Teoria dei Numeri 1 – Parte 3

Titolo nota 08/09/2008

Esercizio 6 $p^4 - q^4$ p, q primi con almeno 2 cifre

Domanda: MCD di tutti questi numeri.

Modulo 2 $p^4 \equiv q^4 \equiv 1$ perchè p e q sono dispari

$\Rightarrow \quad 2 \mid p^4 - q^4$ sempre

Modulo 3 $p^2 \equiv 1$ e $q^2 \equiv 1$ perchè $(p,3) = (q,3) = 1$
$p^4 \equiv 1$ e $q^4 \equiv 1$

$\Rightarrow \quad 3 \mid p^4 - q^4$ sempre

Modulo 5: $p^4 \equiv q^4 \equiv 1$ (picc. F.T.)

$\Rightarrow \quad 5 \mid p^4 - q^4$ sempre

Se d è dispari $\quad d^2 \equiv 1 \pmod 4$, meglio $d^2 \equiv 1 \pmod 8$

Se d è dispari $\quad d^4 \equiv 1 \pmod{16}$ FATTO GENERALE

$\Rightarrow$ $p^4 - q^4$ è sempre div. per 16

Abbiamo dim. che $p^4 - q^4$ è sempre div. per $16 \cdot 3 \cdot 5$

Non può essere di più. Basta provare con $p = 13 \quad q = 11$

$$13^4 - 11^4 = 16 \cdot 3 \cdot 5 \cdot \text{fattori primi} \geq 11$$
$$(13^2 - 11^2)(13^2 + 11^2)$$

Non può essere che $23 \mid p^4 - q^4$ sempre (basta prendere $p = 23$)

Tutti i primi ≥ 11 non possono essere nel M.C.D.

— o — o —

8 d_n = MCD tra n^2+100 e $(n+1)^2+100$

Quali sono i possibili valori di d_n

n^2+100 $\qquad$ $n^2+2n+101$

Supponiamo che p sia un primo t.c.

$p \mid n^2+100$ e $p \mid n^2+2n+101$

Allora p | la diff., quindi $p \mid 2n+1$

Quindi $p \mid n^2+100$ e $p \mid 2n+1$. In particolare

$p \mid 4n^2+400$ e $p \mid 2n+1$ (in realtà è un se e solo se)

$$\begin{array}{r|l} 4n^2+400 & 2n+1 \\ -4n^2-2n & \hline & 2n-1 \\ \hline -2n+400 & \\ +2n+1 & \\ \hline 401 & \end{array}$$

$$4n^2+400 = (2n+1)(2n-1)+401$$

p $\quad$ p

Quindi $p \mid 401$. Ho usato che p sia primo? NO

Ho così detto che $d \mid 401$, quindi $d = 1, 401$

Occorre trovare esempi in cui $d=1$ ed esempi in cui $d=401$

$n=1$

perché $d \mid 2n+1$

è ragionevole provare $n=200$

OCCORRE FARE IL CONTROLLO NEL TESTO

—o—o—

Problema 9 $f : \mathbb{N} \to \mathbb{N}$ $\quad f(0) = f(1) = 0$

$$f(2n) = 2f(n) + 1 \qquad f(2n+1) = 2f(n)$$

Capire come è fatta f.

Oss. 1 Esiste un'unica f che verifica le proprietà

Induzione a blocchetti di 2

$f(0)$ e $f(1)$	NOTE	
$f(2)$ e $f(3)$	$n=1$	
$f(4)$ e $f(5)$	$n=2$	

Calcoliamo un po' di valori

$f(0) = 0$	$0 \to 0$
$f(1) = 0$	$1 \to 0$
$f(2) = 1$	$10 \to 1$
$f(3) = 0$	$11 \to 0$
$f(4) = 3$	$100 \to 11$
$f(5) = 2$	$101 \to 10$
$f(6) = 1$	$110 \to 1$
$f(7) = 0$	$111 \to 0$
$f(8) = 7$	$1000 \to 111$

f TRASPORMA GLI ZERI IN UNI E VICEVERSA

Dimostrazione formale: induzione sul NUMERO di cifre k (in base 2)

$k=0$ $\quad k=1$ banale $\quad f(0) = f(1) = 0$

$k \Rightarrow k+1$. Prendo un numero di $k+1$ cifre

$a_1 a_2 a_3 \dots a_k 0 \to b_1 b_2 b_3 \dots b_k + 1$ (bi inverse delle ai)

$2f(n) + 1$

$a_1 a_2 a_3 \dots a_k 1 \to b_1 b_2 b_3 \dots b_k 0$

$2f(n)$

Oss. C'era un problema IMO molto simile in base 4

(a) Partendo da un numero n e combinando ad iterare f, che succede?

Prima o poi arrivo a zero perché ogni volta perdo almeno una cifra

(b) Più piccola partenza per cui si arriva a zero dopo 2008 passi.

Deve avere almeno 2008 cifre e essere alternate 10

$\underbrace{10\,10\,10\,\ldots\,10}_{2008 \text{ cifre}} = 2 + 8 + 32 + \ldots + 2^{2007}$

$= 2\left(1 + 4 + 16 + \ldots + 2^{2006}\right)$

$= 2 \cdot \left(1 + 4 + 4^2 + \ldots + 4^{1003}\right)$

$= 2\,\frac{4^{1004} - 1}{3}$

— o — o —

Problema 10 $\quad y^2 = x^5 - 4 \quad \rightarrow$ solus. intere

↗ se non ci sono, di solito è + facile (c'è speranza di poter usare le congruenze)

[$y^2 = x^5 + 4$ ha come soluzione $x = 2$ e $y = 6$

quindi per ogni p l'equazione ha almeno 1 sol. mod p]

Consideriamo modulo $11 = p$ $\qquad p - 1 = 10$

I residui delle potenze quinte mod 11 sono $0, 1, -1$
I residui TJ-atici mod 11 sono $0, 1, 4, 9, 5, 3$

y^2: $0, 1, 4, 9, 5, 3$

$0, 1, -1, -4, x^5 - 4$

$7, 8, 6$ DIVERSI

$x^5 = z$ Supponiamo $x \not\equiv 0 \pmod{11}$

$z^2 \equiv x^{10} \equiv 1 \pmod{11}$

$z^2 \equiv 1 \pmod{11}$

ok perché modulo primo

$z \equiv \pm 1 \pmod{11}$

$z^2 \equiv 1 \pmod{11}$

$z^2 - 1 \equiv 0 \pmod{11}$

$z^2 - 1 = 11k$

$(z+1)(z-1) = 11k$

$11 \mid z+1 \quad z \equiv 1$

$11 \mid z-1 \quad z \equiv -1$

Ok anche se il modulo è la potenza di un primo $\neq 2$

— o — o ~

p primo $\qquad 1+2+3+\dots+p \equiv 0 \quad (p)$ $\qquad p$ DISPARI

Analogamente $\qquad 1+2+3+\dots+(p-1) \equiv 0 \quad (p)$

Dim 1 $\qquad \boxed{1+(p-1)} + \boxed{2+(p-2)} + \boxed{3+(p-3)} + \dots$

Dim 2 $\qquad 1+2+3+\dots+(p-1) = \dfrac{(p-1)\,p}{2}$ intero

Dim 3 $\qquad \{1,2,3,\dots,p-1\} = \{g, g^2, g^3, \dots, g^{p-1}\}$

$$1+2+3+\dots+(p-1) \equiv g+g^2+g^3+\dots+g^{p-1}$$

$$= g\left(1+g+g^2+\dots+g^{p-2}\right)$$

$$= g\,\frac{\boxed{g^{p-1}-1}}{\boxed{g-1}}$$

$\boxed{g^{p-1}-1}$ MULTIPLO DI p PER LFT

$\boxed{g-1}$ NO p perché $g \not\equiv 1 \ (p)$

p primo $\qquad 1^2+2^2+3^2+\dots+(p-1)^2 \equiv 0 \ (p) \qquad p\neq 2, p\neq 3$

Dim 1 $\qquad k^2+(p-k)^2 = k^2+p^2+k^2-2kp$ $\qquad$ MAH !!!

Dim 2 $\qquad 1^2+2^2+3^2+\dots+n^2 = \dfrac{n(n+1)(2n+1)}{6}$

$n=p-1 \qquad \dfrac{(p-1)\,p\,(2p-1)}{6}$ $\qquad$ MULTIPLO DI p se $p\neq 2$ $p\neq 3$

Dim 3 $\qquad 1^2+2^2+3^2+\dots+(p-1)^2 = g^2+g^4+g^6+\dots+g^{2p-2}$

$$= g^2\left(1+g^2+g^4+\dots+g^{2p-4}\right)$$

$$= g^2\,\frac{g^{2p-2}-1}{g^2-1}$$

g^{2p-2} ↑ $(g^2)^{p-1}$

$\equiv$ ↑ p c'è

↑ p non c'è se $p\neq 2$ e $p\neq 3$

$$g^{2p-2} = \left(g^{p-1}\right)^2 \equiv 1 \ (p)$$

p primo $\qquad 1^k + 2^k + 3^k + \dots + (p-1)^k \equiv 0 \quad (p)$

se $p \dots$

Dim 1 : MAH

Dim 2 : Sì, MA ... (non c'è formula secca per somme potenze k-esime, ma solo una ricorrente in funzione delle prec.)

Dim 3 : $\underbrace{1^k + 2^k + 3^k + \dots + (p-1)^k}_{\text{basta in realtà siano tutte classi diverse}} = g^k + g^{2k} + \dots + g^{(p-1)k}$

$= g^k (1 + g^k + g^{2k} + \dots + g^{(p-2)k})$

$= g^k \dfrac{\boxed{g^{k(p-1)} - 1}}{g^k - 1}$ $\quad p$ c'è $\quad (g^{p-1})^k \equiv 1 \quad (p)$

Il fattore $g^k - 1$ è multiplo di $p \iff g^k \equiv 1 \quad (p)$

$\iff (p-1) \mid k$

Se $(p-1) \nmid k$, allora sotto p non c'è, dunque la somma è $\equiv 0 \ (p)$

Se $(p-1) \mid k$, allora

$1^k \equiv 1$
$2^k \equiv 1$
$3^k \equiv 1$
$4^k \equiv 1$

] sono tutte potenze $(p-1)$-esime, dunque 1 per LFT.

Quindi $1^k + 2^k + 3^k + \dots + (p-1)^k \equiv$

$1 + 1 + 1 + \dots + 1 \equiv p-1 \ (p)$

Quindi è sempre $\equiv 0 \ (p)$ se $k < p-1$, cioè $k \leq p-2$

GRAN FINALE

Dato un polinomio $Q(x)$ a coeff. interi di grado $\leq p-2$ abbiamo che

$$Q(1) + Q(2) + Q(3) + \dots + Q(p-1) + Q(p) \equiv 0 \pmod{p}$$

$$Q(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_{p-2} x^{p-2}$$

a_0	a_0	a_0	$\dots$	$= p a_0$
a_1	$2a_1$	$3a_1$		$= a_1 (1+2+3+\dots+p)$
a_2	$4a_2$	$9a_2$		$= a_2 (1^2+2^2+\dots+p^2)$
a_3	$8a_3$	$27a_3$		$= a_3 (1^3+2^3+\dots+p^3)$
$\vdots$	$\vdots$	$\vdots$		
a_{p-2}	$2^{p-2} a_{p-2}$	$3^{p-2} a_{p-2}$		

e così via !!!

Basta in realtà che non ci sia nessun monomio di grado multiplo di $(p-1)$.