

4 Generalità sulle congruenze polinomiali, Teorema di Lagrange e Teorema di Chevalley

Sia $f(X)$ un polinomio non nullo a coefficienti interi ed n un intero positivo. Ci occuperemo ora della ricerca delle (eventuali) soluzioni della congruenza polinomiale:

$$f(X) \equiv 0 \pmod{n}. \quad (1)$$

Vale in proposito il seguente risultato:

Teorema 4.1. *Sia $n = p_1^{e_1} p_2^{e_2} \cdot \dots \cdot p_r^{e_r}$, con p_i primo, $e_i \geq 1$ ed $r \geq 1$. Le soluzioni della congruenza (1) coincidono con le soluzioni del sistema di congruenze:*

$$\begin{cases} f(X) \equiv 0 \pmod{p_i^{e_i}} \\ 1 \leq i \leq r. \end{cases} \quad (2)$$

Dimostrazione. Se \hat{x} è una soluzione di (1), ovviamente \hat{x} è anche soluzione di ogni congruenza del sistema (2). Viceversa, se \hat{x} è soluzione di (2), allora $p_i^{e_i} \mid f(\hat{x})$ per ogni i , e, poiché $\text{MCD}(p_i^{e_i}, p_j^{e_j}) = 1$ (se $i \neq j$), possiamo concludere che $n = p_1^{e_1} \dots p_r^{e_r} \mid f(\hat{x})$ (cfr. Esercizio 1.2). \square

Osservazione 4.2. Supponiamo che, fissato i , con $1 \leq i \leq r$, $f(X) \equiv 0 \pmod{p_i^{e_i}}$ ammetta s_i soluzioni distinte, che denotiamo con y_{ij_i} ($1 \leq j_i \leq s_i$). Posto $s := \prod_{i=1}^r s_i$, al variare di i , $1 \leq i \leq r$, per ogni scelta di y_{ij_i} con $1 \leq j_i \leq s_i$ si ottiene un sistema di congruenze lineari del tipo:

$$\begin{cases} X \equiv y_{ij_i} \pmod{p_i^{e_i}} \\ 1 \leq i \leq r. \end{cases}$$

In base al Teorema Cinese dei Resti ed al Teorema 4.1, ciascuno di tali s sistemi di congruenze fornisce una sola soluzione alla congruenza (1) ed è evidente che sistemi diversi forniscono soluzioni incongruenti (modulo n); dunque (2) ammette $s = \prod_{i=1}^r s_i$ soluzioni distinte.

Dal precedente ragionamento discende che, se denotiamo con $N(f(X), n)$ il numero delle soluzioni della congruenza (1) e se $n = hk$ con $\text{MCD}(h, k) = 1$, allora:

$$N(f(X), n) = N(f(X), h) \cdot N(f(X), k).$$

Ad esempio le soluzioni della congruenza:

$$X^2 + 3X + 2 \equiv 0 \pmod{6}$$

sono le stesse del sistema di congruenze:

$$\begin{cases} X^2 + 3X + 2 \equiv 0 \pmod{2} \\ X^2 + 3X + 2 \equiv 0 \pmod{3} \end{cases}$$

ovvero:

$$\begin{cases} X^2 + X \equiv 0 \pmod{2} \\ X^2 + 2 \equiv 0 \pmod{3} \end{cases}.$$

La prima congruenza del sistema ha soluzioni $\{y_{11} = 0, y_{12} = 1\} \pmod{2}$, la seconda congruenza ha soluzioni $\{y_{21} = 1, y_{22} = 2\} \pmod{3}$. Le soluzioni dei quattro sistemi seguenti, ottenuti variando $i, 1 \leq i \leq 2$, e $j, 1 \leq j \leq 2$,

$$\begin{cases} X \equiv y_{1i} \pmod{2} \\ X \equiv y_{2j} \pmod{3} \end{cases}$$

sono date da $x = 4, 1, 2, 5 \pmod{6}$. Questi valori di x sono, dunque, tutte le soluzioni della congruenza data $\pmod{6}$.

Dalle considerazioni precedenti discende anche che il problema della risoluzione di (2) può essere ricondotto allo studio di due problemi.

I PROBLEMA: Determinare le soluzioni di un sistema di congruenze lineari del tipo:

$$\begin{cases} X \equiv a_i \pmod{m_i} \\ 1 \leq i \leq r \end{cases}$$

con $a_i \in \mathbb{Z}$ e $\text{MCD}(m_i, m_j) = 1$ se $i \neq j$.

II PROBLEMA: Determinare le soluzioni di una congruenza polinomiale del tipo:

$$f(X) \equiv 0 \pmod{p^e}$$

con $f(X) \in \mathbb{Z}[X], f(X) \neq 0, p$ primo ed $e \geq 1$.

Al I Problema dà completa risposta il Teorema Cinese dei Resti (cfr. Paragrafo 3). Un metodo di approccio al II Problema consiste in un procedimento di tipo induttivo:

II PROBLEMA (A): Determinare le soluzioni di una congruenza polinomiale del tipo:

$$f(X) \equiv 0 \pmod{p}$$

con $f(X) \in \mathbb{Z}[X], f(X) \neq 0$ e p primo.

II PROBLEMA (B): Supponendo di aver determinato le soluzioni di una congruenza polinomiale del tipo:

$$f(X) \equiv 0 \pmod{p^n},$$

determinare le soluzioni della congruenza:

$$f(X) \equiv 0 \pmod{p^{n+1}},$$

con $f(X) \in \mathbb{Z}[X]$, $f(X) \neq 0$, p primo ed $n \geq 1$.

In altri termini, una soluzione di $f(X) \equiv 0 \pmod{p^e}$ per $e \geq 2$ è determinata per successive approssimazioni (a meno di potenze di p) a partire dalle soluzioni di $f(X) \equiv 0 \pmod{p}$. L'algoritmo che descriveremo è ispirato al cosiddetto metodo di Newton utilizzato in analisi.

Affrontiamo dapprima il II Problema (B). A tale scopo richiamiamo alcune proprietà formali dei polinomi.

Definizione 4.3. Sia $f(X) = \sum_{i=0}^m a_i X^i \in \mathbb{Z}[X]$. Si chiama *polinomio derivato di $f(X)$* il polinomio:

$$(f(X))' := a_1 + 2a_2 X + \cdots + m a_m X^{m-1} = \sum_{i=1}^m i a_i X^{i-1}.$$

Per comodità di notazione il polinomio $(f(X))'$ verrà denotato in seguito anche con $f'(X)$, o semplicemente con f' , se non ci saranno pericoli di ambiguità.

In generale, si chiama *k -esimo polinomio derivato di $f(X)$* (con $k \geq 1$) il polinomio $f^{(k)} := f^{(k)}(X) := (f^{(k-1)}(X))'$.

Si conviene di porre $f(X) =: f^{(0)}(X)$.

Il seguente risultato è di dimostrazione immediata:

Lemma 4.4. *Siano $f, g \in \mathbb{Z}[X]$ ed $a \in \mathbb{Z}$. Allora:*

(a) $(f + g)' = f' + g'$;

(b) $(af)' = af'$;

(c) $(fg)' = f'g + fg'$. □

Vale, inoltre, il seguente risultato “formale” analogo alla formula di Taylor:

Lemma 4.5. *Sia $f(X) = \sum_{i=0}^m a_i X^i \in \mathbb{Z}[X]$, con $m := \deg(f(X))$. Per ogni $\alpha \in \mathbb{Z}$ si ha:*

$$f(X + \alpha) = f(X) + \frac{f'(X)}{1!} \alpha + \frac{f''(X)}{2!} \alpha^2 + \cdots + \frac{f^{(m)}(X)}{m!} \alpha^m.$$

Inoltre, per ogni k tale che $0 \leq k \leq m$, risulta:

$$\frac{f^{(k)}(X)}{k!} \in \mathbb{Z}[X].$$

Dimostrazione. In base al Lemma 4.4 (a), (b) (cioè, per “la proprietà di linearità” della derivazione), è sufficiente limitarsi al caso in cui $f(X) = X^i$. In tal caso, $f^{(k)}(X) = i(i-1)\dots(i-k+1)X^{i-k}$, per ogni k , con $0 \leq k \leq i$. Si ha allora, in base alla Definizione 4.3 ed alla nota formula del binomio di Newton¹:

$$\begin{aligned} f(X + \alpha) &= (X + \alpha)^i = \sum_{k=0}^i \binom{i}{k} X^{i-k} \alpha^k = \\ &= \sum_{k=0}^i \frac{i(i-1)\dots(i-k+1)}{k!} X^{i-k} \alpha^k = \\ &= \sum_{k=0}^i f^{(k)}(X) \frac{1}{k!} \alpha^k. \end{aligned}$$

L'ultima affermazione del lemma è ovvia, in quanto, in generale per

$$f(X) = \sum_{i=0}^m a_i X^i,$$

risulta:

$$\frac{f^{(k)}(X)}{k!} = \sum_{i=k}^m \binom{i}{k} a_i X^{i-k},$$

dove $\binom{i}{k}$, per $0 \leq k \leq i$, è un intero essendo uguale a $\frac{i!}{k!(i-k)!}$. \square

Osservazione 4.6. Sia $f(X) \in \mathbb{Z}[X]$ come nel lemma precedente, se calcoliamo tale polinomio in un intero $\dot{x} \in \mathbb{Z}$ e se poniamo $x := \dot{x} + \alpha$ allora dal lemma precedente otteniamo la ben nota uguaglianza:

$$f(x) = f(\dot{x}) + \frac{f'(\dot{x})}{1!}(x - \dot{x}) + \frac{f''(\dot{x})}{2!}(x - \dot{x})^2 + \dots + \frac{f^{(m)}(\dot{x})}{m!}(x - \dot{x})^m.$$

Al Problema II (B) fornisce una risposta completa il seguente teorema:

Teorema 4.7. Sia $f(X) \in \mathbb{Z}[X]$, $f(X) \neq 0$; sia p un primo ed $n \in \mathbb{Z}$, $n > 0$. Supponiamo che la congruenza:

$$f(X) \equiv 0 \pmod{p^n} \tag{*}_n$$

¹Presi comunque $\alpha, \beta \in \mathbb{Z}[X]$ (ovvero, più generalmente, presi in un qualunque anello con caratteristica 0), si dimostra facilmente per induzione su $r \geq 1$ che:

$$(\alpha + \beta)^r = \sum_{k=0}^r \binom{r}{k} \alpha^{r-k} \beta^k$$

sia risolubile e che, di questa congruenza, siano note le soluzioni $\{y_1, \dots, y_r\} \pmod{p^n}$. Consideriamo la congruenza:

$$f(X) \equiv 0 \pmod{p^{n+1}} \quad (*_{n+1})$$

Le (eventuali) soluzioni di $(*_{n+1}) \pmod{p^{n+1}}$ sono della forma:

$$x_t := y + tp^n,$$

dove y è una soluzione di $(*_n)$ e $t \in \mathbb{Z}$, $0 \leq t \leq p-1$. Precisamente si presentano tre casi:

I Caso. Se $f'(y) \not\equiv 0 \pmod{p}$, x_t è soluzione di $(*_{n+1})$ se, e soltanto se, risulta:

$$t \equiv -\frac{f(y)}{p^n} (f'(y))^{p-2} \pmod{p}.$$

II Caso. Se $f'(y) \equiv 0 \pmod{p}$ e $f(y) \equiv 0 \pmod{p^{n+1}}$, allora x_t è soluzione di $(*_{n+1})$, per ogni t , con $0 \leq t \leq p-1$.

III Caso. Se $f'(y) \equiv 0 \pmod{p}$ e $f(y) \not\equiv 0 \pmod{p^{n+1}}$, x_t non è soluzione di $(*_{n+1})$, per nessun valore di t , con $0 \leq t \leq p-1$.

Consequentemente, la soluzione y di $(*_n)$, $y \in \{y_1, \dots, y_r\}$, determina:

- nel I Caso, una ed una sola soluzione di $(*_{n+1}) \pmod{p^{n+1}}$, e cioè:

$$x := y - f(y)(f'(y))^{p-2};$$

- nel II Caso, p soluzioni distinte di $(*_{n+1}) \pmod{p^{n+1}}$, e cioè:

$$x_t = y + tp^n, \quad 0 \leq t \leq p-1;$$

- nel III Caso, nessuna soluzione di $(*_{n+1}) \pmod{p^{n+1}}$.

[Nel I Caso, y è detta *soluzione non singolare* di $(*_n)$, mentre negli altri casi, y è detta *soluzione singolare* di $(*_n)$.]

Dimostrazione. Una (eventuale) soluzione di $(*_{n+1})$ è ovviamente soluzione di $(*_n)$ e dunque $x \equiv y \pmod{p^n}$, per un qualche y soluzione di $(*_n)$, cioè $y \in \{y_1, \dots, y_r\}$, ovvero $x = y + kp^n$, dove k è un intero opportuno. Poiché la soluzione x deve essere determinata $\pmod{p^{n+1}}$, allora dividendo k per p , abbiamo $k = qp + t$, dove $0 \leq t \leq p-1$. Quindi:

$$x = x_t := y + tp^n, \quad 0 \leq t \leq p-1.$$

Si noti che $f(y) \equiv 0 \pmod{p^n}$, quindi $f(y)/p^n \in \mathbb{Z}$.

In base al Lemma 4.5, posto $m := \deg(f(X))$, si ha:

$$f(x_t) = f(y + tp^n) = f(y) + \frac{f'(y)}{1!} tp^n + \dots + \frac{f^{(m)}(y)}{m!} (tp^n)^m.$$

Poiché $n + 1 \leq 2n < \dots < n \cdot m$, si ha $0 \equiv p^{2n} \equiv \dots \equiv p^{nm} \pmod{p^{n+1}}$ e quindi, dall'uguaglianza precedente, si ottiene:

$$f(x_t) \equiv f(y) + f'(y)tp^n \pmod{p^{n+1}}.$$

Pertanto $x_t = y + tp^n$ è soluzione di $(*_n)$ se, e soltanto se, esiste t , con $0 \leq t \leq p - 1$, tale che:

$$0 \equiv f(y) + f'(y)tp^n \pmod{p^{n+1}},$$

ovvero, “cancellando” p^n (cfr. Proposizione 1.9):

$$f'(y)t \equiv -\frac{f(y)}{p^n} \pmod{p}.$$

In conclusione, per ogni y soluzione di $(*_n)$, poniamo:

$$a = a(y) := f'(y), \quad b = b(y) := -\frac{f(y)}{p^n}.$$

Allora, per risolvere $(*_{n+1})$ ci siamo ricondotti a discutere della risolubilità della congruenza lineare in una nuova indeterminata (denotata T) con coefficienti $a = a(y)$, $b = b(y)$ che dipendono da y , al variare di y tra le soluzioni di $(*_n)$:

$$aT \equiv b \pmod{p} \quad (\bullet_y)$$

Per tale congruenza (\bullet_y) , distinguiamo tre casi:

I Caso. Se $a \not\equiv 0 \pmod{p}$, per ogni $y \in \{y_1, \dots, y_r\}$, la congruenza lineare (\bullet_y) ha una ed una sola soluzione $t \equiv a^{-1} \cdot b \equiv a^{p-2}b \pmod{p}$.

In tal caso, $x_t = y + p^nt \equiv y - p^n \frac{f(y)}{p^n} (f'(y))^{p-2} = y - f(y)(f'(y))^{p-2} \pmod{p^{n+1}}$ è l'unica soluzione di $(*_{n+1}) \pmod{p^{n+1}}$ determinata dalla soluzione y di $(*_n)$.

II Caso. Se $a \equiv b \equiv 0 \pmod{p}$, la congruenza (\bullet_y) degenera, cioè è soddisfatta per ogni t , con $0 \leq t \leq p - 1$.

In tal caso, per ogni $y \in \{y_1, \dots, y_r\}$, le soluzioni distinte di $(*_{n+1})$ (cioè non congruenti modulo p^{n+1}) sono esattamente p , e sono date da:

$$x_t = y + tp^n, \quad 0 \leq t \leq p - 1.$$

III Caso. Se $a \equiv 0 \pmod{p}$ e $b \not\equiv 0 \pmod{p}$, allora (\bullet_y) non è risolubile. Quindi, $x_t = y + tp^n$ non è mai soluzione di $(*_{n+1})$, comunque si prenda t , con $0 \leq t \leq p - 1$. Cioè, in altri termini, la soluzione $y \in \{y_1, \dots, y_r\}$ di $(*_n)$ non determina alcuna soluzione di $(*_{n+1})$. \square

Vogliamo illustrare il risultato precedente con quattro esempi.

Esempio 4.8. Consideriamo la congruenza:

$$X^4 - 1 \equiv 0 \pmod{25}.$$

Notiamo, innanzitutto, che $X^4 - 1 \equiv 0 \pmod{5}$, per il “Piccolo” Teorema di Fermat, ha quattro soluzioni: $y_1 = 1, y_2 = 2, y_3 = 3, y_4 = 4$.

Se $f(X) := X^4 - 1$ allora $f'(X) = 4X^3$. Essendo $f'(y_i) \not\equiv 0 \pmod{5}$ per ogni $1 \leq i \leq 4$, allora ciascuna y_i determina un'unica soluzione di $f(X) \equiv 0 \pmod{25}$ data da:

$$x_i := y_i + \bar{t}_i \cdot 5,$$

dove \bar{t}_i è l'unica soluzione (mod 5) della seguente congruenza lineare nella indeterminata T associata ad y_i (che denotiamo semplicemente con (\bullet_i) invece che con (\bullet_{y_i})):

$$a(y_i)T \equiv b(y_i) \pmod{5} \quad (\bullet_i)$$

dove $a(y_i) := f'(y_i)$ e $b(y_i) := -\frac{f(y_i)}{5}$, per $1 \leq i \leq 4$.

Per $i = 1$, $a(1) = 4$, $b(1) = 0$, quindi la congruenza:

$$4T \equiv 0 \pmod{5} \quad (\bullet_1)$$

ha come soluzione $\bar{t}_1 = 0$, dunque $x_1 = y_1 = 1 \pmod{25}$.

Per $i = 2$, $a(2) = 32$, $b(2) = -3$, quindi la congruenza:

$$2T \equiv -3 \pmod{5} \quad (\bullet_2)$$

ha come soluzione $\bar{t}_2 = 1$, dunque $x_2 = 2 + 1 \cdot 5 = 7 \pmod{25}$.

Per $i = 3$, $a(3) = 108$, $b(3) = -16$, quindi la congruenza:

$$3T \equiv -1 \pmod{5} \quad (\bullet_3)$$

ha come soluzione $\bar{t}_3 = 3$, dunque $x_3 = 3 + 3 \cdot 5 = 18 \pmod{25}$.

Per $i = 4$, $a(4) = 256$, $b(4) = -51$, quindi la congruenza:

$$T \equiv -1 \pmod{5} \quad (\bullet_4)$$

ha come soluzione $\bar{t}_4 = -1$, dunque $x_4 = 4 - 5 = -1 \equiv 24 \pmod{25}$.

Può essere utile riassumere il procedimento precedente nella seguente tabella:

p	n	$p^n \rightsquigarrow p^{n+1}$	$f(X)$	$f'(X)$
5	1	$5 \rightsquigarrow 25$	$X^4 - 1$	$4X^3$

mod p^n	mod p				mod p^{n+1}
y	$f'(y)$	$\frac{f(y)}{p^n}$	$f'(y)T \equiv -\frac{f(y)}{p^n}$	t	$x_t = y + tp^n$
1	4	0	$4T \equiv 0$	0	1
2	32	3	$2T \equiv -3$	1	7
3	108	16	$3T \equiv -1$	3	18
4	256	51	$T \equiv -1$	4	24

Il precedente esempio può essere generalizzato nella maniera seguente:

Esempio 4.9. Sia p un primo ed e un intero ≥ 1 . La congruenza:

$$f(X) := X^{p-1} - 1 \equiv 0 \pmod{p^e}$$

ha esattamente $p - 1$ soluzioni distinte.

Infatti, se $e = 1$, tale risultato è un'ovvia conseguenza del "Piccolo" Teorema di Fermat. Sia $e \geq 2$ e sia y una soluzione di $f(X) \equiv 0 \pmod{p^{e-1}}$. È subito visto che $f'(y) = (p-1)y^{p-2} \not\equiv 0 \pmod{p}$ (essendo $y^{p-1} \equiv 1 \pmod{p}$) e, dunque, si è nel I Caso del Teorema 4.7.

Esempio 4.10. Consideriamo la congruenza:

$$X^{10} - 1 \equiv 0 \pmod{25}.$$

Notiamo innanzitutto che la congruenza

$$X^{10} - 1 \equiv 0 \pmod{5}$$

ha due soluzioni: $y_1 = 1, y_2 = 4$.

Infatti $X^{10} = (X^4)^2 X^2$, dunque $X^{10} - 1 \equiv (X^4)^2 X^2 - 1 \pmod{5}$. Dal momento che, per il "Piccolo" Teorema di Fermat, $x^4 \equiv 1 \pmod{5}$, per ogni x non congruo a 0 $\pmod{5}$, allora le soluzioni di $X^{10} - 1 \equiv 0 \pmod{5}$ coincidono con le soluzioni di $X^2 - 1 \equiv 0 \pmod{5}$, che sono appunto $y_1 = 1$ ed $y_2 = 4$ (per maggiori dettagli, cfr. anche la successiva Definizione 4.12 (e)).

Se $f(X) := X^{10} - 1$, allora $f'(X) = 10X^9$ e quindi $f'(y_i) \equiv 0 \pmod{5}$ per $i = 1, 2$. Inoltre, $f(y_i) \equiv 0 \pmod{25}$, per $i = 1, 2$ (ciò è ovvio per $y_1 = 1$, per $y_2 = 4$ è subito visto che $4^5 \equiv -1 \pmod{25}$). Infatti, $4^2 \equiv -9 \pmod{25}$, $4^4 \equiv 81 \equiv 6 \pmod{25}$, $4^5 \equiv 24 \equiv -1 \pmod{25}$, dunque $4^{10} \equiv (-1)^2 \equiv 1 \pmod{25}$. Pertanto, y_1 determina le seguenti 5 soluzioni della congruenza data:

$$x_{1,t} := 1 + t \cdot 5, \quad \text{per } 0 \leq t \leq 4.$$

Analogamente, y_2 determina le seguenti 5 soluzioni della congruenza data:

$$x_{2,t} := 4 + t \cdot 5, \quad \text{per } 0 \leq t \leq 4.$$

In conclusione, la congruenza assegnata ha 10 soluzioni $\pmod{25}$. Può essere utile riassumere il procedimento precedente nella seguente tabella:

p	n	$p^n \rightsquigarrow p^{n+1}$	$f(X)$	$f'(X)$
5	1	$5 \rightsquigarrow 25$	$X^{10} - 1$	$10X^9$

mod p^n	mod p				mod p^{n+1}
y	$f'(y)$	$\frac{f'(y)}{p^n}$	$f'(y)T \equiv \frac{-f'(y)}{p^n}$	t	$x_t = y + tp^n$
1	0	0	\curvearrowright	0, 1, 2, 3, 4	1, 6, 11, 16, 21
4	0	0	\curvearrowright	0, 1, 2, 3, 4	74, 9, 14, 19, 24

L'esempio precedente si generalizza nella forma seguente:

Esempio 4.11. Sia p un primo dispari. La congruenza:

$$f(X) = X^{p\frac{p-1}{2}} - 1 \equiv 0 \pmod{p^2} \quad (*_2)$$

ammette $\frac{p(p-1)}{2}$ soluzioni distinte.

Si verifica preliminarmente che la congruenza $f(X) \equiv 0 \pmod{p}$ ammette esattamente $\frac{p-1}{2}$ soluzioni distinte.

Osserviamo, innanzitutto, che le soluzioni di:

$$f(X) = X^{p\frac{p-1}{2}} - 1 \equiv 0 \pmod{p} \quad (*_1)$$

sono le stesse di quelle della congruenza:

$$g(X) = X^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$$

dal momento che la congruenza $X^p \equiv X \pmod{p}$ ha come soluzioni tutti gli elementi di un sistema completo di residui (cfr. per maggiori dettagli la successiva Definizione 4.12 (e)).

Mostriamo, poi, che $g(X) \equiv 0 \pmod{p}$ ha esattamente $\frac{p-1}{2}$ soluzioni (mod p). Per questo, abbiamo bisogno del seguente

Lemma 4.12. *Sia p un primo dispari. Le due congruenze:*

$$X^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p} \quad (*)$$

$$X^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p} \quad (**)$$

ammettono ciascuna $\frac{p-1}{2}$ soluzioni distinte (modulo p). L'unione di tali insiemi di soluzioni costituisce un sistema ridotto di residui (modulo p).

Dimostrazione. Certamente $x = 0$ non è soluzione nè di (*) nè di (**) e le due congruenze non possono ammettere soluzioni comuni perché $p > 2$. Considerato il sistema ridotto di residui $S^* = \{1, 2, \dots, p-1\}$, basterà allora provare che (almeno) $\frac{p-1}{2}$ elementi di S^* verificano (*) e che (almeno) altrettanti verificano (**).

Osserviamo innanzitutto che gli interi

$$1^2, 2^2, \dots, \left[\frac{p-1}{2}\right]^2$$

sono primi con p e, a due a due incongruenti (modulo p).

Infatti se h, k sono interi tali che $1 \leq h, k \leq \frac{p-1}{2}$ e $h^2 \equiv k^2 \pmod{p}$, allora, $h^2 - k^2 = (h+k)(h-k) \equiv 0 \pmod{p}$ e quindi, $h \equiv k \pmod{p}$ (da cui $h = k$), oppure $h \equiv -k \pmod{p}$, cioè $h \equiv p-k \pmod{p}$, e perciò $h = p-k$, il che è assurdo.

Pertanto è possibile costruire un sistema ridotto di residui (modulo p), diciamo U^* , scegliendo opportunamente altri $\frac{p-1}{2}$ interi, che denotiamo con $t_1, \dots, t_{\frac{p-1}{2}}$, nella maniera seguente:

$$U^* := \{1^2, 2^2, \dots, \left[\frac{p-1}{2}\right]^2, t_1, \dots, t_{\frac{p-1}{2}}\}.$$

Confrontando S^* con U^* , è chiaro che, per $\frac{p-1}{2}$ elementi $a \in S^*$, risulta $a \equiv h^2 \pmod{p}$ (con $1 \leq h \leq \frac{p-1}{2}$), mentre per altri $\frac{p-1}{2}$ elementi $a \in S^*$ risulta $a \equiv t_i \pmod{p}$ (con $1 \leq i \leq \frac{p-1}{2}$).

I Caso: Sia $a \equiv h^2 \pmod{p}$, con $1 \leq h \leq \frac{p-1}{2}$. Allora $a^{\frac{p-1}{2}} \equiv h^{p-1} \equiv 1 \pmod{p}$ (infatti $p \nmid h$ e, dunque, è applicabile il Teorema 3.1): pertanto a è soluzione di (*).

II Caso: Sia $a \in S^*$ tale che $a \equiv t_i \pmod{p}$. Per ogni $k \in S^*$, l'insieme $T^* := \{k, 2k, \dots, (p-1)k\}$ è ancora un sistema ridotto di residui (modulo p) (cfr. Esercizio 2.10) e, dunque, esiste un unico elemento $k' \in S^*$ tale che $kk' \equiv a \pmod{p}$. L'elemento k' è detto *associato di k relativamente ad $a \pmod{p}$* e, per ipotesi, è distinto da k . Infatti, se fosse $k = k'$, allora $a \equiv k^2 \equiv (p-k)^2 \pmod{p}$ e uno dei due interi $k, p-k$ dovrebbe essere minore o uguale a $\frac{p-1}{2}$. Ciò è escluso, in quanto stiamo supponendo $a \equiv t_i \pmod{p}$ (con $1 \leq i \leq \frac{p-1}{2}$).

Allora, fissato $a \in S^*$ con $a \equiv t_i \pmod{p}$, gli elementi di S^* si ripartiscono in due sottoinsiemi (disgiunti) di elementi non associati, cioè:

$$S^* : \{h_1, \dots, h_{\frac{p-1}{2}}\} \sqcup \{h'_1, \dots, h'_{\frac{p-1}{2}}\}$$

in modo che:

$$h_j h'_j \equiv a \pmod{p}, \quad 1 \leq j \leq \frac{p-1}{2}.$$

Ne segue che:

$$(p-1)! = h_1 h'_1 \dots h_{\frac{p-1}{2}} h'_{\frac{p-1}{2}} \equiv \underbrace{a \cdot a \cdot \dots \cdot a}_{(p-1)/2 \text{ volte}} = a^{\frac{p-1}{2}} \pmod{p}$$

e dunque, in base al Teorema di Wilson:

$$(p-1)! \equiv -1 \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

In tal caso, a è soluzione di (**). La tesi è così dimostrata. \square

Esempio 4.10 (seguito). Abbiamo visto sopra che le soluzioni di $(*_1)$ coincidono con quelle di $(*)$. Sia y una delle $\frac{p-1}{2}$ soluzioni distinte di

$$X^{p(\frac{p-1}{2})} - 1 \equiv 0 \pmod{p}.$$

allora: $f'(y) = p \left(\frac{p-1}{2}\right) \cdot y^{p(\frac{p-1}{2})-1} \equiv 0 \pmod{p}$. Inoltre, si vede facilmente che $f(y) \equiv 0 \pmod{p^2}$. Infatti $y^{p(\frac{p-1}{2})} - 1 = kp$ per qualche k , elevando al quadrato abbiamo che

$$k^2 p^2 = (y^{p(\frac{p-1}{2})} - 1)^2 = y^{p(p-1)} + 1 - 2y^{p(\frac{p-1}{2})} \quad (\diamond)$$

Inoltre, $\varphi(p^2) = p(p-1)$ e quindi per il Teorema di Euler:

$$z^{p(p-1)} \equiv 1 \pmod{p^2}$$

per ogni z relativamente primo con p^2 . Dunque, per $z = y$, da (\diamond) abbiamo che:

$$0 \equiv 2 - 2y^{p(\frac{p-1}{2})} \pmod{p^2}$$

e dunque che

$$y^{p(\frac{p-1}{2})} - 1 \equiv 0 \pmod{p^2}.$$

Dunque siamo nella condizione del II Caso del Teorema 4.7 e ciò permette di concludere quanto enunciato nell'Esempio 4.11.

Veniamo ora al Problema II (A). Non esiste un procedimento teorico generale per determinare se una congruenza del tipo:

$$f(X) \equiv 0 \pmod{p},$$

con p primo e $f(X) \in \mathbb{Z}[X]$, ammetta soluzioni e, nel caso affermativo, per calcolarle esplicitamente. Ci limiteremo qui a svolgere semplici considerazioni generali tendenti a semplificare il problema e che, comunque, saranno utili nel seguito per la risoluzione delle congruenze quadratiche (modulo p), cioè congruenze del tipo $f(X) \equiv 0 \pmod{p}$, dove $f(X) \in \mathbb{Z}[X]$ e $\deg(f) = 2$.

Cominciamo con la seguente definizione che estende ai polinomi a coefficienti in \mathbb{Z} la nozione di congruenza $(\text{mod } n)$:

Definizione 4.13. Sia $n \in \mathbb{Z}, n > 0$ e siano

$$f = \sum_{i=0}^r a_i X^i, \quad g = \sum_{j=0}^s b_j X^j \in \mathbb{Z}[X].$$

(a) Si dice che il polinomio f è *identicamente congruo a zero modulo n* (in simboli, $f(X) \equiv_X 0 \pmod{n}$) se $a_i \equiv 0 \pmod{n}$ preso comunque $1 \leq i \leq r$.

(b) Si dice che f è *identicamente congruo a g modulo n* (e si scrive $f \equiv_X g \pmod{n}$) se $f - g$ è identicamente congruo a zero modulo n (cioè se risulta $a_i \equiv b_i \pmod{n}$, per ogni i tale che $0 \leq i \leq \min(r, s)$ e se ad esempio $r = \min(r, s) < s$ allora $b_j \equiv 0 \pmod{n}$, per ogni j , con $r + 1 \leq j \leq s$).

(c) Se $f(X) \not\equiv_X 0 \pmod{n}$, si chiama *grado di f modulo n* (e si scrive $\deg_n(f)$) il massimo intero m tale che $a_m \not\equiv 0 \pmod{n}$.

(d) Si dice che f *divide g modulo n* (e si scrive $f \mid g \pmod{n}$) se esiste $h \in \mathbb{Z}[X]$ tale che $fh \equiv_X g \pmod{n}$.

(e) Si dice inoltre che $f(X)$ è *equivalente a $g(X)$ modulo n* , (in simboli $f(X) \sim g(X) \pmod{n}$) se, per ogni $a \in \mathbb{Z}$, $f(a) \equiv g(a) \pmod{n}$.

Se $f(X) \sim g(X) \pmod{n}$, allora le congruenze:

$$f(X) \equiv 0 \pmod{n} \quad \text{e} \quad g(X) \equiv 0 \pmod{n}$$

hanno le stesse soluzioni (modulo n).

Osservazione 4.14. (1) Si consideri l'omomorfismo suriettivo tra anelli di polinomi:

$$\bar{\varphi}_n : \mathbb{Z}[X] \longrightarrow (\mathbb{Z}/n\mathbb{Z})[X], \quad f \mapsto \bar{f},$$

che estende in modo naturale l'omomorfismo canonico suriettivo

$$\varphi_n : \mathbb{Z} \longrightarrow (\mathbb{Z}/n\mathbb{Z}),$$

(cioè $\bar{\varphi}_n$ è così definito:

per ogni $f := \sum_{i=0}^m a_i X^i \in \mathbb{Z}[X]$, $\bar{\varphi}_n(f) = \bar{f} := \sum_{i=0}^m \bar{a}_i X^i$, con $\bar{a}_i := a_i + n\mathbb{Z} =: \varphi_n(a)$).

È del tutto evidente che:

(a') $f \equiv_X 0 \pmod{n} \iff \bar{f} = 0$ (in $(\mathbb{Z}/n\mathbb{Z})[X]$);

(b') $f \equiv_X g \pmod{n} \iff \bar{f} = \bar{g}$ (in $(\mathbb{Z}/n\mathbb{Z})[X]$);

(c') $\deg_n(f) = \deg(\bar{f})$;

(d') $f \mid g \pmod{n} \iff \bar{f} \mid \bar{g}$ (in $(\mathbb{Z}/n\mathbb{Z})[X]$).

(2) Si noti che, per ogni intero $n \geq 0$, se $f \equiv_X g \pmod{n}$, allora $\deg_n(f) = \deg_n(g)$. Si noti, inoltre, che se p è un numero primo e $f, g \in \mathbb{Z}[X]$ sono due polinomi non identicamente congrui a $0 \pmod{p}$, allora $\deg_p(fg) = \deg_p(f) + \deg_p(g)$. Una uguaglianza di tale tipo in generale non vale \pmod{n} , se n non è un primo: ad esempio se $f = 2X - 1$, $g = 2X + 1$ e se $n = 4$, allora $\deg_n(fg) = 0$ mentre $\deg_n(f) = \deg_n(g) = 1$.

Proposizione 4.15. Siano $a, n \in \mathbb{Z}$, $n > 0$ ed $f, g \in \mathbb{Z}[X]$. Risulta:

(a) $(X - a) \mid f \pmod{n}$ se, e soltanto se, $f(a) \equiv 0 \pmod{n}$.

(b) Se $f \equiv_X g \pmod{n}$, allora $f \sim g \pmod{n}$. In particolare, quindi, le congruenze:

$$f(X) \equiv 0 \pmod{n} \quad \text{e} \quad g(X) \equiv 0 \pmod{n}$$

hanno le stesse soluzioni.

Dimostrazione. Semplice esercizio. \square

Osservazione 4.16. La prima affermazione della Proposizione 4.15 (b) non si inverte, in generale. Ad esempio posto $f(X) = X$, $g(X) = X^p$ con p primo, si ha che $f \not\equiv_X g \pmod{p}$ (cfr. Definizione 4.13 (b)), mentre $f(a) \equiv g(a) \pmod{p}$, per ogni $a \in \mathbb{Z}$, cioè $f \sim g \pmod{p}$ (cfr. Corollario 3.2).

Corollario 4.17. Sia $n \in \mathbb{Z}$, $n > 0$, e sia $f := \sum_{i=0}^m a_i X^i \in \mathbb{Z}[X]$. Posto $\hat{f}(X) := \sum_{i=0}^m \hat{a}_i X^i$ con $a_i \equiv \hat{a}_i \pmod{n}$, $0 \leq \hat{a}_i \leq n-1$ e $0 \leq i \leq m$, allora $\deg_n(f) = \deg(\hat{f})$ ed inoltre:

$$f(X) \equiv_X \hat{f}(X) \pmod{n}. \quad \square$$

Corollario 4.18. Sia p primo ed $f(X) \in \mathbb{Z}[X]$. Esiste un polinomio $\tilde{f}(X) \in \mathbb{Z}[X]$ di grado $\leq p-1$, eventualmente uguale al polinomio nullo, tale che:

$$f(X) \sim \tilde{f}(X) \pmod{p}.$$

Dimostrazione. Sia $f(X) := \sum_{i=0}^m a_i X^i$ con $m := \deg_p(f(X))$.

Se $m \leq p-1$, si pone $\tilde{f} := f$.

Se invece $m \geq p$, si pone:

$$\tilde{f} := \sum_{i=0}^{p-1} a_i X^i + \sum_{j=p}^m a_j X^{r_j},$$

dove r_j , con $1 \leq r_j \leq p-1$, è il “resto” del seguente “tipo particolare” di divisione di j per $p-1$:

$$j = q_j(p-1) + r_j, \quad (\text{con } p \leq j \leq m).$$

In altri termini sostituiamo X^p con X , essendo $X^p \sim X$, X^{p+1} con X^2 , essendo $X^{p+1} \sim X^2$, etc.. Utilizzando il “Piccolo” Teorema di Fermat, si verifica subito che:

$f(a) - \tilde{f}(a) \equiv 0 \pmod{p}$ per ogni $a \in \mathbb{Z}$ e da ciò segue la tesi. \square

Per illustrare il Corollario 4.18, si noti che se p è un primo dispari e $f(X) := X^{p(\frac{p-1}{2})} - 1$ allora $\tilde{f}(X) = X^{\frac{p-1}{2}} - 1$. Abbiamo già notato sopra (Esempio 4.11) che:

$$f(X) \sim \tilde{f}(X) \pmod{p}.$$

Teorema 4.19. (Teorema di Lagrange)

Sia p un primo ed $f \in \mathbb{Z}[X]$ tale che $\deg_p(f) = m \geq 1$. La congruenza:

$$f(X) \equiv 0 \pmod{p}$$

ammette al più m soluzioni distinte (cioè incongruenti modulo p).

Dimostrazione. Si procede per induzione su $m \geq 1$.

Se $m = 1$, allora $f(X) \equiv a_0 + a_1X \equiv 0 \pmod{p}$, con $\text{MCD}(a_1, p) = 1$. In tal caso è ben noto (cfr. Lemma 2.3) che la congruenza ammette un'unica soluzione (modulo p).

Sia $m \geq 2$ ed assumiamo che il teorema sia vero per ogni polinomio di grado positivo $\leq m - 1$ (modulo p). Se la congruenza in esame non ha soluzioni, la tesi è ovvia; se viceversa $a \in \mathbb{Z}$ ne è una soluzione, si divide $f(X)$ per $X - a$ ottenendo un polinomio $q(X) \in \mathbb{Z}[X]$ tale che:

$$f(X) = (X - a)q(X) + f(a).$$

Da ciò segue che $f(X) \equiv_X (X - a)q(X) \pmod{p}$ e pertanto le congruenze:

$$f(X) \equiv 0 \pmod{p} \quad \text{e} \quad (X - a)q(X) \equiv 0 \pmod{p}$$

hanno lo stesso insieme di soluzioni (modulo p). Se ora $b \in \mathbb{Z}$ è un'altra soluzione della prima congruenza e se $b \not\equiv a \pmod{p}$, allora $(b - a)q(b) \equiv 0 \pmod{p}$ e quindi, essendo p primo, $q(b) \equiv 0 \pmod{p}$.

Tenendo presente che $\deg_p(q) \leq m - 1$, la tesi discende immediatamente dalla ipotesi induttiva applicata alla congruenza $q(X) \equiv 0 \pmod{p}$. \square

Corollario 4.20. *Siano f, p ed m come nel Teorema 4.19 e sia \tilde{f} in $\mathbb{Z}[X]$ come nel Corollario 4.18 (cioè $f \sim \tilde{f} \pmod{p}$ e $\deg_p(\tilde{f}) \leq p - 1$), allora la congruenza $f(X) \equiv 0 \pmod{p}$ ha al più \tilde{m} soluzioni distinte (modulo p), dove $\tilde{m} := \deg_p(\tilde{f}) \leq \deg_p(f)$.*

Dimostrazione. Semplice conseguenza del Teorema 4.19, applicato ad \tilde{f} , dal momento che le congruenze

$$f(X) \equiv 0 \pmod{p} \quad \text{e} \quad \tilde{f}(X) \equiv 0 \pmod{p}$$

hanno le stesse soluzioni (modulo p). \square

Esempio 4.21. Sia $p = 3$, $f(X) = X^5 + X + 1$. Allora $\deg_3(f) = 5$, $X^5 \sim X^3 \sim X \pmod{3}$, quindi $f := X + X + 1 = 2X + 1$. Pertanto le soluzioni della congruenza $X^5 + X + 1 \equiv 0 \pmod{3}$ sono al più tante quante le soluzioni di $2X + 1 \equiv 0 \pmod{3}$, cioè una. Precisamente, $\tilde{f}(X) \equiv 0 \pmod{3}$ (e $f(X) \equiv 0 \pmod{3}$) hanno un'unica soluzione, che è data da $x \equiv 1 \pmod{3}$.

Osservazione 4.22. Il Teorema di Lagrange non vale, in generale, per congruenze modulo un intero non primo. Ad esempio, la congruenza:

$$X^2 - 1 \equiv 0 \pmod{8}$$

ammette quattro soluzioni distinte (e cioè 1, 3, 5, 7), pur essendo il polinomio di secondo grado, $\deg_8(X^2 - 1) = 2$. Per un'estensione di questo esempio rinviamo al successivo Esercizio 4.4.

Corollario 4.23. *Conservando le notazioni ed ipotesi del Teorema 4.19 e denotando con a_1, a_2, \dots, a_t ($0 \leq t \leq m$) le soluzioni distinte di $f(X) \equiv 0 \pmod{p}$, si ha:*

$$f(X) \equiv_X g(X)(X - a_1)^{e_1}(X - a_2)^{e_2} \cdots (X - a_t)^{e_t} \pmod{p}$$

dove e_1, e_2, \dots, e_t sono interi positivi tali che $\sum_{i=1}^t e_i \leq m$ e dove $g(X)$ in $\mathbb{Z}[X]$, $\deg_p(g) \geq 0$ e la congruenza $g(X) \equiv 0 \pmod{p}$ non è risolubile.

Dimostrazione. Basta iterare l'argomentazione usata nella dimostrazione del Teorema 4.19. \square

Proposizione 4.24. *Sia p primo, $f \in \mathbb{Z}[X]$ e t il numero delle soluzioni distinte della congruenza:*

$$f(X) \equiv 0 \pmod{p}.$$

Risulta:

$$t = \deg_p(f) \iff f \mid (X^p - X) \pmod{p}.$$

Dimostrazione. Notiamo innanzitutto che, per il Corollario 4.23,

$$X^p - X \equiv_X X(X - 1)(X - 2) \cdots (X - (p - 1)) \pmod{p}$$

(\Rightarrow) Se $t = \deg_p(f)$, allora per il Corollario 4.23

$$f(X) \equiv_X (X - a_1)(X - a_2) \cdots (X - a_t) \pmod{p}$$

con $\{a_1, a_2, \dots, a_t\} \subseteq \{0, 1, \dots, p - 1\}$.

Dunque è ovvio che $f(X) \mid (X^p - X) \pmod{p}$.

(\Leftarrow) Se $f(X)g(X) \equiv_X X^p - X \pmod{p}$ per un qualche $g(X) \in \mathbb{Z}[X]$, allora per l'Osservazione 4.13 (2) $\deg_p(f(X)g(X)) = \deg_p(f(X)) + \deg_p(g(X)) = \deg_p(X^p - X) = p$ ed inoltre le seguenti congruenze:

$$\begin{aligned} X^p - X &\equiv 0 \pmod{p} \\ f(X)g(X) &\equiv 0 \pmod{p} \end{aligned} \quad (*fg)$$

hanno le stesse soluzioni. Poiché la prima congruenza ha p soluzioni, anche la seconda congruenza deve avere p soluzioni.

Osserviamo che le soluzioni della congruenza $(*fg)$ sono le soluzioni di almeno una delle seguenti due congruenze:

$$\begin{aligned} f(X) &\equiv 0 \pmod{p} & (*f) \\ g(X) &\equiv 0 \pmod{p} & (*g) \end{aligned}$$

Per il Teorema di Lagrange $(*f)$ ha al più $\deg_p(f)$ soluzioni e $(*g)$ ha al più $\deg_p(g)$ soluzioni, quindi $(*fg)$ ha al più $\deg_p(f(X)) + \deg_p(g(X)) = p$ soluzioni. Pertanto, affinché accada che $(*fg)$ abbia esattamente p soluzioni distinte, deve accadere che tanto $(*f)$ quanto $(*g)$ abbiano ciascuna il massimo numero di soluzioni distinte possibili e cioè, rispettivamente, $\deg_p(f)$ e $\deg_p(g)$ (inoltre, le soluzioni di $(*f)$ debbono essere distinte da quelle di $(*g)$). \square

Osservazione 4.25. (1) Utilizzando la definizione di divisibilità di polinomi (mod n) si definisce facilmente anche un MCD di due polinomi $f, g \in \mathbb{Z}[X]$ (mod n) essendo un polinomio $h \in \mathbb{Z}[X]$ che verifica le seguenti due proprietà:

- $h \mid f$ e $h \mid g$ (mod n);
- $h' \mid f$ e $h' \mid g$ (mod n) $\Rightarrow h' \mid h$ (mod n).

È subito visto che se esiste un MCD (mod n) di due polinomi f, g questo è “essenzialmente unico” a meno di congruenze (mod n) ed è denotato brevemente con $\text{MCD}_n(f, g)$. Se poi $n = p$ è un numero primo, allora si dimostra che, presi comunque due polinomi non identicamente congrui a 0 (mod p), esiste sempre $\text{MCD}_p(f, g)$.

(2) La Proposizione 4.23 è un semplice corollario del seguente risultato più generale:

Siano $p, f(X)$ e t come nella Proposizione 4.24. Sia $h \in \mathbb{Z}[X]$ il massimo comun divisore dei polinomi f e $X^p - X$ (mod p). Risulta allora:

$$t = \deg_p(h).$$

Dimostrazione. Con le notazioni del Corollario 4.23, ricordiamo che possiamo scrivere $f \equiv_X g \cdot (X - a_1)^{e_1} \cdot (X - a_2)^{e_2} \cdot \dots \cdot (X - a_t)^{e_t}$ ed inoltre $X^p - X \equiv_X X(X - 1) \cdot \dots \cdot (X - (p - 1))$ (mod p) (cfr. Corollario 3.2). Da ciò segue facilmente che $\text{MCD}_p(f, X^p - X)$ esiste ed è dato da $h := (X - a_1)(X - a_2) \cdot \dots \cdot (X - a_t)$ e dunque che $\deg_p(h) = t$. \square

Terminiamo questo paragrafo con un teorema dimostrato da C. Chevalley e che riguarda polinomi in più indeterminate.

Sia $f \in \mathbb{Z}[X_1, \dots, X_r]$, dunque possiamo rappresentare f nella maniera seguente:

$$f = \sum_{0 \leq i_1, \dots, i_r \leq t} a_{i_1, i_2, \dots, i_r} X_1^{i_1} X_2^{i_2} \dots X_r^{i_r},$$

con $a_{i_1, i_2, \dots, i_r} \in \mathbb{Z}$ e $i_1, i_2, \dots, i_r \geq 0$.

Poniamo, per semplicità di notazione, $f = \sum_{\mathbf{i}} a_{\mathbf{i}} \mathbf{X}^{\mathbf{i}}$, dove $\mathbf{i} := (i_1, \dots, i_r)$ è un multi-indice e $\mathbf{X}^{\mathbf{i}} := X_1^{i_1} X_2^{i_2} \dots X_r^{i_r}$. L'intero $i_1 + i_2 + \dots + i_r$ si chiama *grado (complessivo)* del monomio $a_{i_1, i_2, \dots, i_r} X_1^{i_1} X_2^{i_2} \dots X_r^{i_r}$. Il massimo dei gradi dei monomi del polinomio f si dice *grado (complessivo)* di f e viene denotato con $\deg(f)$. Se $n \geq 0$ si denota con $\deg_n(f)$ il massimo dei gradi (complessivi), $i_1 + i_2 + \dots + i_r$, dei monomi del polinomio f per i quali $a_{i_1, i_2, \dots, i_r} \not\equiv 0 \pmod{n}$.

Definizione 4.26. Sia $f := \sum_{\mathbf{i}} a_{\mathbf{i}} \mathbf{X}^{\mathbf{i}} \in \mathbb{Z}[X_1, X_2, \dots, X_r]$ e sia $n \geq 0$. Diremo che il polinomio f è *identicamente congruo a zero (modulo n)*, in simboli $f \equiv_{\mathbf{X}} 0 \pmod{n}$, se $a_{\mathbf{i}} \equiv 0 \pmod{n}$ per ciascun multi-indice \mathbf{i} .

Se $f, g \in \mathbb{Z}[X_1, X_2, \dots, X_r]$, diremo che f è *identicamente congruo a g (modulo n)*, in simboli $f \equiv_{\mathbf{X}} g \pmod{n}$, se $f - g \equiv_{\mathbf{X}} 0 \pmod{n}$.

Diremo che f è *equivalente a g (modulo n)*, in simboli $f \sim g \pmod{n}$, se preso comunque $(a_1, \dots, a_r) \in \mathbb{Z}^r$,

$$f(a_1, \dots, a_r) \equiv g(a_1, \dots, a_r) \pmod{n}$$

È ovvio che, se $f \equiv_{\mathbf{X}} g \pmod{n}$, allora $\deg_n(f) = \deg_n(g)$. Inoltre:

$$f \equiv_{\mathbf{X}} g \pmod{n} \Rightarrow f \sim g \pmod{n}.$$

Abbiamo già osservato per polinomi in una indeterminata che non è vero il viceversa.

Proposizione 4.27. *Sia $f \in \mathbb{Z}[X_1, X_2, \dots, X_r]$, sia m il grado complessivo di f e sia p un numero primo.*

Esiste un polinomio $\tilde{f} \in \mathbb{Z}[X_1, X_2, \dots, X_r]$, eventualmente nullo, con il grado di \tilde{f} in ciascuna indeterminata $\leq p-1$, tale che

$$f \sim \tilde{f} \pmod{p}.$$

Dimostrazione. Per ogni $k \geq p-1$, si consideri una divisione con il “resto” di k rispetto a $(p-1)$, del “tipo particolare” seguente:

$$k = q \cdot (p-1) + r \quad \text{con } 1 \leq r \leq p-1.$$

È ovvio che, per ogni $1 \leq i \leq r$, se $k = q \cdot (p-1) + r$ allora:

$$X_i^k \sim X_i^r \pmod{p}.$$

Applicando questa “trasformazione” ad ogni indeterminata X_i ed ad ogni esponente $\geq p-1$, si ottiene un polinomio \tilde{f} che soddisfa alla proprietà enunciata. \square

Proposizione 4.28. *Siano $f, g \in \mathbb{Z}[X_1, X_2, \dots, X_r]$ sia p un primo fissato e siano $\tilde{f}, \tilde{g} \in \mathbb{Z}[X_1, X_2, \dots, X_r]$ come nella Proposizione 4.27.*

$$\tilde{f} \sim \tilde{g} \pmod{p} \iff \tilde{f} \equiv_{\mathbf{X}} \tilde{g} \pmod{p}$$

Dimostrazione. (\Rightarrow) Passando al polinomio $f-g$, basta dimostrare che se $h \in \mathbb{Z}[X_1, X_2, \dots, X_r]$, con grado di $h \leq p-1$ in ogni indeterminata, allora:

$$h \sim 0 \pmod{p} \Rightarrow h \equiv_{\mathbf{X}} 0 \pmod{p}.$$

Si proceda per induzione sul numero delle indeterminate r .

Se $r = 1$, un polinomio di grado $\leq p-1$ con p radici distinte deve essere identicamente congruo a zero (modulo p) per il Teorema di Lagrange.

Sia $(x_2, \dots, x_r) \in \mathbb{Z}^{r-1}$, poniamo:

$$w(X_1) := h(X_1, x_2, \dots, x_r) = \sum_{j=0}^{p-1} h_j(x_2, \dots, x_r) X_1^j \in \mathbb{Z}[X_1].$$

Riapplicando il Teorema di Lagrange a $w(X_1)$ abbiamo che:

$$w \equiv_{X_1} 0 \pmod{p}, \text{ cioè } h_j \sim 0 \pmod{p}, \text{ per ogni } j.$$

Dunque, per ipotesi induttiva, h_j è identicamente congruo a 0 (modulo p) per ogni j , e quindi $h \equiv_{\mathbf{X}} 0 \pmod{p}$.

(\Leftarrow) È banale. \square

Nel 1935 E. Artin congetturò che una congruenza polinomiale priva di termine noto (modulo p), con p primo, ha sempre una soluzione non banale se il numero delle indeterminate del polinomio è maggiore del grado (complessivo) del polinomio. Ad esempio, se $a, b, c \in \mathbb{Z}$, con $abc \not\equiv 0 \pmod{p}$,

$$aX^2 + bY^2 + cZ^2 \equiv 0 \pmod{p}$$

ha sempre almeno una soluzione non banale. Tale congettura fu dimostrata nel 1936 da C. Chevalley.

Teorema 4.29. (C. Chevalley)

Sia p un primo e siano $f, g \in \mathbb{Z}[X_1, X_2, \dots, X_r]$ due polinomi ciascuno con grado (complessivo) $\leq r - 1$.

(a) *Se la congruenza*

$$f(X_1, X_2, \dots, X_r) \equiv 0 \pmod{p} \tag{3}$$

è risolubile, allora ha almeno due soluzioni.

(b) *Se g è un polinomio privo di termine noto (ad esempio un polinomio omogeneo non costante), allora la congruenza*

$$g(X_1, X_2, \dots, X_r) \equiv 0 \pmod{p} \tag{4}$$

ha sempre una soluzione non banale.

Dimostrazione. **(b)** segue immediatamente da **(a)**, in quanto la congruenza (4) possiede sempre la soluzione banale $(0, 0, \dots, 0)$.

(a) Supponiamo che (3) possieda un'unica soluzione:

$$(a_1, a_2, \dots, a_r) \pmod{p}.$$

Consideriamo il polinomio

$$h(X_1, X_2, \dots, X_r) := 1 - f(X_1, X_2, \dots, X_r)^{p-1}$$

Siano $x_1, x_2, \dots, x_r \in \mathbb{Z}$, è ovvio che:

$$h(x_1, \dots, x_r) \equiv \begin{cases} 1 \pmod{p}, & \text{se } x_i \equiv a_i \pmod{p}, \text{ per ogni } i \\ 0 \pmod{p}, & \text{altrimenti.} \end{cases}$$

Sia \tilde{h} un polinomio di grado $\leq p-1$ in ciascuna indeterminata tale che $h \sim \tilde{h} \pmod{p}$ (cfr. Proposizione 4.27).

Si consideri, poi, il seguente polinomio:

$$h^*(X_1, X_2, \dots, X_r) := \prod_{i=1}^r (1 - (X_i - a_i)^{p-1})$$

È subito visto che $h^* \sim h \pmod{p}$ e dunque $h^* \sim \tilde{h} \pmod{p}$. Quindi, per la Proposizione 4.28, $h^* \equiv_{\mathbf{X}} \tilde{h} \pmod{p}$. Questo è impossibile perchè $\deg_p(h^*) = (p-1) \cdot r$, mentre $\deg_p(\tilde{h}) \leq \deg_p(h) = (p-1)\deg_p(f) < (p-1) \cdot r$. Pertanto la congruenza (3) non può possedere un'unica soluzione. \square

4. Esercizi e Complementi

4.1. Siano p un primo ed e, d due interi positivi. Mostrare che:

(a) Se la congruenza $f(X) \equiv 0 \pmod{p}$ ammette s soluzioni distinte e tutte non singolari, lo stesso è vero per la congruenza $f(X) \equiv 0 \pmod{p^e}$, per ogni $e \geq 1$.

(b) Se $d \mid (p-1)$, la congruenza $X^d - 1 \equiv 0 \pmod{p^e}$ ha esattamente d soluzioni per ogni $e \geq 1$.

[Suggerimento. (a). Sia y una soluzione non singolare della congruenza

$$f(X) \equiv 0 \pmod{p^n} \quad (*_n)$$

e sia $x = y + \bar{t}p^n$ l'unica soluzione della congruenza

$$f(X) \equiv 0 \pmod{p^{n+1}} \quad (*_{n+1})$$

con $1 \leq n \leq e-1$. Utilizzando il Lemma 4.5 per il polinomio $f'(X)$ calcolato in x , abbiamo che

$$f'(x) = f'(y) + \bar{t}p^n f''(y) + \dots \equiv f'(y) \pmod{p}.$$

(b). Se $y^d \equiv 1 \pmod{p}$, allora $dy^{d-1} \not\equiv 0 \pmod{p}$. L'asserto discende da (a) e dalla Proposizione 4.24 (cfr. anche il successivo Lemma 5.11).]

4.2. (a) Verificare le seguenti congruenze polinomiali modulo un primo p dispari:

$$(1) X^{p-1} - 1 \equiv_X (X-1)(X-2) \cdots [X-(p-1)] \pmod{p};$$

$$(2) X^{p-2} + X^{p-3} + \cdots + X + 1 \equiv_X (X-2)(X-3) \cdots [X-(p-1)] \pmod{p}.$$

(b) Utilizzando la (1) di (a), ridimostrare il Teorema di Wilson.

[Suggerimento. (a)(1) Si osservi che $(X-k) \mid (X^{p-1} - 1) \pmod{p}$, per ogni k ($1 \leq k \leq p-1$).

(2) segue da (1) e dal fatto che $X^{p-1} - 1 = (X-1)(X^{p-2} + X^{p-3} + \cdots + X + 1)$.

(b) Basta porre $X = p$ in (1).]

4.3. Sia $f(X) \in \mathbb{Z}[X]$ con $\deg(f) \geq 1$. Dimostrare che esistono infiniti primi p tali che la congruenza $f(X) \equiv 0 \pmod{p}$ è risolubile.

[Suggerimento. Se $f(X) = a_0 + a_1X + \cdots + a_nX^n$, allora $f(a_0X) = a_0(1 + Xg(X))$, con $g(X) \in \mathbb{Z}[X]$.

Questa osservazione permette di ricondurci al caso in cui $a_0 = 1$ ovvero $f(X) = 1 + Xg(X)$. Supponiamo, per assurdo, che $f(X) \equiv 0$ sia risolubile soltanto $\pmod{p_i}$ per $i = 1, 2, \dots, t$. Poniamo $N := p_1p_2 \cdots p_t$. Dal momento che $\lim_{x \rightarrow +\infty} |f(x)| = +\infty$, è ovviamente possibile trovare $h \gg 0$ in modo tale che, per $M := N^h$, $|f(M)| \neq 1$. Poiché $f(M) = 1 + Mg(M)$, allora deve essere $\text{MCD}(f(M), M) = 1$. Pertanto se $p \mid M$ allora $p \nmid f(M)$ e quindi perveniamo ad un assurdo.]

4.4. Mostrare che, per ogni $s > 0$, esiste un intero $N > 0$ tale che la congruenza $X^2 \equiv 1 \pmod{N}$ ha più di s soluzioni.

[Suggerimento. Se p è un primo dispari, $X^2 \equiv 1 \pmod{p}$ ha le due soluzioni $1, p-1$. Quindi, se p_1, p_2, \dots, p_r sono primi distinti, $X^2 \equiv 1 \pmod{p_1p_2 \cdots p_r}$ ha esattamente 2^r soluzioni distinte. Basta trovare r tale che $2^r > s$ e porre $N = p_1p_2 \cdots p_r$.]

4.5. Verificare che il Corollario 4.18 non è più valido se si sostituiscono p e $p-1$ rispettivamente con n e $\varphi(n)$ (con $n \in \mathbb{Z}, n \geq 2$).

[Suggerimento. Si scelga, ad esempio, $n = 4$ e $f(X) = X^3 - X$.]

4.6. Siano p , $f(X)$ e t definiti come nella Proposizione 4.24.

Posto $F := \text{MCD}(f, X^p - X)$, massimo comun divisore calcolato in $\mathbb{Z}[X]$, è vero che $t = \deg_p(F)$?

[Suggerimento. La risposta è negativa: si ponga $p = 5$ ed $f(X) = (X + 2)(X + 1)^2$ da cui $t = 2$ e $F(X) = X + 1$, perché

$$\begin{aligned} X^5 - X &= X(X^4 - 1) = \\ &= X(X^2 - 1)(X^2 + 1) = \\ &= X(X + 1)(X - 1)(X^2 + 1). \end{aligned}$$

4.7. (Teorema di Warning) Sia $f \in \mathbb{Z}[X_1, \dots, X_r]$, con $\deg(f) < r$, e sia p un numero primo. La congruenza $f \equiv 0 \pmod{p}$ ha un numero di soluzioni (in \mathbb{Z}^r) divisibile per p .

[Suggerimento. Seguire un'argomentazione simile a quella utilizzata per dimostrare il Teorema di Chevalley. Precisamente se $\mathbf{a}_i = (a_{i1}, a_{i2}, \dots, a_{ir})$, per $i = 1, 2, \dots, s$, sono le soluzioni della congruenza data, considerare il polinomio:

$$h^*(X_1, X_2, \dots, X_r) := \sum_{i=1}^s \prod_{j=1}^r (1 - (X_j - a_{ij})^{p-1}).$$

4.8. Determinare le soluzioni della congruenza:

$$f(X) := X^2 + X + 7 \equiv 0 \pmod{27}.$$

[Soluzione. La congruenza:

$$X^2 + X + 7 \equiv 0 \pmod{3} \tag{*1}$$

ha un'unica soluzione $y \equiv 1 \pmod{3}$.

Consideriamo la congruenza:

$$X^2 + X + 7 \equiv 0 \pmod{3^2}. \tag{*2}$$

Osserviamo che $f'(X) = 2X + 1$, quindi $f'(y) \equiv 0 \pmod{3}$. Inoltre, $f(1) \equiv 0 \pmod{9}$, dunque gli elementi $y_1 = 1$, $y_2 = 1 + 3 = 4$, $y_3 = 1 + 2 \cdot 3 = 7$ sono le soluzioni di $(*2)$.

Per calcolare le soluzioni della congruenza data:

$$X^2 + X + 7 \equiv 0 \pmod{3^3} \tag{*3}$$

osserviamo che:

$$\begin{aligned} f'(y_1) &= 3 \equiv 0 \pmod{3} & f(y_1) &= 9 \equiv 9 \pmod{27} \\ f'(y_2) &= 9 \equiv 0 \pmod{3} & f(y_2) &= 27 \equiv 0 \pmod{27} \\ f'(y_3) &= 15 \equiv 0 \pmod{3} & f(y_3) &= 63 \equiv 9 \pmod{27}. \end{aligned}$$

Quindi, y_1 non determina soluzioni di $(*3)$ (cioè non esiste nessuna soluzione t della congruenza

$$3t \equiv -\frac{9}{9} = -1 \pmod{3} \tag{\bullet_1}$$

e quindi nessun intero $x = y_1 + t \cdot 3^2$ è tale che $f(x) \equiv 0 \pmod{27}$). Mentre, y_2 determina tre soluzioni di $(*_3)$ date da:

$$x_{2,1} = y_2 + 0 \cdot 3^2 = 4, \quad x_{2,2} = y_2 + 1 \cdot 3^2 = 13, \quad x_{2,3} = y_2 + 2 \cdot 3^2 = 22 \pmod{27}$$

(dal momento che la congruenza

$$9T \equiv -\frac{27}{9} = -3 \pmod{3} \tag{*2}$$

è risolubile per $t = 0, 1, 2 \pmod{3}$).

Infine, y_3 non determina soluzioni di $(*_3)$ (in quanto la congruenza

$$15T \equiv -\frac{63}{9} = -7 \equiv -1 \pmod{3} \tag{*3}$$

non è risolubile).

In definitiva, le soluzioni della congruenza assegnata sono: $x = 4, 13, 22 \pmod{27}$.]