Senior 2006 - Teoria dei numeri 2 - 4, 7, 9, 10

Titolo nota 13/09/2006

7 $2^n \equiv n \pmod p$

$n \equiv 1 \pmod p$ $\qquad n = kp+1$

$2^{kp+1} \equiv 1 \pmod p$ $\qquad (2^{p-1})^k \equiv 1$

$p-1 \mid kp+1 = n$

$$\begin{cases} n \equiv 1 \pmod p \\ n \equiv 0 \pmod{p-1} \end{cases}$$

9 $n = 5^{5^{5^5}} \equiv$ $\qquad 10^5 = 5^5 \cdot 2^5$

$5^{5^{5^5}} \equiv 5^{16J+5} \equiv 5^5 \pmod{32}$

$\phi(32) = 16$

$5^{5^{5^5}} \equiv 5^{8R+5} \equiv 5 \pmod{16}$

$5^{5^5} \equiv 5^{4K+1} \equiv 5^{4K} \cdot 5 \equiv 5 \pmod{8}$

$5^5 \equiv 5^{2+2} \cdot 5^1 \equiv 5 \equiv 1 \pmod{4}$

$5 \equiv 1 \pmod{2}$

$$\begin{cases} n \equiv 0 \pmod{5^5} \\ n \equiv 5^5 \pmod{2^5} \end{cases} \Rightarrow n \equiv 5^5 \pmod{100000}$$

03125

9

d = ragione

m = lunghezza

$$\begin{cases} x + d \equiv 0 & (p_1^m) \\ x + 2d \equiv 0 & (p_2^m) \\ \vdots & \\ x + md \equiv 0 & (p_m^m) \end{cases}$$

10 $D = \{ n \in \mathbb{N} \mid n \mid 2^n + 1 \}$

1. $p \in D$?

$2^m \equiv -1 \quad (m)$

$2^p \equiv -1 \quad (p)$

$2^p \equiv 2^{p-1} \cdot 2 \equiv 1 \cdot 2 \equiv -1 \quad (p)$

$3 \equiv 0 \quad (p)$ $\quad p = 3.$

2. $p^k \in D$.

$2^{p^k} \equiv -1 \quad (p^k)$

$2^{p^k} \equiv -1 \quad (p)$

$\underbrace{((2^p)^p)^{p \cdots p}}_{*} \equiv 2 \equiv -1 \quad (p)$ $\quad p = 3$

$a^{p-1} \equiv 1 \quad (p)$

$a^p \equiv a \quad (p)$

3^K INDUZIONE SU K:

$K=1$

$2^3 \equiv -1 \ (3)$ ✓

$2^{3^K} \equiv -1 \ (3^K)$

$b = 2^{3^K}$ $\quad b \equiv -1 \ (3^K)$

$3^K \mid b+1$

$b \equiv -1 \ (3)$

$b^2 - b + 1 \equiv 1 - (-b) + 1 \equiv 0 \ (3)$

$2^{3^{K+1}} \equiv -1 \ (3^{K+1})$

$\left(2^{3^K}\right)^3 \overset{?}{\equiv} -1 \ (3^{K+1})$

$b^3 \overset{?}{\equiv} -1 \ (3^{K+1})$

$3^{K+1} \mid b^3 + 1 = (b+1)(b^2 - b + 1)$

$3^K \quad 3 \quad ?$

$3^{K+1} \mid \left(2^{3^K}\right)^3 + 1 = 2^{3^{K+1}} + 1$

4. $2^m \equiv -1 \pmod m$

IL PIÙ PICCOLO PRIMO CHE DIVIDE m

$2^m \equiv -1 \pmod p$

$2^{2m} \equiv 1 \pmod p$

$\begin{cases} \mathrm{ord}_p(2) \mid 2m \\ \mathrm{ord}_p(2) \mid p-1 \end{cases} \Rightarrow \mathrm{ord}_p(2) \mid (2m, p-1) = \boxed{2}$

$\mathrm{ord}_p(2) = \frac{1}{2}$

① $\mathrm{ord}_p(2) = 1$

$2 \equiv 1 \pmod p$

$1 \equiv 0 \pmod p$ NO

② $\mathrm{ord}_p(2) = 2$

$2^2 \equiv 1 \pmod p \Rightarrow \boxed{p=3}$

3. $pq \in D$

$p=3$ $\quad 3q \mid 2^{3q} \equiv -1 \quad (3q)$

$$\begin{cases} 2^{3q} \equiv -1 \ (3) \Rightarrow (-1)^q \equiv 1 \\ 2^{3q} \equiv -1 \ (q) \Rightarrow (2^3)^q \equiv -1 \ (q) \end{cases}$$

$$2^3 \equiv -1 \ (q)$$

$$3 \cdot 3 = 9 \equiv 0 \ (q) \quad \boxed{q=3}$$

$p=3, \ q=3$

5. $p^2 q \in D$

1. $q=3$ $\quad 2^{3p^2} \equiv -1 \quad (3p^2)$

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

$$((2^3)^p)^p \equiv (2^3)^p \equiv 2^3 \equiv -1 \ (p)$$

$$9 \equiv 0 \ (p)$$

$p=3$ NON ACCETTABILE

2. $p=3$ $\quad 2^{9q} \equiv -1 \pmod{9q}$

$(2^9)^q \equiv -1 \pmod{9}$

$2^9 \equiv -1 \pmod{9} \Rightarrow 2^9+1 \equiv 0 \pmod{9}$

$9 \mid 513 = 3^3 \cdot 19$

$9 \neq 3 \quad 9 = 19$

$2^{9 \cdot 19} \equiv -1 \pmod{9 \cdot 19}$

$2^{9 \cdot 19} \equiv -1 \pmod{9}$ $\quad \phi(9) = 6 = \phi(3^2) = 3^2 - 3$

$(2^{6+3})^{19} \equiv (2^3)^{19} \equiv 2^3 \equiv -1 \pmod{9}$

$p=3 \quad 9=19$

FINE