Lezione 3 - Teoria dei Numeri

Problema 1
Sia k un numero pari. È possibile scrivere 1 come la somma dei reciproci di k interi dispari?

Soluzione: Siano $n_1, \ldots, n_k$ interi dispari tali che

$$1 = \frac{1}{n_1} + \cdots + \frac{1}{n_k}.$$

Allora segue che

$$n_1 \ldots n_k = \frac{n_1 n_2 \ldots n_k}{n_1} + \frac{n_1 n_2 \ldots n_k}{n_2} + \ldots + \frac{n_1 n_2 \ldots n_k}{n_k}.$$

Osserviamo che poiché i vari n_i sono tutti dispari, allora tutti i vari termini coinvolti nelle somme sono dispari. Poiché a destra vi sono k termini dispari, allora il termine di destra è pari, mentre $n_1 \ldots n_k$ è dispari, il che è assurdo.

Problema 2
[Cesenatico 2013]
In quali basi $b > 6$ la scrittura 5654 rappresenta la potenza di un numero primo?

*Soluzione:*Se b è la nostra base, la scrittura $N = 5654$ diventa $N = 5b^3 + 6b^2 + 5b + 4 = (b+1)(5b^2 + b + 4)$ per il Teorema di Ruffini. Osserviamo che se $b + 1$ è dispari, allora $5b^2 + b + 4$ deve essere pari: quindi, in ogni caso si ha che 2 deve dividere $(b + 1)(5b^2 + b + 4) = N$. Poiché peró N deve essere una potenza di un numero primo, si deve avere $N = 2^k$, per qualche $k > 0$. Osserviamo che i divisori di N devono essere a loro volta potenze di 2, quindi si deve avere $b + 1 = 2^c$ e $5b^2 + b + 4 = 2^d$ con c, d interi positivi tali che $c + d = k$. Poiché $5b^2 + b + 4 \geq b + 1$ allora segue $d \geq c$, e quindi $b + 1 | 5b^2 + b + 4$. Tuttavia, poiché $5b^2 + b + 4 = (5b - 4)(b + 1) + 8$, allora si deve avere $b + 1 | 8$; poiché $b > 6$, si deve avere necessariamente $b = 7$, in cui si ha $N = 5 \cdot 7^3 + 6 \cdot 7^2 + 5 \cdot 7 + 4 = 2048 = 2^{11}$.

Problema 3
Siano a ed n due interi positivi, con $n > 1$. Provare che se $a^n - 1$ è un numero primo allora $a = 2$ ed n è un numero primo.

Soluzione: Osserviamo che se $a = 1$ allora $1^n - 1 = 0$, quindi possiamo suppore $a \geq 2$. Supponiamo per assurdo che $a > 2$: allora

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

e poiché $a - 1 > 1$ e $a^{n-2} + \ldots + a + 1 > 1$, $a^n - 1$ non puó essere un numero primo. Quindi $a = 2$. Supponiamo ora, sempre per assurdo, che $n = pq$, con p e q interi positivi maggiori di 1. Allora, ricordando che $a = 2$, si ha

$$2^n - 1 = (2^p)^q - 1 = (2^p - 1)(2^{p(q-1)} + 2^{p(q-2)} + \ldots + 2^p + 1)$$

e poiché $2^p - 1 > 1$ e $2^{p(q-1)} + 2^{p(q-2)} + \ldots + 2^p + 1 > 1$, segue di nuovo che $2^n - 1$ non puó essere un numero primo. Quindi se $a^n - 1$ è un numero primo si deve avere $a = 2$, ed n deve essere un numero primo.

Problema 4
Dimostrare che la frazione $\frac{21n+4}{14n+3}$ è irriducibile per ogni numero naturale n.

Soluzione: Una frazione è irriducibile se il massimo comun divisore tra il numeratore e il denominatore è 1. Sia quindi $d = MCD(21n + 4, 14n + 3)$. Usando la proprietà $MCD(a, b) = MCD(a, a - b)$, si ha

$$d = MCD(21n+4, 14n+3) = MCD(21n+4, 7n+1) = MCD(21n+4, 1) = 1,$$

e quindi la frazione $\frac{21n+4}{14+3}$ è irriducibile.

Problema 5
Provare che due numeri di Fibonacci consecutivi sono coprimi.

Soluzione: Denotiamo con F_i l'i-esimo numero di Fibonacci. Ricordiamo che si ha $F_n = F_{n-1} + F_{n-2}$, $F_0 = 0$, $F_1 = F_2 = 1$. Procediamo per induzione. Come caso base, osserviamo che $MCD(F_0, F_1) = 1$ e $MCD(F_1, F_2) = 1$. Supponiamo ora la tesi vera per un certo N fissato, e proviamola per $N + 1$. Si ha

$$MCD(F_N, F_{N+1}) = MCD(F_N, F_{N+1} - F_N) = MCD(F_N, F_{N-1}) = 1$$

per l'ipotesi induttiva.

Problema 6
Provare che per ogni $n \geq 3$ intero positivo, esistono n divisori positivi distinti $d_1, \ldots, d_n$ di $n!$ tali che

$$d_1 + \ldots + d_n = n!.$$

Soluzione: Proveremo per induzione la seguente affermazione:

Per ogni n intero positivo, esistono n divisori positivi distinti $d_1, \ldots, d_n$ di $n!$, tali che $d_1 = 1$ e $d_1 + \ldots + d_n = n!$.

Notiamo che questa affermazione ha un'ipotesi in piú rispetto alla tesi del problema, ma ci servirá nell'induzione.

Come caso base osserviamo che per $n = 3$, si ha $d_1 = 1$ e $3! = 1 + 2 + 3$. Assumiamo ora che l'affermazione sia valida fino ad un certo intero positivo n, e proviamola per $n + 1$.

Allora si ha

$$n! = d_1 + \ldots + d_n,$$

e inoltre $d_1 = 1$. Poiché $(n+1)! = (n+1) \cdot n!$, allora si ha

$$(n+1)! = (n+1)d_1 + (n+1)d_2 + \ldots + (n+1)d_n,$$

e inoltre $(n+1)d_1 = n+1$. Poiché peró sia n che 1 sono divisori di $(n+1)!$, allora, posto $D_1 = 1$, $D_2 = n$, $D_i = (n+1)d_{i-1}$ per ogni $i = 3, \ldots, n+1$, si ha

$$(n+1)! = D_1 + D_2 + \ldots + D_{n+1}.$$

Poiché i vari d_i sono divisori di $n!$ allora i vari $D_i = (n+1)d_{i-1}$ sono divisori di $(n+1)!$ per $i = 3, \ldots, n+1$ (ricordiamo che D_1, D_2 sono divisori di $(n+1)!$). Inoltre, sempre dalla formula dei vari D_i possiamo dedurre che i vari D_i sono tra loro distinti, da cui la tesi.

Problema 7
Siano m, n interi positivi tali che $m > n$ e

$$mcm(m,n) + MCD(m,n) = m + n.$$

Provare che n divide m.

Soluzione: Ricordiamo che n divide m se e solo se $mcm(m,n) = m$. Supponiamo ora che $mcm(m,n) \neq m$. Allora $mcm(m,n)$ ha un fattore primo che m non ha: quindi possiamo dedurre che $mcm(m,n) \geq 2m$. Poiché $MCD(m,n) \geq 1$, segue

$$mcm(m,n) + MCD(m,n) \geq 2m + 1 > m + n,$$

il che contraddice le ipotesi.

Problema 8

[Cesenatico 2012]

Sia $x_1, x_2, x_3, \ldots$ la successione definita per ricorrenza come segue:

$$\begin{cases} x_1 = 4 \\ x_{n+1} = x_1 x_2 x_3 \ldots x_n + 5 \quad \textit{per } n \geq 1 \end{cases}$$

(I primi termini della successione sono quindi $x_1 = 4$, $x_2 = 9$, $x_3 = 4 \cdot 9 + 5 = 41$, ...).

Trovare tutte le coppie di interi positivi $\{a, b\}$ tali che $x_a x_b$ è un quadrato perfetto.

<u>*Soluzione*</u>: Osserviamo che per $n \geq 1$ si ha $x_1 x_2 \ldots x_{n-1} = x_n - 5$. Da questo possiamo dedurre che, se $a < b$, allora

$$MCD(x_a, x_b) = MCD(x_a, x_b - x_1 x_2 \ldots x_{b-1}) = MCD(x_a, 5),$$

quindi l'unico fattore primo in comune che potrebbe esserci tra x_a e x_b è 5. Tuttavia, osserviamo che x_1 non è divisibile per 5: proviamo che nessun x_i è divisibile per 5. Sia x_N il primo termine della successsione divisibile per 5. Allora $5 | x_N - 5$, ovvero $5 | x_1 \ldots x_{N-1}$. Poiché 5 è un numero primo, si deve avere allora $5 | x_i$ per qualche $i < N$, il che è assurdo per la scelta di N. Quindi 5 non divide nessun termine della successione x_n: da questo possiamo dedurre che $MCD(x_a, x_b) = 1$ per ogni a, b interi positivi. In particolare, $x_a x_b$ sará un quadrato perfetto se e solo se sia x_a che x_b sono quadrati perfetti.

Proviamo ora che se x_a è un quadrato perfetto allora $a = 1$ o $a = 2$. Osserviamo che x_1, x_2 sono due quadrati perfetti; sia ora $a > 2$. Allora $x_a = x_1 x_2 \ldots x_{a-1} + 5$, e poiché $3 | x_2$, considerando l'equazione modulo 3 si ottiene $x_a \equiv 2 \pmod 3$. Tuttavia, si puó verificare rapidamente che nessun quadrato perfetto è pari a 2 modulo 3: quindi gli unici quadrati perfetti sono x_1 e x_2, da cui otteniamo l'unica soluzione $\{1, 2\}$.

Problema 9

Provare che un numero composto da 2^n cifre identiche ha almeno n fattori primi.

<u>*Soluzione*</u>: Considerando il numero $D \ldots D$ composto da 2^n cifre D, si ha $D \ldots D = D \cdot 1 \ldots 1$, e quindi se provassimo che $1 \ldots 1$ ha n fattori primi allora seguirebbe la tesi per ogni numero di questo tipo.

Sia I_k il numero composto da 2^k cifre 1. Proviamo che I_k ha k fattori primi per induzione. Come caso base, osserviamo che $k = 1$ si ha $I_1 = 11$, che

ha un fattore primo. Supponiamo ora la tesi vera fino ad un certo $k-1 \in \mathbb{Z}^+$, e proviamola per k. Rappresentando in base dieci I_k, otteniamo

$$I_k = 1 \ldots 1 = 10^0 + 10^1 + \ldots + 10^{2^k-1}.$$

Osserviamo da questa rappresentazione che

$$I_k = 10^0 + 10^1 + \ldots + 10^{2^k-1} =$$
$$= (10^0 + 10^1 + \ldots + 10^{2^{k-1}-1}) + 10^{2^{k-1}} \left((10^0 + 10^1 + \ldots + 10^{2^{k-1}-1})\right) =$$
$$= (10^{2^{k-1}} + 1)I_{k-1}.$$

Tuttavia si vede sempre dalla rappresentazione in base dieci che

$$(10^{2^{k-1}} + 1) = 9I_{k-1} + 2.$$

Quindi

$$MCD(10^{2^{k-1}} + 1, I_{k-1}) = MCD(10^{2^{k-1}} + 1, 10^{2^{k-1}} + 1 - 9I_{k-1}) =$$
$$= MCD(10^{2^{k-1}} + 1, 2) = 1$$

in quanto $10^{2^{k-1}} + 1$ è dispari. Poiché i due fattori sono coprimi, allora I_k contiene almeno $k-1$ fattori primi, da I_{k-1}, più un fattore primo (distinto da quelli di I_{k-1}) di $10^{2^{k-1}} + 1$: quindi I_k ha almeno k fattori primi, da cui la tesi.

Problema 10

[Cesenatico 1999]

(a) Determinare tutte le coppie (x, k) di interi positivi che soddisfano l'equazione $3^k - 1 = x^3$.

(b) Dimostrare che per ogni intero $n > 1$, $n \neq 3$, non esiste nessuna coppia (x, k) di interi positivi che soddisfi l'equazione $3^k - 1 = x^n$.

Soluzione:

(a) Dall'equazione deduciamo $3^k = x^3 + 1 = (x+1)(x^2 - x + 1)$. Da questa scomposizione deduciamo che $(x+1)$ deve dividere 3^k, e quindi deve essere a sua volta una potenza di 3 (perché 3 è un numero primo). Quindi $x = 3^a - 1$ per qualche $a \in \mathbb{N}$. Sostituendo si ricava

$$3^k = 3^a[(3^a - 1)^2 - (3^a - 1) + 1] = 3^a(3^{2a} - 3 \cdot 3^a + 3),$$

ovvero $3^{k-a} = 3^{2a} - 3^{a+1} + 3 = 3(3^{2a-1} - 3^a + 1)$. Osserviamo che se $a > 1$ si ha $3^{2a-1} - 3^a + 1 > 1$ e inoltre $3^{2a-1} - 3^a + 1$ non è divisibile per 3, il che è una contraddizione. Allora si deve avere $a = 0$, da cui $x = 0$, che non è positivo. Se invece $a = 1$ allora si ha $x = 2$, e quindi $k = 2$, che è quindi l'unica soluzione accettabile.

(b) Facciamo due casi a seconda della paritá di n:

- Supponiamo che n sia pari. Posto $n = 2m$ e $y = x^m$ si ha $3^k - 1 = x^{2m} = y^2$. Considerando quest'ultima equazione modulo 3 si ha $y^2 \equiv -1 \pmod 3$, che (si verifica direttamente) non ha soluzioni modulo 3. Quindi in questo caso non abbiamo soluzioni.
- Supponiamo che n sia dispari. In questo caso riscriviamo tutto come

$$3^k = x^n + 1 = (x+1)(x^{n-1} - x^{n-2} + \ldots - x + 1).$$

Osserviamo che poiché tutti i divisori di 3^k sono a loro volta potenze di 3 (perché 3 è un numero primo) allora possiamo dedurre che esistono a, b interi positivi tali che

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

Sia

$$p_1(X) = X^{n-1} - X^{n+2} - \ldots - X + 1 \quad p_2(X) = (X+1).$$

Osserviamo che per il teorema di Ruffini con $X = -1$ si ha che esiste un polinomio $q(X)$ tale che $p_1(X) = q(X)p_2(X) + p_1(-1)$, e poiché n è dispari osserviamo che $p_1(-1) = (-1)^{n-1} - (-1)^{n-2} + \ldots - (-1) + 1 = 1 + 1 + \ldots + 1 = n$. Quindi $p_1(X) = q(X)p_2(X) + n$. Quindi si ha

$$MCD(3^a, 3^b) = MCD(x^{n-1} - x^{n-2} + \ldots - x + 1, x + 1) =$$
$$= MCD(p_1(x), p_2(x)) = MCD(p_1(x) - q(x)p_2(x), p_2(x)) =$$
$$= MCD(n, p_2(x)).$$

e quindi $MCD(3^a, 3^b) = MCD(n, p_2(x))$. Poiché a e b sono interi positivi, segue che 3 deve essere un divisore di questo MCD, e quindi in particolare $3|n$. Posto $n = 3m$, e $y = x^m$, l'equazione originale diventa $3^k - 1 = y^3$. Ma per il punto (a) di questo problema si ha che l'unica soluzione accettabile di questa equazione è $k = 2$, $y = 2$, da cui si ha $x^m = 2$. Ma questo implica necessariamente $x = 2, m = 1$, da cui $n = 3$, e quindi questa soluzione non è accettabile. Quindi non ci sono soluzioni.

Problema 11
Provare che l'equazione

$$(x+1)^2 + \ldots + (x+99)^2 = y^z$$

non ha soluzioni intere con $z > 1$.

Soluzione: Svolgendo i vari quadrati si ottiene

$$(x+1)^2+\ldots+(x+99)^2 = x^2+2x+1+\cdots+x^2+2\cdot 99x+99^2 =$$

$$= 99x^2+2x(1+2+\ldots+99)+(1^2+2^2+\ldots+99^2).$$

Ricordiamo che (si puó provare per induzione)

$$(1+2+\ldots+N)=\frac{N(N+1)}{2}, \quad (1^2+2^2+\ldots+N^2)=\frac{N(N+1)(2N+1)}{6},$$

da cui possiamo ricavare subito che

$$(x+1)^2+\ldots+(x+99)^2 = 99x^2+50\cdot 99x+33\cdot 50\cdot 199.$$

Osserviamo che 3 divide $99x^2+50\cdot 99x+33\cdot 50\cdot 199$, quindi y deve essere un multiplo di 3. Questo implica che 3^z deve dividere $99x^2+50\cdot 99x+33\cdot 50\cdot 199$. Ma 9 divide $99x^2$ e $50\cdot 99x$, mentre non divide $33\cdot 50\cdot 199$, quindi 9 non divide $99x^2+50\cdot 99x+33\cdot 50\cdot 199$, quindi si deve avere necessariamente $z=1$.

Problema 12

[Cesenatico 1995]

Trovare tutte le coppie di interi positivi x, y tali che

$$x^2+615=2^y.$$

Soluzione: Consideriamo l'equzione modulo 3: si ha $x^2\equiv 2^y \pmod 3$. Poiché 3 non divide 2^y e $x^2\equiv 1 \pmod 3$ se 3 non divide x, allora si deve avere che y è un intero pari. Sia $y=2k$. L'equazione diventa

$$x^2+615=(2^k)^2 \Longrightarrow (2^k-x)(2^k+x)=615.$$

Osserviamo che poiché $2^k+x>0$ allora 2^k-x deve essere positivo: quindi $0<2^k-x<2^k+x$. Poiché i divisori di $615=5*103$ sono $1,5,103,615$, dalla considerazione precedente deduciamo che si possono avere solo due casi:

1. $2^k-x=1$, $2^k+x=615$. Allora si ha $2^k=\frac{615+1}{2}=308$, ma poiché 308 non è una potenza di 2 non si hanno soluzioni.
2. $2^k-x=5$, $2^k+x=103$. Allora si ha $2^k=\frac{103+5}{2}=64$, da cui $k=6$, e quindi $y=12$. Infine da $2^k-x=5$ si ricava $x=59$.

Quindi si ricava l'unica soluzione $x=59$, $y=12$.

Problema 13
Si provi che, qualunque siano k, m, n interi non negativi, il numero $N = 4^{5k+2} + 9^{5m-1} + 5^{5n}$ è divisibile per 11.

Soluzione: Consideriamo l'espressione di N modulo 11. Osserviamo che $4 \equiv 2^2 \pmod{11}$, cosí come $9 \equiv 3^2 \pmod{11}$ e $5 \equiv 4^2 \pmod{11}$. Allora $4^{5k+2} \equiv 2^{10k+4} \equiv 2^4 \equiv 5 \pmod{11}$, mentre $9^{5m-1} \equiv 3^{10m-2} \equiv 3^8 \equiv 5 \pmod{11}$ e infine $5^{5n} \equiv 4^{10n} \equiv 1 \pmod{11}$. Sommando quindi si ha

$$N \equiv 4^{5k+2} + 9^{5m-1} + 5^{5n} \equiv 5 + 5 + 1 \equiv 0 \pmod{11}.$$

Problema 14
Sia k un intero positivo dispari, e sia n un intero positivo. Provare che

$$(1 + \ldots + n) | (1^k + \ldots + n^k).$$

Soluzione: Prima di iniziare, facciamo la seguente osservazione: Se k è un intero dispari e $M \in \mathbb{Z}^+$ un intero fissato, per ogni $i \in \mathbb{Z}$ si ha $(M-i)^k \equiv (-i)^k \equiv (-1)^k i^k \equiv -i^k \pmod{M}$, ovvero

$$i^k + (M-i)^k \equiv 0 \pmod{M} \tag{1}$$

Possiamo ricavare esplicitamente il termine a sinistra. Infatti $1+\ldots+n = \frac{n(n+1)}{2}$.

Facciamo ora due casi.

1. Se n è pari, allora consideriamo la somma $1^k + \ldots + n^k$ modulo $n+1$ e modulo $\frac{n}{2}$. Se consideriamo questa somma modulo $n+1$, accoppiando il termine i^k con $(n+1-i)^k$ otteniamo

$$1^k + \ldots + n^k \equiv$$

$$\equiv (1^k + (n)^k) + (2^k + (n-1)^k) + \ldots + \left(\left(\frac{n}{2}\right)^k + \left(\frac{n}{2}+1\right)^k \right) \pmod{n+1}.$$

Applicando ad ogni termine l'equazione 1 con $M = n+1$ si ottiene

$$1^k + \ldots + n^k \equiv 0 \pmod{n+1},$$

quindi $n+1$ divide $1^k + \ldots + n^k$.

Se invece ragioniamo modulo $\frac{n}{2}$, i termini $\frac{n}{2}$ e n spariscono; accoppiando ora il termine i^k con $(n-i)^k$ otteniamo

$$1^k + \ldots + n^k \equiv$$

$$\equiv (1^k+(n-1)^k)+(2^k+(n-2)^k)+\ldots+\left(\left(\frac{n}{2}-1\right)^k+\left(\frac{n}{2}+1\right)^k\right) \pmod{n/2}.$$

Applicando di nuovo l'equazione 1 con $M = \frac{n}{2}$ ricaviamo che $\frac{n}{2}$ divide $1^k + \ldots + n^k$: poiché $n+1$ e $\frac{n}{2}$ sono coprimi, possiamo dedurre che $\frac{n(n+1)}{2}$ divide $1^k + \ldots + n^k$, ovvero la tesi.

2. Se invece n è dispari, è sufficiente ripetere lo stesso ragionamento modulo $\frac{n+1}{2}$ e modulo n, ottenendo lo stesso risultato.

Problema 15
Trovare tutti gli interi n tali che $n! + 5$ è un cubo perfetto.

Soluzione: Osserviamo che modulo 9 si puó avere solo $x^3 \equiv -1, 0, +1 \pmod 9$. Tuttavia, se $n \geq 6$, allora $n! \equiv 0 \pmod 9$, e quindi $n! + 5 \equiv 5 \pmod 9$, e quindi $n! + 5$ non può essere un cubo perfetto. Facendo gli altri casi a mano si ricava facilmente che l'unica soluzione possibile è $n = 5$, per cui si ha $5! + 5 = 5^3$.

Problema 16
[Cesenatico 2006]
Determinare tutti i valori di m, n, p tali che

$$p^n + 144 = m^2,$$

dove m ed n sono interi positivi e p è un numero primo.

Soluzione: Riscriviamo l'equazione come

$$m^2 - 144 = p^n \Longrightarrow (m-12)(m+12) = p^n.$$

Poiché p è un numero primo, questo implica che sia $(m-12)$ che $(m+12)$ devono essere potenze di p. Quindi si ha che esistono x, y numeri naturali tali che $m - 12 = p^x$ e $m + 12 = p^y$ (osserviamo che $x < y$), da cui segue che

$$p^y - p^x = (m+12) - (m-12) = 24 \Longrightarrow p^x(p^{y-x} - 1) = 24.$$

Facciamo ora due casi:

1. Se $x = 0$ allora segue $p^y - 1 = 24$, da cui $p^y = 25$, che implica per sostituzione $p = 5$, $y = 2$, $m = 13$, $n = 2$.

2. Se $x > 0$ allora p^x è un divisore proprio (perché 24 non è la potenza di un numero primo) di 24, e poiché $24 = 2^3 \cdot 3$ si deve avere $p = 2$ oppure $p = 3$. Se $p = 2$ allora $p^{y-x} - 1$ è un divisore dispari di 24 maggiore di p^x (e quindi maggiore di 1): da questo ricaviamo che $p^{y-x} - 1 = 3$, e quindi $p^x = 8$, da cui segue che $x = 3$ e $y = 5$. Sostituendo $m - 12 = p^x$ si ottiene $m = 20$, e sostituendo in $(m-12)(m+12) = 8 \cdot 32 = 256$, da cui si ottiene $n = 8$. Resta il caso $p = 3$. Allora p^x è un divisore proprio di 24 multiplo di 3: quindi $p^x = 3$, da cui $x = 1$. Allora $m - 12 = p^x$ restituisce $m = 15$, e $m + 12 = 27 = p^y$, da cui $(m-12)(m+12) = 3 \cdot 27 = 81$, da cui $p^n = 81$, e quindi $n = 4$.

Quindi le uniche soluzioni $m = 13, n = 2, p = 5$, $m = 15, n = 4, p = 3$ e $m = 20, n = 8, p = 2$.

Problema 17
Sia p un numero primo. Provare che esistono infiniti interi positivi n tali che p divida $2^n - n$.

Soluzione: Cerchiamo un numero naturale n che sia congruo a 1 modulo p, tale che $2^n \equiv 1 \pmod{p}$: un tale n soddisferà la nostra tesi. Un n siffatto è una soluzione del seguente sistema:

$$\begin{cases} x \equiv 0 & (\text{mod } p-1) \\ x \equiv 1 & (\text{mod } p) \end{cases}$$

Poiché i moduli $p-1$ e p sono coprimi, allora per il Teorema Cinese del Resto questo sistema avrà soluzione modulo $p(p-1)$: quindi, esisteranno infiniti numeri naturali che soddisfano questo sistema, da cui la tesi.

Problema 18
Sia p è un numero primo, $p \equiv 3 \pmod{4}$.
Trovare le soluzioni (x, y, z, t) dell'equazione diofantea

$$x^2 + y^2 = p(z^2 + t^2).$$

Soluzione: Osserviamo che $(0, 0, 0, 0)$ è una soluzione dell'equazione diofantea. Sia ora (x, y, z, t) una soluzione di questa equazione tale che $(x, y, z, t) \neq (0, 0, 0, 0)$. Osserviamo che se p divide x o y, allora p deve dividere entrambi. Quindi scrivendo $x = px_1$ e $y = py_1$, si ha

$$x^2 + y^2 = p(z^2 + t^2) \Longrightarrow p(x_1^2 + y_1^2) = z^2 + t^2,$$

e quindi se (x, y, z, t) è una soluzione dell'equazione e p divide uno tra x e y allora $(z, t, \frac{x}{p}, \frac{y}{p}) \neq (0, 0, 0, 0)$ è una soluzione di questa equazione. Quindi,

per discesa infinita, deve esistere una soluzione minima (x, y, z, t) della nostra equazione tale che p non divide né x né y (se ne divide uno allora divide anche l'altro, e quindi si ricade nel caso precedente). In questo caso consideriamo l'equazione modulo p, ottenendo

$$x^2 + y^2 \equiv 0 \pmod{p} \Longrightarrow x^2 \equiv -y^2 \pmod{p}.$$

Sia ora $d = \frac{p-1}{2}$. Poiché $p \equiv 3 \pmod 4$ allora d è dispari, e $2d = p - 1$. Allora elevando ambo i membri alla d si ottiene

$$(x^2)^d \equiv (-y^2)^d \pmod{p} \Longrightarrow x^{p-1} \equiv (-1)^d y^{p-1} \pmod{p}$$

e quindi per il Piccolo Teorema di Fermat segue che $1 \equiv -1 \pmod p$ il che è un assurdo. Quindi l'unica soluzione è $(x, y, z, t) = (0, 0, 0, 0)$.

Problema 19
Sia p un numero primo, e sia a tale che $a^3 \equiv 1 \pmod p$, $a \not\equiv 1 \pmod p$. Provare che

$$(1 + a)^6 \equiv 1 \pmod{p}.$$

Soluzione: Osserviamo che $a^3 - 1 \equiv (a - 1)(a^2 + a + 1) \pmod p$, e poiché $a \not\equiv 1 \pmod p$ ricaviamo che $a^2 + a + 1 \equiv 0 \pmod p$, ovvero $1 + a \equiv -a^2 \pmod p$. Quindi $(1 + a)^6 \equiv (-a^2)^6 \equiv a^{12} \equiv 1 \pmod p$.

Problema 20
Dimostrare che per ogni primo $p > 3$ il numero $9^p - 8^p - 1$ è divisibile per 73.

Soluzione: Notiamo che $8 \equiv 9^2 \pmod{73}$. Quindi

$$9^p - 8^p - 1 \equiv 9^p - 9^{2p} - 1 \equiv -(9^{2p} - 9^p + 1) \pmod{73}.$$

Ricordiamo dalle scomposizioni notevoli che $9^{2p} - 9^p + 1 = \frac{9^{3p}+1}{9^p+1}$; tuttavia, per trasportare questa frazione modulo p ci serve che $9^p + 1 \not\equiv 0 \pmod{73}$. Calcolando le potenze di 9 modulo 73 (sono sei in tutto) osserviamo che si ha $9^p + 1 \equiv 0 \pmod{73}$ se e solo se $p \equiv 3 \pmod 6$. In questo caso quindi 3 divide p. Ma poiché p è un numero primo allora l'unica possibilitá sarebbe $p = 3$. In conclusione, per ogni primo $p > 3$ si ha $9^p + 1 \not\equiv 0 \pmod{73}$, e quindi

$$9^p - 8^p - 1 \equiv 9^p - 9^{2p} - 1 \equiv -(9^{2p} - 9^p + 1) \equiv \frac{9^{3p} + 1}{9^p + 1} \equiv \frac{729^p + 1}{9^p + 1} \equiv 0 \pmod{73}$$

e quindi il numero $9^p - 8^p - 1$ è divisibile per 73.

Problema 21

[Cesenatico 2008]

Determinare tutte le terne (a, b, c) di numeri interi maggiori di zero tali che

$$a^2 + 2^{b+1} = 3^c.$$

Soluzione: Poiché 3^c è sempre dispari, mentre 2^{b+1} è sempre pari in quanto $b \geq 1$, allora a deve essere un intero dispari. Quindi possiamo scrivere $a = 2k+1$, con $k \in \mathbb{N}$, e sviluppando otteniamo $a^2 = 4k^2+4k+1$, da cui ricaviamo che $a^2 \equiv 1 \pmod 4$. Inoltre, essendo $b + 1 \geq 2$, possiamo ricavare che 2^{b+1} è un multiplo di 4, quindi considerando l'equazione modulo 4 ricaviamo che $3^c \equiv 1 \pmod 4$, e si verifica che questo accade se e solo se c è pari. Sia quindi $c = 2h$, con $h \in \mathbb{N}$. Allora

$$a^2 + 2^{b+1} = 3^c \Longrightarrow 2^{b+1} = 3^{2h} - a^2 \Longrightarrow 2^{b+1} = (3^h - a)(3^h + a).$$

Poiché $3^h - a$ e $3^h + a$ dividono entrambi 2^{b+1} segue (perché 2 è un numero primo) che entrambi devono essere potenze di 2, quindi devono esistere $x, y \in \mathbb{N}$ tali che $3^h - a = 2^x$, $3^h + a = 2^y$. Osserviamo che in quanto $a > 0$ allora $2^x < 2^y$ e quindi $x < y$. Notiamo che da $x < y$ ricaviamo che $MCD(3^h - a, 3^h + a) = MCD(2^x, 2^y) = 2^x$. Ma per una proprietá del massimo comun divisore si ha $MCD(3^h - a, 3^h + a) = MCD(3^h - a, 3^h + a - 3^h + a) = MCD(3^h - a, 2a)$. Ma poiché a è dispari, allora da $MCD(3^h - a, 2a) = 2^x$ segue che $MCD(3^h - a, 2a)$ puó essere solo 1 o 2, e quindi $3^h - a = 1$ oppure $3^h - a = 2$. Ma essendo a dispari, segue che $3^h - a$ è pari, quindi possiamo concludere che si deve avere $3^h - a = 2$. Quindi $3^h - a = 2$, $3^h + a = 2^b$, da cui ricaviamo che $3^h = \frac{2^b+2}{2}$, ovvero $3^h = 2^{b-1} + 1$. Consideriamo ora l'equazione $3^h = 2^{b-1} + 1$, ovvero $2^{b-1} = 3^h - 1$. Facciamo dei casi:

1. Calcolando a mano le soluzioni per $b = 1$ e $b = 2$ si ottiene una soluzione per $b = 2$: in questo caso si ha $h = 1$, e sostituendo in $3^h + a = 2^b$ restituisce $a = 1$, e quindi nell'equazione del testo otteniamo la soluzione $a = 1, b = 2, c = 2$.

2. Se $b \geq 3$ allora $2^{b-1} \equiv 0 \pmod 4$, e quindi $3^h \equiv 1 \pmod 4$, che, come abbiamo giá visto in questo stesso esercizio, implica che h è pari. Allora, posto $h = 2h'$, si ha $2^{b-1} = (3^{h'} - 1)(3^{h'} + 1)$, e quindi ragionando come prima si deve avere che sia $3^{h'} - 1$ che $3^{h'} + 1$ devono essere potenze di 2: poichpéró questi due numeri non possono essere entrambi divisibili per 4, questo si puó avere solo nei seguenti casi:

   - $3^{h'} - 1 = 1$, che porta chiaramente ad un assurdo.

- $3^{h'} - 1 = 2$, ovvero $3^{h'} = 3$. Quindi $h' = 1$, da cui segue $h = 2$. Sostituendo in $3^h = 2^{b-1} + 1$ si ha $2^{b-1} = 8$, da cui $b = 4$. Sostituendo ora in $3^h + a = 2^b$ si ricava $a = 7$, e quindi sostituendo il tutto nell'equazione principale si ricava $7^2 + 2^5 = 3^c$, da cui $3^c = 81$: otteniamo quindi la soluzione $a = 7, b = 4, c = 4$.

Le uniche soluzioni sono quindi $(1, 2, 2)$ e $(7, 4, 4)$.

Problema 22

Sia a un intero positivo pari, e siano m, n due interi positivi tali che $m < n$.

1. *Provare che $MCD(a^{2^m} + 1, a^{2^n} + 1) = 1$.*

2. *Dedurre da questo che esistono infiniti numeri primi.*

Soluzione:

1. Iniziamo osservando che per ogni intero positivo k si ha

$$a^{2^{k+1}} - 1 = (a^{2^k} - 1)(a^{2^k} + 1).$$

Quindi per ogni intero positivo k, $a^{2^k} - 1 | a^{2^{k+1}} - 1$ e $a^{2^k} + 1 | a^{2^{k+1}} - 1$. Reiterando questo ragionamento per ogni k compreso tra m e n, possiamo dedurre che se $m < n$ allora $a^{2^m} + 1 | a^{2^n} - 1$, ovvero $a^{2^n} - 1 = \lambda(a^{2^m} + 1)$ per qualche λ intero positivo. Quindi

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

$$= MCD(a^{2^n} + 1, 2) = 1$$

in quanto $a^{2^n} + 1$ è dispari.

2. Consideriamo la successione $x_1, x_2, \ldots$ definita come $x_i = a^{2^i} + 1$ per ogni $i \geq 1$. Per il punto 1, due termini della successione non hanno nessun fattore primo in comune: quindi per ogni i esisterá un numero primo p_i che divide solo x_i. Per definizione, i vari p_i sono distinti: quindi poiché la successione è infinita anche i numeri primi devono essere in numero infinito.

Problema 23

Sia $n \geq 2$ un intero positivo, e siano $1 = d_1 < d_2 < \ldots < d_k = n$ i suoi divisori positivi. Sia $S = d_1d_2 + d_2d_3 + d_3d_4 + \ldots + d_{k-1}d_k$.

Provare che:

1. *$S < n^2$.*

2. *S divide n^2 se e solo se n è un numero primo.*

<u>*Soluzione*</u>*:* Osserviamo che se d è un divisore di n, anche $\frac{n}{d}$ lo è. In particolare, se osserviamo la sequenza ordinata dei divisori, notiamo che $d_k = \frac{n}{d_1}$, e piú in genere $d_{k+1-i} = \frac{n}{d_i}$. Inoltre notiamo che

$$\frac{1}{d_i d_{i+1}} \leq \frac{d_{i+1} - d_i}{d_i d_{i+1}} = \frac{1}{d_i} - \frac{1}{d_{i+1}}.$$

Quindi

$$S = d_1d_2 + d_2d_3 + \ldots + d_{k-1}d_k = \frac{n}{d_k}\frac{n}{d_{k-1}} + \frac{n}{d_{k-1}}\frac{n}{d_{k-2}} + \ldots + \frac{n}{d_2}\frac{n}{d_1} =$$

$$= n^2\left(\frac{1}{d_k d_{k-1}} + \frac{1}{d_{k-1}d_{k-2}} + \ldots + \frac{1}{d_2 d_1}\right) \leq$$

$$\leq n^2\left(\left(\frac{1}{d_{k-1}} - \frac{1}{d_k}\right) + \left(\frac{1}{d_{k-2}} - \frac{1}{d_{k-1}}\right) + \ldots + \left(\frac{1}{d_1} - \frac{1}{d_2}\right)\right) = n^2\left(\frac{1}{d_1} - \frac{1}{d_k}\right),$$

quindi poiché $\frac{1}{d_1} < 1$ si ricava che $S < n^2$.

Per il secondo punto, osserviamo che se n è un numero primo allora $d_1 = 1$, $d_2 = n$, e $S = d_1d_2 = n$ divide n^2. Se invece n non è un numero primo, sia $p < n$ il piú piccolo numero primo che divide n. Osserviamo che p è anche il piú piccolo primo che divide n^2, e inoltre si ha $k > 2$, $d_k = n$ e $d_{k-1} = \frac{n}{p}$. Per definizione $S > d_{k-1}d_k = \frac{n^2}{p}$: quindi S è un intero positivo compreso tra $\frac{n^2}{p}$ e n^2. Supponiamo per assurdo che S divide n^2. Allora $\frac{n^2}{S} < p$ è un divisore di n^2 minore di p, il che è assurdo. Quindi se n non è un numero primo S non puó dividere n^2.

Problema 24

Sia N un intero positivo tale che

$$N^5 = 21^5 + 23^5 + 37^5 + 79^5 + 84^5.$$

Determinare N.

Soluzione: Dall'equazione possiamo subito ricavare che $N \geq 85$, e inoltre

$$N^5 = 21^5 + 23^5 + 37^5 + 79^5 + 84^5 < 5 \cdot 84^5 < (84 \cdot 2)^5 = 168^5,$$

quindi $N < 168$. Studiamo questa equazione in vari moduli:

1. Modulo 2 osserviamo solo che ogni potenza di un numero dispari è ancora un numero dispari, e ogni potenza di un numero pari è ancora un numero pari. Quindi si ha

   $$N^5 \equiv 1 + 1 + 1 + 1 + 0 \equiv 0 \pmod 2,$$

   da cui 2 divide N^5, e di conseguenza 2 divide N.

2. Modulo 3 si ha $N^5 \equiv 0^5 + 2^5 + 1^5 + 1^5 + 0^5 \equiv 1^5 + 1^5 + 2^5 \pmod 3$, e poiché $1^5 \equiv 1 \pmod 3$ e $2^5 \equiv 2 \pmod 3$ si ricava $N^5 \equiv 1 \pmod 5$, da cui, sempre per le stesse considerazioni, otteniamo $N \equiv 1 \pmod 3$.

3. Modulo 5, per il Piccolo Teorema di Fermat sappiamo che $a^5 \equiv a \pmod 5$ per ogni a, quindi

   $$N^5 \equiv 1 + 3 + 2 + 4 + 4 \equiv 4 \pmod 5,$$

   da cui, applicando di nuovo il Piccolo Teorema di Fermat, otteniamo $N \equiv 4 \pmod 5$.

4. Infine, modulo 7 notiamo che $23 \equiv 37 \equiv 79 \equiv 2 \pmod 7$, mentre 21 e 84 sono multipli di 7. Allora

   $$N^5 \equiv 2^5 + 2^5 + 2^5 \equiv 32 + 32 + 32 \equiv 5 \pmod 7.$$

   Svolgendo le potenze modulo 7 otteniamo

   $$1^5 \equiv 1, 2^5 \equiv 4, 3^5 \equiv 5, 4^5 \equiv 2, 5^5 \equiv 3, 6^5 \equiv 6 \pmod 7,$$

   quindi possiamo osservare che dovremmo avere $N \equiv 3 \pmod 7$.

Combinando tutti questi dati otteniamo il sistema

$$\begin{cases} N \equiv 0 & \pmod 2 \\ N \equiv 1 & \pmod 3 \\ N \equiv 4 & \pmod 5 \\ N \equiv 3 & \pmod 7 \end{cases}$$

Poiché i moduli sono coprimi, per il Teorema Cinese del Resto vi sono soluzioni di questo sistema modulo $2 \cdot 3 \cdot 5 \cdot 7 = 210$; svolgendo i conti, si deve ottenere $N \equiv 94 \pmod{210}$. Poiché inoltre $85 \leq N < 168$, osserviamo che l'unica soluzione possibile è $N = 94$.