# **HOCHSCHULE ESSLINGEN**

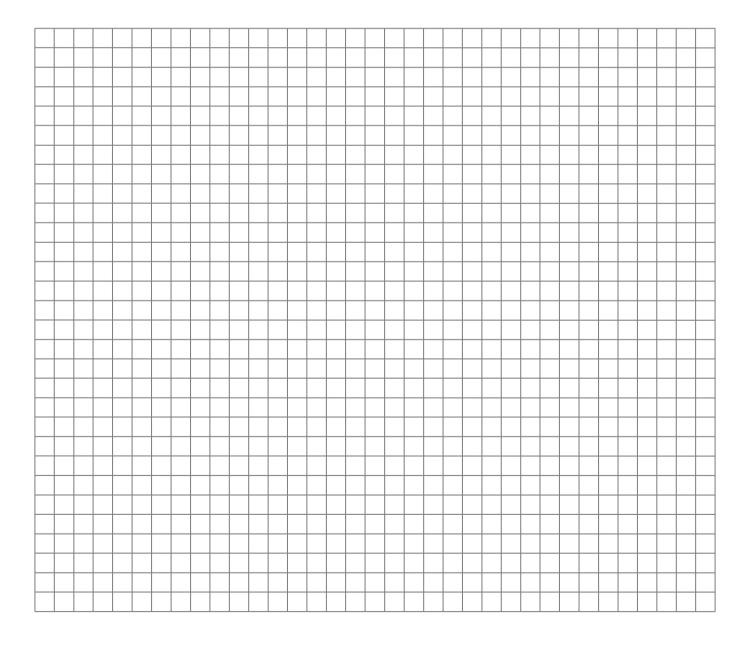
Sommersemes	ster 22	Zahl der Blätter: 8 Blatt 1 von 8			
Studiengang: Dozent:	SWB: Strecker	Semester:	SWB2		
Prüfungsfach:	Diskrete Mathematik	Prüfungsnummer:	1052034		
Hilfsmittel:	Literatur; Manuskript; ausgegebener Taschenrechner Casio FX-87DE PLUS oder Casio FX-87DE PLUS 2nd Edition	Zeit: 90 min. 60 Punkte			

#### Aufgabe 1 (8 Punkte)

Gegeben sei die zweistellige natürliche Zahl 10a+b mit  $a,b\in\{1,2,...,9\}$  Man zeige: Wenn  $a+b\mid 10a+b$  gilt, dann gilt  $3\mid 10a+b$ 

*Hinweis*:  $a + b \mid 10a + b \Leftrightarrow 10a + b \equiv 0 \mod (a + b)$ 

Schließen Sie daraus auf  $9a \equiv 0 \mod (a + b)$  und nutzen Sie Ihre Kenntnisse über Teilbarkeit.



Sommersemester 22	Blatt 2 von 8			
Prüfungsfach: Diskrete Mathematik	Prüfungsnummer: 1052034			

### Aufgabe 2 (7 Punkte)

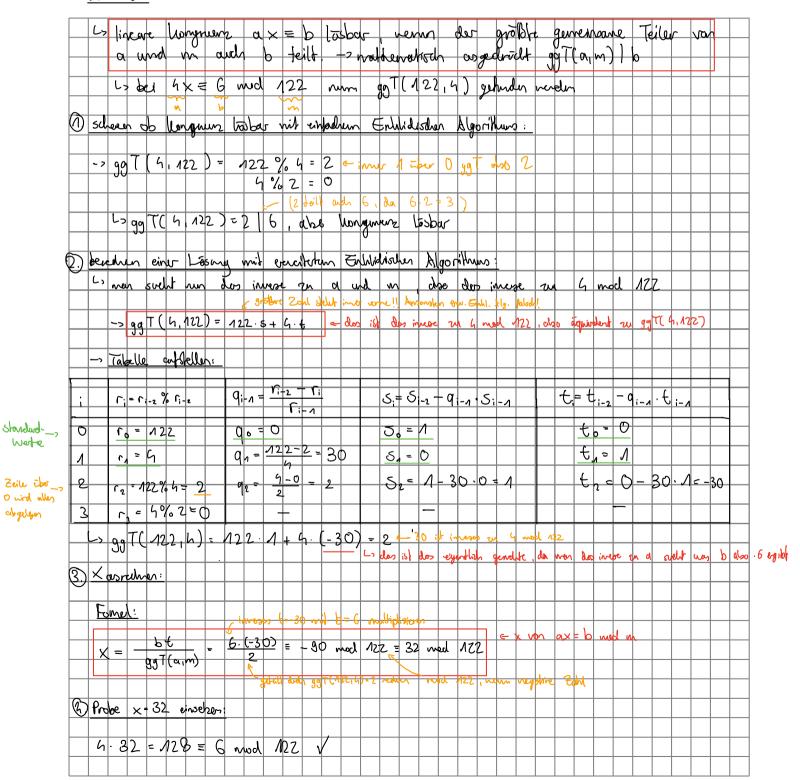
weste

citypleson

Gegeben sei die Kongruenz

 $4x \equiv 6 \mod 122$ 

Begründen Sie, ob diese Kongruenz lösbar ist, und berechnen Sie ggf. eine Lösung. Ansah:



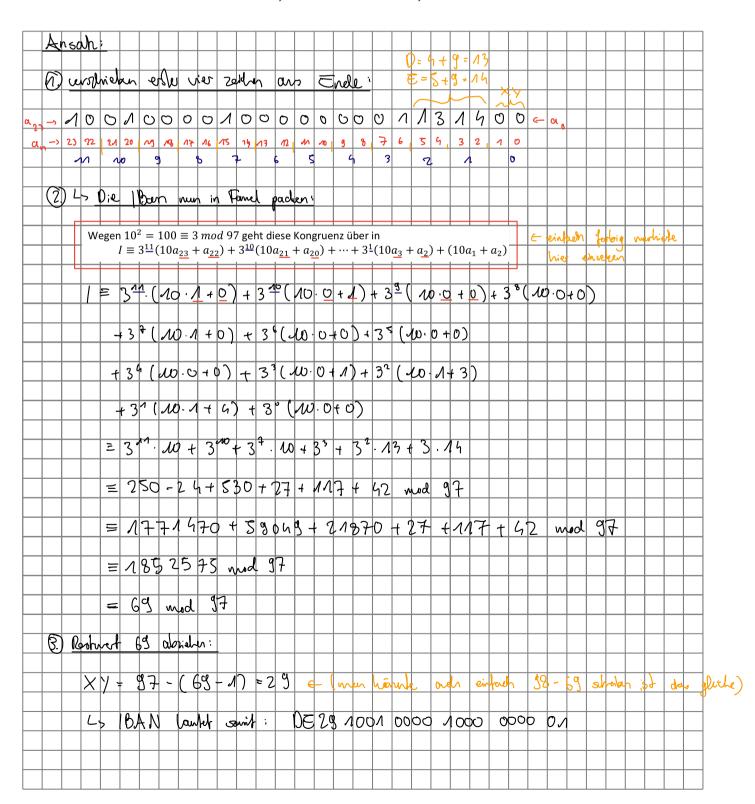
Sommersemester 22	Blatt 3 von 8				
Prüfungsfach: Diskrete Mathematik	Prüfungsnummer: 1052034				

#### Aufgabe 3 (8 Punkte)

Berechnen Sie die Prüfsumme XY für die IBAN

DEXY 1001 0000 1000 0000 01

<u>Hinweis</u>, falls Sie auf einen TR verzichten, nutzen Sie im Skript 5.2.3 und die Ergebnisse  $3^7 \equiv 53 \mod 97, 3^{10} \equiv -24 \mod 97, 3^{11} \equiv 25 \mod 97$ 

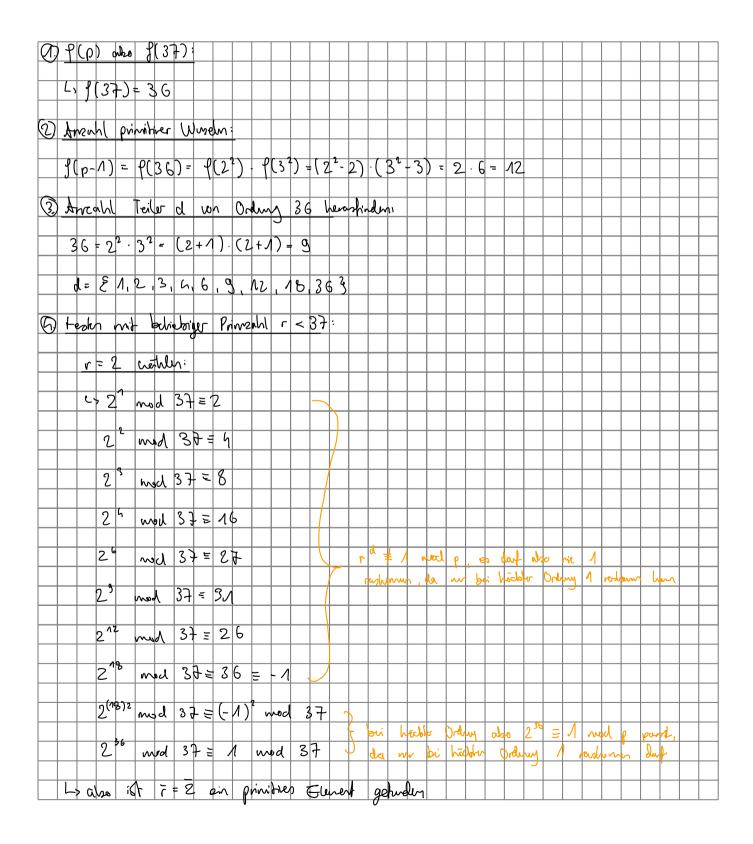


							Bla	att 4	ł vc	n 8	3							
Prüfungsfach: Diskrete Mathematik	,	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59
Tulungsiach. Diskrete Mathematik		61 6	67	71	73	79	83	89	97	101	103	107	109	113	127	131	137	139
alle Primzulla O bis 100:	1.	49 1	.51	157	163	167	173	179	181	191	193	197	199	211	223	227	229	233
ufgabe 4 (7 Punkte)		39 2	:41	251	257	263	269	271	277	281	283	293	307	311	313	317	331	337
argabe 4 (7 1 unkte)	3	47 3	149	353	359	367	373	379	383	389	397	401	409	419	421	431	433	439
erechnen Sie $\varphi(20570)$	4.	43 4		457	461	463	467	479	487	491	499		509		523	541	547	557
ποσιμού στο φ (2007 σ)				571	577	587	593	599	601	607	613		619		641	643	647	653
inweis: Bekannte Teilbarkeitsregeln				673	677	683	691	701	709	719	727				751	757	761	769
•				797 911	919	929	937	941	947	953	839 967				991	997	881	883
		67 3	107	911	313	323	937	541	347	933	307	9/1	377	903	991	337		
bevali:			$\perp$		$\perp$		$\perp$	$\perp$	$\perp$					$\perp$			_	
		_	$\perp$	_	$\perp$	$\perp$	$\perp$		_				4		1		_	
C> Printablor Enlegues:		$\perp$	_	_	_	_	$\perp$		_			_	_	$\perp$	_		_	
		_	$\perp$	_	$\perp$	$\perp$	_	_	-			_	_	_	-		_	_
) 20570 in Prindolpharen terleyen:		$\perp$	+	+	+	+	+	+	$\vdash$			_	_	+	-		$\dashv$	_
1070 0 1000		+	+	+	+	+	+	+	-			_	+	+	-		+	-
-> 20570 = 2. W285	$\vdash$	+	+	+	+	+	+	+	-		$\square$	-	+	+	+	$\vdash \vdash$	$\dashv$	-
= 2 5.2057		+	+	+	+	+	+	-	-			-	+	+	+		-	
- 12, 3, 6, 03, 4	$\vdash$	+	+	+	+	+	+	+	$\vdash$			$\dashv$	+	+	+	$\vdash$	$\dashv$	+
= 2 · 5 · 11 · 187		+	+	+	+	+	+	+	+				+	+	+		$\dashv$	+
2 9 7(7) 7/6 1	$\vdash$	+	+	+	+	+	+	+	+			$\dashv$	+	+	+	$\vdash$	$\dashv$	+
= 7.5.11.17.1	1/1		+	+	+	+	+						+	+	+		$\dashv$	
		$\dashv$	$\top$	+	+	$\top$	+		+				+	+	+		$\dashv$	$\top$
- 2.5.11.17			$\top$	+	+	$\top$	+		+				$\dagger$	+			$\dashv$	
	$\Box$	$\top$	$\top$	$\top$	$\top$	$\top$	$\top$	$\top$	$\top$		П	$\top$	$\top$	$\top$	$\top$	$\Box$	$\dashv$	$\top$
) P(20570) durch P(Printalber) both	40;		$\top$	$\top$	$\top$	$\top$	$\top$		$\top$		П		$\top$	$\top$			$\neg$	
) f(20570) durch f (frindallour) borch f(20570) = f(2). f(5). f(112).	_ gr	wds	sathic	th g	ill:	4(	p*)	- p	4-1	u-1	د ۸	12-	1.1	2-4	11 <sup>2</sup>	11		
1(20870) = P(2) · 1(5) · 1(111) ·	9(h	.71																
$= 1 \cdot 4 \cdot (11^2 - 11^4) \cdot$	16																	
= 1.4.110.16																		
			$\perp$	$\perp$		$\perp$	$\perp$		$\perp$				_	$\perp$			$\perp$	$\perp$
= 7040 = (mult gentry)	ober	des	Wei	е	tre	ahl	<del>de</del> -	teile	rher	den	)	_	4	$\perp$	-		$\perp$	_
		_	$\perp$	4	$\perp$	$\perp$	$\perp$	+	_		$\square$	_	4	$\perp$	-		_	_
		+	$\perp$	+	+	+	+	+	+		$\square$	$\perp$	+	+	+	$\square$	$\dashv$	_
		+	+	+	+	+	+	+	-		$\square$	_	+	+	+		$\dashv$	_
+++++++++++++++++++++++++++++++++++++++		+	+	+	+	+	+	_	+		$\vdash \vdash$	_	+	+	+		_	-
+++++++++++++++++++++++++++++++++++++++		+	+	+	+	+	+	+	+		$\vdash \vdash$	+	+	+	+	$\vdash \vdash$	$\dashv$	+
+++++++++++++++++++++++++++++++++++++++		+	+	+	+	+	+	+					+	+	+		_	
+++++++++++++++++++++++++++++++++++++++		+	+	+	+	+	+	+	+			+	+	+	+		+	-
+++++++++++++++++++++++++++++++++++++++		+	+	+	+	+	+	+	-		$\vdash \vdash$	+	+	+	+	$\vdash$	$\dashv$	_
+++++++++++++++++++++++++++++++++++++++		+	+	+	+	+	+	+	_		$\vdash \vdash$	-	+	+	+	$\vdash \vdash$		_
+++++++++++++++++++++++++++++++++++++++		+	+	+	+	+	+	+	+		$\vdash$	_	+	+	+		+	
+++++++++++++++++++++++++++++++++++++++		+	+	+	+	+	+	+				-	+	+	+	H		
+++++++++++++++++++++++++++++++++++++++		+	+	+	+	+	+	+	+		$\vdash$	+	+	+	+	$\vdash$	$\dashv$	+
<del>                                     </del>		+	+	+	+	+	+	+	+		$\vdash$	+	+	+	+	Н	+	+

Sommersemester 22	Blatt 5 von 8			
Prüfungsfach: Diskrete Mathematik	Prüfungsnummer: 1052034			

## Aufgabe 5 (8 Punkte)

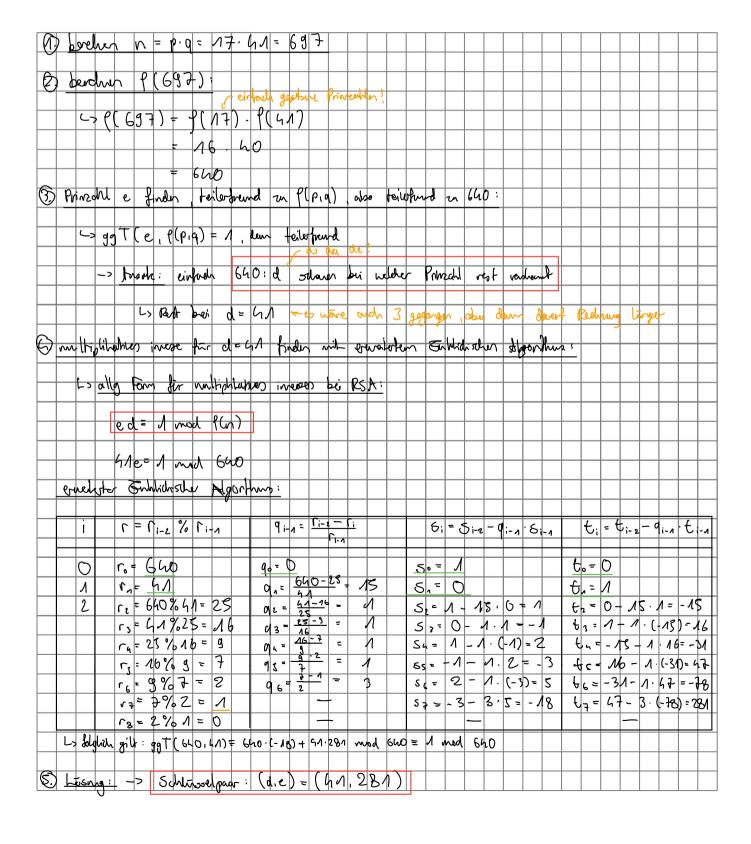
Geben Sie eine primitive Wurzel von  $\mathbb{Z}_{37}^{\times}$  an.



Sommersemester 22	Blatt 6 von 8			
Prüfungsfach: Diskrete Mathematik	Prüfungsnummer: 1052034			

#### Aufgabe 6 (7 Punkte)

Berechnen Sie zum Primzahlpaar (p,q) = (17,41) ein RSA-Schlüsselpaar mit öffentlichem e und privatem Schlüssel d so, dass  $d \not\equiv e \mod \varphi(pq)$  ist.



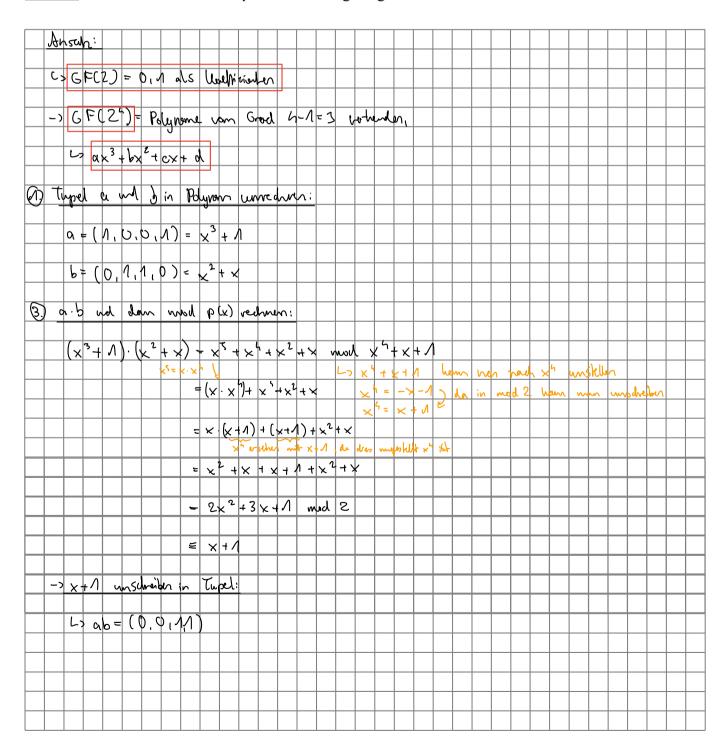
Sommersemester 22	Blatt 7 von 8			
Prüfungsfach: Diskrete Mathematik	Prüfungsnummer: 1052034			

#### Aufgabe 7 (8 Punkte)

Wir betrachten das Galois-Feld  $GF(2^4)$  und das irreduzible Polynom  $q(X) := X^4 + X + \overline{1} \in \mathbb{Z}_2[X]$ 

- a) Berechnen Sie für  $a := (1,0,0,1) \in GF(2^4)$  und  $b := (0,1,1,0) \in GF(2^4)$  das Produkt  $ab \mod g(X)$
- b) Wie lautet das zu  $a := (1, 0, 0, 1) \in GF(2^4)$  Inverse  $a^{-1}$ ?

*Hinweis*: Die Irreduzibilität von q braucht nicht gezeigt zu werden.



## GF(22):

 $q(X) = X^2 + X + 1. \bot$ 

#### Sommersemester 22

Prüfungsfach: Diskrete Mathematik

Polynom	Tupel	Binär	Exponent von X	Exponent von $X + 1$
0	(0,0)	00	_	_
1	(0, 1)	01	0	0
X	(1,0)	10	1	2
X+1	(1, 1)	11	2	1

Für n=4 können wir zunächst wie bereits bekannt die Elemente des Körpers  $GF(2^4)$  in einer  $\overline{q(X)=X^3+X+1}$ Tabelle notieren.

Polynom	Tupel	Binär	Exponent von X
0	(0,0,0,0)	0000	_
1	(0,0,0,1)	0001	0
X	(0,0,1,0)	0010	1
X + 1	(0,0,1,1)	0011	4
X <sup>2</sup>	(0, 1, 0, 0)	0100	2
$X^2 + 1$	(0, 1, 0, 1)	0101	8
$X^2 + X$	(0, 1, 1, 0)	0110	5
$X^2 + X + 1$	(0, 1, 1, 1)	0111	
X <sup>3</sup>	(1,0,0,0)	1000	3
$X^3 + 1$	(1,0,0,1)	1001	
$X^3 + X$	(1,0,1,0)	1010	9
$X^3 + X + 1$	(1,0,1,1)	1011	
$X^3 + X^2$	(1, 1, 0, 0)	1100	
$X^3 + X^2 + 1$	(1, 1, 0, 1)	1101	
$X^3 + X^2 + X$	(1, 1, 1, 0)	1110	
$X^3 + X^2 + X + 1$	(1, 1, 1, 1)	1111	

# GF(23):

Polynom	Tupel	Binär	Exponent von X
0	(0,0,0)	000	_
1	(0,0,1)	001	0
X	(0, 1, 0)	010	1
X+1	(0, 1, 1)	011	3

	$X^2$	(1,0,0)	100	2
	$X^2 + 1$	(1,0,1)	101	6
	$X^2 + X$	(1, 1, 0)	110	4
Г	$X^2 + X + 1$	(1, 1, 1)	111	5

Für die Addition in  $GF(2^3)$  gilt beispielsweise

$$(0,1,1) + (1,0,1) = (0+1,1+0,1+1) \equiv (1,1,0) \mod 2$$
  
 $\Leftrightarrow (X+1) + (X^2+1) = X^2 + X + 2 \equiv X^2 + X \mod 2$   
 $011 \ XOR \ 101 = 110$ 

