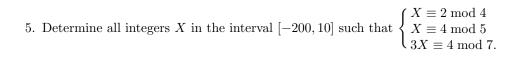
Family Name			Name					\dots Student $ID(Matricola)$: \dots					
Solve the problems adding													
EXTRA SHEETS WILL B	EACC	EPTE	D. 1 Pr	oblem =	= 4 mag	rks. Du	ration:	2 hour	s. No question	ns allowed in	the first hour		
and in the last 20 minutes.													
	1	2	3	4	5	6	7	8	TOTAL	7			
1. Answer the following q	uestions	s provi	ding a i	ustifica	tion of o	one line	•						
1, 11110 6110 10110	0.0001011	provi		ab 01110a	01011 01	3110 11110	•						
a. Is the Diffie-Hellm	ann key	excha	nge pro	tocol or	nly defi	ned for	the cycl	lic grou	$p \mathbf{F}_{p^n}^*$?				
1 T ' 1 1 1 1 1 1 1		· · <u>:</u> · · · ·	1					;:					
b. Is it true that there of generators?	e are no	n-isom	orpnic i	іпіте пе	eias in w	nich th	e respec	tive mu	itiplicative gre	oups nave th	e same number		
or generators:													
c. If $f, g \in \mathbf{F}_p[x]$ have	$_{\rm e}$ the sa	me deg	ree, is i	t true t	hat the	splittir	ng field	of f con	ntains the roo	ts of q ?			
* /3 - Pt 1			,			•	O	v		Ü			

2. After having written recursive formulas for the calculation of the Bezout identity between two integers, compute that identity for (1345, 9875). Next compute the greatest common divisor (1345.9875) using the binary algorithm.

d. Write down all irreducible polinomials in $\mathbf{F}_2[x]$ with degree less or equal to 4.

3.	After having shown that 3 is a primitive root modulo 31, campute the discrete logarithm $\log_3 2 \in \mathbf{Z}/30\mathbf{Z}$ using the algorithm Baby Steps Giant Steps.
4.	Outline some cryptographic systems that base their security on the problem of discrete logarithm .



7. Determine the degree over \mathbf{F}_{13} of the splitting field of the polynomial

$$(T^{13^8} - 27T^{13^5} + 26T^{13^4})(T^2 + 13T + 27)(T^3 + 14)(T^{13^8} + 25T^{13}) \in \mathbf{F}_{13}[T].$$

8. After having explained briefly the algorithm of successive squares, compute $\alpha^{1047} \in \mathbf{F}_7[\alpha], \alpha^3 = \alpha - 2$.