Lezione 3 - Teoria dei Numeri

Problema 1 *Determinare il più piccolo numero primo p che divide $Q(n) = n^2 + n + 23$ per qualche n intero.*

Soluzione: Osserviamo che $Q(1) = 25$, quindi p può essere 2, 3 oppure 5. Banalmente p non può essere 2 perché $Q(n)$ è dispari. Non può neanche essere 3 poiché $Q(n)$ modulo 3 è congruo a 1 o a 2. La soluzione è dunque $p = 5$.

Problema 2 *Dati tre numeri consecutivi x,y,z, dimostrare che $x^3 + y^3 + z^3$ è un multiplo di 9.*

Soluzione: Dato che i residui cubici modulo 9 sono $-1, 0$ e 1 e i tre numeri sono consecutivi, $x^3 + y^3 + z^3$ è congruo a $-1 + 0 + 1 = 0$.

Problema 3 *Quante coppie ordinate di numeri interi (x, y) soddisfano l'equazione $\sqrt{x} + \sqrt{y} = \sqrt{1998}$?*

Soluzione: Banalmente, x e y devono essere positivi. Elevando al quadrato entrambi i membri dell'equazione scritta come $\sqrt{y} = \sqrt{1998} - \sqrt{x}$ si ottiene $y = 1998 + x - 2\sqrt{1998x}$, ma poiché y è intero, allora anche $\sqrt{1998x}$ deve essere intero. Essendo $1998 = 2 \cdot 3^3 \cdot 37$, allora x deve essere della forma $x = 2 \cdot 3 \cdot 37 \cdot h^2$. Si verifica facilmente che gli unici valori di h per cui sia $\sqrt{1998} - \sqrt{x}$ che $\sqrt{1998} - \sqrt{y}$ sono positivi sono $h = 1$ e $h = 2$. Allora le uniche due coppie (x, y) sono $(222, 888)$ e $(888, 222)$.

Problema 4 *Dimostra che la somma di 9999 quadrati consecutivi non può essere un quadrato perfetto.*

Soluzione: Si tratta di dimostrare che l'equazione

$$(n-4999)^2 + \ldots + (n-1)^2 + n^2 + (n+1)^2 + \ldots + (n+4999)^2 = h^2$$

non ha soluzioni. Sviluppando i quadrati:

$$9999n^2 + 2\sum_{i=1}^{4999} i^2 = h^2$$

$$9999n^2 + 2\frac{(4999)(5000)(9999)}{6} = h^2$$

$$9999n^2 + (4999)(5000)(3333) = h^2.$$

Allora $3 \mid h \Rightarrow 9 \mid h^2$, ma 9 non divide il primo membro, assurdo.

Problema 5 *(Test di Ammissione Scuola Superiore di Catania 2011-12) Determinare il numero di interi positivi con le seguenti proprietà:*

- *hanno al più 1000 cifre;*
- *sono divisibili per 9;*
- *hanno almeno due cifre 9.*

Soluzione: Gli interi positivi con al più 1000 cifre sono 10^{1000}. Quelli divisibili per 9 hanno la caratteristica che la somma delle loro cifre è anche divisibile per 9. Dato un numero con $n < 1000$ cifre, basta aggiungere a sinistra $1000 - n$ zeri, cosicchè tutti i numeri fino a 1000 cifre possono essere visti come l'insieme X dei numeri rappresentati delle stringhe di 1000 simboli scelti nell'insieme delle 10 cifre. I numeri di X che sono divisibili per 9 formano un insieme Y di cardinalità pari a:

$$\frac{10^{1000} - 1}{9} + 1.$$

Fissato k $(0 \leq k \leq 1000)$, denotiamo con A_k l'insieme dei numeri di Y che contengono esattamente k cifre 9. Poiché gli insiemi A_0 e A_1 sono disgiunti, la risposta che cerchiamo sarà data dalla differenza tra la cardinalità di Y e la somma delle cardinalità di A_0 e A_1.
I numeri di A_0 possono essere costruiti nel seguente modo. Prima si formano tutte le stringhe

$$c_1 c_2 c_3 \cdots c_{998} c_{999}$$

dove c_i $(1 \leq i \leq 999)$ sono cifre dell'insieme $\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$ e si aggiunge la cifra c_{1000} così costruita:

$$c_{1000} = 9 - r, \text{ con } r = \sum_{i=1}^{999} c_i \,(\text{mod } 9).$$

La cardinalità di A_0 è quindi 9999. Per costruire A_1 proseguiamo nel seguente modo: costruiamo tutti i numeri di 999 cifre divisibili per 9 e che non contengono alcuna cifra 9 (questi sono 9998). Per ogni siffatto numero di A_0 inseriamo una cifra 9 o a sinistra della prima cifra, o a destra dell'ultima cifra o tra due cifre consecutive (questa cosa si può fare in 1000 modi diversi). Per questo motivo la cardinalità di A_1 sarà pari a $1000 \cdot 9^{998}$. Pertanto la risposta è

$$\begin{aligned} &\frac{10^{1000} - 1}{9} + 1 - 9^{999} - 1000 \cdot 9^{998} = \\ &= \frac{10^{1000} - 1 + 9 - 9^{1000} - 1000 \cdot 9^{999}}{9} = \\ &= \frac{10^{1000} + 8 - 1009 \cdot 9^{999}}{9}. \end{aligned}$$

Problema 6 *Dimostra che, dato un polinomio a coefficienti interi, se la somma dei coefficienti è dispari e il termine noto è dispari allora il polinomio non ha radici intere.*

Soluzione: Sia $p(x) = a_n x^n + \ldots + a_1 x + a_0$ un polinomio a coefficienti interi. Dalle ipotesi abbiamo che sia $p(0)$ che $p(1)$ sono dispari. Supponiamo per assurdo che esista una soluzione α:

- Se α è pari, $\alpha = 2t$ per qualche t. Si ha $p(2t) = a_n(2t)^n + \ldots + a_1 2t + a_0$ che è la somma di n termini pari e uno dispari, quindi è dispari e non può essere 0.
- Se α è dispari, $\alpha = 2t+1$ per qualche t. Si ha $p(2t+1) = a_n(2t+1)^n + \ldots + a_1(2t+1) + a_0$ che ha la stessa parità di $a_n + \ldots + a_1 + a_0 = p(1)$, che è dispari e non può essere 0.

Problema 7 *Siano $a, b, c, \in \mathbb{Z}$ non nulli tali che $a^2 + b^2 = c^2$. Dimostra che abc è divisibile per* 60.

Soluzione:

- I quadrati modulo 3 sono solo 0 o 1. Supponiamo per assurdo che nessuno tra a, b, c sia divisibile per 3. L'unico caso che rimane è $1+1 \equiv 1 \pmod 3$, assurdo.
- Necessariamente, esattamente uno tra a, b, c deve essere pari oppure a, b, c sono tutti pari. In quest'ultimo caso, il prodotto è divisibile per 8. Consideriamo allora il primo caso, supponendo ad esempio che solo a sia pari. Supponiamo per assurdo che a non sia divisibile per 4. Allora $\bmod 8$ si ha $4 + 1 \equiv 1$, assurdo.
- I quadrati modulo 5 sono solo 0, 1 e -1. Supponiamo per assurdo che nessuno tra a, b, c sia divisibile per 5. Allora si dovrebbe avere $\pm 1 \pm 1 = \pm 1$, assurdo.

Dunque uno tra a, b, c è divisibile per 3, uno per 4, e uno per 5. Dunque il prodotto abc è divisibile per $3 \cdot 4 \cdot 5 = 60$.

Problema 8 *Sia $f(x) = x^2 - x$, dimostrare che l'equazione $4f(a) = f(b)$ non ha soluzione per a, b interi positivi.*

Soluzione: Dobbiamo dimostrare che $4a^2 + 4a - b^2 - b = 0$ è impossibile. Risolvendo l'equazione di secondo grado per a otteniamo un determinante pari a $16(b^2 + b + 1)$. Se esistessero soluzioni intere allora $b^2 + b + 1$ dovrebbe essere un quadrato per qualche b. Notiamo però che per ogni intero positivo n, $n^2 < n^2 + n + 1 < (n + 1)^2$, quindi $b^2 + b + 1$ non può essere un quadrato perfetto.

Problema 9 *Risolvere l'equazione $5x^2 - 6xy + 7y^2 = 383$ in $\mathbb{Z}$.*

Soluzione: Riscrivendo l'equazione come $(x - y)^2 + (2x - y)^2 + 5y^2 = 383$, deduciamo che $y^2 \leq \frac{383}{5}$, allora $y \in [-8, 8]$. Risolvendo secondo la x la diofantea come se fosse un'equazione di secondo grado, otteniamo $\Delta = 7660 - 104y^2$. Analizzando l'espressione $\bmod 3$, notiamo che il Δ è un quadrato perfetto se e solo se $y \equiv 0 \pmod 3$, quindi i valori ammissibili per y sono $-6, -3, 0, 3, 6$.
Sostituendo ricaviamo che le uniche coppie (x, y) di soluzioni possibili sono $(10, 3)$ e $(-10, -3)$.

Problema 10 *Risolvere per tutti gli interi non negativi x, y l'equazione $x^3 + 7x^2 + 35x + 27 = y^3$.*

Soluzione: Osserviamo subito che $y > x$. Poniamo quindi $y = x + k$ con k intero positivo e riscriviamo l'equazione come $(3k-7)x^2+(3k^2-35)x+(k^3-27) = 0$. Ovviamente affinché l'equazione abbia soluzione dobbiamo evitare che tutti i termini a sinistra siano positivi, quindi è necessaria la condizione $k \leq 3$.
Controlliamo a mano i casi $k = 1, k = 2, k = 3$ e otteniamo facilmente che le uniche soluzioni sono $x = 0, y = 3$ e $x = 4, y = 7$.

Problema 11 *Trova tutte le coppie ordinate (a, b) di interi positivi che soddisfano l'equazione $ab + 63 = 20 \cdot mcm(a, b) + 12 \cdot MCD(a, b)$.*

Soluzione: Sapendo che $\text{MCD}(a, b) \cdot \text{mcm}(a, b) = ab$, ponendo $x = \text{mcm}(a, b)$ e $y = \text{MCD}(a, b)$, l'equazione diventa $xy+63 = 20x+12y$. Mediante semplici passaggi algebrici si ottiene:

$$xy - 20x - 12y + 63 = 0$$

$$xy - 20x - 12y + 240 - 240 + 63 = 0$$

$$(x - 12)(y - 20) = 177$$

. Poiché $177 = 3 \cdot 59$ e $x > y$, abbiamo due possibilità:

- $x - 12 = 59$ e $y - 20 = 3 \Rightarrow x = 71$ e $y = 23$, che è incompatibile con qualsiasi scelta di a e b;
- $x-12 = 177$ e $y-20 = 1 \Rightarrow x = 189$ e $y = 21$, da cui $a = 189$ e $b = 21$ o viceversa.

Problema 12 *Dato un intero positivo n e tre cifre non nulle a, b, c, sia A_n l'intero formato da n cifre uguali ad a, B_n l'intero formato da n cifre uguali ad b, e C_n l'intero formato da $2n$ cifre uguali ad c. Qual è il massimo valore di $a + b + c$ per cui esistono almeno due valori distinti di n tali che $C_n - B_n = A_n^2$?*

Soluzione: Osserviamo che $A_n = a(1 + 10 + \ldots + 10^{n-1}) = a \cdot \frac{10^n-1}{9}$. Allo stesso modo $B_n = b \cdot \frac{10^n-1}{9}$ e $C_n = c \cdot \frac{10^{2n}-1}{9}$. La relazione $C_n - B_n = A_n^2$ si può allora scrivere come

$$c \cdot \frac{10^{2n}-1}{9} - b \cdot \frac{10^n-1}{9} = a \cdot \left(\frac{10^n-1}{9}\right)^2.$$

Poiché $n > 0$, $10^n > 1$ e possiamo semplificare un fattore $\frac{10^n-1}{9}$ per ottenere:

$$c \cdot (10^n + 1) - b = a^2 \cdot \frac{10^n-1}{9}.$$

Trattandosi di un'equazione lineare in 10^n, se due valori distinti di n soddisfano l'equazione, allora tutti i valori di n la soddisfano. Affinché il primo membro sia uguale al secondo, si deve avere $c = \frac{a^2}{9}$ e $b = \frac{2a^2}{9}$. Si deve allora massimizzare la quantità $a+b+c = a+\frac{a^2}{3}$, ovvero a. Poiché b e c sono interi, a dev'essere un multiplo di 3. Tuttavia se $a = 9$, $b = 18$ che contraddice $b \leq 9$. Allora $a = 6$, $b = 8$ e $c = 4$ danno il massimo valore $a + b + c = 18$.

Problema 13 *Quanti numeri naturali a quattro cifre abcd, con $a \neq 0$, sono tali che i tre numeri a due cifre $ab < bc < cd$ formino una successione aritmetica crescente? Esempio: 4692 soddisfa le ipotesi poiché $46, 69, 92$ sono in successione aritmetica.*

Soluzione: Si noti che $a \leq b \leq c$. I numeri $10a + b$,$10b + c$ e $10c + d$ devono essere in successione aritmetica. Affinché ciò si verifichi, si deve avere $(10c+d)-(10b+c) = (10b+c)-(10a+b)$, ovvero $10(c-2b+a) = 2c-b-d$. Poiché il primo membro è multiplo di 10, si hanno tre possibilità per il secondo membro:

- $2c - b - d = -10 \Rightarrow$ l'ipotesi $a \leq b \leq c$ viene contraddetta.
- $2c - b - d = 0 \Rightarrow c - 2b + a = 0$. Ciò significa che le stesse cifre sono in successione aritmetica: si ottengono le 9 soluzioni 1234, 1357, 2345, 2468, 3456, 3579, 4567, 5678, 6789.
- $2c - b - d = 10 \Rightarrow c - 2b + a = 1$.

Problema 14 *Trova le soluzioni intere non negative (x, y, k) dell'equazione $x^4 - y^4 = 2^k$.*

Soluzione: Scomponendo il primo membro si ottiene $(x^2+y^2)(x+y)(x-y)=2^k$, ovvero esistono $a,b,c\in\mathbb{N}$ tali che

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

Dalle prime due equazioni si ottiene $x=2^{a-1}+2^{b-1}$, $y=2^{a-1}-2^{b-1}$. Sostituendo nella terza equazione:

$$2^{2a-1}+2^{2b-1}=2^c$$

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

Notiamo che il primo membro deve essere una potenza di 2, ma $(2^{2a-2b}+1)$ è dispari oppure è uguale a 2. Allora necessariamente $2^{2a-2b}+1=2\Rightarrow 2a-2b=0\Rightarrow a=b$, ovvero $x+y=x-y$. Allora le uniche soluzioni possibili sono quelle con $y=0$, cioè tutte quelle del tipo $(2^{k'},0,4k')$ al variare di k' in $\mathbb{N}$.

Problema 15 *Trova le soluzioni dell'equazione*

$$2^z+2=r^2$$

con $z\in\mathbb{Z}$ *e* $r\in\mathbb{Q}$.

Soluzione: Poniamo $r=\frac{p}{q}$ dove p e q sono due interi coprimi. L'equazione diventa $q^2 2^z+2q^2=p^2$. Distinguiamo i seguenti casi:

- $z>0$. Scriviamo l'equazione come $2(2^{z-1}+1)q^2=p^2$. Notiamo che affinché il primo membro sia un quadrato perfetto, deve esserlo anche $2(2^{z-1}+1)$. Allora $(2^{z-1}+1)$ deve contenere un fattore 2 e ciò è possibile solo se $z-1=0$. Effettivamente sostituendo si trova due prime coppie di soluzioni (z,r) date da $(1,\pm 2)$.
- $z=0$. Si ha $r=\sqrt{3}\notin\mathbb{Q}$.
- $z<0$. Poniamo $z=-x$. L'equazione diventa $q^2 2^{-x}+2q^2=p^2$, moltiplicando per 2^x otteniamo $q^2+2^{x+1}q^2=2^x p^2$, quindi $2^x \mid q^2$, adesso consideriamo due casi:
  - $x=2k$ pari, allora $2^k \mid q=2^k q_1$, quindi $q_1^2+2q^2=p^2$. Dunque q_1 divide p, ma divide anche q, da cui necessariamente $q_1=1$. Risulta $q=2^k$, quindi otteniamo $p^2=2^{2k+1}+1$, cioè $(p-1)(p+1)=2^{2k+1}$,

in altri termini $p+1$ e $p-1$ sono due potenze 2 che differiscono di 2 e ciò accade solo con 2^1, 2^2, dunque $p = \pm 3$, $q = \pm 2$, ottenendo $r = \pm\frac{3}{2}$.

- se $x = 2k+1$ dispari allora $2^{k+1} \mid q = 2^{k+1}q_1$. Otteniamo $2q_1^2 + 2^{2k+3}q_1^2 = p^2$, quindi $q_1 \mid p$, il che vuol dire $q_1 = 1 \Rightarrow 2^{2k+3}+2 = p^2$, il che è impossibile (modulo 4), quindi in questo caso non ci sono soluzioni.

Problema 16 *Dimostra che $2^n + 3^n$, con $n \in \mathbb{Z}$, non può essere il quadrato di un numero razionale.*

Soluzione: Distinguiamo tre casi. Se n è positivo, dimostriamo che $2^n + 3^n = x^2$ non ha soluzioni intere. In $\mathbb{Z}_3$ l'espressione diventa $2^n = x^2$. Poiché un quadrato mod 3 può essere soltanto 1 o 0 e 3 non divide 2^n, deve essere $2^n \equiv 1 \pmod 3$, da cui si vede facilmente che n è pari. Allora si può porre $n = 2k$ e l'espressione diventa $4^k + 9^k = x^2$. Considerando l'equazione mod 5, si hanno due possibilità: $1 + 1 \equiv x^2$ oppure $-1 - 1 \equiv x^2$, ma x^2 può essere congruo soltanto a -1, 0 o 1.

Il caso $n = 0$ conduce a $x^2 = 2$, impossibile.

Per il caso in cui $n < 0$, poniamo $m = -n$. L'equazione diventa

$$\frac{1}{2^m} + \frac{1}{3^m} = \frac{p^2}{q^2}$$

con $MCD(p, q) = 1$. Riscriviamola come $(2^m + 3^m)q^2 = 6^m p^2$. Notiamo che, poiché p e q sono coprimi, si deve avere $q^2 \mid 6^m$, ovvero $q^2 = 2^a \cdot 3^b$ con $a, b \leq m$. Naturalmente, essendo q^2 un quadrato, a e b devono essere pari. Allora

$$p^2 = \frac{(2^m + 3^m)}{2^{m-a} \cdot 3^{m-b}} \;\Rightarrow\; 2^m + 3^m = 2^{m-a} \cdot 3^{m-b} \cdot p^2.$$

Abbiamo che $m - a$ e $m - b$ sono entrambi pari o entrambi dispari. Se sono entrambi pari, il secondo membro è un quadrato, e ciò è impossibile per il caso $n > 0$. Se sono entrambi dispari si ha $2^{m-a} \equiv 2 \pmod 6$, $3^{m-b} \equiv 3 \pmod 6$, ovvero il primo membro non è divisibile per 6 ma il secondo lo è, impossibile.

Problema 17 *Dimostra che la successione $a_n = \sqrt{24n+1}$ contiene tutti i primi eccetto 2 e 3.*

Soluzione: Ogni primo > 3 può essere scritto nella forma $6k \pm 1$ con $k \in \mathbb{N}$. Risolviamo dunque l'equazione

$$a_n = \sqrt{24n+1} = 6k \pm 1$$

$$24n = 36k^2 \pm 12k$$

$$n = \frac{3k^2 \pm k}{2}$$

$$n = \frac{k(3k \pm 1)}{2}$$

Allora per k intero si ha che n è intero. Quindi per ogni p primo esiste un k intero tale che esiste un n intero che soddisfa l'equazione. Quindi per ogni p primo esiste un n tale che $p = \sqrt{24n+1}$.

Problema 18 *Trova le soluzioni intere dell'equazione $y^2 = x^3 - 432$.*
(Suggerimento: non esistono a, b, c interi non nulli tali che $a^3 + b^3 = c^3$).

Soluzione: Moltiplicando entrambi i membri per $6^3 = 216$ si ottiene $216y^2 = 216x^3 - 432 \cdot 216$, da cui $216x^3 = 216y^2 + 216 \cdot 432$. Il secondo membro può essere riscritto come $(y+36)^3 - (y-36)^3$. Poiché non esistono a, b, c interi non nulli tali che $a^3 + b^3 = c^3$, rimangono tre possibilità:

- $x = 0 \Rightarrow$ non ci sono soluzioni in $\mathbb{Z}$.
- $y = 36 \Rightarrow x = 12$.
- $y = -36 \Rightarrow x = 12$.

Problema 19 *Trova le soluzioni intere dell'equazione $x^2 + y^2 + z^2 = 2xyz$.*

Soluzione: Poiché il secondo membro è pari, deve esserlo anche il primo. Allora esattamente uno tra x, y, z è pari oppure sono tutti e tre pari. Se esattamente uno è pari, poiché i quadrati dispari mod 4 possono essere solo 1, il primo membro è solo divisibile per 2, mentre il secondo per 4; assurdo. Quindi x, y, z sono tutti e tre pari. Possiamo dunque sostituire

$$x = 2x_1, \;\; y = 2y_1, \;\; z = 2z_1.$$

Otteniamo

$$x_1^2 + y_1^2 + z_1^2 = 4xyz.$$

Osserviamo nuovamente che x_1, y_1, z_1 sono tutti pari e sostituiamo $x_1 = 2x_2,\ \ y_1 = 2y_2,\ \ z_1 = 2z_2$. Iterando i passaggi si ottiene:

$$\begin{aligned} x = 2x_1 = 4x_2 = 8x_3 = \ldots = 2^n x_n \ \ \forall n \\ y = 2y_1 = 4y_2 = 8y_3 = \ldots = 2^n y_n \ \ \forall n \\ z = 2z_1 = 4z_2 = 8z_3 = \ldots = 2^n z_n \ \ \forall n \end{aligned}$$

Ovvero 2^n dovrebbe dividere x, y, z per ogni n. Allora l'unica terna possibile di soluzioni è $(0, 0, 0)$.

Problema 20 *Sia data la sequenza*

$$\begin{cases} a_0 = p \\ a_{n+1} = 2a_n + 1. \end{cases}$$

con p primo.
Per quali p la sequenza è formata solo da primi?

Soluzione: Non esiste un tale p. Sommando 1 a entrambi i membri della formula ricorsiva, otteniamo $a_{n+1}+1 = 2(a_n+1)$, ovvero $a_n+1 = 2^n(p+1) \Rightarrow a_n = 2^n p + 2^n - 1$.

Poiché se $p = 2$, $a_1 = 5$ è primo, possiamo supporre senza perdita di generalità che p sia dispari. Abbiamo che $a_n \equiv 2^n - 1 \pmod p\ \forall n$, in particolare allora $a_{p-1} \equiv 2^{p-1} - 1 \equiv 1 - 1 \equiv 0$ (per il piccolo Teorema di Fermat). Allora a_{p-1} è un multiplo di p. Osserviamo che a_{p-1} è strettamente maggiore di p, quindi non può essere primo.

Problema 21 *Quante soluzioni ha $x^2 \equiv 1 \pmod n$ con $n = p_1 \cdot \ldots \cdot p_m$ dove $p_1, \ldots, p_m$ sono primi distinti diversi da 2?*

Soluzione: Sono 2^m. Infatti risolviamo $x^2 \equiv 1 \pmod p_i$. Ci sono solo due soluzioni possibili perché $x^2 - 1 \equiv 0 \pmod p_i \Leftrightarrow (x-1)(x+1) \equiv 0 \pmod p_1 \Leftrightarrow x \equiv 1$ oppure $x = -1 \pmod p_i$. Quindi ogni soluzione dell'equazione $x^2 \equiv 1 \pmod n$ conduce al sistema

$$\begin{cases} x \equiv \pm 1 \pmod p_1 \\ \vdots \\ x \equiv \pm 1 \pmod p_m \end{cases}$$

Proviamo ora che ogni sistema di questo tipo ammette una ed una sola soluzione. Dal Teorema Cinese del Resto si ha che il sistema

$$\begin{cases} x \equiv (-1)^{e_1} \pmod{p}_1 \\ \vdots \\ x \equiv (-1)^{e_m} \pmod{p}_m \end{cases}$$

con $e_i \in \{0, 1\}$ ha una soluzione y modulo n ed inoltre, dovendo questa essere unica, $\forall i \in \{1, \ldots, n\}$ si ha $y^2 \equiv 1 \pmod{p}_i \Rightarrow y^2 \equiv 1 \pmod{n}$. Rimane da dimostrare che le m-uple distinte $(e_1, \ldots, e_m) \neq (e'_1, \ldots, e'_m)$ generano soluzioni distinte $y \neq y'$, ma ciò è ovvio perché se le m-uple sono distinte, esiste $i \in \{1, \ldots, n\}$ tale che $e_i \neq e'_i$, da cui $y \neq y' \pmod{p}_i \Rightarrow y \neq y' \pmod{n}$. Segue che il numero di soluzioni coincide con il numero di m-uple $(e_1, \ldots, e_m)$, che sono 2^m.

Problema 22 *Trovare tutti gli $n \in \mathbb{N}$ per cui $n \mid 2^n - 1$.*

Soluzione: Banalmente $n = 1$ è soluzione. Supponiamo allora $n > 1$, chiaramente n è dispari. Inoltre non è primo: se lo fosse, per il piccolo Teorema di Fermat si avrebbe $2^n \equiv 2 \cdot 2^{n-1} \equiv 2 \pmod{n}$, ovvero $n \nmid 2^n - 1$. Allora n è un numero dispari composto. Sia p il suo più piccolo fattore primo. Essendo allora $p - 1$ e n coprimi, per l'identità di Bezout si ha che esistono $a, b \in \mathbb{Z}$ tali che $an + b(p - 1) = 1$. Allora possiamo scrivere $2 = 2^1$ come $2^{an+b(p-1)}$. Considerando l'espressione mod p, abbiamo che $2^{an} \cdot 2^{b(p-10)} \equiv 2^{an} \cdot 1$ (per il piccolo Teorema di Fermat); inoltre poiché 2^n dev'essere $\equiv 1 \pmod{n}$ e $p \mid n$, anche mod p si deve avere $2^n \equiv 1$. Allora si ha $2 \equiv 2^{an} \cdot 2^{b(p-10)} \equiv 1 \cdot 1 \pmod{p}$, impossibile.

Problema 23 *Dimostrare che non esistono soluzioni dell'equazione*

$$x^n - y^n = 2^k$$

con x, y, n, k interi positivi e $n > 2$.
Suggerimento: si consiglia di risolvere prima il Problema 14.

Soluzione: Supponiamo per assurdo che esistano soluzioni. Ci sono due casi:

- n è dispari.

  L'equazione diventa $(x-y)(x^{n-1}+x^{n-2}y+\ldots+y^{n-1})=2^k$. Scegliamo la soluzione (x_0,y_0,n_0,k_0) in modo che k_0 sia minimo. Abbiamo che $(x_0^{n_0-1}+x_0^{n_0-2}y_0+\ldots+y_0^{n_0-1})$ contiene un numero dispari di addendi, quindi affinché questo sia pari si devono avere x_0 e y_0 entrambi pari. Allora poniamo $x_0=2a$ e $y_0=2b$, ottenendo $a^{n_0}-b^{n_0}=2^{k_0-n_0}$. Se $k_0-n_0>0$, abbiamo contraddetto la minimalità di k_0. Se $k_0-n_0=0$, l'equazione diventa $a_0^n-b_0^n=1$, che chiaramente non ha soluzioni intere positive.

- n è pari.

  Dal Problema 14 sappiamo che con $n=4$ l'equazione non ha soluzioni intere positive. Ponendo $n>4$ scegliamo stavolta la soluzione (x_0,y_0,n_0,k_0) tale che n_0 sia minimo. Essendo $n_0=2m$ per qualche m, l'equazione può essere riscritta come $(x_0^m-y_0^m)(x_0^m+y_0^m)=2^k$. Ma allora $x_0^m-y_0^m=2^h$ per qualche h, con $m>2$. Se m è dispari, per il primo punto non ci sono soluzioni. Se m è pari, abbiamo contraddetto il fatto che n_0 sia minimo.

Problema 24 *Dimostra che l'equazione $x^p+y^q=z^r$, con x,y,z coprimi a due a due, e $\frac{1}{p}+\frac{1}{q}+\frac{1}{r}<1$ ha un numero finito di soluzioni.*

Soluzione: Problema aperto!

Problema 25 *Dimostra che, se 2^x e 3^x sono interi, allora x è intero.*

Soluzione: Problema aperto!