Stage Urbi et Orbi - Lez. 5A

Titolo nota

10 gennaio 2020 (14.30-17.30) - docente: Prof. **Emanuele Callegari** - Università di Roma ***Tor Vergata***

www.problemisvolti.it

POLINOMI

OSSERVAZIONE 1 DAREMO PER ACQUISITO CHE LO STUDENTE CONOSCA LE NOZIONI DI BASE SUI POLINOMI (SOMMA, PRODOTTO, GRADO). CI LIMITIAMO A RICHIAMARE IL CONCETTO DI COMPOSIZIONE: DATI DUE POLINOMI $P(x)$ E $Q(x)$ IL POLINOMIO $P(Q(x))$, COMPOSIZIONE TRA $P(x)$ E $Q(x)$, È PER DEFINIZIONE IL POLINOMIO CHE SI OTTIENE SCRIVENDO $Q(x)$ AL POSTO DELLA x DI $P(x)$ E SVILUPPANDO I CALCOLI.
AD ESEMPIO SE $P(x)=x^2+1$ E $Q(x)=x+2$ SI HA:

$$P(Q(x))=(Q(x))^2+1=(x+2)^2+1=x^2+4x+4+1=x^2+4x+5$$

SI NOTI CHE, IN GENERALE, $P(Q(x))\neq Q(P(x))$. AD ESEMPIO, SE $P(x)$ E $Q(x)$ SONO I POLINOMI DELL'ESEMPIO PRECEDENTE, OTTENIAMO:

$$Q(P(x))=P(x)+2=x^2+1+2=x^2+3\neq P(Q(x))$$

PROB. 1 TROVARE TUTTI I POLINOMI A COEFFICIENTI REALI $P(x)$ TALI CHE $P(x^2)=(P(x))^2$.

SVOLGIMENTO È IMMEDIATO INDOVINARE E VERIFICARE CHE VANNO BENE TUTTI I POLINOMI DEL TIPO $P(x)=x^n$ CON n INTERO NON NEGATIVO.
IN TAL CASO INFATTI SI HA $P(x^2)=(x^2)^n=x^{2n}=(x^n)^2=(P(x))^2$.
RIMANE DA DIMOSTRARE CHE OGNI ALTRO POLINOMIO VA MALE.
A TALE SCOPO BASTA DIMOSTRARE CHE SE UN POLINOMIO VA BENE ALLORA SODDISFA LE 2 CONDIZIONI:

a) IL TERMINE DI GRADO MASSIMO HA COEFFICIENTE 1.

b) NON CI SONO ALTRI TERMINI OLTRE A QUELLO DI GRADO MASSIMO.

PER MOSTRARE (a), PRESO $P(x) = a x^n + (\text{...TERMINI DI GRADO INFERIORE...})$,
NOTIAMO CHE IL TERMINE DI GRADO MASSIMO DI $P(x^2)$ È $a x^{2n}$ MENTRE
QUELLO DI $(P(x))^2$ È $a^2 x^{2n}$. QUINDI L'UNICO MODO CHE HANNO DI ESSERE
UGUALI È CHE SIA $a=1$. QUESTO DIMOSTRA (a).
PER MOSTRARE (b) SUPPONIAMO, PER ASSURDO, CHE CI SIA ALMENO UN ALTRO
TERMINE OLTRE A QUELLO DI GRADO MASSIMO, CIOÈ CHE $P(x)$ SIA DELLA FORMA:

$$P(x) = x^n + a x^m + (\text{... EVENTUALI TERMINI DI GRADO MINORE DI } m \text{ ...})$$

DOVE $n > m$.
MA ALLORA:

$$P(x^2) = x^{2n} + a x^{2m} + (\text{.... TERMINI DI GRADO INFERIORE ...})$$

MENTRE:

$$(P(x))^2 = x^{2n} + 2a x^{n+m} + (\text{.... TERMINI DI GRADO INFERIORE...})$$

QUINDI $(P(x))^2$ HA UN TERMINE DI GRADO $m+n$ CHE A $P(x^2)$ MANCA.
QUINDI NESSUN POLINOMIO CON PIÙ DI UN TERMINE PUÒ ANDAR BENE.
CIÒ DIMOSTRA (b).
QUINDI ABBIAMO MOSTRATO CHE GLI UNICI POLINOMI CHE VANNO BENE SONO QUELLI
DELLA FORMA $P(x) = x^n$.

PROB. 2 TROVARE TUTTI I POLINOMI $P(x)$ TALI CHE $P(P(x)) = x^{10} + 5x^3 + 3x^2 + 1$.

PRIMA DI RISOLVERE IL PROBLEMA FACCIAMO LA SEGUENTE:

OSSERVAZIONE 2 IL GRADO DI $P(q(x))$ È IL PRODOTTO DEI GRADI DI $P(x)$ E $q(x)$.

INFATTI SE $P(x)$ HA GRADO n E $q(x)$ HA GRADO m ALLORA:

$$P(x) = a x^n + (\text{... TERMINI DI GRADO INFERIORE ...})$$
$$q(x) = b x^m + (\text{... TERMINI DI GRADO INFERIORE ...})$$

QUINDI:

$$P(q(x)) = a(b x^m + \dots)^n + \dots = a b^n x^{m \cdot n} + (\text{.... TERMINI DI GRADO INFERIORE...})$$

QUINDI $P(q(x))$ HA GRADO $m \cdot n$.
TORNIAMO QUINDI ALLO:

SVOLGIMENTO PROB.2 GRAZIE ALL'OSSERVAZIONE 2, SE $P(x)$ HA GRADO n ALLORA $P(P(x))$ HA GRADO n^2, QUINDI NON PUÒ MAI ESSERE UN POLINOMIO DI GRADO 10.

QUINDI NON C'È ALCUN $P(x)$ CHE SODDISFA LA CONDIZIONE RICHIESTA.

PROB.3 [P.7 GARA STAGE 2018] TROVARE A SAPENDO CHE ESISTE UN POLINOMIO $P(x)$ A COEFFICIENTI REALI TALE CHE $P(P(x)) = x^4 + 16x^3 + Ax^2 - 48x - 14$.

SVOLGIMENTO GRAZIE ALL'OSSERVAZIONE 2 $P(x)$ È DI SECONDO GRADO QUINDI:

(1) $$P(x) = ax^2 + bx + c$$

DI CONSEGUENZA:

(2) $$P(P(x)) = a(ax^2+bx+c)^2 + b(ax^2+bx+c) + c$$

DA CUI SEGUE:

$$P(P(x)) = a^3x^4 + (\dots \text{TERMINI DI GRADO INFERIORE} \dots)$$

MA IL TERMINE DI GRADO 4 DI $P(P(x))$ DEVE ESSERE x^4, DI CONSEGUENZA DEVE ESSERE $a^3 = 1$, CIOÈ $a = 1$.

QUINDI (1) DIVENTA:

(3) $$P(x) = x^2 + bx + c$$

E (2) DIVENTA:

(4) $$P(P(x)) = (x^2+bx+c)^2 + b\cdot(x^2+bx+c) + c$$

DA CUI SEGUE:

$$P(P(x)) = x^4 + 2bx^3 + (\dots \text{TERMINI DI GRADO INFERIORE} \dots)$$

E SICCOME IL TERMINE DI TERZO GRADO DI $P(P(x))$ DEVE ESSERE $16x^3$, L'UNICA POSSIBILITÀ È CHE SIA $b=8$.

QUINDI (3) DIVENTA:

(5) $$P(x) = x^2 + 8x + c$$

E (4) DIVENTA:

(6) $$P(P(x)) = (x^2+8x+c)^2 + 8(x^2+8x+c) + c$$

IL TERMINE DI PRIMO GRADO DI (6) È $2\cdot 8x\cdot c + 8\cdot 8x$, CIOÈ $16(c+4)x$, QUINDI, SE VOGLIAMO CHE SIA UGUALE A $-48x$, DEVE ESSERE $c=-7$.

QUINDI L'UNICA POSSIBILITÀ È CHE SIA:

(7) $P(x) = x^2 + 8x - 7$

DA CUI SI OTTIENE:

(8) $P(P(x)) = (x^2+8x-7)^2 + 8(x^2+8x-7) - 7 =$

$= \ldots = x^4 + 16x^3 + 58x^2 - 48x - 14.$

QUESTO SIGNIFICA CHE IL $P(x)$ DATO DA (7) SODDISFA EFFETTIVAMENTE TUTTE LE CONDIZIONI RICHIESTE, VISTO CHE IL TERMINE NOTO DI (8) È PROPRIO -14. E FINALMENTE, VISTO CHE IL TERMINE DI SECONDO GRADO DI (8) È $58x^2$, POSSIAMO CONCLUDERE CHE $A = 58$.

PROB. 4 TROVARE TUTTI I POLINOMI $P(x)$ TALI CHE $P(x) = P(x+1)$.

SVOLGIMENTO DI QUESTO PROBLEMA PROPONIAMO DUE MODI PER RISOLVERLO: IL PRIMO È PIÙ SEMPLICE, ANCHE SE PIÙ CALCOLOSO, E CI PERMETTE DI INTRODURRE UNA NOTAZIONE CHE CI SARÀ UTILE; IL SECONDO, CON MENO CALCOLI MA CONCETTUALMENTE MENO SEMPLICE, CI CONSENTE DI INTRODURRE IL PRINCIPIO DI IDENTITÀ DEI POLINOMI

I° MODO DEFINIAMO L'OPERATORE Δ TRA POLINOMI NEL MODO SEGUENTE:

PER OGNI POLINOMIO $P(x)$, IL POLINOMIO $\Delta P(x)$ È QUELLO CHE SI OTTIENE CALCOLANDO $P(x+1) - P(x)$. AD ESEMPIO, SE $P(x) = x^2 + 3x + 2$, SI HA:

$\Delta P(x) = P(x+1) - P(x) = (x+1)^2 + 3(x+1) + 2 - (x^2 + 3x + 2) =$

$= x^2 + 2x + 1 + 3x + 3 + 2 - x^2 - 3x - 2 = 2x + 4$

SI NOTI CHE, CON TALE NOTAZIONE, LA CONDIZIONE $P(x) = P(x+1)$ EQUIVALE ALLA CONDIZIONE $\Delta P(x) = 0$.

ORA, NEL CASO DEL GENERICO IN CUI $P(x)$ HA GRADO n, CIOÈ:

$P(x) = a x^n + b x^{n-1} + (\ldots \text{TERMINI DI GRADO INFERIORE} \ldots)$

SI HA:

$\Delta P(x) = P(x+1) - P(x) =$

$= a(x+1)^n + b(x+1)^{n-1} + (\ldots) - a x^n - b x^{n-1} - (\ldots) =$

$= \cancel{a x^n} + n a x^{n-1} + (\ldots) + \cancel{b x^{n-1}} + (\ldots) - \cancel{a x^n} - \cancel{b x^{n-1}} - (\ldots) =$

$= n a x^{n-1} + (\ldots \text{TERMINI DI GRADO INFERIORE} \ldots)$

ABBIAMO CIOÈ SCOPERTO CHE VALE LA SEGUENTE:

OSSERVAZIONE 3 SE $P(x)$ HA GRADO n ALLORA $\Delta P(x)$ HA GRADO $n-1$.

IN BASE A TALE OSSERVAZIONE, SOLO I POLINOMI DI GRADO 0, CIOÈ LE COSTANTI, POSSONO SODDISFARE LA CONDIZIONE $\Delta P(x)=0$, CIOÈ $P(x+1)=P(x)$.

II° MODO SI UTILIZZA IL COSIDETTO:

PRINCIPIO DI IDENTITÀ DEI POLINOMI DATI 2 POLINOMI $P(x)$ E $Q(x)$, ENTRAMBI DI GRADO MINORE O UGUALE A n, SE ESISTONO $n+1$ VALORI $x_0, x_1, \dots, x_n$, TUTTI DISTINTI, TALI CHE $P(x_0)=Q(x_0)$, $P(x_1)=Q(x_1), \dots, P(x_n)=Q(x_n)$, ALLORA $P(x)$ E $Q(x)$ SONO LO STESSO POLINOMIO.

CHE HA COME CONSEGUENZA OVVIA IL SEGUENTE:

COROLLARIO 1 SE DUE POLINOMI ASSUMONO GLI STESSI VALORI PER INFINITI VALORI DELLA x, ALLORA SONO LO STESSO POLINOMIO.

PIÙ AVANTI DAREMO UNA DIMOSTRAZIONE DEL PRINCIPIO DI IDENTITÀ DEI POLINOMI USANDO IL TEOREMA DI RUFFINI. PER ORA CI LIMITIAMO A UTILIZZARLO PER RISOLVERE IL **PROB. 4**.

A TALE SCOPO OSSERVIAMO CHE SE $P(x)$ HA LA PROPRIETÀ $P(x)=P(x+1)$ ALLORA

$$\begin{aligned} P(0)&=P(0+1)=P(1)\\ P(1)&=P(1+1)=P(2)\\ P(2)&=P(2+1)=P(3)\\ &\vdots\\ P(n)&=P(n+1) \end{aligned}$$

INSOMMA $P(x)$ ASSUMEREBBE IN INFINITI ALTRI PUNTI (= TUTTI GLI INTERI) IL VALORE ASSUNTO IN ZERO, CIOÈ $P(0)$. MA ANCHE IL POLINOMIO COSTANTE UGUALE A $P(0)$ ASSUME GLI STESSI VALORI DI $P(x)$ SU TALI PUNTI, QUINDI, GRAZIE AL COROLLARIO 1, $P(x)$ COINCIDE COL POLINOMIO COSTANTE UGUALE A $P(0)$

QUINDI, SE $P(x)$ HA LA PROPRIETÀ $P(x)=P(x+1)$, È NECESSARIAMENTE UN POLINOMIO COSTANTE.

IL VICEVERSA È OVVIO: TUTTI I POLINOMI COSTANTI SODDISFANO $P(x)=P(x+1)$.

CONCLUDIAMO QUINDI CHE I POLINOMI RICHIESTI SONO TUTTI E SOLI QUELLI COSTANTI

PROB. 5 [P.15 GARA STAGE 2018] TROVARE TUTTI I POLINOMI A COEFFICIENTI REALI $P(x)$ CHE SODDISFANO LA CONDIZIONE $(P(x))^2 = P(P(x)) - 3$.

SVOLGIMENTO PER COMINCIARE OSSERVIAMO CHE NESSUN POLINOMIO DI GRADO 0 SODDISFA LA CONDIZIONE. INFATTI, SE FOSSE $P(x) = a$, LA CONDIZIONE DIVENTEREBBE:

$$a^2 = a - 3$$

CIOÈ:

$$a^2 - a + 3 = 0$$

CHE NON È SODDISFATTA PER ALCUN VALORE REALE DI a.

VISTO CHE NESSUN POLINOMIO COSTANTE SODDISFA LA CONDIZIONE, CERCHIAMO ORA $P(x)$ TRA I POLINOMI NON COSTANTI.

PER FARLO C'È OVVIAMENTE ANCHE IL METODO CALCOLOSO, CHE CONSISTE NEL RICONOSCERE CHE LA PROPRIETÀ PUÒ ESSERE SODDISFATTA SOLO SE $P(x)$ HA GRADO 2, CIOÈ SE È DELLA FORMA

$$P(x) = ax^2 + bx + c.$$

DOPODICHÈ, PROCEDENDO IN MODO SIMILE A QUANTO FATTO NEL PROB. 3, SI IMPOSTANO LE CONDIZIONI SU a, b E c EGUAGLIANDO I COEFFICIENTI DEI TERMINI CON LO STESSO GRADO CHE SI OTTENGONO NEI 2 MEMBRI DI:

$$(P(x))^2 = P(P(x)) - 3 \tag{9}$$

I CALCOLI PERÒ SONO UN PÒ LUNGHI, PER CUI PREFERIAMO PROPORRE ALLO STUDENTE UN APPROCCIO ALTERNATIVO CHE ORA ANDIAMO A DESCRIVERE.

UNA VOLTA APPURATO CHE $P(x)$ NON È UN POLINOMIO COSTANTE, COME CONSEGUENZA DEL COROLLARIO 1 ABBIAMO CHE $P(x)$ ASSUME INFINITI VALORI DIVERSI.

PER CIASCUN VALORE Y ASSUNTO DA $P(x)$, LA (8) DIVENTA

$$(Y)^2 = P(Y) - 3$$

CIOÈ:

$$P(Y) = Y^2 + 3$$

CIÒ SIGNIFICA CHE, PER INFINITI VALORI DI Y, IL POLINOMIO $P(x)$ E IL POLINOMIO $x^2 + 3$ ASSUMONO GLI STESSI VALORI.

QUINDI, GRAZIE AL COROLLARIO 1, $P(x) = x^2 + 3$.

PROB. 6 DIRE QUAL È IL RESTO DI $(x^5-3x^4+5x^2-4x+3):(x-2)$.

SVOLGIMENTO SI POTREBBE OVVIAMENTE ESEGUIRE LA DIVISIONE E PRENDERE IL RESTO. PER MINIMIZZARE I CALCOLI PERÒ RAGIONIAMO IN UN ALTRO MODO.

DIRE CHE:

$$(x^5-3x^4+5x^2-4x+3):(x-2)=Q(x) \quad \text{CON RESTO } R(x)$$

SIGNIFICA DIRE CHE $Q(x)$ ED $R(x)$ SONO TALI CHE

$$(x^5-3x^4+5x^2-4x+3)=(x-2)\cdot Q(x)+R(x) \tag{10}$$

CON $R(x)$ DI GRADO MINORE DI $(x-2)$, CIOÈ $R(x)=z$ POLINOMIO COSTANTE.

MA ALLORA CALCOLANDO LA (10) PER $x=2$ SI OTTIENE

$$(2^5-3\cdot 2^4+5\cdot 2^2-4\cdot 2+3)=(2-2)\cdot Q(2)+z$$

CIOÈ:

$$-1=0\cdot Q(2)+z$$

DA CUI SEGUE $z=-1$.

COL METODO UTILIZZATO NEL PROB. 6 SI DIMOSTRA IL:

TEOREMA DI RUFFINI DATO UN POLINOMIO $P(x)$, IL RESTO DELLA DIVISIONE TRA $P(x)$ E $(x-c)$ È UN POLINOMIO COSTANTE UGUALE A $P(c)$.

DIMOSTRAZIONE DIRE CHE $P(x):(x-c)=Q(x)$ CON RESTO $R(x)$ SIGNIFICA CHE:

$$P(x)=Q(x)\cdot(x-c)+R(x)$$

CON $R(x)$ DI GRADO ZERO, CIOÈ $R(x)=z$ È UN POLINOMIO COSTANTE.

VALUTANDO TALE ESPRESSIONE PER $x=c$ SI OTTIENE:

$$P(c)=Q(c)\cdot(c-c)+z$$

DA CUI SEGUE $z=P(c)$.

COROLLARIO 2 DATO IL POLINOMIO $P(x)$, L'EQUAZIONE $P(x)=0$ HA UNA SOLUZIONE

$x = c$ SE E SOLO SE $P(x)$ È DIVISIBILE PER $x - c$.

DIMOSTRAZIONE PER IL TEOREMA DI RUFFINI IL RESTO È $P(c)$, QUINDI DIRE CHE $x = c$ È SOLUZIONE, CIOÈ CHE $P(c) = 0$, EQUIVALE A DIRE CHE IL RESTO È ZERO, CIOÈ CHE $P(x)$ È DIVISIBILE PER $(x - c)$.

COROLLARIO 3 SE $P(x)$ HA GRADO MINORE O UGUALE A n E CI SONO $n+1$ VALORI DISTINTI $x_0, x_1, \dots, x_n$ TALI CHE $P(x_0) = P(x_1) = \dots = P(x_n) = 0$, ALLORA $P(x)$ È IL POLINOMIO IDENTICAMENTE NULLO.

DIMOSTRAZIONE SI DIMOSTRA PER INDUZIONE SUL GRADO DI $P(x)$.

PER $n = 0$ INFATTI È OVVIO.

MOSTRIAMO ORA CHE SE VALE PER $n = k$ VALE ANCHE PER $n = k+1$.

INFATTI SE $P(x)$ SI ANNULLA PER $x = x_0, x_1, \dots, x_k, x_{k+1}$ ED HA GRADO $\leq k+1$, USANDO IL COROLLARIO 2 POSSO SCRIVERE:

$$P(x) = q(x) \cdot (x - x_{k+1})$$

DOVE $q(x)$ HA GRADO $\leq k$ E SI ANNULLA PER $x = x_0, x_1, \dots, x_k$.

MA ALLORA, PER L'IPOTESI INDUTTIVA $q(x)$ È IDENTICAMENTE NULLO E, DI CONSEGUENZA, ANCHE $P(x)$ LO È.

QUINDI, PER IL PRINCIPIO DI INDUZIONE, L'AFFERMAZIONE VALE PER OGNI n.

OSSERVAZIONE 4 IL COROLLARIO 3 CI GARANTISCE CHE IL NUMERO DI SOLUZIONI DI UN'EQUAZIONE ALGEBRICA NON SUPERA MAI IL SUO GRADO.

OSSERVAZIONE 5 PER DIMOSTRARE IL PRINCIPIO DI IDENTITÀ DEI POLINOMI BASTA APPLICARE IL COROLLARIO 3 AL POLINOMIO DIFFERENZA.

PROB. 7 [P. 12 GARA STAGE 2018] TROVARE IL RESTO DI $P(x) : (x^2 + x - 2)$ SAPENDO CHE $P(x) : (x-1)$ HA RESTO 16 E CHE $P(x) : (x+2)$ HA RESTO 10.

SVOLGIMENTO SI TRATTA DI USARE IL TEOREMA DI RUFFINI E LE PROPRIETÀ:

(11) $P(x) : (x-1)$ HA RESTO 16

(12) $P(x) : (x+2)$ HA RESTO 10

LA (11) SIGNIFICA CHE ESISTE $Q(x)$ TALE CHE:

(13) $$P(x) = Q(x)\cdot(x-1) + 16$$

CALCOLANDO LA (13) PER $x=-2$ SI OTTIENE:

(14) $$P(-2) = Q(-2)\cdot(-2-1) + 16.$$

GRAZIE ALLA (12) E AL T. DI RUFFINI SI HA $P(-2)=10$, QUINDI (14) DIVENTA:

$$10 = Q(-2)\cdot(-3) + 16$$

DA CUI SEGUE:

$$Q(-2) = 2$$

CHE, SEMPRE GRAZIE AL T. DI RUFFINI, È COME DIRE CHE ESISTE $H(x)$ TALE CHE:

(15) $$Q(x) = H(x)(x+2) + 2.$$

SOSTITUENDO LA (15) NELLA (13) SI OTTIENE:

$$P(x) = \big(H(x)(x+2)+2\big)(x-1) + 16 =$$

$$= H(x)(x+2)(x-1) + 2x - 2 + 16 =$$

$$= H(x)(x^2+x-2) + 2x + 14$$

CHE CI DICE PROPRIO CHE $P(x):(x^2+x-2)$ HA RESTO $2x+16$.

PROB. 8 [P.6 GARA STAGE 2018] DATO $P(x) = -3x^{81} + 10x^{61} + x^{29} + 6x^{21} + 2x^3 + x^2 + 9x + 53$

TROVARE IL RESTO DI $P(x):(x^{20}+2)$.

SVOLGIMENTO (I° MODO) ESEGUIRE MATERIALMENTE LA DIVISIONE È TROPPO LUNGO.

PROVIAMO, CON QUALCHE MANIPOLAZIONE, A SCRIVERE UGUALMENTE NELLA FORMA

$$P(x) = Q(x)\cdot(x^{20}+2) + R(x)$$

IN MODO TALE DA POTER DIRE CHE L'$R(x)$ CHE CI RITROVIAMO È IL RESTO.

AD ESEMPIO, IL TERMINE $-3x^{81}$ LO TRATTIAMO COSÌ:

$$-3x^{81} = -3x\cdot(x^{20})^4 = -3x\big((x^{20}+2)-2\big)^4 =$$

$$= -3x\Big((x^{20}+2)^4 - 4\cdot(x^{20}+2)^3\cdot 2 + 6(x^{20}+2)^2 4 - 4(x^{20}+2)\cdot 8 + 16\Big) =$$

$$= (\dots)\cdot(x^{20}+2) - 48x$$

QUINDI, IN DEFINITIVA, SIAMO RIUSCITI A SCRIVERE $-3x^{81}$ NELLA FORMA:

$$-3x^{81} = A(x)\cdot(x^{20}+2) - 48x$$

ANALOGAMENTE, IL TERMINE $10x^{61}$, SI SCRIVE NELLA FORMA.

$$10x^{61} = B(x)\cdot(x^{20}+2) + 40x .$$

A QUESTO PUNTO SI HA:

$$P(x) = -3x^{81} + 10x^{61} + x^{24} + 6x^{21} + 2x^3 + x^2 + 9x + 53 =$$

$$= A(x)(x^{20}+2) - 68x + B(x)(x^{20}+2) + 60x + x^2\cdot((x^{20}+2)-2) + 6x\left((x^{20}+2)-2\right) + 2x^3 + x^2 + 9x + 53 =$$

$$= \left(A(x) + B(x) + x^2 + 6x\right)(x^{20}+2) + \left(-68x + 60x - 2x^2 - 12x + 2x^3 + x^2 + 9x + 53\right) =$$

$$= (\dots\dots)(x^{20}+2) + (x^2 - 11x + 53)$$

QUINDI IL RESTO CERCATO È $x^2 - 11x + 53$.

OSSERVAZIONE 6 C'È UN MODO PIÙ RAPIDO DI RISOLVERE IL PROB. 8, CHE PERÒ PRESUPPONE L'INTRODUZIONE DELLE CLASSI DI RESTO PER I POLINOMI, COSA CHE CI ACCINGIAMO A FARE.

DEFINIZIONE 1 DATI 3 POLINOMI $P(x)$, $q(x)$ ED $M(x)$, DIREMO CHE:

$$P(x) \equiv q(x) \pmod{M(x)}$$

SE $p(x) : m(x)$ E $q(x) : m(x)$ HANNO LO STESSO RESTO.

DEFINIZIONE 2 (EQUIVALENTE ALLA PRECEDENTE) DATI 3 POLINOMI $P(x)$, $q(x)$ ED $M(x)$, DIREMO CHE:

$$P(x) \equiv q(x) \pmod{M(x)}$$

SE $p(x) - q(x)$ È DIVISIBILE PER $M(x)$.

VERIFICA DELL'EQUIVALENZA

SE $P(x) : M(x)$ E $q(x) : M(x)$ HANNO LO STESSO RESTO $R(x)$ ALLORA ESISTONO $A(x)$ E $B(x)$ TALI CHE:

$$P(x) = A(x)\cdot M(x) + R(x)$$

$$q(x) = B(x)\cdot M(x) + R(x)$$

DA CUI SI OTTIENE:

$$P(x) - q(x) = \left(A(x) - B(x)\right)\cdot M(x)$$

CIOÈ $P(x) - Q(x)$ È DIVISIBILE PER $M(x)$.

SE INVECE I RESTI FOSSERO STATI DIVERSI SI SAREBBE OTTENUTO:

$$P(x) = A(x)\cdot M(x) + R_1(x)$$

$$q(x) = B(x)\cdot M(x) + R_2(x)$$

DA CUI SAREBBE SEGUITO.

$$p(x) - q(x) = \big(A(x) - B(x)\big)\cdot M(x) + \big(R_1(x) - R_2(x)\big)$$

CON $R_1(x) - R_2(x)$ POLINOMIO NON NULLO DI GRADO MINORE DI $M(x)$.

CIÒ SIGNIFICA CHE $P(x) - q(x)$ NON È DIVISIBILE PER $M(x)$.

QUINDI $P(x) - q(x)$ È DIVISIBILE PER $M(x)$ SE E SOLO SE $P(x) : M(x)$ E $q(x) : M(x)$ HANNO LO STESSO RESTO.

PROPOSIZIONE 1 DATI I POLINOMI $a(x)$, $A(x)$, $b(x)$, $B(x)$, ED $M(x)$, TALI CHE:

(16) $$a(x) \equiv A(x) \pmod{M(x)}$$

E

(17) $$b(x) \equiv B(x) \pmod{M(x)}$$

ALLORA SI HA:

(18) $$a(x) + b(x) \equiv A(x) + B(x) \pmod{M(x)}$$

E

(19) $$a(x) \cdot b(x) \equiv A(x) \cdot B(x) \pmod{M(x)}$$

DIMOSTRAZIONE IN BASE ALLA DEFINIZIONE 2 LA (16) SIGNIFICA CHE ESISTE UN POLINOMIO $k(x)$ TALE CHE $a(x) - A(x) = k(x)\cdot M(x)$, CIOÈ:

(20) $$a(x) = A(x) + k(x)\cdot M(x)$$

ANALOGAMENTE LA (17) SIGNIFICA CHE ESISTE $H(x)$ TALE CHE:

(21) $$b(x) = B(x) + H(x)\cdot M(x)$$

SOMMANDO MEMBRO A MEMBRO (20) E (21) SI OTTIENE:

$$a(x) - b(x) = A(x) - B(x) + \big(k(x) - H(x)\big)\cdot M(x)$$

CHE EQUIVALE A (18).

INVECE PER DIMOSTRARE (19) BASTA MOLTIPLICARE MEMBRO A MEMBRO (16) E (17) OTTENENDO:

$$a(x)\cdot b(x) = \big(A(x) + k(x)M(x)\big)\cdot\big(B(x) + H(x)\cdot M(x)\big) =$$

$$= A(x)\cdot B(x) + \big(k(x)B(x) + H(x)A(x) + k(x)H(x)M(x)\big)\cdot M(x)$$

CIOÈ CHE $a(x)\cdot b(x) - A(x)\cdot B(x)$ È UN MULTIPLO DI $M(x)$, CHE È APPUNTO CIÒ CHE SIGNIFICA (19).

OSSERVAZIONE 2 ORA SIAMO PRONTI AD ESIBIRE UNA SOLUZIONE PIÙ BREVE DEL PROB. 8:

SVOLGIMENTO PR. 8 (II MODO)

CON LA NOTAZIONE APPENA INTRODOTTA POSSIAMO SCRIVERE:

$$x^{20} \equiv -2 \pmod{(x^{20}+2)}$$

QUINDI, GRAZIE ALLA PROPOSIZIONE 1, TUTTE LE VOLTE CHE NEL POLINOMIO $P(x)$ SOSTITUISCO x^{20} CON -2 LA CLASSE DI RESTO MODULO $(x^{20}+2)$ NON CAMBIA. QUINDI SI HA:

$$P(x) = -3x^{81} + 10x^{61} + x^{24} + 6x^{21} + 2x^3 + x^2 + 9x + 53 =$$

$$= -3x\cdot(x^{20})^4 + 10x\cdot(x^{20})^2 + x^3\cdot(x^{20}) + 6x\cdot(x^{20}) + 2x^3 + x^2 + 9x + 53 \equiv$$

(CONGRUENZA MODULO $(x^{20}+2)$)

$$\equiv -3x\cdot(-2)^4 + 10x\cdot(-2)^2 + x^3\cdot(-2) + 6x\cdot(-2) + 2x^3 + x^2 + 9x + 53 =$$

$$= -48x + 40x - 2x^3 - 12x + 2x^3 + x^2 + 9x + 53 =$$

$$= x^2 - 11x + 53.$$

A QUESTO PUNTO, POICHÈ IL GRADO DI $x^2-11x+53$ È MINORE DI QUELLO DI $x^{20}+2$. DIRE CHE $P(x) \equiv x^2-11x+53 \pmod{(x^{20}+2)}$ EQUIVALE A DIRE CHE IL RESTO DI $P(x):(x^{20}+2)$ È PROPRIO $x^2-11x+53$.