

HOCHSCHULE ESSLINGEN

Wintersemester 22/23	Zahl der Blätter: 10 Blatt 1 von 10
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)

Welche Primzahlen p sind von der Form $p = n^3 + 1$ mit $n \in \mathbb{N}$

Hinweis: Es ist $n^3 + 1 = (n+1)(n^2 - n + 1)$ und $0 \notin \mathbb{N}$

↳ Zum Verständnis: Primzahl zahl > 1 und nur 2 Teiler (1 und sich selbst)

mit dem Hinweis gilt:

$$p = (n+1)(n^2 - n + 1) \leftarrow \text{einfach aussehen von } n^3 + 1$$

Es gilt: Primzahl nur durch 1 und sich selbst teilbar

↳ Betrachtung der Faktoren:

$(n+1) \underbrace{(n^2 - n + 1)}$ einer der Faktoren muss 1 sein und einer die Zahl selbst

Fall 1:

$$n+1 = 1 \mid -1$$

↳ $n=0$ müsste rechnen dann dieser Faktor 1 sein könnte, dies ist aber nicht möglich, da 0 nicht Teil der natürlichen Zahlen ist in diesem Fall

$$\text{Fall 2: } n^2 - n + 1 = 1 \mid -1$$

$$\rightarrow n^2 - n = 0 \quad n_1 = 1, n_2 = 0,$$

$\rightarrow n=0$ ist auch nicht möglich

\rightarrow kann also nur $n=1$ möglich sein

\rightarrow einsetzen von $n=1$ in ursprüngliche Gleichung:

$$\rightarrow p = 1^3 + 1 = 2 \text{ kann nur die gewünschte Form besitzen}$$

Aufgabe 2 (7 Punkte)

Zeigen Sie mit Hilfe einer Wahrheitstafel, dass der logische Ausdruck

$$[(p \Rightarrow q) \wedge \neg q] \Rightarrow \neg p$$

für alle Wahrheitswerte von p und q wahr, also eine Tautologie ist.

Erklärung zu Symbolen:

Beide Ausdrücke müssen gleichzeitig wahr sein

$$[(p \Rightarrow q) \wedge \neg q] \Rightarrow \neg p$$

q ist wahr nicht q
wenn p wahr

\neg = negation, also Gegenteil einer Aussage

wenn z.B. p wahr ist dann ist $\neg p$ falsch

\Rightarrow = "impliziert" oder "wenn ... dann ..."

wenn der gesuchte
Vorlesungsausdruck wahr
ist, dann muss
auch das Gegenteil
von p also $\neg p$
wahr sein

wird als Versprechen gegeben, also p verspricht

wahr zu sein, dann muss q auch wahr
sein. Wenn p falsch ist wurde vorzugsweise

nichts versprochen und q ist egal ob wahr/falsch:

$p \Rightarrow q$: wahr falsch

$W \rightarrow W$

$W \rightarrow F$

$F \rightarrow W$

↑

$F \rightarrow F$

einiger Fall der Falsch ist!

eigentliche Aufgabe: Tabelle erstellen mit allen Möglichkeiten

(

p	q	$p \Rightarrow q$	$\neg q$	$(p \Rightarrow q) \wedge \neg q$	$\neg p$	$[(p \Rightarrow q) \wedge \neg q] \Rightarrow \neg p$
0	0	1	1	1	1	1
0	1	1	0	0	1	1
1	1	1	0	0	0	1
1	0	0	1	0	0	1

$\neg q$ ist einfach
immer wahr wenn
 q falsch ist

hier einfach vergessen
wenn beide
Bedingungen wahr
sind

Es wurde nur einmal ein
Versprechen gegeben, wel dort
waren beide Bedingungen wahr,
wenn kein Versprechen gegeben
automatisch wahr.

Wintersemester 22/23	Blatt 3 von 10
Prüfungsfach: Diskrete Mathematik	Prüfungsnummer: 1052034

Aufgabe 3 (8 Punkte)

Zerlegen Sie mit dem Faktorisierungsverfahren von Fermat die Zahl $n = 40991$ in zwei nichttriviale Faktoren.

Hinweis: $\lceil \sqrt{n} \rceil = 203 \leftarrow = a$

Was ist Faktorisierungsverfahren von Fermat?

↳ Faktorisierungsverfahren von Fermat ist eine Methode zur Zerlegung einer ungeraden Zahl in zwei Faktoren.

→ beruht auf: $n = a^2 - b^2 \leftarrow n$ (ungerade Zahl) = Differenz von zwei Quadraten

↳ lässt sich umformen zu: $n = (a+b)(a-b)$

Ziel:

→ mit vorgegebenem n (40991) und a (203) solange a erhöhen +1 bis man b findet, von dem man Wurzel ziehen kann $\rightarrow b^2 = a^2 - n$

① Startpunkt festlegen:

↳ Hinweis beacht! $\lceil \sqrt{n} \rceil \approx 203 \rightarrow \lceil \sqrt{40991} \rceil \approx 203$

, also starten mit $a = 203$

② passendes b finden indem:

↳ $b^2 = a^2 - n \leftarrow 203^2 - n$, also gerade Zahl

mit 203+1 verändern solange bis passt
 $b^2 = 203^2 - 40991 = 41209 - 40991 = 218 \leftarrow 218 \neq$ passendes Quadrat, es wurde kein passendes Quadrat gefunden, deshalb mit 204 versuchen!

$$b^2 = 41616 - 40991 = 625 \quad |T$$

$b = 25$ → nun passendes b gefunden, welches quadratisch werden kann

③ aufstellen der Gleichung:

$$\lceil \text{somit } \lceil n = 204^2 - 25^2 = (204+25)(204-25) = 229 \cdot 179 \rceil \rceil$$

eine nicht triviale Zerlegung von $n = 40991$

(nicht triviale Zerlegung bedeutet, dass n in zwei Faktoren zerlegt wird, die beide >1 sind.)

Aufgabe 4 (7 Punkte)

Lösen Sie die simultanen Kongruenzen mit dem Chinesischen Restsatz.

$$\begin{aligned} x &\equiv 2 \pmod{\frac{17}{m_1}} \\ x &\equiv 4 \pmod{\frac{15}{m_2}} \end{aligned}$$

Ansatz:

① bestimmen der Moduli-Produkte: ← immer bei chinesischem Restsatz wenn moduli prim sind

$$N = 17 \cdot 15 \leftarrow \text{da ja } 17 \text{ und } 15 \text{ produkt aus beiden}$$

$$\approx 255$$

$$\text{ggT}(17, 15) : 17 \% 15 = 2$$

$$15 \% 2 = 1$$

$$2 \% 1 = 0$$

② Multiplikativer Inverses berechnen:

$$\text{ggT}(17, 15) = 17 : 15 = 1 \text{ Rest } 2 \quad \text{3-euklidischer Algorithmus}$$

$$\begin{array}{rcl} 15 : 2 & = & 7 \text{ Rest } 1 \\ 2 : 1 & = & 2 \text{ Rest } 0 \end{array} \quad \text{ggT immer einsturz Rest 0 also 1}$$

$$\hookrightarrow \text{ggT}(17, 15) = 1$$

$$\hookrightarrow \text{Ziel: } M_1 \text{ finden sodass } \frac{15}{m_2} \cdot M_1 \equiv 1 \pmod{\frac{17}{m_1}} \quad \text{← eigentliche Umarbeit der Aufgabe}$$

$$M_2 \text{ finden sodass } \frac{17}{m_1} \cdot M_2 \equiv 1 \pmod{\frac{15}{m_2}}$$

für M_1 : in Taschenrechner eingeben von 1 bis ... für M_1

$$\hookrightarrow 15 \cdot 8 \div R 17 \leftarrow \text{so Eingabe in Taschenrechner}$$

$$\hookrightarrow \text{d.h. } M_1 = 8$$

$$\text{für } M_2 = 8$$

↪ einsetzen in Formel:

$$\text{allg. Formel: } x = \frac{a_1 \cdot m_2}{m_2} \cdot x_1 + \frac{a_2 \cdot m_1}{m_1} \cdot x_2 \quad \left(\begin{array}{l} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{array} \right)$$

$$\hookrightarrow x = 2 \cdot \frac{15}{m_2} \cdot 8 + 4 \cdot \frac{17}{m_1} \cdot 8 = 784$$

Aufgabe 5 (8 Punkte)

✓ immer gleiche Formel für Kongruenzgenerator

Gegeben sei der lineare Kongruenzgenerator $x_n \equiv ax_{n-1} + b \pmod{m}$

Für welches Tripel

$$(a, b, m) \in \{(133, 91, 1452), (131, 91, 1452), (66, 39, 1452)\}$$

a b m a b m a b m

wird die Periode maximal?

Bedingungen:1. b und m teilerfremd sein→ wenn $m : h$ nicht teilbar, dann nur $(a-1)$ durch die Primfaktorzerlegungen von m sein↳ wenn $m : h$ teilbar ist, dann nur $(a-1) : h$ teilbar seinAnsatz:① $m = 1452$ Primfaktor zerlegen:

$$\begin{aligned} 1452 &= 2 \cdot 2 \cdot 3 \cdot 61 \\ &= 2 \cdot 2 \cdot 3 \cdot 11 \cdot 11 \\ &= 2^2 \cdot 3 \cdot 11^2 \end{aligned}$$

② Bedingungen testen: $(66, 39, 1452)$ schiedet aus weil $\text{ggT}(39, 1452) = 3$ $(131, 91, 1452)$ kein m ggT mit B aber dafür $a-1$, also 130, kein Teiler von h , obwohl $m = 1452$ Teiler von h hat $(133, 91, 1452)$ erfüllt alle Bedingungen, da $\text{ggT}(91, 1452) = 1$ und $(a-1)$ teilbardurch Primfaktorzerlegung von m also 2, 3, 11

Aufgabe 6 (7 Punkte)

Man zeige, dass in \mathbb{Z}_{23}^\times die Restklasse $\bar{11}$ primitiv ist und bestimme damit die Untergruppe der quadratischen Reste in den Restklassen \mathbb{Z}_{23}

Hinweis: Der Casio-TR versagt bei hohen Potenzen und produziert falsche Ergebnisse. Potenzen nach und nach steigern und mit den Resten rechnen oder gleich händisch.

Aufgabe: man soll zeigen, dass $\bar{11}$ in \mathbb{Z}_{23}^\times primitiv ist

Ansatz:

Sei r Zahl g bei der Man findet ob primitiv Element also hier $r=11$

$k = \text{alle Potenzen von } 1 \text{ bis } p-1, k \neq 1$

$k = \text{alle Teiler } d \text{ von } 22 \text{ aber } k \neq 22$

also $\varphi(p) = p-1 = 22$

① $\varphi(p)$ herleiten:

$$p=23 \rightarrow \varphi(p-1) = 22$$

② maximale lokale Ordnung und Teiler d herleiten von φ :

$$d = \{1, 2, 11, 22\} \rightarrow 11 \text{ ist fächerende Zahl von } p$$

③ mit teilnehmenden Zahl $\bar{11}$ alle Exponenten d testen ob $\bar{11}^d \equiv 1 \pmod{23}$:

$$\bar{11}^1 \equiv \bar{11} \pmod{23}$$

$$\bar{11}^2 \equiv 6 \pmod{23}$$

$$\bar{11}^3 \equiv \bar{11}^1 \cdot \bar{11}^2 \pmod{23} \equiv 9 \cdot 5 \equiv 22 \pmod{23}$$

$$\bar{11}^{11} \equiv -1 \pmod{23}$$

$$\bar{11}^{11 \cdot 2} \equiv (-1)^2 \pmod{23}$$

$$\bar{11}^{22} \equiv 1 \pmod{23}$$

\hookrightarrow somit bewiesen, dass $\bar{11}$ primitiv Element, da Satz von Fermat sagt, dass
 $\bar{11}^k \equiv 1 \pmod{23}$ für k teiler von $\varphi(23)=22$ ist und $k < \varphi(23)$ sein muss
 primitiv Element, wenn $\bar{11}^k \not\equiv 1 \pmod{23}$ ist wobei $k < \varphi(23)$

\rightarrow Rundnotiz: wenn z.B. $d=2, 4, 6, 8$, dann obwohl $6^2 \equiv 2 \pmod{7}$ auch $6^4, 6^6, 6^8$ möglich
 \downarrow kann übernommen werden dann einfach 2 potenzieren
 ohne zu testen, da vielfache von 2 , also $(6^2)^3 \equiv 6^6 \pmod{7} \equiv 2^3 \pmod{7}$

④ Gruppe der quadratischen Reste:

$$\rightarrow Q = \{\bar{11}^{2m} \mid m = 1, 2, \dots, 11\}$$

\hookrightarrow quadratische Rest nur bis $\bar{11}$, da $(\bar{11}^2)^m = \bar{11}^{22}$ ist und $\varphi=22$ ist, höher als $\bar{11}$ und p
 übertreffen, deshalb nur bis $\bar{11}$.

Allgemeiner Ansatz: ① = Primzahlteileren ② = restlichen für andere Zahlen

① wann muss $\varphi(p)$ herausfinden (Teilerfreunde Zahlen):

② \rightarrow bei Primzahlen φ einfach $p-1$, bei anderen Zahlen Teilerfreunde durch Primfaktorzerlegung

③ \rightarrow allgemein Teilerfreund wenn $\text{ggT}(g, p) = 1$, also ggT 1, dann teilerfrei

\hookrightarrow die Teilerfreunden sind die Restklassen welche man erhalten will z.B. $\varphi(10) = \{1, 3, 7, 9\}$

② maximal höchste Ordnung und zu testende Ordnungen verbinden: \hookrightarrow diese will man g^d erhalten, also nicht alle von 1-S, wie es bei Primzahlen der Fall wäre

③ \rightarrow maximal höchste Ordnung ist bei Primzahlen immer $\varphi(p) = p-1$

\rightarrow man sucht Teiler d von p als Potenz, somit kann man später nicht alle Ordnungen testen \rightarrow Teiler d von $\varphi(p-1)$ findet man durch Primfaktorzerlegung her

④ \rightarrow maximal höchste Ordnung ist bei nicht primzahlen nicht immer $\varphi(m)$

\rightarrow als $\varphi(8) = \varphi(2) \cdot \varphi(4) = \varphi(2)^3 = 2^3 - 2^1 = 4$, \rightarrow allg. Regel: $\varphi(p^k) = p^k - p^{k-1}$ also höchste Potenz von 1-4

$\rightarrow \varphi(16) = \varphi(2) \cdot \varphi(8) = 1 \cdot 4 = 4$, \rightarrow höchste Potenz 4

\hookrightarrow p rückt von 1-p also alle p als Potenz ausprobieren,

③ mit beliebiger teilerfreudner Zahl testen ob $g^p \not\equiv 1 \pmod{p}$: bei Primzahlen alle d, die teiler von p ausprobieren

④ \rightarrow bei Primzahlen meistens mit den Teilerfreunden 2, 3, 5 als g für $g^d \not\equiv 1 \pmod{p}$ versuchen

\hookrightarrow hoch d=1 trivial, da immer 1, hoch d=2 trivial, da immer Zahl selbst vorsteht hier p ist prim

\rightarrow rest d durchteilen z.B. $7^3 \equiv 1 \pmod{37}$ nicht möglich, da Rest 1

\rightarrow also die Teilerfreuden hoch d potenzieren (d ist Teiler von p also bei $p=37 \rightarrow \varphi(37) = p-1 = 36$)

⑤ \rightarrow bei nicht primzahlen zuvor bestimmte Teilerfreunde ob $g^p \not\equiv 1 \pmod{m}$ potenzieren

\hookrightarrow m ist die zu prüfende Zahl

\rightarrow z.B. bei 8 $\rightarrow 1, 3, 5, 7$ potenzieren mit φ, φ reicht von 1-4, da $\varphi(8) = 4$ teilerfrei

$\rightarrow 1^2 = 1 \pmod{8}, 3^2 = 1 \pmod{8}, 5^2 = 1 \pmod{8}, 7^2 = 1 \pmod{8}$

\hookrightarrow in 8 gibt es hier sozusagen keine primiven Elemente!

$\varphi(p)$ Bedeutung: Anzahl der Teilerfreunden!

Satz von Gauß:

\rightarrow Kriterium dafür ob gegebene Zahl primitive Wurzel modulo einer Primzahl ist oder nicht

\rightarrow Für Primzahl p und Zahl g, die zu p teilerfrei ist, ist g eine primitive Wurzel modulo

\hookrightarrow deswegen wird Tabelle angebracht \hookrightarrow einfache andere Darstellung für d, also teilerfrei

p, wenn für jeden Teiler d von $p-1$ die Kongruenz $g^{(p-1)/d} \not\equiv 1 \pmod{p}$ gilt

\rightarrow Das heißt g ist eine primitive Wurzel mod p, wenn keine Potenz von g

(mit Exponent der ein echter Teiler von p-1 ist) kongruent zu 1 modulo p ist

\rightarrow um zu prüfen ob Zahl g eine primitive Wurzel mod p ist, muss man

prüfen ob für jeden Teiler d von p-1 die Bedingung $g^{(p-1)/d} \not\equiv 1 \pmod{p}$

Begriffserklärung:

a^{-1} nur darstellung es ist nicht wirklich z.B. -5^{-1} sondern irgend eine Zahl, welche man durch geeigneten Euclidischen Algorithmus berechnet!

\rightarrow multipikativer Inverses: einfach etwas a^{-1} , dass multipliziert mit Zahl a $a \cdot a^{-1} = 1 \text{ mod } n$ ergibt

\rightarrow m und p: p ist häufig Primzahl

\rightarrow quadratischer Rest: Zahl a ist ein quadratischer Rest modulo n , wenn es Zahl x gibt, sodass $x^2 \equiv a \text{ mod } n$, dies bedeutet dann a Quadrat einer Zahl modulo n ist.

\rightarrow Primzahl p und p-1: 1 bis $p-1$ sind alle Zahlen die teilerfremd zu p sind, da p ja Primzahl, diese bilden eine Gruppe unter der Multiplikation modulo p .

\rightarrow Teiler d von p-1: Jeder Teiler d von $p-1$ hat eine spezielle Bedeutung. Wenn $p-1$ durch d teilbar ist, dann gilt es bestimmte Eigenheiten und Muster, die in der Gruppe der Zahlen modulo p beobachtet werden können.

\rightarrow Exponent d: Exponent d Zahl, die gilt, dass $a^d \equiv 1 \text{ mod } p$ für jede Zahl a , die zu p teilerfremd ist. Natürlich für primitive Wurzel

\rightarrow primitive Restklassen: Menge aller zu n teilerfreien Zahlen, modifiziert durch n . Sie bilden eine Gruppe unter der Multiplikation modulo n . Wenn n eine Primzahl ist, dann sind alle Zahlen von 1 bis $n-1$ primitive Restklassen modulo n .

\rightarrow primitive Wurzel: primitive Wurzel modulo n ist Zahl, deren Potenzen modulo n jede Zahl erzeugen, die zu n teilerfremd ist. Wenn g eine primitive Wurzel modulo n ist, dann kann man jede zu n teilerfremde Zahl als $g^k \text{ mod } n$ für k darstellen

\rightarrow man will die primitive Wurzel g einer Primzahl p haben, da durch potenzieren von g alle Restklassen (von 1 bis $p-1$, mod p) erzeugen kann

$\rightarrow g^1 \text{ mod } p, g^2 \text{ mod } p, \dots, g^{p-1} \text{ mod } p \rightarrow$ jede Zahl von 1 bis $p-1$ kommt einmal als Restklasse!

\rightarrow Bsp: Wenn Primzahl $p=7$ und wir herausfinden, dass die primitive Wurzel $g=3$ ist, dann bedeutet das, dass die Potenzen von 3 mod 7 alle Zahlen von 1 bis 6 erzeugen.

Exponent spiegelt hier nicht $\rightarrow 3^1 \equiv 3 \text{ mod } 7$

Teiler d wieder!

$$3^2 \equiv 9 \equiv 2 \text{ mod } 7$$

$$3^3 \equiv 27 \equiv 6 \text{ mod } 7$$

$$3^4 \equiv 81 \equiv 4 \text{ mod } 7$$

$$3^5 \equiv 243 \equiv 5 \text{ mod } 7$$

$$3^6 \equiv 729 \equiv 1 \text{ mod } 7$$

Ring:

- algebraische Struktur, die aus Menge von Elementen besteht, zusammen mit zwei Operationen die üblicherweise als Addition und Multiplikation bezeichnet werden. Operationen müssen bestimmte Eigenschaften erfüllen, wie Assoziativität, das vorhandensein eines additiven neutralen Elements ("null" Element) und vorhandensein eines additiven inversen Elements für jedes Element im Ring.
- im Kontext primärer Restklassen oft ein Ring der ganzen Zahlen modulo n bezeichnet mit \mathbb{Z}_n , dieser Ring besteht aus den Restklassen bezüglich der Division durch n .
- Elemente des Rings: Elemente von \mathbb{Z}_n sind Restklassen $0, 1, 2, \dots, n-1$
- Operationen: Addition, Multiplikation, jeweils mod n . W.l.o.g. wenn man zwei Zahlen in dem Ring Ring addieren oder multiplizieren diese mod n nehmen

→ Bsp: \mathbb{Z}_{23}^{\times}

- \mathbb{Z}_{23} : Ring der ganzen Zahlen mod 23, Elemente des Rings sind die Restklassen von Zahlen wenn sie durch 23 geteilt werden, also mod 23.
→ Also Elemente 0 - 22
→ Addition, Subtraktion, Multiplikation mod 23 ausreicht
- \mathbb{Z}_{23}^{\times} : \times wird verwendet um die multiplikative Gruppe eines Rings zu bezeichnen
In diesem Fall bezieht sich Gruppe der zu 23 teilerfremden Zahlen innerhalb von \mathbb{Z}_{23}
Da 23 eine Primzahl ist, sind alle Zahlen von 1 bis 22 teilerfremd zu 23.
Also ist \mathbb{Z}_{23}^{\times} die Menge $\{1, 2, 3, \dots, 22\}$

→ Jedes Element hat multiplikatives Inverses. Für jedes Element a in \mathbb{Z}_{23}^{\times} gibt es b in \mathbb{Z}_{23}^{\times} , sodass $a \cdot b = 1 \pmod{23}$

Hinweis:

$$\begin{aligned} p &= 13 & f(13) &= 13 \\ 2^6 &\equiv 12 \pmod{13} \\ 2^6 &\equiv -1 \pmod{13} \\ 2^{12} &\equiv -1^2 \pmod{13} \\ 2^{24} &\equiv 1 \pmod{13} \end{aligned}$$

Wenn frage nach inversem einfach schreif das hier hinschreiben:

Wie lautet nun das Inverse von r ?

→ Einfachste Antwort $r^{-1} = r^{p-2}$ ← falls nach inversem gefragt werden sollte.

→ zweit einfachste Lösung: $r \times x \equiv 1 \pmod{p} \leftarrow p = \text{Primzahl}$
 ↑ r -teilerfremde Zahl

Aufgabe 7 (8 Punkte)

Gegeben seien die Primzahl $p = 59$, die sichere Primzahl $q = \frac{p-1}{2} = 29$ und das primitive Element $g = \overline{14}$ der primen Restklassen \mathbb{Z}_p^\times

Ferner seien Sender-Exponent s und Empfänger-Exponent e gegeben als

$$s \equiv 6 \pmod{q} \quad \text{und} \quad e \equiv 13 \pmod{q}$$

Der Sender möchte nun die Nachricht $m \equiv 5 \pmod{q}$ Elgamal-verschlüsselt an den Empfänger senden.

- Berechnen Sie ein erzeugendes Element h und geben Sie das öffentliche Tripel (h, G, h^e) explizit, d.h., ausgerechnet an.
- Berechnen Sie die Chiffre $c_0 := h^s$ und $c_1 := (h^e)^s m$ und geben Sie das Tupel (c_0, c_1) explizit, d.h., ausgerechnet an.
- Entschlüsseln Sie nun die auf Empfängerseite angekommene Nachricht (c_0, c_1) und zeigen Sie damit die Richtigkeit Ihrer Rechnungen.

Hinweis: Rechnen Sie ohne den Casio-TR oder berechnen Sie zunächst kleine Potenzen \pmod{p} . Der Casio-TR rechnet sonst möglicherweise falsch.

① g definieren:

$$g = \langle \bar{g}^1 \rangle = \langle 14 \rangle = 14^2 \pmod{59} = 19 \pmod{59}$$

Primzahl p

② g^e definieren:

$$g^e = 14^e \pmod{59} = 14^{13} \pmod{59} \equiv 57 \pmod{59} \equiv -2 \pmod{59}$$

Empfänger Exponent

③ G definieren:

$$G = \{14^{2m} \mid m = 1, 2, \dots, \frac{q-1}{2}\}$$

④ öffentliches Tripel:

$$(g, G, g^e) = (14, G, 57)$$

⑤ c_0, c_1 berechnen:

$$c_0 = g^s \pmod{59} = 14^6 \pmod{59} \equiv 48 \pmod{59}$$

Sender Exponent

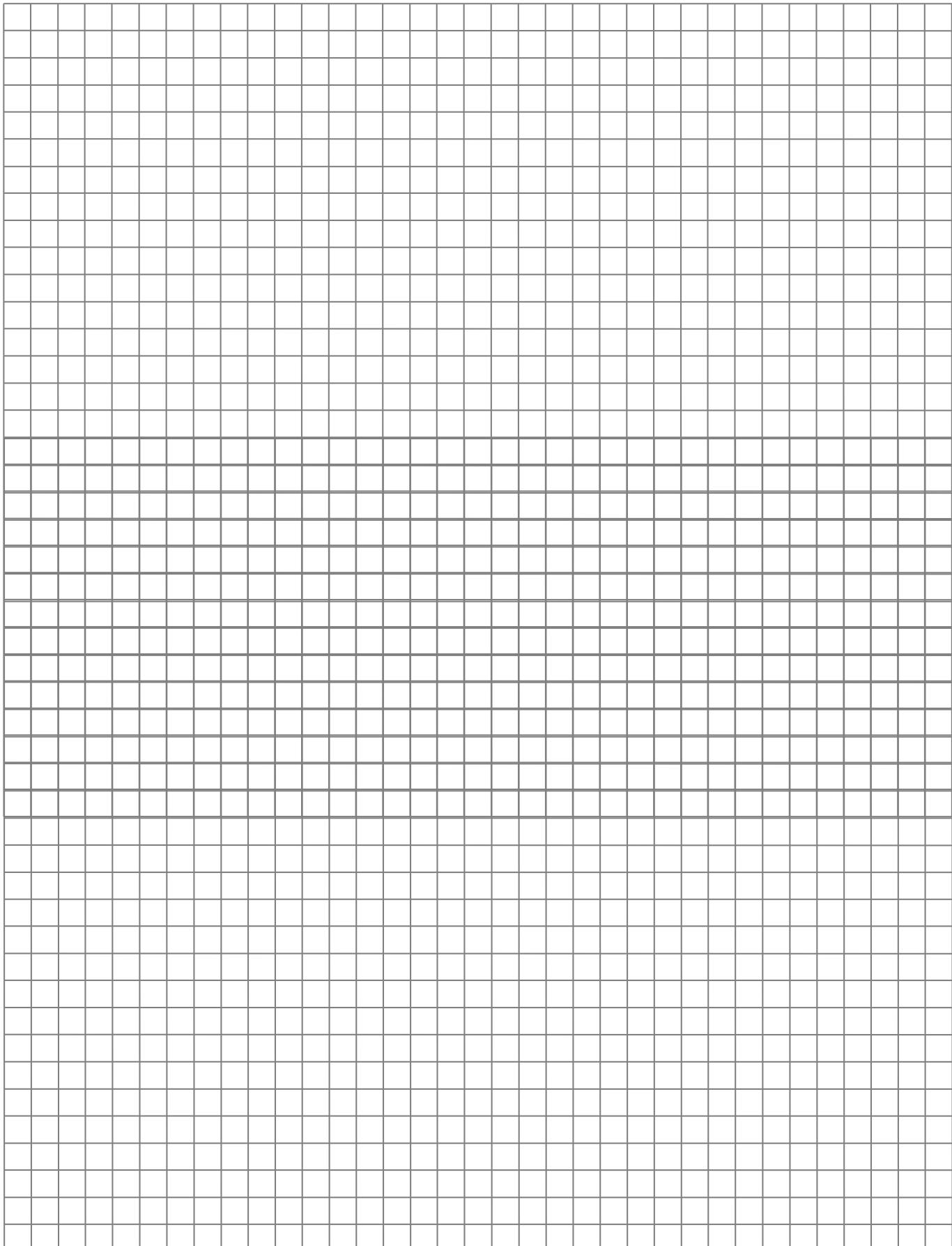
$$c_1 = (g^e)^s \cdot m = 57^6 \cdot 5 \pmod{59} \equiv 25 \pmod{59}$$

$$(c_0, c_1) = (48, 25)$$

⑥ Verifikation:

$$c_0^{q-e} \cdot c_1 = 48^{59-13} \cdot 25 = 48^{46} \cdot 25 \equiv 5 \pmod{59} \rightarrow m=5$$

Wintersemester 22/23	Blatt 8 von 10
Prüfungsfach: Diskrete Mathematik	Prüfungsnummer: 1052034



Aufgabe 8 (7 Punkte)

Wir rechnen im Galois-Feld $GF(2^4)$. Gegeben sei das irreduzible Polynom

$$GF(2^4) \text{ bedeutet einfach } 4 \text{ Bits} \\ i(X) := X^4 + X^3 + 1 \in \mathbb{Z}_2[X]$$

und die Elemente

$$a := (1, 1, 0, 1), b := (0, 1, 1, 1)$$

(umgekehrt zu Polynom $x^4 + x^3 + 0 + x^0$ und $0^4 + x^3 + x^1 + x^0$)

aus dem Körper $GF(2^4)$

Berechnen Sie mit dem Algorithmus der Russischen Bauernmultiplikation das Produkt ab

Hinweis: Die Irreduzibilität von $i(X)$ braucht nicht gezeigt zu werden.

$$i(x) = x^4 + x^3 + 1$$

① $i(x)$ umformen in Binärkode:

$$\begin{array}{r} i = 1 1 0 0 1 \\ \uparrow \uparrow \uparrow \uparrow \uparrow \\ x^4 x^3 x^2 x^1 x^0 \end{array}$$

a	b	q	Kommentare
$\begin{array}{r} 1 1 0 1 \\ \text{deshalb ungerade} \end{array}$	$\begin{array}{r} 0 1 1 1 \\ \text{deshalb ungerade} \end{array}$	$\begin{array}{r} 0 0 0 0 \\ \text{b von oben genommen} \end{array}$	a ungerade → übertragen und schriftlich in vertikale Tabelle
$\begin{array}{r} 1 1 0 \\ \uparrow \uparrow \uparrow \\ \text{bei } a \text{ immer } 0 \text{ einrufen} \end{array}$	$\begin{array}{r} 1 1 1 0 \\ \uparrow \uparrow \uparrow \uparrow \\ \text{bei } b \text{ immer } 0 \text{ einrufen} \end{array}$	$\begin{array}{r} b \oplus q \\ = 0 1 1 1 \oplus 0 0 0 0 \\ = 0 1 1 1 \end{array}$	a gerade → deshalb q unverändert
$\begin{array}{r} 1 1 \\ \uparrow \uparrow \\ GF(2^4) = 8 \text{ aber nur } 4 \text{ Bit lang, deshalb overflow!} \end{array}$	$\begin{array}{r} 1 1 1 0 0 \\ \uparrow \uparrow \uparrow \uparrow \uparrow \\ b \oplus i \\ = 1 1 1 0 0 \\ \oplus 1 1 0 0 1 \\ = 0 0 1 0 1 \end{array}$	$\begin{array}{r} 0 1 1 1 \\ \uparrow \uparrow \uparrow \uparrow \uparrow \\ \text{deshalb überhang und Schrift} \\ \text{in vertikale Tabelle} \end{array}$	a ungerade → deshalb überhang und Schrift in vertikale Tabelle
1	$\begin{array}{r} 1 0 1 0 \\ \uparrow \uparrow \uparrow \uparrow \\ \text{nicht zu tun} \end{array}$	$\begin{array}{r} b \oplus q \\ = 1 0 1 \oplus 0 1 1 1 \\ = 0 1 0 \\ b \oplus q \\ = 1 0 1 0 \oplus 0 1 0 \\ = 1 0 0 0 \end{array}$	$\begin{array}{r} b \oplus i \\ \uparrow \uparrow \uparrow \uparrow \uparrow \\ \text{b überflow, 5 Stk in 4 Bit} \\ \rightarrow b \oplus i \end{array}$
0			a ungerade → überhang Schrift

übertragen:

→ wenn a ungerade: $b \oplus q$

schriften:

→ immer egal ob a ungerade gerade: → 0 von rechts einrufen bei a, 0← bei b

Wintersemester 22/23	Blatt 10 von 10
Prüfungsfach: Diskrete Mathematik	Prüfungsnummer: 1052034

