Matematica Olimpica

Maria Archetti

Stage Olimpico Territoriale · Liceo Da Vinci Treviso

Indirizzi e-mail: *archetti.maria@maxplanck.edu.it*

Stage di Matematica Olimpica: Teoria dei Numeri

02 febbraio 2024

Presentazione del corso

Programma

1. Definizioni fondamentali: Congruenze, Funzione ϕ di Eulero, Equazioni Diofantee
2. Teorema Cinese del Resto
3. Teorema di Eulero-Fermat
4. Piccolo Teorema di Fermat
5. Applicazioni ai problemi di Matematica Olimpica

Presentazione del corso

Programma

1. Definizioni fondamentali: Congruenze, Funzione ϕ di Eulero, Equazioni Diofantee
2. Teorema Cinese del Resto
3. Teorema di Eulero-Fermat
4. Piccolo Teorema di Fermat
5. Applicazioni ai problemi di Matematica Olimpica

Presentazione del corso

Programma

1. Definizioni fondamentali: Congruenze, Funzione ϕ di Eulero, Equazioni Diofantee
2. Teorema Cinese del Resto
3. Teorema di Eulero-Fermat
4. Piccolo Teorema di Fermat
5. Applicazioni ai problemi di Matematica Olimpica

Presentazione del corso

Programma

1. Definizioni fondamentali: Congruenze, Funzione ϕ di Eulero, Equazioni Diofantee
2. Teorema Cinese del Resto
3. Teorema di Eulero-Fermat
4. Piccolo Teorema di Fermat
5. Applicazioni ai problemi di Matematica Olimpica

Presentazione del corso

Programma

1. Definizioni fondamentali: Congruenze, Funzione ϕ di Eulero, Equazioni Diofantee
2. Teorema Cinese del Resto
3. Teorema di Eulero-Fermat
4. Piccolo Teorema di Fermat
5. Applicazioni ai problemi di Matematica Olimpica

Materiali e strumenti utili allo studio

Testi consigliati

- Damantino S., Campeotto E. “Aritmetica Modulare”, Collana U Math
- Facchini A. “Algebra e Matematica Discreta”, Decibel Zanichelli
- Franciosi S., De Giovanni F. “Elementi di Algebra", Aracne

Altri materiali e strumenti

- Videolezioni Stage Senior

Materiali e strumenti utili allo studio

Testi consigliati

- Damantino S., Campeotto E. “Aritmetica Modulare”, Collana U Math
- Facchini A. “Algebra e Matematica Discreta”, Decibel Zanichelli
- Franciosi S., De Giovanni F. “Elementi di Algebra", Aracne

Altri materiali e strumenti

- Videolezioni Stage Senior

Congruenze e classi resto

DEF[CLASSI RESTO]: dato $m \geq 2$ intero positivo definiamo

CLASSI RESTO modulo m

$$[0]_m = \{a \in \mathbb{Z} |\ a \div m \text{ resto} = 0\}$$

$$[1]_m = \{a \in \mathbb{Z} |\ a \div m \text{ resto} = 1\}$$

$$\dots$$

$$[m-1]_m = \{a \in \mathbb{Z} |\ a \div m \text{ resto} = m-1\}$$

Congruenze e classi resto

DEF[CLASSI RESTO]: dato $m \geq 2$ intero positivo definiamo

CLASSI RESTO modulo m

$$[0]_m = \{a \in \mathbb{Z} |\ a \div m \text{ resto} = 0\}$$

$$[1]_m = \{a \in \mathbb{Z} |\ a \div m \text{ resto} = 1\}$$

$$\dots$$

$$[m-1]_m = \{a \in \mathbb{Z} |\ a \div m \text{ resto} = m-1\}$$

Congruenze e classi resto

DEF[CLASSI RESTO]: dato $m \geq 2$ intero positivo definiamo

CLASSI RESTO modulo m

$$[0]_m = \{a \in \mathbb{Z} |\ a \div m \text{ resto} = 0\}$$

$$[1]_m = \{a \in \mathbb{Z} |\ a \div m \text{ resto} = 1\}$$

$$\dots$$

$$[m-1]_m = \{a \in \mathbb{Z} |\ a \div m \text{ resto} = m-1\}$$

Congruenze e classi resto

Se due interi a, b *stanno nella stessa classe modulo* m *diremo che*

a congruo b modulo m

DEF: $m \geq 2$ intero positivo; $a,\ b \in \mathbb{Z}$

$$a \equiv b \mod m \iff a - b = k \cdot m, \quad k \in \mathbb{Z}$$

ESEMPI: $17 \in [2]_5 \qquad -17 \in [3]_5\,, \qquad 87 \equiv 22 \mod 5.$

Congruenze e classi resto

Se due interi a, b *stanno nella stessa classe modulo* m *diremo che*

a congruo b modulo m

DEF: $m \geq 2$ intero positivo; $a,\ b \in \mathbb{Z}$

$$a \equiv b \mod m \iff a - b = k \cdot m, \quad k \in \mathbb{Z}$$

ESEMPI: $17 \in [2]_5 \qquad -17 \in [3]_5\,, \qquad 87 \equiv 22 \mod 5.$

Operazioni e Congruenze

Teorema: dati gli interi $m \geq 2,\ a_1,\ a_2,\ b_1,\ b_2$ tali che

$$[a_1]_m = [a_2]_m \qquad a_1 \equiv a_2 \mod m$$

$$[b_1]_m = [b_2]_m \qquad b_1 \equiv b_2 \mod m$$

allora

$$[a_1 + b_1]_m = [a_2 + b_2]_m \qquad a_1 + b_1 \equiv a_2 + b_2 \mod m$$

$$[a_1 \cdot b_1]_m = [a_2 \cdot b_2]_m \qquad a_1 \cdot b_1 \equiv a_2 \cdot b_2 \mod m$$

IMPORTANTE: LE CONGRUENZE SI "COMPORTANO BENE" CON SOMME E PRODOTTI!

Problema

Problema: Trovare la cifra delle unità del numero 2007^{2007}

Sol: osserviamo che $2007 = 2 \cdot 10^3 + 7$, quindi trovare la cifra delle unità corrisponde a determinare la *classe modulo 10* del numero dato.

$$\left[2007^{2007}\right]_{10} = \left[7 \cdot 7 \cdot \cdots \cdot 7\right]_{10}$$

analizziamo le potenze di 7 modulo 10

$$[7 \cdot 7]_{10} = [9]_{10} = [-1]_{10}$$

$$[(7 \cdot 7) \cdots (7 \cdot 7) \cdot 7]_{10} = [(-1) \cdots (-1) \cdot 7]_{10} = [-7]_{10} = [3]_{10}$$

la cifra delle unità è pari a 3.

Problema

Problema: Trovare la cifra delle unità del numero 2007^{2007}

Sol: osserviamo che $2007 = 2 \cdot 10^3 + 7$, quindi trovare la cifra delle unità corrisponde a determinare la *classe modulo 10* del numero dato.

$$[2007^{2007}]_{10} = [7 \cdot 7 \cdot \cdots \cdot 7]_{10}$$

analizziamo le potenze di 7 modulo 10

$$[7 \cdot 7]_{10} = [9]_{10} = [-1]_{10}$$

$$[(7 \cdot 7) \cdots (7 \cdot 7) \cdot 7]_{10} = [(-1) \cdots (-1) \cdot 7]_{10} = [-7]_{10} = [3]_{10}$$

la cifra delle unità è pari a 3.

Problema

Problema: Trovare la cifra delle unità del numero 2007^{2007}

Sol: osserviamo che $2007 = 2 \cdot 10^3 + 7$, quindi trovare la cifra delle unità corrisponde a determinare la *classe modulo 10* del numero dato.

$$\left[2007^{2007}\right]_{10} = \left[7 \cdot 7 \cdot \cdots \cdot 7\right]_{10}$$

analizziamo le potenze di 7 modulo 10

$$[7 \cdot 7]_{10} = [9]_{10} = [-1]_{10}$$

$$[(7 \cdot 7) \cdots (7 \cdot 7) \cdot 7]_{10} = [(-1) \cdots (-1) \cdot 7]_{10} = [-7]_{10} = [3]_{10}$$

la cifra delle unità è pari a 3.

Problema

Problema: Trovare la cifra delle unità del numero 2007^{2007}

Sol: osserviamo che $2007 = 2 \cdot 10^3 + 7$, quindi trovare la cifra delle unità corrisponde a determinare la *classe modulo 10* del numero dato.

$$\left[2007^{2007}\right]_{10} = \left[7 \cdot 7 \cdot \cdots \cdot 7\right]_{10}$$

analizziamo le potenze di 7 modulo 10

$$[7 \cdot 7]_{10} = [9]_{10} = [-1]_{10}$$

$$[(7 \cdot 7) \cdots (7 \cdot 7) \cdot 7]_{10} = [(-1) \cdots (-1) \cdot 7]_{10} = [-7]_{10} = [3]_{10}$$

la cifra delle unità è pari a 3.

Problema

Problema: Trovare la cifra delle unità del numero 2007^{2007}

Sol: osserviamo che $2007 = 2 \cdot 10^3 + 7$, quindi trovare la cifra delle unità corrisponde a determinare la *classe modulo 10* del numero dato.

$$\left[2007^{2007}\right]_{10} = \left[7 \cdot 7 \cdot \cdots \cdot 7\right]_{10}$$

analizziamo le potenze di 7 modulo 10

$$[7 \cdot 7]_{10} = [9]_{10} = [-1]_{10}$$

$$[(7 \cdot 7) \cdots (7 \cdot 7) \cdot 7]_{10} = [(-1) \cdots (-1) \cdot 7]_{10} = [-7]_{10} = [3]_{10}$$

la cifra delle unità è pari a 3.

Problema

Problema: Trovare la cifra delle unità del numero 2007^{2007}

Sol: osserviamo che $2007 = 2 \cdot 10^3 + 7$, quindi trovare la cifra delle unità corrisponde a determinare la *classe modulo 10* del numero dato.

$$\left[2007^{2007}\right]_{10} = \left[7 \cdot 7 \cdot \cdots \cdot 7\right]_{10}$$

analizziamo le potenze di 7 modulo 10

$$[7 \cdot 7]_{10} = [9]_{10} = [-1]_{10}$$

$$[(7 \cdot 7) \cdots (7 \cdot 7) \cdot 7]_{10} = [(-1) \cdots (-1) \cdot 7]_{10} = [-7]_{10} = [3]_{10}$$

la cifra delle unità è pari a 3.

Problema

Problema: Trovare la cifra delle unità del numero 2007^{2007}

Sol: osserviamo che $2007 = 2 \cdot 10^3 + 7$, quindi trovare la cifra delle unità corrisponde a determinare la *classe modulo 10* del numero dato.

$$\left[2007^{2007}\right]_{10} = \left[7 \cdot 7 \cdot \cdots \cdot 7\right]_{10}$$

analizziamo le potenze di 7 modulo 10

$$[7 \cdot 7]_{10} = [9]_{10} = [-1]_{10}$$

$$[(7 \cdot 7) \cdots (7 \cdot 7) \cdot 7]_{10} = [(-1) \cdots (-1) \cdot 7]_{10} = [-7]_{10} = [3]_{10}$$

la cifra delle unità è pari a 3.

Operazioni e Congruenze

IMPORTANTE: LE CONGRUENZE, in generale, NON SI "COMPORTANO BENE" CON I QUOZIENTI!

$$2 \equiv 12 \mod 10 \qquad \text{MA} \qquad 1 \not\equiv 6 \mod 10$$

valgono i seguenti risultati

Teorema: sia $a \equiv b \mod m$, allora

- se $\text{MCD}(c;m) = 1$ si ha che anche $\frac{a}{c} \equiv \frac{b}{c} \mod m$;
- se invece $\text{MCD}(c;m) = d > 1$ si ha che anche $\frac{a}{c} \equiv \frac{b}{c} \mod \frac{m}{d}$

Operazioni e Congruenze

IMPORTANTE: LE CONGRUENZE, in generale, NON SI "COMPORTANO BENE" CON I QUOZIENTI!

$$2 \equiv 12 \mod 10 \qquad \text{MA} \qquad 1 \not\equiv 6 \mod 10$$

valgono i seguenti risultati

Teorema: sia $a \equiv b \mod m$, allora

- se $\text{MCD}(c;m) = 1$ si ha che anche $\frac{a}{c} \equiv \frac{b}{c} \mod m$;
- se invece $\text{MCD}(c;m) = d > 1$ si ha che anche $\frac{a}{c} \equiv \frac{b}{c} \mod \frac{m}{d}$

Operazioni e Congruenze

IMPORTANTE: LE CONGRUENZE, in generale, NON SI "COMPORTANO BENE" CON I QUOZIENTI!

$$2 \equiv 12 \mod 10 \qquad \text{MA} \qquad 1 \not\equiv 6 \mod 10$$

valgono i seguenti risultati

Teorema: sia $a \equiv b \mod m$, allora

- se $\text{MCD}(c;m) = 1$ si ha che anche $\frac{a}{c} \equiv \frac{b}{c} \mod m$;
- se invece $\text{MCD}(c;m) = d > 1$ si ha che anche $\frac{a}{c} \equiv \frac{b}{c} \mod \frac{m}{d}$

Operazioni e Congruenze

IMPORTANTE: LE CONGRUENZE, in generale, NON SI "COMPORTANO BENE" CON I QUOZIENTI!

$$2 \equiv 12 \mod 10 \qquad \text{MA} \qquad 1 \not\equiv 6 \mod 10$$

valgono i seguenti risultati

Teorema: sia $a \equiv b \mod m$, allora

- se $\text{MCD}(c;m) = 1$ si ha che anche $\frac{a}{c} \equiv \frac{b}{c} \mod m$;
- se invece $\text{MCD}(c;m) = d > 1$ si ha che anche $\frac{a}{c} \equiv \frac{b}{c} \mod \frac{m}{d}$

Teorema Cinese del Resto

Teorema Cinese del Resto TCR:

Se MCD$(m_1; m_2) = 1$ allora il sistema di congruenze

$$\begin{cases} x \equiv a_1 \mod m_1 \\ x \equiv a_2 \mod m_2 \end{cases}$$

risulta equivalente alla conguemza

$$x \equiv a_3 \mod m_1 \cdot m_2$$

Problema

Problema: Quanti sono i numeri interi $0 \leq n \leq 2021$ tali che il numero $p(n) = 91^n - 48^n - 44^n + 1$ è multiplo di 2021?

Sol: dobbiamo risolvere $p(n) \equiv 0 \mod 2021$. Osserviamo che $2021 = 43 \cdot 47$, quindi la congruenza è equivalente per TCR al sistema

$$\begin{cases} p(n) \equiv 0 \mod 43 \\ p(n) \equiv 0 \mod 47 \end{cases}$$

$$\begin{cases} (2 \cdot 43 + 5)^n - (43 + 5)^n - (43 + 1)^n + 1 \equiv 0 \mod 43 \\ (2 \cdot 47 - 3)^n - (47 + 1)^n - (47 - 3)^n + 1 \equiv 0 \mod 47 \end{cases}$$

il sistema è verificato per ogni n, la risposta è dunque 2022.

Problema

Problema: Quanti sono i numeri interi $0 \leq n \leq 2021$ tali che il numero $p(n) = 91^n - 48^n - 44^n + 1$ è multiplo di 2021?

Sol: dobbiamo risolvere $p(n) \equiv 0 \mod 2021$. Osserviamo che $2021 = 43 \cdot 47$, quindi la congruenza è equivalente per TCR al sistema

$$\begin{cases} p(n) \equiv 0 \mod 43 \\ p(n) \equiv 0 \mod 47 \end{cases}$$

$$\begin{cases} (2 \cdot 43 + 5)^n - (43 + 5)^n - (43 + 1)^n + 1 \equiv 0 \mod 43 \\ (2 \cdot 47 - 3)^n - (47 + 1)^n - (47 - 3)^n + 1 \equiv 0 \mod 47 \end{cases}$$

il sistema è verificato per ogni n, la risposta è dunque 2022.

Problema

Problema: Quanti sono i numeri interi $0 \leq n \leq 2021$ tali che il numero $p(n) = 91^n - 48^n - 44^n + 1$ è multiplo di 2021?

Sol: dobbiamo risolvere $p(n) \equiv 0 \mod 2021$. Osserviamo che $2021 = 43 \cdot 47$, quindi la congruenza è equivalente per TCR al sistema

$$\begin{cases} p(n) \equiv 0 \mod 43 \\ p(n) \equiv 0 \mod 47 \end{cases}$$

$$\begin{cases} (2 \cdot 43 + 5)^n - (43 + 5)^n - (43 + 1)^n + 1 \equiv 0 \mod 43 \\ (2 \cdot 47 - 3)^n - (47 + 1)^n - (47 - 3)^n + 1 \equiv 0 \mod 47 \end{cases}$$

il sistema è verificato per ogni n, la risposta è dunque 2022.

Problema

Problema: Quanti sono i numeri interi $0 \leq n \leq 2021$ tali che il numero $p(n) = 91^n - 48^n - 44^n + 1$ è multiplo di 2021?

Sol: dobbiamo risolvere $p(n) \equiv 0 \mod 2021$. Osserviamo che $2021 = 43 \cdot 47$, quindi la congruenza è equivalente per TCR al sistema

$$\begin{cases} p(n) \equiv 0 \mod 43 \\ p(n) \equiv 0 \mod 47 \end{cases}$$

$$\begin{cases} (2 \cdot 43 + 5)^n - (43 + 5)^n - (43 + 1)^n + 1 \equiv 0 \mod 43 \\ (2 \cdot 47 - 3)^n - (47 + 1)^n - (47 - 3)^n + 1 \equiv 0 \mod 47 \end{cases}$$

il sistema è verificato per ogni n, la risposta è dunque 2022.

Problema

Problema: Quanti sono i numeri interi $0 \leq n \leq 2021$ tali che il numero $p(n) = 91^n - 48^n - 44^n + 1$ è multiplo di 2021?

Sol: dobbiamo risolvere $p(n) \equiv 0 \mod 2021$. Osserviamo che $2021 = 43 \cdot 47$, quindi la congruenza è equivalente per TCR al sistema

$$\begin{cases} p(n) \equiv 0 \mod 43 \\ p(n) \equiv 0 \mod 47 \end{cases}$$

$$\begin{cases} (2 \cdot 43 + 5)^n - (43 + 5)^n - (43 + 1)^n + 1 \equiv 0 \mod 43 \\ (2 \cdot 47 - 3)^n - (47 + 1)^n - (47 - 3)^n + 1 \equiv 0 \mod 47 \end{cases}$$

il sistema è verificato per ogni n, la risposta è dunque 2022.

La funzione ϕ di Eulero

La funzione ϕ di Eulero associa ad ogni n intero positivo il NUMERO di interi positivi minori di n coprimi con n.

$$\phi(n) = |\{a \in \mathbb{N} |\ a < n\ \wedge\ \text{MCD}(a;n) = 1\}|$$

ESEMPI: $\phi(6) = 2$, $\phi(5) = 4$, $\phi(7) = 6$.

- per ogni primo p vale
$$\phi(p) = p - 1$$
- per ogni potenza di primo p^k vale
$$\phi(p^k) = p^k - p^{k-1} = (p-1) \cdot p^{k-1}$$

La funzione ϕ di Eulero

La funzione ϕ di Eulero associa ad ogni n intero positivo il NUMERO di interi positivi minori di n coprimi con n.

$$\phi(n) = |\{a \in \mathbb{N} |\ a < n\ \wedge\ \text{MCD}(a;n) = 1\}|$$

ESEMPI: $\phi(6) = 2$, $\phi(5) = 4$, $\phi(7) = 6$.

- per ogni primo p vale
$$\phi(p) = p - 1$$
- per ogni potenza di primo p^k vale
$$\phi(p^k) = p^k - p^{k-1} = (p-1) \cdot p^{k-1}$$

La funzione ϕ di Eulero

La funzione ϕ di Eulero associa ad ogni n intero positivo il NUMERO di interi positivi minori di n coprimi con n.

$$\phi(n) = |\{a \in \mathbb{N} |\ a < n\ \wedge\ \text{MCD}(a;n) = 1\}|$$

ESEMPI: $\phi(6) = 2$, $\phi(5) = 4$, $\phi(7) = 6$.

- per ogni primo p vale
$$\phi(p) = p - 1$$
- per ogni potenza di primo p^k vale
$$\phi(p^k) = p^k - p^{k-1} = (p-1) \cdot p^{k-1}$$

La funzione ϕ di Eulero

SE MCD$(a;b) = 1$ allora $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$

se $n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_i^{k_i}$ la formula generale sarà quindi

$$\phi(n) = (p_1 - 1) \cdot (p_2 - 1) \cdots (p_i - 1) \cdot p_1^{k_1 - 1} \cdots p_i^{k_i - 1}$$

Teorema di Eulero-Fermat

$$\text{Se MCD}(a;m) = 1 \quad \text{allora} \quad a^{\phi(m)} \equiv 1 \mod m$$

Conseguenza: Se MCD$(a;m) = 1$ le potenze di a modulo m sono PERIODICHE di periodo che DIVIDE $\phi(m)$.

La funzione ϕ di Eulero

SE MCD$(a;b) = 1$ allora $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$

se $n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_i^{k_i}$ la formula generale sarà quindi

$$\phi(n) = (p_1 - 1) \cdot (p_2 - 1) \cdots (p_i - 1) \cdot p_1^{k_1 - 1} \cdots p_i^{k_i - 1}$$

Teorema di Eulero-Fermat

Se MCD$(a;m) = 1$ allora $a^{\phi(m)} \equiv 1 \mod m$

Conseguenza: Se MCD$(a;m) = 1$ le potenze di a modulo m sono PERIODICHE di periodo che DIVIDE $\phi(m)$.

La funzione ϕ di Eulero

SE MCD$(a;b) = 1$ allora $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$

se $n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_i^{k_i}$ la formula generale sarà quindi

$$\phi(n) = (p_1 - 1) \cdot (p_2 - 1) \cdots (p_i - 1) \cdot p_1^{k_1 - 1} \cdots p_i^{k_i - 1}$$

Teorema di Eulero-Fermat

Se MCD$(a;m) = 1$ allora $a^{\phi(m)} \equiv 1 \mod m$

Conseguenza: Se MCD$(a;m) = 1$ le potenze di a modulo m sono PERIODICHE di periodo che DIVIDE $\phi(m)$.

La funzione ϕ di Eulero

SE MCD$(a;b) = 1$ allora $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$

se $n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_i^{k_i}$ la formula generale sarà quindi

$$\phi(n) = (p_1 - 1) \cdot (p_2 - 1) \cdots (p_i - 1) \cdot p_1^{k_1 - 1} \cdots p_i^{k_i - 1}$$

Teorema di Eulero-Fermat

Se MCD$(a;m) = 1$ allora $a^{\phi(m)} \equiv 1 \mod m$

Conseguenza: Se MCD$(a;m) = 1$ le potenze di a modulo m sono PERIODICHE di periodo che DIVIDE $\phi(m)$.

La funzione ϕ di Eulero

Dal Teorema di Eulero-Fermat si può dedurre il

Piccolo Teorema di Fermat: sia p un primo qualunque

$$\underline{\text{Se MCD}(a;p)=1} \quad \text{allora} \quad a^{p-1} \equiv 1 \mod p$$

Problema: Quanti sono i numeri primi p per cui $p^4 - 26$ è primo?

Sol: per ogni primo $p \neq 5$, si ha $\text{MCD}(p;5) = 1$. Inoltre $\phi(5) = 4$. Per il Piccolo Teorema di Fermat si ha quindi $p^4 \equiv 1 \mod 5$ da cui segue, essendo $26 \equiv 1 \mod 5$,

$$p^4 - 26 \equiv 1 - 1 \equiv 0 \mod 5.$$

Abbiamo dimostrato che per ogni $p \neq 5$, $p^4 - 26$ NON è primo poiché risulta divisibile per 5. Infine se consideriamo $p = 5$ otteniamo $5^4 - 26 = 599$ che è primo. La risposta è 1.

La funzione ϕ di Eulero

Dal Teorema di Eulero-Fermat si può dedurre il

Piccolo Teorema di Fermat: sia p un primo qualunque

$$\underline{\text{Se MCD}(a;p)=1} \quad \text{allora} \quad a^{p-1} \equiv 1 \mod p$$

Problema: Quanti sono i numeri primi p per cui $p^4 - 26$ è primo?

Sol: per ogni primo $p \neq 5$, si ha $\text{MCD}(p;5) = 1$. Inoltre $\phi(5) = 4$. Per il Piccolo Teorema di Fermat si ha quindi $p^4 \equiv 1 \mod 5$ da cui segue, essendo $26 \equiv 1 \mod 5$,

$$p^4 - 26 \equiv 1 - 1 \equiv 0 \mod 5.$$

Abbiamo dimostrato che per ogni $p \neq 5$, $p^4 - 26$ NON è primo poiché risulta divisibile per 5. Infine se consideriamo $p = 5$ otteniamo $5^4 - 26 = 599$ che è primo. La risposta è 1.

La funzione ϕ di Eulero

Dal Teorema di Eulero-Fermat si può dedurre il

Piccolo Teorema di Fermat: sia p un primo qualunque

$$\underline{\text{Se MCD}(a;p)=1} \quad \text{allora} \quad a^{p-1} \equiv 1 \mod p$$

Problema: Quanti sono i numeri primi p per cui $p^4 - 26$ è primo?

Sol: per ogni primo $p \neq 5$, si ha $\text{MCD}(p;5) = 1$. Inoltre $\phi(5) = 4$. Per il Piccolo Teorema di Fermat si ha quindi $p^4 \equiv 1 \mod 5$ da cui segue, essendo $26 \equiv 1 \mod 5$,

$$p^4 - 26 \equiv 1 - 1 \equiv 0 \mod 5.$$

Abbiamo dimostrato che per ogni $p \neq 5$, $p^4 - 26$ NON è primo poiché risulta divisibile per 5. Infine se consideriamo $p = 5$ otteniamo $5^4 - 26 = 599$ che è primo. La risposta è 1.

La funzione ϕ di Eulero

Dal Teorema di Eulero-Fermat si può dedurre il

Piccolo Teorema di Fermat: sia p un primo qualunque

$$\underline{\text{Se MCD}(a;p)=1} \quad \text{allora} \quad a^{p-1} \equiv 1 \mod p$$

Problema: Quanti sono i numeri primi p per cui $p^4 - 26$ è primo?

Sol: per ogni primo $p \neq 5$, si ha $\text{MCD}(p;5) = 1$. Inoltre $\phi(5) = 4$. Per il Piccolo Teorema di Fermat si ha quindi $p^4 \equiv 1 \mod 5$ da cui segue, essendo $26 \equiv 1 \mod 5$,

$$p^4 - 26 \equiv 1 - 1 \equiv 0 \mod 5.$$

Abbiamo dimostrato che per ogni $p \neq 5$, $p^4 - 26$ NON è primo poiché risulta divisibile per 5. Infine se consideriamo $p = 5$ otteniamo $5^4 - 26 = 599$ che è primo. La risposta è 1.

Equazioni Diofantee non lineari

Problema: determinare tutte le soluzioni intere dell'equazione

$$y^2 = x^5 - 4$$

Sol: *Osservazione Importante:* se un 'equazione ha soluzioni intere allora ammette soluzione anche modulo m per ogni intero $m \geq 2$. Di conseguenza, se risulta IMPOSSIBILE per qualche primo p ,l'equazione non avrà soluzioni intere.

Compare una potenza 5, mi conviene cercare un primo che abbia una ϕ di Eulero multipla di 5, un primo con questa caratteristica è $p = 11$ con funzione di Eulero $\phi(11) = 10$.

Equazioni Diofantee non lineari

Problema: determinare tutte le soluzioni intere dell'equazione

$$y^2 = x^5 - 4$$

Sol: *Osservazione Importante:* se un 'equazione ha soluzioni intere allora ammette soluzione anche modulo m per ogni intero $m \geq 2$. Di conseguenza, se risulta IMPOSSIBILE per qualche primo p ,l'equazione non avrà soluzioni intere.

Compare una potenza 5, mi conviene cercare un primo che abbia una ϕ di Eulero multipla di 5, un primo con questa caratteristica è $p = 11$ con funzione di Eulero $\phi(11) = 10$.

Equazioni Diofantee non lineari

Problema: determinare tutte le soluzioni intere dell'equazione

$$y^2 = x^5 - 4$$

Sol: *Osservazione Importante:* se un 'equazione ha soluzioni intere allora ammette soluzione anche modulo m per ogni intero $m \geq 2$. Di conseguenza, se risulta IMPOSSIBILE per qualche primo p ,l'equazione non avrà soluzioni intere.

Compare una potenza 5, mi conviene cercare un primo che abbia una ϕ di Eulero multipla di 5, un primo con questa caratteristica è $p = 11$ con funzione di Eulero $\phi(11) = 10$.

Equazioni Diofantee non lineari

continuazione soluzione: Considero l'equazione modulo 11 perché le potenze quinte modulo 11 sono solo tre $[0]_{11}$, $[1]_{11}$, $[-1]_{11}$. Di conseguenza modulo 11 la quantità $x^5 - 4$ apparterrà ad una classe tra

$$[0-4]_{11} = [-4]_{11}\,, \qquad [1-4]_{11} = [-3]_{11}\,, \qquad [-1-4]_{11} = [-5]_{11}.$$

Nessuna di queste tre classi può essere un quadrato modulo 11.

Infatti i quadrati modulo 11 sono $0,\ 1,\ 4,\ 9,\ 16 \equiv 5,\ 25 \equiv 3 \mod 11$.

L'equazione non ha soluzioni intere.

Problemi

Qualche ulteriore piccola sfida...

- **Problema**: determinare tutte le soluzioni intere dell'equazione $7004 = x^3 - y^3$
- **Problema**: esiste un quadrato perfetto la cui espressione in base 10 termini con le cifre 02?
- **Problema**: esistono 2013 interi consecuitivi ognuno divisibile per una quinta potenza maggiore di 1?

Problemi

Qualche ulteriore piccola sfida...

- **Problema**: determinare tutte le soluzioni intere dell'equazione $7004 = x^3 - y^3$
- **Problema**: esiste un quadrato perfetto la cui espressione in base 10 termini con le cifre 02?
- **Problema**: esistono 2013 interi consecuitivi ognuno divisibile per una quinta potenza maggiore di 1?