derme for 3 mod 5 es. ∫3X=1 (mod5) lorviere in Zp p poro (x=3=2(mods) Compo S (3) moltyhione
Fold (4) denone per eleuti my zero mcd(3,5)=1Field | leagi (a) amocrature (xy17=×(yz); (x+x)+z= (a) Commusation > xy= yx > xxy= y+x C) dutin lusting> X(4+2)= X/4XZ tra le apprime e nottifbame insemi commissioni - muni aufleri - runni Easturli [-uteri mod p (prino) l'usure degli unteri mon è un compo un quibo \frac{2}{3} un e un utter ESEMPLO GF(22)=6-F(4)={0,1,x,x2} GF(22)= Z/X/(mx2+x+1) $X \cdot X = X^2 = X + 1 \pmod{X^2 + X + 1}$ teleut +10 € 1 t41+x=x2

```
D+X=X
ス・
3,
```

1.
$$0+x=x$$

2. $x+x=0$

3. $1\cdot x=x$

4. $1+x=x^2$

5. addoxine moltyluotune

2 mo commutative e

e anocentive, next to

leggy di olimulutur

 $\times (y+z)=xy+xz$
 $+x/y,z$
 $+x/y,z$
 $+x/y,z$
 $+x/y,z$
 $+x/y,z$
 $+x/y,z$

2. $+x/z=x+1+x=1$

 $x^2 = x^{-1}$ e use x^2 e'il moltyblatta usero di X.

un compo è un urseur che auxturent gli element 001 (170) « che 1. noltybare e adobtelle roduste a a. 0+x=X, $\forall X$ v. $1\cdot X=X$, $\forall X$ c. somutative, amount up e distributive ornowine (a+b)+c=a+(b+c) ense l'additure uveno Connectation x+ (x)=0 distributive ente il moltybetus ure X ()+5)=XX+X5 (*(とう)とこなけた 3. x.x=1 em compo é churso per settrosaul x-y=x+(-x)

M= (a G) MM e un cufo 122 (1) moltyleane un commodite A·B ≠ B·A (2) M=? re det M=0 Jungseure dei survi reoli 70 add ok un e un auto XER30 nulty ok devote ax 5-7=(2) -2 & Ryo Julitroco Per ogni potura pn (p muse n)o untero) c'è un solo compo fruito an esoutoueut prelements'-(Se n/1 gli uter m (mod pa) $\begin{cases} \text{ sum mo u coufo} & p x \equiv 1 \pmod{p^n} \end{cases}$ / rin ha solwaire quiet u courter fuita (F(ph) un mo gli neteri mod pa ma Nous artenti diversomente

Z[X] l'unu di tutti i poliumi $a(x) = \sum_{i=0}^{m-1} a_i x^i \qquad \text{polivomor} \\ a = 0 \qquad \text{monico re} \\ a = 1$ di grado m-1 evendo m entero) o m-1 m-1eneudo $ai \in \mathbb{Z}_2 = \{0,1\}$ Z[x] (modqx+qx++ qx+40) in genere $a_n = 1$ l'un compo GF(2ⁿ) Polimer mmar re volo re il foliumo di grado n'è viriduculla es. n=2 polinomi Z [x] pu n=2 modi grodon-1 gli elembi grado o 1 1 quelli di, $X^2 \rightarrow X.X$ reducalelle operatore $(1+X^2) \rightarrow (1+X)=1+X^2$ reducalelle $(1+X+X^2) \rightarrow X(1+X)$ reducalele $(1+X+X^2)$ [Relibucible]

allnow GF(22) = Z[x](mod x?tx+1)
20,1, x, x+13 som i residui quomdo ni devide il poli nomio vriducibele X2tXt1
folderne, sothorne moltyluorus (mod x? + X + 1)
Triducible nymtice che il folumo ? (x)
$(dignation) \Rightarrow T(x) \neq f(x)g(x) \text{ in } \mathbb{Z}_2[X]$
had laternaire au poliumu of
grado inferme f(x) egx) (or grado
PROCEDURA Compor funto em pa elementi (X), f(x), g(x), p puno m > 1 wero 200), f(x), g(x), E XII
p puro m /21 where
Zp meti med p.
1. Z[x] e l'ureur dei folmoni on

2. Geegli 7(x) poliurus vriidu alub mod p di grado n

3. GF(pm) de Z[x] mod ((x) é un compo a prélementi.

ESEMPLO moltylicaters unersodi $a(x) = x^2 + 1 \quad \text{in } GF(2B) = Z[x] \pmod{x^8 + x^4 + x^4 + x^4 + 1}$ Ro=M(X)hartor una divinire 四= Q(X) x3+x4+x3+x+1= (x6+x4+x)(x2+1) + 1 a= x4x4x $(x^{6}+x^{4}+x)(x^{7}+1) = x^{6}+x^{6}+x^{3}+x^{4}+x^{4}+x =$ $\equiv X^{\frac{8}{4}} \times^{\frac{4}{4}} \times^{\frac{3}{4}} + X \equiv 1 \pmod{\times B_{+} \times^{\frac{4}{4}} \times^{\frac{8}{4}} \times^{\frac{1}{4}}}$ $a(x) = x^2 + 1 = 000000101 = {05}$ hex $\bar{\alpha}^{(x)} = x^{6+x} + x = 01010010 = \{52\}$ Reg

ESEMPLO Venficone el cooline dell'elements (X+1) del compo Z[X](X3+X+1). l'ordine d' 23-1=7; refortsi: $(\chi+1)^{7} \operatorname{mod}(\chi^{3} + \chi + 1) = 1$ Afflichenus S&M 1, have (X+1) $|| (x+1)^{2}(x+1) = x+1$ $|(x+1)^{2}(x+1) = (x+1)(x+1)$ $= x^{3}+x^{2}+x+1 = x^{2}$ $|(x^{2})^{2}(x+1) = x^{5}+x^{4} = 1$ (mead x +x+1) x3+x+1/x3+x2+x+1 x3+x+1

logentu dupli

2

b(x) = a(x) (mod e(x))

uni a(x) e b(x) deserme to

en u GF(4)

a(x) = x = d(x)

b(x)= 1

 $\chi^3 = 1$ A = 3

(mod x2txt1)

Faltmusermi di folimi



Z[x] l'vurieur di tutti i famileli Mucheo con foliverni della voudel $f(x) = a \times x + a \times x + \dots + ax + ab = 0$ $= \sum_{i=1}^{n-1} q_i \chi^i$ di grado POLINO MID (n-1) enerdo ni rutero)o. NOVICO refficientations eld vettre a n eleventi (dn) dn -2) ..., d1) 20) eneudo i coethiceudí $a_i \in \mathbb{Z}_p$; $o \subseteq a_i \subseteq p^{-1}$ Humano di folivori di pado (h-1) è e avoir mosto di compune il retture a re elembi con elementi reelti tra poliversi. Di gunde infutanta produce e il cuso p=2 e'é unem di tutti a poliumi con ai EZ=(0,1)





Tra folivorni f(x1 E X [x]
n' definizero le operarin di
· additione
Sothazione
o oliverione
nordando de ser la nomifoloxiono dei coefficenti linegra operare modulo p.
Adesempro $f(x) \in \mathbb{Z}[x]$
$f(x) = x^{6} + x^{3} + 1$ $g(x) \in \mathbb{Z}[x]$
$\mathbf{u}(\mathbf{x}) = \mathbf{x} + 1$
(x)+g(x)=(x+x+x+2/moa 2
$= x^6 + x^3 + x \pmod{2}$
$f(x)-y(x) = x^6+x^3+x = f(x)+g(x)$
si può face con x6+x3+1 = 1001001 EXC
grado niax =6=(n-1) degf(x)y=6 e poi
x = x
Vettre livour lugan
$1001010 \equiv x^{6} + x^{2} + x$



Prodoto

$$(x^{3}+x+1)(x+1) = (x^{4}+x^{3}+x^{2}+2x+1) \mod 2$$

$$= x^{4}+x^{3}+x^{2}+1$$

$$= x^{4}+x^{3}+x^{2}+1$$

$$= x^{4}+x^{3}+x^{2}+1$$

$$= x^{2}+x+1$$

$$= x^$$





rel cono di sopra

$$\eta(x) = x^2 + x + 1 = z(x)$$

$$q(x) = x^{2} + 1$$

$$t(x) = x = t(x)$$

allera

$$x^{4+x^{3}+1} = (x^{2}+1)(x^{2}+x+1)+X$$

all'outsuebica modulare des mon utin potrosse che n' pena scriber

over afflicare le auguence

$$x^4 + x^3 + 1 \equiv x \pmod{x^2 + x + 1}$$

Si posissans alles le operation rell'useur di polinoin modurai

$$f(x) \in \mathbb{Z}[x](\max_{x \in X} x^2 + x + 1)$$





Profesto al folivouro di remoto prooto

X²+X+1

X + X+1 l'inneuer 2 (mod x?+x+1)

l'fattso alori 4 foliumi oli globlo (n-1=1) (0;1;x;x+1)e questo un compo finito. l'e mol fono olefime i noltylicoteri uversi per tutor gli elemetri un melle, se e rolo se, il foliverus rusolulo X2+X+1 di grudo n=2 e IRRIDUABILE (équishente di priva) e col un unilse curposto dal modato di polimum di procoto informe, al nommo n-1 (= 1 in questo corto n=2). Per exemple X2+1= (x+1)(X+1) e RIDUCIBILE in Z [x], in quarto





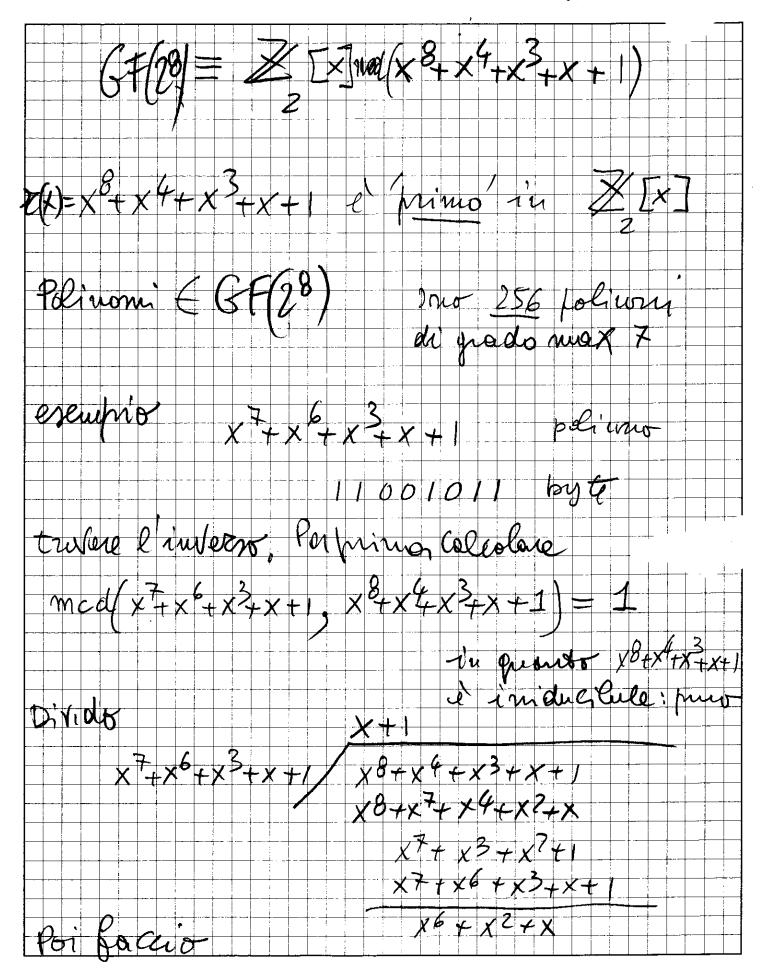




x2+X+1/x2 antimenolo $x^3 = x \cdot x^2 = x \cdot (x+1) \equiv x^2 + 1 \equiv 1$ mod x(txt1) X3+XC+X XI+X X7+X+1 quadi X, x2 = 1 (mod x2+X+1)









0)

Xt1

		X-	<u> </u>	
	x6+		7 ₊ x 6 ₊ x 3 7 ₊ x 3 ₊ x 2	
Allna		±	6+ x7+x	
570=17()	$() = x^{8} + x^{4} + x^{6} +$	x3+X+1		STOP
$q_1 = x + 2z = x + 4$	×2+×			
$9_2 = Xt$ $2_3 = 1$	STOP. 3=MAX	to=0;7	t_=1 t	$2 = t_0 - q_1 t_1$ $3 = t_1 - q_2 t_1$ $3 = a^{-1}$
the second secon) -(x+1)·1 1- (x+1)(x		(4+1 = X°	2= 4 1
Infoldi	$q^{-1}(x) = x^{2} \cdot (x^{7} + x^{6} + x^{6})$		+x ⁸ +x5, y3.	+ 2 = 1
	x2. (x7+x6+,	, • • • • • • • • • • • • • • • • • • •	(mod xx	(4+x2+X+1)

|---<u>-</u>



(10)

	X + 1
	x9+x8+x5+x3+x2
1	x9+ x5 + x4+ x2+ x X8+ x4+ x3+ x
	x8+x4+x3+x+1
	Joh





ESISTENZA DI CAMPI FINITI	
in $\mathbb{Z}[x]$ c'e' almeno 1 Jer ogni grado	oliumio miducilule
Jer ogen grado	$m \geqslant 1$
Prindi c'e' un compo fi	
per tutti i primi pe t	utti ghi unteru m>1.
Per ogni grado n e p	nuo p clearin
Jenune un oughite of	i promo u e c'e'
alvens in Coup Lines	d'preleurs.
A pui toliani unidu	
judo consposo p	
tubbi ISOMORFI to lus	- Quint C'e un
Selo Compo Louto di g	udesto par de vo
	St(by)
Se m=1	
	= 6 t (p)



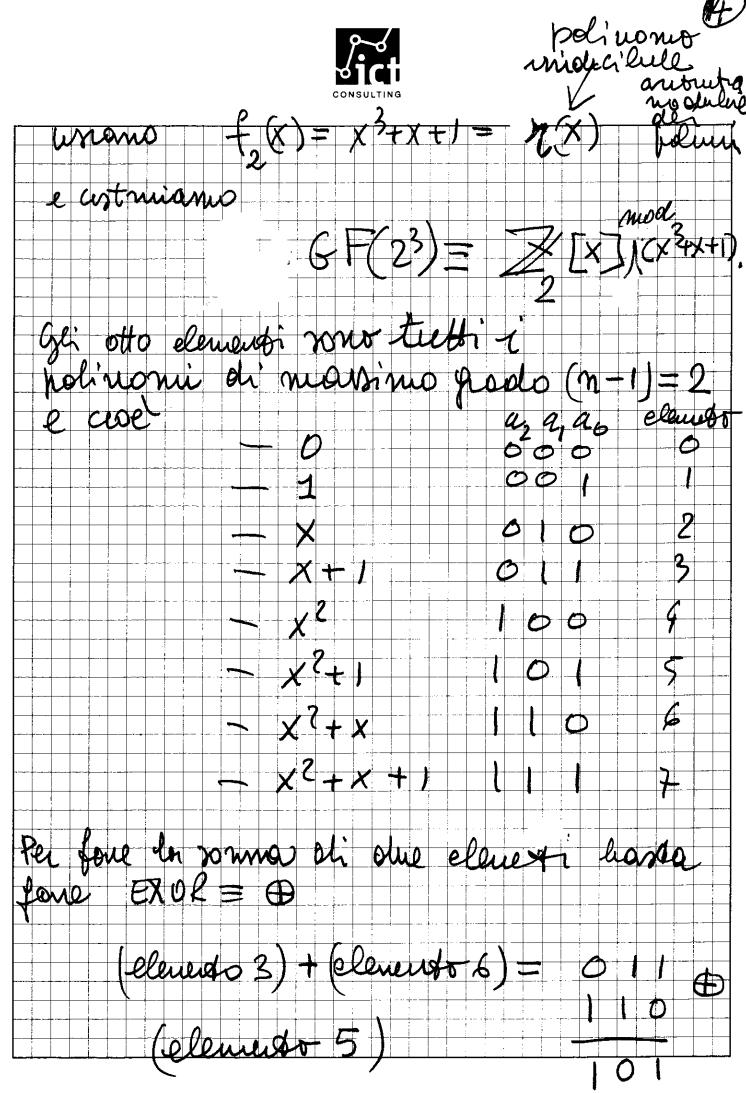


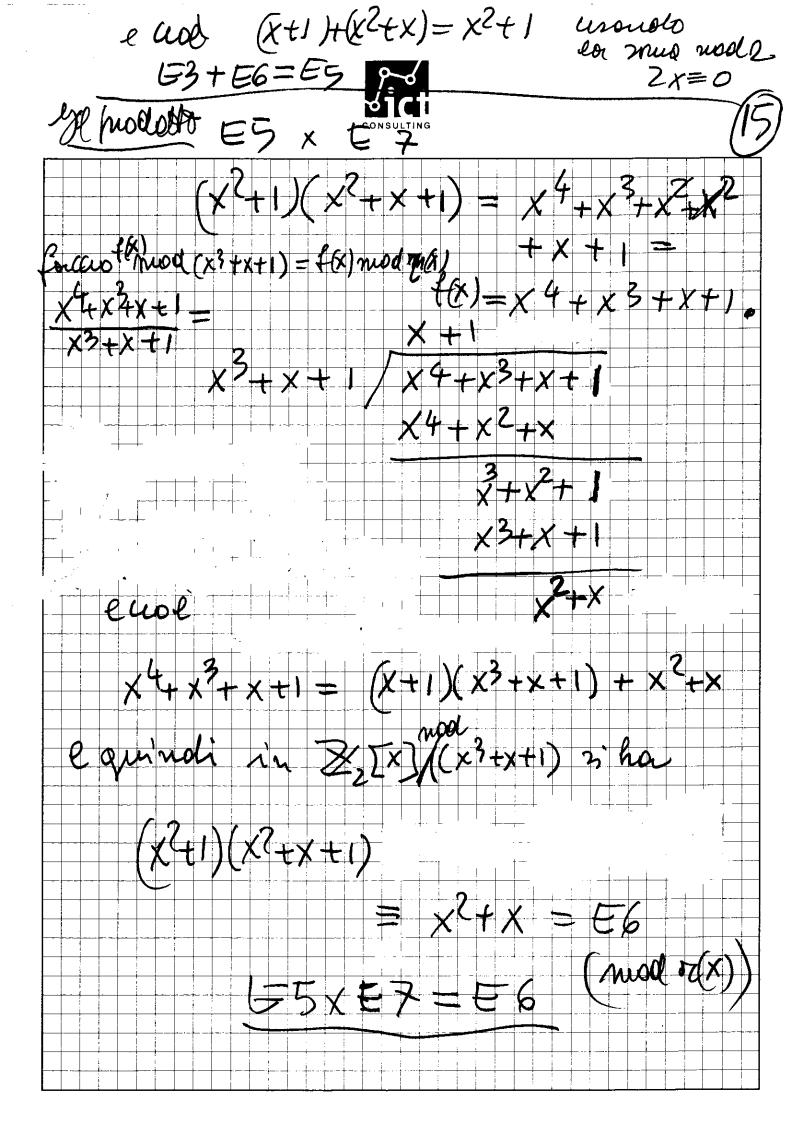
eleve 2 Cours ay molt elevert cheo di ordi Hudans erchion zolnolité del el compo de co OL anno e do nathan goods Cocchiono wideal

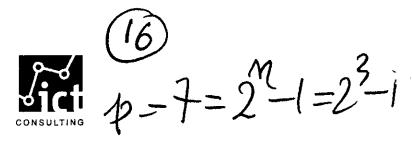


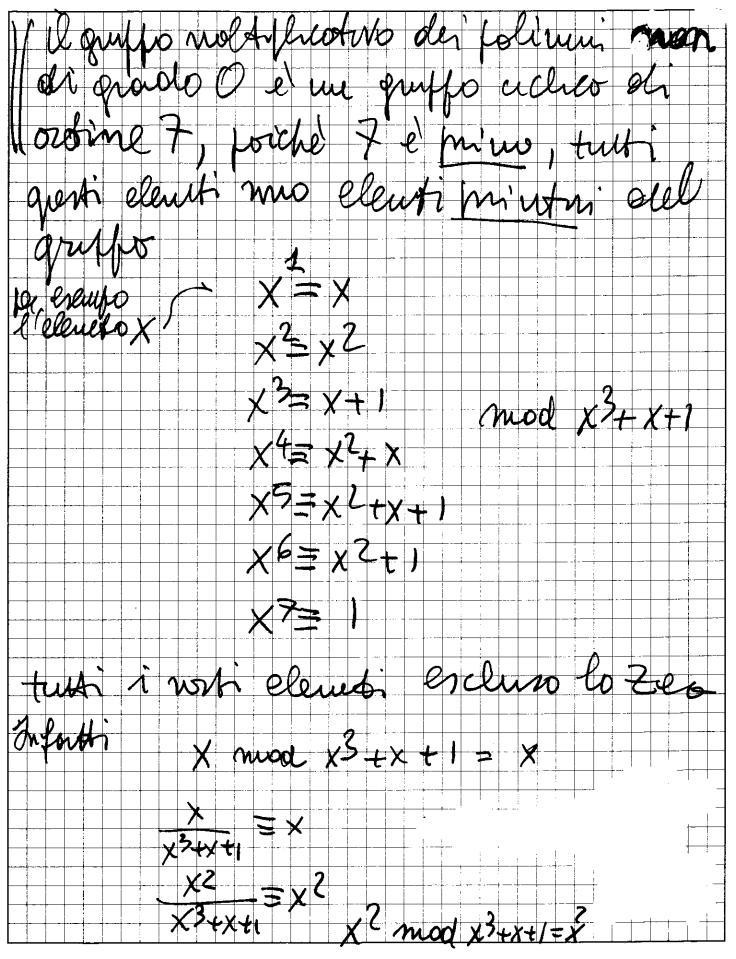


muo 16 defferenti miducilule, eleve enero groots marino Cu Qz ora nducilule RIDUCONO MODZ **TUtt**l = (x+1)(x2+1) 2010 IRRIDUCIBIL UTAVIA











= X.(X+1)= X4X X4= X2+X x, x4= x5= $\cdot \times (x^2 + x) = x^3 + x^2$ $x^5 = x^3 + x^2$ X3+XC X Z = X LX+1 X.X5= X6= $= \chi(\chi^2 e \chi t i) = \chi^3 t \chi^2 t \chi$ x3+x2+x x3+x2+x x5= x2+1 x7=x(x2+1)=x3ex= x3+x x3+x+1

sici (18)

Compo findo GF(23) (X3+x+1) MOLTIPUCATORI (NVERS) 000 €2=×=W 00(2 → 5 000 ES=X2+1=W-1 011 00 EUCLIDE ESTESO 101 5 ← 2 m < d(x, x3+x+1) 110 10(x)=x3+x+1 LI) 7 a(x) = x26= 10(K) rueca di a(K) 21= Q(X) tole the 20= 149,+72 a(e)·ae)=1 (mod x 3+x+1) X/X3+X+1 9(x)=x2 to=0; t1=1 22(x)=X+1 t,=to-9,t1= X+1/x 21=292+23 $=0-x^2=x^2$ X+19,(x)=1 t3=t1-92t2= 23(X)=1 STOP. = 1 - 1 • x2 = x4+1 a(x)= x2+1



(19)

X2+X

 $\chi^3+\chi^2$

 X^7+X

 $\times^{0}+x+1$

 $\times + 1/x^3 + x + 1$

Altro esempio

$$\mathbf{v}(x) = x^3 + x + 1$$

$$Q(X) = X + 1$$

$$q(x) = ?$$

$$= 0 - (x^2 + x) \cdot 1 = x^2 + x$$

$$\overline{a} = x^2 + x$$

$$(x+1)(x^2+x)=x^3+x^2+x^2+x=$$

$$= X^{3} + X$$





 $t_2 = D - (x^6 + x^4 + x) = x^6 + x^6 + x = \bar{e}$ $x(x) = x^2 + 1 = 000000101 = \{05\}_{\text{flax}}$ $\vec{c}(x) = x^4 + x^4 + x = 010110010 = \{52\}_{\text{flax}}$

Z_[x] (x8+x+x+x+1) a(x)=x2+x+1 $x^{4}x54x3$ a(81? x4x+1/x8+x4+x3+x+1 X8+ x7+ x6 X7+X4X4+X+X+Xt1 20= P(X) x7+x9x5 4= e(x) X5+X++X3+X+1 9,=x6+x5+x3 x54x4x3 72= X+1 X+1 X+1/x2+x+1 9,= X 23= 1. STOP 3=MAX X2x / to=0) t=1 t2=to-9,t1=0-(x4x5+x3)=x4x5+x3 t3= t1-92t2 = = 1- (x(x6+x5+x3)=x7+x4x4+1=9) (2+x6+x4-1)(x2+x+1)= x9 +x8+x6+x2+x8+x7+x5+x+x7+x6+x41 = = x9+x5+x4+x2+x+1 x&x4x3x+1/x3+x5+x4+x2+x+1

X9+X5+X4+X8+X X9+X5+X4+X8+X I.CVD

Moltiploxure i'u 7(x)=x8+x4 x3 x+1 = 19 BIT = 1000011011 Modiffichiano 11001011 [88] (x7+x6+x3+x+1) Fr (x)= = x4x7x4x4x= = (x7+x3+x2+1)+ (x2x4+x3+x+1) $=(X^{7}+X^{3}+X^{2}+1)$ mod $(X^{4}+X^{3}+X+1)$ > SHIF LEFT & APPEND A'O"
FINESTRA A 8 BIT (9 BITS) [BBIT] -> SUBTRACT X4x4xx X+1 7 110010110 A

0 10001 101

(x7+ x3+x2+1) K

QUINDI LA MOC	L'ALGORITMO GF(28) PER TIPULAZIONE PER X, E/	(23)
	a soliB put di una fontu	

- 1. Sporta à let di una fontaone a n'intrep e ougques une 10' crue ulturo bet
 - 2. Se il privo lut e' 0, STOP.
 - 3. Se el privabit é 1, XOR 100011011
- · PERX3 ni fa tre volte. PER xⁿ ni fa n volte
- ordes: Xh x x + x j h>k>j

 n'ha mine h volte e n'othere il puro termo

 n'ha mine h volte e n'othere il puro termo

 pri la zende k 4 11 4 4 x endo 11

 n u trera j 11 11 11 x y trerro terme.

 e untive n'fa EXOR & de 3 termini

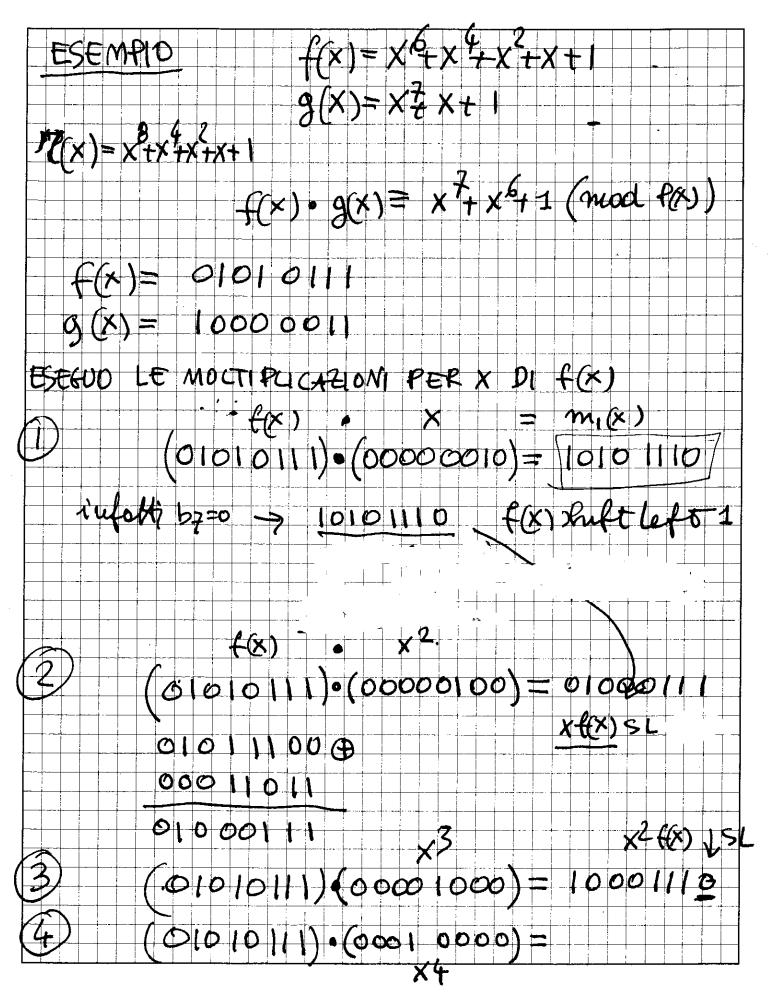


x8+x4+x3+x+1=2(x) 6F/28 x8 mod 2(x)= \ 2(x)-x8 5F(29) x much 2(x)=) 2 (x)-xn] P(x) = b7 x7 b6 x6+ b5x5+ 54x4-5, x+ 5x+6 X . f(x) = (b, x + b, mod > (1) bz = 0 allro il toliuno e ali prado 7 ed e 012 un e recessence ressure notuture allue in has alle (1 X • ((x)=(box + box + bax + b +(x4+x3+x+1) LO MOUTIPLE CAZIONE PER X E UNO SCO REI MENTO A SIMISTRA DI UN BIT'S EGUND DA XOR CON 000 (1011) che respresente (x+x3+x+1)

X=(0000 0010)={02} ו ((x)= 875 873=(1000 0111 SHIFT LEFT 0000 (1) 000110 0001010 {6€}⊕({02}-{6€}) 110 1110 0000 0011 1101 1100 0110 111086 ES 10110010









000110 0000011 00001110 1010111) • (0100 0000) 00011100 (01010 111) · (1000 0000)= 00111000 Pertordo 01010111). (10000011)= (0000000) (0000 0010) (1000 0000) (01010111) (0101011) @ (1010 1110) @ (00111000) 11000001 = X7+X6+