Teoria dei Numeri 2 – Parte 3

Titolo nota 10/09/2008

N2 – Esercizio 10

$$D = \{ n \in \mathbb{N} : n \text{ divide } 2^n + 1 \}$$

(a) Trovare tutti i primi che stanno in D $(n = p)$

$$p \mid 2^p + 1 \iff 2^p \equiv -1 \ (p) \implies 2^{2p} \equiv 1 \ (p)$$

$$\iff 4^p \equiv 1 \ (p)$$

In generale $4^k \equiv 1 \ (p) \iff \text{ord}_p(4) \mid k$

Nel caso particolare $4^p \equiv 1 \ (p) \iff \text{ord}_p(4) \mid p$

$\text{ord}_p(4)$ ↗ 1 $\text{ord}_p(4)$

↘ p → troppo grande perché $\text{ord}_p(\dots) \mid (p-1)$

$\text{ord}_p(4) = 1 \iff 4^1 \equiv 1 \ (p) \iff 4 \equiv 1 \ (p)$

$\Rightarrow \boxed{p=3}$ È banale controllare che $3 \in D$.

— o — o —

(d) Tutti gli elementi di D sono multipli di 3.

Sia n t.c. n divide 2^n+1 e SIA p il + piccolo primo che divide n

Voglio dim. che $p=3$.

n divide $2^n+1 \iff 2^n \equiv -1 \ (n)$

$\Rightarrow 2^n \equiv -1 \ (p)$

$\Rightarrow 4^n \equiv 1 \ (p)$

$\iff \boxed{\text{ord}_p(4) \mid n}$ FATTO 1 (dalle Hp del problema)

$\boxed{\text{ord}_p(4) \mid (p-1)}$ FATTO 2 (teo. generale)

FATTO 1 + FATTO 2 $\Rightarrow$ $\text{ord}_p(4) \mid$ $\boxed{\text{MCD tra } n \text{ e } (p-1)}$

UGUALE AD 1

Il MCD è uguale ad 1 perchè p è il + piccolo primo che divide n, quindi n e p-1 non possono avere fattori in comune.

$\Rightarrow \text{ord}_p(4) = 1 \Rightarrow$ (come prima) $4^1 \equiv 1 \ (p) \Rightarrow p = 3$

— o — o —

Variante

$$E = \{ n \in \mathbb{N} : 12^n + 1 \text{ è multiplo di } n \}$$

Tesi: tutti gli elementi di E sono multipli di 13

Sia p il + piccolo primo che divide n

$$12^n + 1 \equiv 0 \ (n) \iff 12^n \equiv -1 \ (n)$$

$$\Rightarrow 12^n \equiv -1 \ (p)$$

$$\Rightarrow 144^n \equiv 1 \ (p)$$

$$\Rightarrow \operatorname{ord}_p(144) \mid n \quad \leftarrow \text{FATTO 1}$$

$$\operatorname{ord}_p(144) \mid (p-1) \quad \leftarrow \text{FATTO 2}$$

$\Rightarrow \operatorname{ord}_p(144)$ | MCD tra n e $p-1$ che è 1

$\Rightarrow \operatorname{ord}_p(144) = 1 \Rightarrow 144^1 \equiv 1 \ (p) \Rightarrow 11 \cdot 13 \equiv 0 \ (p)$

$p =$ 11 → Non va bene perché $12^n \equiv -1 \ (11)$ il che è assurdo

13 → OK

— o — o —

(c) $D = \{ n \in \mathbb{N} : n \text{ divide } 2^n + 1 \}$ $(n > 1)$

$n = pq$ con p e q primi $\Rightarrow$ wlog $p = 3$

$n = 3q$

$2^{3q} \equiv -1 \ (3q) \iff 8^q \equiv -1 \ (3q)$

$\Rightarrow 64^q \equiv 1 \ (3q)$

$\Rightarrow 64^q \equiv 1 \ (q)$

$\Rightarrow \text{ord}_q(64) \mid q$

$\Rightarrow \text{ord}_q(64) = \begin{cases} \boxed{1} \\ q \rightarrow \text{Troppo grande perché ord} \mid (q-1) \end{cases}$

$\Rightarrow 64 \equiv 1 \ (q) \Rightarrow q = \begin{cases} 3 \\ 7 \end{cases}$

Verifica $q=3$, cioè $n=3$ $\quad 3 \mid 2^3+1 \iff 3 \mid 513$ Ok

Verifica $q=7$, cioè $n=21$ $\quad 21 \mid 2^{21}+1$

$2^{21}+1 \overset{?}{\equiv} 0 \quad (21)$

$2^{21}+1 \equiv 0 \quad (3)$ Ok

$2^{21}+1 \equiv 0 \quad (7)$

$2^{21}+1 \equiv (2^3)^7+1 \equiv 2 \quad (7)$ NO

L'unica soluzione è $p=3$, $q=3$.

— o — o —

(e) $n = p^2 q$, cioè $n = 3p^2$ o $n = 9q$

DISTINTI

$\boxed{n=3p^2}$ $\quad 2^n \equiv -1 \quad (n) \iff 2^{3p^2} \equiv -1 \quad (3p^2)$

$\Rightarrow 8^{p^2} \equiv -1 \quad (3p^2)$

$$\Rightarrow 64^{p^2} \equiv 1 \quad (3p^2)$$

$$\Rightarrow 64^{p^2} \equiv 1 \quad (p)$$

Butto via tanto !!

$$\Rightarrow \operatorname{ord}_p(64) \mid p^2 \quad \Rightarrow \operatorname{ord}_p(64) = \begin{cases} 1 \\ p \\ p^2 \end{cases}$$ Troppo grandi

$$\Rightarrow \operatorname{ord}_p(64) = 1 \quad \Rightarrow \quad p = \begin{cases} 3 \\ 7 \end{cases}$$

cioè $\boxed{n = 27}$, $n = 3 \cdot 7^2$

p e q non sono distinti

Resta da verificare $n = 3 \cdot 7^2$ ← NO

$$2^{3 \cdot 7^2} + 1 \equiv 8^{7^2} + 1 \equiv 2 \pmod 7$$

quindi non può essere $\equiv 0 \pmod{3 \cdot 7^2}$

$n = 99$

$$2^n + 1 \equiv 0 \ (n) \iff 2^n \equiv -1 \ (n)$$

$$\iff 2^{99} \equiv -1 \ (99)$$

$$\iff 512^9 \equiv -1 \ (99)$$

$$\Rightarrow 512^{29} \equiv 1 \ (99)$$

$$\Rightarrow 512^{29} \equiv 1 \ (9)$$

$$\text{ord}_9(512) \mid 29$$

$$\Rightarrow \text{ord}_9(512) = \begin{cases} 1 \\ 2 \\ 9 \\ 29 \end{cases}$$

1 → si dimostra che non va bene

9, 29 → Troppo grandi

Se $\text{ord}_q(512) = 1$, allora $512 \equiv 1 \pmod q$, ma allora

$512^9 \equiv 1 \pmod q$ ma noi sappiamo che

$512^9 \equiv -1 \pmod q$ assurdo perché non può essere $q = 2$ per 1000 motivi

L'unica poss. rimasta è che $\text{ord}_q(512) = 2$

$\Rightarrow 512 \equiv -1 \pmod q \Rightarrow 513 \equiv 0 \pmod q$

$\Rightarrow q$ divide $513 = 27 \cdot 19$

$\Rightarrow q = \begin{cases} 3 \leftarrow \text{no perché li volevamo distinti} \\ 19 \leftarrow \text{sì dopo verifica.} \end{cases}$

L'unica soluzione del tipo pq^2 (con $p \neq q$) è $9 \cdot 19$

(b) Trovare tutte le potenze di un primo in D

$n = p^k$, quindi $n = 3^k$

$k=1$	$3 \mid 2^3+1$	$\rightsquigarrow$ ok
$k=2$	$9 \mid 2^9+1$	$\rightsquigarrow$ ok
$k=3$	....	$\rightsquigarrow$ ok

Congettura: $3^k \mid (2^{3^k}+1)$ per ogni k, quindi tutte le potenze di 3 vanno bene

Induzione: $k=1$ e $k=2$ ok

$k \Rightarrow k+1$

$$2^{3^{k+1}} + 1 = 2^{3 \cdot 3^k} + 1 = \left[2^{3^k}\right]^3 + 1 \qquad A^3+1$$

$$= \left(2^{3^k}+1\right)\left(2^{2 \cdot 3^k} - 2^{3^k} + 1\right)$$

$$(A+1)\left(A^2 - A + 1\right)$$

$$= \underbrace{\left(2^{3^k}+1\right)}_{\text{Divisibile per } 3^k}\underbrace{\left(2^{2\cdot 3^k}-2^{3^k}+1\right)}_{\text{ci basta che sia divisibile per 3}}$$

lo è perché modulo 3 è $1-2+1\equiv 0$

$\Rightarrow$ ogni passaggio guadagno ALMENO un fattore 3.

—o—o—

(b) esteso Abbiamo dim. che

$3^k \mid 2^{3^k}+1$

$k=1$ $\quad 3 \mid 2^3+1$ anche $9 \mid 2^3+1$

$k=2$ $\quad 9 \mid 2^9+1$ anche $27 \mid 2^9+1$

Congettura: $3^{k+1} \mid 2^{3^k}+1$. Dimostrazione: stessa di prima, perché ad ogni passaggio guadagno un 3+ passo base vero

Ulteriore rilancio:

$$3^{k+1} \parallel 2^{3^k} + 1$$

Dim: ① Vero nel passo base

② Far vedere che nel passo induttivo si guadagna un 3 ma non un 9.

$$\left(2^{2\cdot 3^k} - 2^{3^k} + 1\right) \quad \text{modulo } 9$$

$2^{2\cdot 3^k} = 2^{\text{multiplo di } 6} \equiv 1 \quad (9)$ LFT

$2^{3^k} = 2^{\text{multiplo dispari di } 3} = 8^{\text{dispari}} \equiv -1 \quad (9)$

TUTTO MODULO 9 è $1 - (-1) + 1 \equiv 3 \pmod 9$

FATTO GENERALE p primo

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

quali fattori primi può avere questo termine $P(a)$

Supponiamo che un primo q divida $P(a)$ $\iff$

$$P(a) \equiv 0 \quad (q) \implies a^p - 1 \equiv 0 \quad (q)$$

$$\iff a^p \equiv 1 \quad (q)$$

$$\implies \mathrm{ord}_q(a) \mid p$$

$$\implies \mathrm{ord}_q(a) = \begin{cases} 1 \\ p \end{cases}$$

Caso 1: $\mathrm{ord}_q(a) = 1 \Rightarrow a \equiv 1 \pmod q$

$\Rightarrow P(a) \equiv 1^{p-1} + 1^{p-2} + \dots + 1 + 1 \equiv p \equiv 0 \pmod q$

$\Rightarrow \boxed{q = p}$

Caso 2: $\mathrm{ord}_q(a) = p$, ma allora $p = \mathrm{ord} \dots \mid (q-1)$

quindi $q \equiv +1 \pmod p$

Prima conclusione: se q divide $P(a)$, allora

- $q = p$
- $q \equiv 1 \pmod p$

Seconda conclusione: se $q = p$, allora

$$P(a) \equiv p \pmod{p^2} \quad \text{cioè} \quad p \,\|\, P(a)$$

Dimostrazione: siamo nel 1° caso, quello in cui $a \equiv 1 \ (p)$ p e q sono lo stesso

quindi $a = kp+1$, ma allora

$$P(a) = 1 + a + a^2 + a^3 + \dots + a^{p-1}$$

$$= 1 + (kp+1) + (kp+1)^2 + (kp+1)^3 + \dots \quad \text{MODULO } p^2$$

$$= 1 + (kp+1) + (1+2kp) + (1+3kp) + (1+4kp) + \dots$$

$$= p + kp\,\underbrace{(1+2+3+\dots+(p-1))}_{\text{multiplo di } p} \equiv p \pmod{p^2}$$

p: somma di tutti gli 1