innanzitutto che $2017 \equiv 1 \pmod{17}$. Calcolando a mano le terze potenze modulo 7 si vede che esse possono essere soltanto $-1, 0$

o 1. In particolare, si ha

$$\begin{cases} x^3 \equiv 1 \pmod 7 \text{ se } x \equiv 1, 2, 4 \pmod 7 \\ x^3 \equiv 0 \pmod 7 \text{ se } x \equiv 0 \pmod 7 \\ x^3 \equiv -1 \pmod 7 \text{ se } x \equiv 3, 5, 6 \pmod 7 \end{cases}.$$

Per questo motivo, a meno di scambiare x, y e z, vi sono solo due casi possibili:

1. $x^3 \equiv y^3 \equiv 0 \pmod 7$ e $z^3 \equiv 1 \pmod 7$. In questo caso, per il suggerimento x, y e z devono essere minori di 13, e poiché $x \equiv y \equiv 0 \pmod 7$ si deve avere $x = y = 7$ e quindi $z^3 = 2017 - 7^3 - 7^3 = 1331 = 11^3$.

2. $x^3 \equiv -1 \pmod 7$, $y^3 \equiv z^3 \equiv 1 \pmod 7$. In questo caso, osserviamo che x è contenuto nell'insieme $\{3, 5, 6, 10, 12\}$, mentre y, z sono contenuti nell'insieme $\{1, 2, 4, 8, 9, 11\}$. Osserviamo ora che le terze potenze modulo 3 hanno lo stesso comportamento delle terze potenze modulo 7; in particolare si ha

$$\begin{cases} x^3 \equiv 1 \pmod 9 \text{ se } x \equiv 1, 4, 7 \pmod 9 \\ x^3 \equiv 0 \pmod 9 \text{ se } x \equiv 3, 6, 0 \pmod 9 \\ x^3 \equiv -1 \pmod 9 \text{ se } x \equiv 2, 5, 8 \pmod 9 \end{cases}.$$

   Quindi procedendo come prima si vede che anche modulo 9 vi sono solo due casi possibili (in questo caso non possiamo scambiare x, y, z perché li abbiamo già fissati ragionando modulo 7, ma i casi sono analoghi):

   - Due tra x^3, y^3, z^3 fanno 0 modulo 9 e uno fa 1 modulo 9. Combinando queste ipotesi con quanto visto modulo 7 osserviamo che uno tra y^3, z^3 deve fare 0 modulo 9.

     Supponiamo quindi $y^3 \equiv 0 \pmod 9$ (il caso $z^3 \equiv 0 \pmod 9$ è identico). Poiché y è contenuto nell'insieme $\{1, 2, 4, 8, 9, 11\}$, si deve avere allora necessariamente $y = 9$, ovvero $y^3 = 729$, e quindi $x^3 + y^3 = 2017 - 729 = 1288$. D'altronde, poiché un altro tra x^3 e z^3 deve fare 0 modulo 9, allora uno tra x e z deve essere 3,6 o 9. Facendo i tre casi, si vede subito che non vi sono soluzioni.

   - Due tra x^3, y^3, z^3 fanno 1 modulo 9 e uno fa -1 modulo 9. Procedendo come nel caso precedente, osserviamo che almeno uno tra y^3 e z^3 deve fare 1 modulo 9.

     Supponiamo quindi $y^3 \equiv 1 \pmod 9$ (il caso $z^3 \equiv 1 \pmod 9$ è analogo). Poiché y è contenuto nell'insieme $\{1, 2, 4, 8, 9, 11\}$, si

deve avere allora necessariamente $y = 1, 4$, ovvero $y^3 = 1$ o $y^3 = 64$, e quindi si ha $x^3 + z^3 = 2016$ o $x^3 + z^3 = 2017 - 64 = 1953$. Ora, osserviamo che in entrambi i casi si ha

$$\max\{x^3, z^3\} \geq \frac{x^3 + z^3}{2} \geq \frac{1953}{2} > 729 = 9^3,$$

quindi il più grande tra x, z può essere solo 10, 11 o 12. Svolgendo questi tre casi a mano, si vede che non vi sono soluzioni accettabili.

Problema 20 *(Francia - TST 2000)*
Trovare tutti gli interi positivi a, b, c tali che

$$a^b + 1 = (a + 1)^c.$$

Soluzione: Innanzitutto, osserviamo che, ponendo $c = 1$ o $b = 1$, in questi casi si deve avere necessariamente $b = c = 1$, e l'equazione è soddisfatta per ogni $a \in \mathbb{N}$.

Possiamo dunque considerare i casi in cui $c \geq 2$ e $b \geq 2$.

Considerando l'equazione modulo $a + 1$ si ha $(-1)^b + 1 \equiv 0 \pmod{a+1}$, dunque b è dispari.

Possiamo allora scomporre

$$a^b + 1 = (a + 1)(a^{b-1} - a^{b-2} + \ldots + 1) = (a + 1)^c.$$

Poichè $c \geq 2$ posso dividere per $a + 1$ e ottenere, considerando nuovamente l'uguaglianza modulo $a + 1$, che $a^{b-1} - a^{b-2} + \ldots + 1 \equiv (a + 1)^{c-1} \equiv 0 \pmod{a+1}$.
Ricordando che b è dispari il primo membro diventa $b \equiv 0 \pmod{a+1}$, ovvero $a + 1|b$. Da ciò segue necessariamente che $a + 1$ è anch'esso dispari, ovvero che a è pari.

Consideriamo ora lo sviluppo binomiale del secondo membro. Si ha

$$a^b + 1 = (a + 1)^c = 1 + ca + \ldots + a^c.$$

Ricordando che $b \geq 2$ possiamo considerare la scrittura precedente in modulo a^2: poiché tutte le potenze di a di esponente almeno 2 fanno 0 modulo a^2 otteniamo $1 \equiv ca + 1 \pmod{a^2}$. Dunque $ca \equiv 0 \pmod{a^2}$, ovvero $a|c$. In particolare, poichè a pari, c sarà anch'esso pari.

Quindi, scriviamo $a = 2m$, $c = 2n$; allora

$$2^b m^b = [(a + 1)^n + 1][(a + 1)^n - 1].$$

Osserviamo ora che

$$MCD\{[(a+1)^n+1],[(a+1)^n-1]\} = MCD\{[(a+1)^n+1],2\} = 2,$$

dove l'ultima uguaglianza segue dalla parità di a. Inoltre, riconsiderando lo sviluppo binomiale, si vede che $2m|(a+1)^n-1$. Allora $(a+1)^n-1 = 2m^b$, in quanto tale fattore deve contenere tutte le potenze di m e non può contenere nessun'altra potenza di 2, altrimenti il massimo comun divisore sarebbe maggiore di 2.

Da ciò si ha anche $(a+1)^n+1 = 2^{b-1}$ e, infine, $2^{b-1} > 2m^b$, ovvero $m = 1$, da cui $a = 2$. Sostituendo nell'equazione $(a+1)^n - 1 = 2m^b$, si vede subito che dobbiamo avere $n = 1$, ovvero $c = 2$, e quindi $b = 3$.

Possiamo allora concludere che l'equazione del problema ha come soluzioni le terne della forma $b = c = 1$, a intero positivo, e la soluzione $a = 2, b = 3, c = 2$.

Problema 21 *(Esame di ammissione Università di Berkeley)*

Il numero $N = 21982145917308330487013369$ *è la tredicesima potenza di un intero positivo* α. *Quale?*

Soluzione: Il numero N ha 26 cifre, quindi $10^{25} < N < 10^{26}$. Poiché $10^{26} = 100^{13}$, ricaviamo che $\alpha < 100$. Inoltre, osserviamo che

$$50^{13} = \frac{100^{13}}{2^{13}} < \frac{100^{13}}{10} = 10^{25},$$

quindi $50 < \alpha < 100$. Inoltre il numero α ha le seguenti proprietà:

- É dispari. In particolare, poiché un numero modulo 4 è congruo al numero formato dalle sue ultime due cifre, si ha $N \equiv 69 \equiv 1 \pmod 4$. Poiché α è dispari, allora $\alpha^2 \equiv 1 \pmod 4$, quindi

  $$N \equiv \alpha^{13} \equiv (\alpha^2)^6 \cdot \alpha \equiv \alpha \pmod 4,$$

  da cui si ha $\alpha \equiv 1 \pmod 4$.

- Non è divisibile per 3. Infatti, poiché la somma delle cifre di N è 107 (che non è un multiplo di 3), si ha che N non è un multiplo di 3, quindi non può esserlo nemmeno α.

- Ha come cifra delle unità 9. Infatti, poiché N è dispari e non è un multiplo di 5, la cifra delle unità di α può essere solo $1, 3, 7, 9$. Tuttavia, svolgendo a mano questi quattro casi si vede che in ogni caso si dovrebbe avere $\alpha^4 \equiv 1 \pmod{10}$ (questo risultato non è casuale!); quindi $N \equiv \alpha^{13} \equiv (\alpha^4)^3 \cdot \alpha \equiv \alpha \pmod{10}$, ovvero $\alpha \equiv 9 \pmod{10}$.

Quindi, il numero α cercato è un intero compreso tra 50 e 100, che ha come cifra delle unità 9, non è divisibile per 3 ed è congruo a 1 modulo 4: l'unico intero che soddisfa tutte queste proprietà è 89.