S25 M/A-CN

Titolo nota 06/09/2025

PROBLEMI CONSIGLIATI × IL MEDIUM: 1-2-3-4
L'ADVANCED: 3-4-5-6-7

~16 INIZIO CORREZIONE

[TYPO SUL 6 ∀C... LA MEDIA ~~È UN INTERO~~ NON STIA IN A]

P1) $S \subseteq \mathbb{Z}/n\mathbb{Z}$ $|S| > n/2$ $\exists a,b,c \in S$ $a \cdot b \equiv c \pmod n$

$S \cdot S = \{a \cdot b \pmod n \mid a,b \in S\}$, vorremmo che $|S \cdot S| > n/2$, cosicché $|S \cdot S| + |S| > n \Rightarrow S \cdot S$ e S non sono disgiunti.

In particolare, basterebbe aver $|S \cdot S| \geq |S|$

$\exists a \in S$ $(a,n) = 1$ $a \cdot S = \{a \cdot b \mid b \in S\}$ $|a \cdot S| = |S|$

infatti se $a \cdot b \equiv a \cdot c \Rightarrow b \equiv c$ $\Rightarrow |S \cdot S| \geq |a \cdot S| = |S|$

Non è detto che esista $a \in S$ invertibile però $\varphi(n)/n$ può essere arbitrariamente basso

Consideriamo quindi $C_d = \{a \in \mathbb{Z}/n\mathbb{Z} \mid (b, n) = d\}$

$\mathbb{Z}/n\mathbb{Z} = \bigsqcup_{d \mid n} C_d$ $S = \bigsqcup_{d \mid n} S_d$ $S_d = S \cap C_d$

$|S| > n/2 = |\mathbb{Z}/n\mathbb{Z}|/2 \Rightarrow \exists d$ t.c. $|S_d| > |C_d|/2$

Oss se $a,b \in C_d \Rightarrow a \cdot b \in C_d$ (↑ non è squarefree)

Prendiamo C_d, consideriamo $a \in C_d \Rightarrow a = a' \cdot d$

$a \cdot b \equiv a \cdot c \Rightarrow d^2 a' \cdot b' \equiv d^2 \cdot a' \cdot c' \pmod n$

[con $a,b,c \in C_d \cap S \Rightarrow \begin{matrix} a = a' \cdot d \\ b = b' \cdot d \\ c = c' \cdot d \end{matrix}$ a', b', c' coprimi con n/d]

$\Rightarrow \quad d \cdot a' \cdot b' \equiv d \cdot a' \cdot c' \pmod{n/d}$

$\Rightarrow d \cdot b' \equiv d \cdot c' \pmod{n/d}$

$\underset{n \text{ squarefree}}{\Longrightarrow} \quad b' \equiv c' \pmod{n/d} \Rightarrow b \equiv c \pmod{n}$.

$\Rightarrow \quad |S_d \cdot S_d| \geq |a \cdot S_d| = |S_d| > |C_d|/2$

$|S_d \cdot S_d| + |S_d| > |C_d| \Rightarrow (S_d \cdot S_d) \cap S_d \neq \emptyset$. □

P2)

$$\left[x_1 \cdot x_2 (x_1 - y_1)(x_2 - y_2)\right]^{\frac{n-1}{2}} \equis 1 \pmod{n}$$

Se n è composto, vince Lind., si sceglie $x_1 = q \mid n$, $0 < q < n$ così che $[\dots]$ non è coprimo con n.

Se $n = p$ è primo, allora $[\dots]^{\frac{p-1}{2}} \equiv 1 \pmod{p} \iff$

$[\dots] = QR \bmod p$

Vogliamo che $x_1(x_1 - y_1)$ e $x_2(x_2 - y_2)$ siano
(QR e QR)
oppure
(NQR e NQR)

Se avessimo $y_1 = a x_1$ $y_2 = b x_2$ $\Rightarrow$

$$x_1 (1-a) x_1 \cdot x_2 \cdot (1-b) x_2 = QR \cdot (1-a) \cdot (1-b)$$

$\Rightarrow$ basta che $(1-a)(1-b)$ sia QR

Vorremmo garantire che $a = b$. Per far ciò, l'unico è che $a \equiv -1$

In altre parole, se L sceglie x, S sceglie $-x$

$\Rightarrow (1-(-1)) \cdot (1-(-1)) \equiv 4 \Rightarrow [\dots] \equiv QR$.

$[\dots] = 4 x_1^2 x_2^2 = (2 x_1 x_2)^2$.

P3 | Magistrini $\leftrightarrow \{1,\dots,2026\} = \mathbb{F}_p^\times$ $\quad p = 2027 \in \mathbb{P}$

biglietti rossi $\leftrightarrow \sigma : \mathbb{F}_p^\times \to \mathbb{F}_p^\times$ permutazione

biglietti blu $\leftrightarrow \tau : \mathbb{F}_p^\times \to \mathbb{F}_p^\times$

$(\sigma, \tau) \longmapsto (\sigma', \tau')$

$\sigma'(\tau(i)) = \sigma(i)$, $\tau'(i) = \tau(i)$ $\rightarrow$ $\sigma' = \sigma \circ \tau^{-1}$, $\tau' = \tau$

$\tau' = \tau \circ \sigma^{-1}$, $\sigma' = \sigma$

OSS Tutte le permutazioni sul problema sono della forma

$\sigma_A(x) \equiv A \cdot x \pmod p$ $\quad A \not\equiv 0 \pmod p$

$\sigma_A \circ \sigma_B = \sigma_{A \cdot B}$

$\sigma_A^{-1} = \sigma_{A^{-1}}$

$\rightsquigarrow$ $(A, B) \longmapsto (A \cdot B^{-1}, B)$

$\longmapsto (A, B \cdot A^{-1})$

(OBBIETTIVO = ARRIVARE A $(1, \not{1})$)

$\rightarrow$ Fissato un generatore modulo p, ci riconduciamo a un problema "additivo" su $\mathbb{Z}/(p-1)\mathbb{Z}$

$(\alpha, \beta) \longmapsto (\alpha - \beta, \beta)$

$\longmapsto (\alpha, \beta - \alpha)$

$A \equiv g^a \rightsquigarrow \alpha$

(OBB. = arrivare a $(0, \dots)$)

Questo problema ricorda l'alg. di Euclide

$\rightsquigarrow$ arriviamo $(d, 0)$ $(0, d)$ se siamo arrivati:

$a(\alpha, 0) \to (\alpha, -\alpha) \to (2\alpha, -\alpha) \to (3\alpha, -\alpha) \to \dots \to (0, -\alpha) \pmod{p-1}$

□

---

5 $n \geq 3$ fissato. $\exists N$ | $\forall p > N$, $\exists x, y, z \in \{1, \dots, p-1\}$ tali che

$$x^n + y^n = z^n \pmod p$$

$$g^{n\alpha} + g^{n\beta} = g^{n\gamma} \quad (p)$$

$$\Leftarrow \left(g^{(n,p-1)\alpha} + g^{(n,p-1)\beta} = g^{(n,p-1)\gamma} \right) (p)$$

$d = (n, p-1)$

$$g^{d\alpha + h} + g^{d\beta + h} = g^{d\gamma + h} \quad (p)$$

$0 < h \leq d \leq n$

Le terne x, y, z della stessa colore $x + y = z$

Lemma di Schur: $\forall r$ intero positivo, $\exists R(r)$ tale che ogni r-colorazione di $\{1, \dots, R(r)\}$, ha 3 interi mono colore $x + y = z$

6 A infinito di interi. p è un primo.

$\exists B \subseteq A$, $|B| = 2p-2$, $\forall C \subseteq B$, $|C| = p$,

$[M(X) =$ media aritm. degli elementi di $X]$

$M(C) \notin A$.

Supponiamo che 2 classi di resto si ripetano infinite volte

$B = B_1 \sqcup B_2$, $b_1 \equiv r_1 \ (p) \ \forall b_1 \in B_1$, $b_2 \equiv r_1' \ (p)$
$\forall b_2 \in B_2$

$$\frac{t r_1 + (p-t) r_1'}{p} = \frac{p r_1' + t(r_1 - r_1')}{p} = r_1 + t\frac{(r_1 - r_1')}{p}$$

Per induzione, $\forall \alpha \in A$, $\alpha > N(n)$, $\alpha \equiv r_n(p^n)$

Supponiamo ∞ molti $\alpha \equiv r_{n+1}(p^{n+1})$, $\alpha \equiv r'_{n+1}(p^{n+1})$

$B = B_1 \sqcup B_2$ $\quad b_1 \equiv r_{n+1}(p^{n+1})$, $b_2 \equiv r'_{n+1}(p^{n+1})$

$$\frac{t r_{n+1} + (p-t) r'_{n+1}}{p} \equiv r_n(p^n)$$

$r'_{n+1} \equiv r_n(p)$

$$\frac{p r'_{n+1}}{p} + \frac{t(r_{n+1} - r'_{n+1})}{p} \equiv r_n(p^n)$$

$$t(r_{n+1} - r'_{n+1}) \equiv 0 \quad (p^n)$$

$$r_{n+1} \equiv r'_{n+1} \quad (p^{n+1}) \;\}$$

$\forall n$, per valori di $\alpha \in A$ molto grandi, si ha $\alpha \equiv r_n(p^n)$

$B = B_1 \sqcup B_2$ ——> "grandi"

$\downarrow$ "piccoli"

$$\frac{(p-t) r_k + \overbrace{\sum_i b_i}}{p} \equiv r_n(p^n)$$

$$\frac{p r_n}{p} + \frac{\ldots - t r_n}{p} \equiv r_n \quad (p^n)$$

$x \equiv \pm r_n \ (p^{n+1})$ $\quad 0 \le r_n < p^n$

$0 \le \pm r_n < p^{n+1}$

Se $r_n \to \infty$ quando $n \to \infty$

x fissato $\quad x = \pm r_n$ assurdo.

r_n è definitivamente costante. (dipende da A

Scelgo gli elementi di $B_1 > p r_\infty$

Quindi anche le somme x sono $> p r_\infty \geq \pm r_n$ per n sufficientemente grande $\square$