HOCHSCHULE ESSLINGEN

Sommersemester 22	Zahl der Blätter: 8 Blatt 1 von 8
Studiengang: SWB: Dozent: 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 $a, b \in \{1,2, \dots ,9\}$
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.

Aufgabe 2 (7 Punkte)

Gegeben sei die Kongruenz

$$4x \equiv 6 \; mod \; 122$$

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

Ansatz:

↳ lineare Kongruenz $ax \equiv b$ lösbar, wenn der größte gemeinsame Teiler von a und m auch b teilt. → mathematisch ausgedrückt $ggT(a,m) \mid b$

↳ bei $\underbrace{4}_{a}x \equiv \underbrace{6}_{b}$ mod $\underbrace{122}_{m}$ muss $ggT(122,4)$ gefunden werden

① schauen ob Kongruenz lösbar mit einfachem Euklidischen Algorithmus:

→ $ggT(4, 122) = 122 \% 4 = 2$ ← immer 1 über 0 ggT also 2

$4 \% 2 = 0$

(2 teilt auch 6, da $6 : 2 = 3$)

↳ $ggT(4, 122) = 2 \mid 6$, also Kongruenz lösbar

② berechnen einer Lösung mit erweitertem Euklidischen Algorithmus:

↳ man sucht nun das inverse zu a und m, also das inverse zu 4 mod 122

größere Zahl steht immer vorne!! Ansonsten erw. Eukl. Alg. falsch!

→ $\boxed{ggT(4,122) = 122 \cdot s + 4 \cdot t}$ ← das ist das inverse zu 4 mod 122, also äquivalent zu $ggT(4,122)$

→ Tabelle aufstellen:

i	$r_i = r_{i-2} \% r_{i-1}$	$q_{i-1} = \frac{r_{i-2} - r_i}{r_{i-1}}$	$s_i = s_{i-2} - q_{i-1} \cdot s_{i-1}$	$t_i = t_{i-2} - q_{i-1} \cdot t_{i-1}$
0	$r_0 = 122$	$q_0 = 0$	$s_0 = 1$	$t_0 = 0$
1	$r_1 = 4$	$q_1 = \frac{122-2}{4} = 30$	$s_1 = 0$	$t_1 = 1$
2	$r_2 = 122 \% 4 = 2$	$q_2 = \frac{4-0}{2} = 2$	$s_2 = 1 - 30 \cdot 0 = 1$	$t_2 = 0 - 30 \cdot 1 = -30$
3	$r_3 = 4 \% 2 = 0$	—	—	—

Standard-Werte →

Zeile über 0 wird alles abgelesen →

↳ $ggT(122,4) = 122 \cdot 1 + 4 \cdot (-30) = 2$ ← -30 ist inverses zu 4 mod 122

↳ das ist das eigentlich gesuchte, da man das inverse zu a sucht was b also ·6 ergibt

③ X ausrechnen:

Formel:

inverses t = -30 mit b = 6 multiplizieren

$$\boxed{x = \frac{bt}{ggT(a,m)} = \frac{6 \cdot (-30)}{2} \equiv -90 \text{ mod } 122 \equiv 32 \text{ mod } 122}$$ ← x von $ax \equiv b$ mod m

geteilt durch $ggT(122,4) = 2$ rechnen   mod 122, wenn negative Zahl

④ Probe x = 32 einsetzen:

$4 \cdot 32 = 128 \equiv 6$ mod 122 ✓

Aufgabe 3 (8 Punkte)

Berechnen Sie die Prüfsumme XY für die IBAN

$$DEXY\ 1001\ 0000\ 1000\ 0000\ 01$$

Hinweis, falls Sie auf einen TR verzichten, nutzen Sie im Skript 5.2.3 und die Ergebnisse

$$3^7 \equiv 53\ mod\ 97, 3^{10} \equiv -24\ mod\ 97, 3^{11} \equiv 25\ mod\ 97$$

Ansatz:

① verschieben erste vier Zahlen ans Ende:

$D = 4 + 9 = 13$
$E = 5 + 9 = 14$

XY

$a_{23} \rightarrow$	1	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	1	1	3	1	4	0	0	$\leftarrow a_0$
$a_n \rightarrow$	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	
	11		10		9		8		7		6		5		4		3		2		1		0		

② ↳ Die IBAN nun in Formel packen:

> Wegen $10^2 = 100 \equiv 3\ mod\ 97$ geht diese Kongruenz über in
> $I \equiv 3^{11}(10a_{23} + a_{22}) + 3^{10}(10a_{21} + a_{20}) + \cdots + 3^1(10a_3 + a_2) + (10a_1 + a_2)$

← einfach farbig markierte hier einsetzen

$$I \equiv 3^{11} \cdot (10 \cdot 1 + 0) + 3^{10}(10 \cdot 0 + 1) + 3^9(10 \cdot 0 + 0) + 3^8(10 \cdot 0 + 0)$$
$$+ 3^7(10 \cdot 1 + 0) + 3^6(10 \cdot 0 + 0) + 3^5(10 \cdot 0 + 0)$$
$$+ 3^4(10 \cdot 0 + 0) + 3^3(10 \cdot 0 + 1) + 3^2(10 \cdot 1 + 3)$$
$$+ 3^1(10 \cdot 1 + 4) + 3^0(10 \cdot 0 + 0)$$
$$\equiv 3^{11} \cdot 10 + 3^{10} + 3^7 \cdot 10 + 3^3 + 3^2 \cdot 13 + 3 \cdot 14$$
$$\equiv 250 - 24 + 530 + 27 + 117 + 42 \quad mod\ 97$$
$$\equiv 1771470 + 59049 + 21870 + 27 + 117 + 42 \quad mod\ 97$$
$$\equiv 1852575 \quad mod\ 97$$
$$= 69 \quad mod\ 97$$

③ Restwert 69 abziehen:

$XY = 97 - (69 - 1) = 29$ ← (man könnte auch einfach $98 - 69$ schreiben ist das gleiche)

↳ IBAN lautet somit: DE29 1001 0000 1000 0000 01

Sommersemester 22	

Prüfungsfach: Diskrete Mathematik

alle Primzahlen 0 bis 100:

2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59
61	67	71	73	79	83	89	97	101	103	107	109	113	127	131	137	139
149	151	157	163	167	173	179	181	191	193	197	199	211	223	227	229	233
239	241	251	257	263	269	271	277	281	283	293	307	311	313	317	331	337
347	349	353	359	367	373	379	383	389	397	401	409	419	421	431	433	439
443	449	457	461	463	467	479	487	491	499	503	509	521	523	541	547	557
563	569	571	577	587	593	599	601	607	613	617	619	631	641	643	647	653
659	661	673	677	683	691	701	709	719	727	733	739	743	751	757	761	769
773	787	797	809	811	821	823	827	829	839	853	857	859	863	877	881	883
887	907	911	919	929	937	941	947	953	967	971	977	983	991	997		

Aufgabe 4 (7 Punkte)

Berechnen Sie $\varphi(20570)$

Hinweis: Bekannte Teilbarkeitsregeln

Ansatz:

↳ Primfaktorzerlegung:

① 20570 in Primfaktoren zerlegen:

$\to 20570 = 2 \cdot 10285$

$= 2 \cdot 5 \cdot 2057$

$= 2 \cdot 5 \cdot 11 \cdot 187$

$= 2 \cdot 5 \cdot 11 \cdot 17 \cdot 11$

$= 2 \cdot 5 \cdot 11^2 \cdot 17$

② $\varphi(20570)$ durch φ(Primfaktoren) berechnen:

grundsätzlich gilt: $\varphi(p^k) = p^k - p^{k-1} = 11^2 - 11^{2-1} = 11^2 - 11^1$

$\varphi(20570) = \varphi(2) \cdot \varphi(5) \cdot \varphi(11^2) \cdot \varphi(17)$

$= 1 \cdot 4 \cdot (11^2 - 11^1) \cdot 16$

$= 1 \cdot 4 \cdot 110 \cdot 16$

$= 7040$ ← (nicht gefragt aber das wäre Anzahl der teilerfremden)

Aufgabe 5 (8 Punkte)

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

① $\varphi(p)$ also $\varphi(37)$:

↳ $\varphi(37) = 36$

② Anzahl primitiver Wurzeln:

$\varphi(p-1) = \varphi(36) = \varphi(2^2) \cdot \varphi(3^2) = (2^2 - 2) \cdot (3^2 - 3) = 2 \cdot 6 = 12$

③ Anzahl Teiler d von Ordnung 36 herausfinden:

$36 = 2^2 \cdot 3^2 = (2+1) \cdot (2+1) = 9$

$d = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$

④ testen mit beliebiger Primzahl $r < 37$:

$r = 2$ wählen:

↳ $2^1 \mod 37 \equiv 2$

$2^2 \mod 37 \equiv 4$

$2^3 \mod 37 \equiv 8$

$2^4 \mod 37 \equiv 16$

$2^6 \mod 37 \equiv 27$

$2^9 \mod 37 \equiv 31$

$2^{12} \mod 37 \equiv 26$

$2^{18} \mod 37 \equiv 36 \equiv -1$

$r^d \not\equiv 1 \mod p$, es darf also nie 1 rauskommen, da nur bei höchster Ordnung 1 rauskommen kann

$2^{(18)2} \mod 37 \equiv (-1)^2 \mod 37$

$2^{36} \mod 37 \equiv 1 \mod 37$

bei höchster Ordnung also $2^{36} \equiv 1 \mod p$ passt, da nur bei höchster Ordnung 1 rauskommen darf

↳ also ist $r = 2$ ein primitives Element gefunden

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 $d \not\equiv e \bmod \varphi(pq)$ ist.

① berechnen $n = p \cdot q = 17 \cdot 41 = 697$

② berechnen $\varphi(697)$:

einfach gegebene Primzahlen!

↳ $\varphi(697) = \varphi(17) \cdot \varphi(41)$
$= 16 \cdot 40$
$= 640$

③ Primzahl e finden, teilerfremd zu $\varphi(p,q)$, also teilerfremd zu 640:

↳ $ggT(e, \varphi(p,q)) = 1$, denn teilerfremd

d da de!

→ Trick: einfach $\boxed{640 : d \text{ schauen bei welcher Primzahl Rest vorhanden}}$

↳ Rest bei $d = 41$ ← es wäre auch 3 gegangen, aber dann dauert Rechnung länger

④ multiplikatives Inverse für $d = 41$ finden mit erweitertem Euklidischen Algorithmus:

↳ allg. Form für multiplikatives Inverses bei RSA:

$\boxed{e\,d \equiv 1 \bmod \varphi(n)}$

$41e \equiv 1 \bmod 640$

erweiterter Euklidischer Algorithmus:

i	$r = r_{i-2} \% r_{i-1}$	$q_{i-1} = \frac{r_{i-2} - r_i}{r_{i-1}}$	$s_i = s_{i-2} - q_{i-1} \cdot s_{i-1}$	$t_i = t_{i-2} - q_{i-1} \cdot t_{i-1}$
0	$r_0 = 640$	$q_0 = 0$	$s_0 = 1$	$t_0 = 0$
1	$r_1 = 41$	$q_1 = \frac{640-25}{41} = 15$	$s_1 = 0$	$t_1 = 1$
2	$r_2 = 640 \% 41 = 25$	$q_2 = \frac{41-16}{25} = 1$	$s_2 = 1 - 15 \cdot 0 = 1$	$t_2 = 0 - 15 \cdot 1 = -15$
	$r_3 = 41 \% 25 = 16$	$q_3 = \frac{25-9}{16} = 1$	$s_3 = 0 - 1 \cdot 1 = -1$	$t_3 = 1 - 1 \cdot (-15) = 16$
	$r_4 = 25 \% 16 = 9$	$q_4 = \frac{16-7}{9} = 1$	$s_4 = 1 - 1 \cdot (-1) = 2$	$t_4 = -15 - 1 \cdot 16 = -31$
	$r_5 = 16 \% 9 = 7$	$q_5 = \frac{9-2}{7} = 1$	$s_5 = -1 - 1 \cdot 2 = -3$	$t_5 = 16 - 1 \cdot (-31) = 47$
	$r_6 = 9 \% 7 = 2$	$q_6 = \frac{7-1}{2} = 3$	$s_6 = 2 - 1 \cdot (-3) = 5$	$t_6 = -31 - 1 \cdot 47 = -78$
	$r_7 = 7 \% 2 = 1$	—	$s_7 = -3 - 3 \cdot 5 = -18$	$t_7 = 47 - 3 \cdot (-78) = 281$
	$r_8 = 2 \% 1 = 0$	—	—	—

↳ folglich gilt: $ggT(640, 41) \equiv 640 \cdot (-18) + 41 \cdot 281 \bmod 640 \equiv 1 \bmod 640$

⑤ Lösung: → $\boxed{\text{Schlüsselpaar: } (d, e) = (41, 281)}$

<u>Aufgabe 7 (8 Punkte)</u>

Wir betrachten das Galois-Feld $GF(2^4)$ und das irreduzible Polynom

$$q(X) := X^4 + X + \bar{1} \in \mathbb{Z}_2[X]$$

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 $ab \bmod q(X)$

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.

Ansatz:

↳ $\boxed{GF(2) = 0,1 \text{ als Koeffizienten}}$

-> $\boxed{GF(2^4)}$ = Polynome vom Grad $4-1=3$ verwenden,

↳ $\boxed{ax^3+bx^2+cx+d}$

1. Tupel a und b in Polynom umrechnen:

$a = (1,0,0,1) = x^3+1$

$b = (0,1,1,0) = x^2+x$

3. a · b und dann mod p(x) rechnen:

$(x^3+1)\cdot(x^2+x) = x^5+x^4+x^2+x \mod x^4+x+1$

$x^5 = x \cdot x^4$

↳ x^4+x+1 kann man nach x^4 umstellen

$= (x \cdot x^4) + x^4 + x^2 + x$

$x^4 = -x-1$ da in mod 2 kann man umdrehen

$x^4 = x+1$

$= x\cdot\underbrace{(x+1)} + \underbrace{(x+1)} + x^2 + x$

x^4 ersetzen mit $x+1$, da dies umgestellt x^4 ist

$= x^2 + x + x + 1 + x^2 + x$

$= 2x^2 + 3x + 1 \mod 2$

$\equiv x+1$

-> $x+1$ umschreiben in Tupel:

↳ $ab = (0,0,1,1)$

Sommersemester 22

Prüfungsfach: Diskrete Mathematik

GF(2^2):

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

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

GF(2^4):

Für $n = 4$ können wir zunächst wie bereits bekannt die Elemente des Körpers $GF(2^4)$ in einer 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^2	$(0,1,0,0)$	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^3	$(1,0,0,0)$	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(2^3):

$q(X) = X^3 + X + 1$

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
X^2+X+1	$(1,1,1)$	111	5

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

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

.

b) das inverse zu a finden:

↳ aus Tabelle weiß man das X erzeugend ist

(1.) -> kleiner Satz von Fermat besagt:

↳ $a^{-1} \equiv \boxed{a^{p-2}}$ ← man verwendet nur das hier zum rechnen

das ist einfach nur Standarddarstellung für inverses und unwichtig

↳ $X^{2^4-2} = X^{16-2} = X^{14}$

(2) Rechnieren mit mod P (also irreduzibles Polynom):

man weiß, dass X erzeuger von allen Polynomen

$X^{14} \equiv X^4 \cdot X^4 \cdot X^4 \cdot X^2 \mod X^4 + X + 1$

man muss zuerst die kleinen ausrechnen

$\equiv (X+1)^3 \cdot X^2$

$\equiv (X^2+2X+1)\cdot(X+1)\cdot X^2 \mod 2$

$\equiv (X^2+1)\cdot(X+1)\cdot X^2$

$\equiv (X^3+X+X^2+1)\cdot X^2$

$= X^5 + X^4 + X^3 + X^2$

$\equiv X\cdot(X+1) + X + 1 + X^3 + X^2$

$\equiv X^2 + X + X + 1 + X^3 + X^2$

$\equiv X^3 + 2X^2 + 2X + 1$

$= X^3 + 1$

Kleiner Satz von Fermat:

↳ Für jede Primzahl p und jede ganze Zahl a, die nicht durch p teilbar ist gilt:

$a^{p-1} \equiv 1 \mod p$

-> kann angewendet werden für das inverse: Inverse von a mod p ist b sodass gilt

↳ $a \cdot b \equiv 1 \mod p$

-> Durch anwenden kleiner Satz von Fermat kann man erkennen dass

↳ $\boxed{a \cdot a^{-1} = a \cdot a^{p-2} \equiv a^{p-1} \equiv 1 \mod p}$

↳ a^{p-1} ist das inverse von a mod p solange a und p teilerfremd

-> man kann sich merken für das inverse rechnet man einfach a^{p-2} aus!!

-> inverse $a^{-1} = a^{p-2}$ ganz einfach!

↳ a^{p-2} am einfachsten!