Rechnen in Restklassenringen mit Anwendungen in der Kryptografie

Bonusvorlesung zum Praktikum Wissenschaftswelt Mathematik 2012

24.4.+8.5.2013, Edith-Stein-Schule, Prof. Dr. Martin Ziegler, FB Mathematik der TU Darmstadt

Definition 1 *Sei $(R,+,\cdot,0,1)$ ein kommutativer Ring.*

i) $r \in R$ *heißt* Nullteiler, *wenn es* $s \in R$ *gibt mit* $s \neq 0$ *aber* $r \cdot s = 0$.
ii) $r \in R$ *heißt* Einheit *von (oder* invertierbar *in) R, wenn es* $s \in R$ *gibt mit* $r \cdot s = 1$. *s ist dann* invers *zu r.* $R^\times$ *bezeichnet die Menge der Einheiten von R.*

Beispiel 2 *i) 0 ist stets Nullteiler.*
ii) Was sind die Nullteiler von $\mathbb{Z}$*?*
iii) Was sind die Einheiten von $\mathbb{Z}$ *?*
iv) Wie sieht es aus bei $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ *?*

Lemma 3 *i) Ein Nullteiler ist keine Einheit.*
ii) Das Produkt zweier Einheiten ist eine Einheit: $(R^\times,\cdot)$ *bildet eine Gruppe.*
iii) Für $a \in R^\times$ *gilt:* $a \cdot x = a \cdot y \;\Rightarrow\; x = y$.
iv) Jedes Ringelement besitzt höchstens ein Inverses.
v) Ist R endlich und $x \in R^\times$*, so ist* $\pi : R \ni r \mapsto x \cdot r \in R$ *eine Permutation.*

Theorem 4 (Euler). *Ist R endlicher kommutativer Ring und* $x \in R^\times$*, so gilt* $x^{|R^\times|} = 1$.

Definition 5 *i) Für ganze Zahlen* a,b *schreibe "*$a|b$*" (gesprochen "a* teilt *b" oder "b ist* Vielfaches *von a") wenn gilt:* $\exists c \in \mathbb{Z} :\; b = a \cdot c$.
ii) r *heißt* Rest bei Division von a durch b *("*$r = a \bmod b$*") wenn gilt* $0 \le r < b$ *und* $\exists c : a = b \cdot c + r$.
iii) $\mathbb{Z}_n := \{0,1,\ldots,n-1\}$ *mit Addition und Multiplikation* $\bmod n$ *heißt* Restklassenring *modulo n.*
iv) $g > 0$ *heißt* größter gemeinsamter Teiler von a und b *("*$g = \mathrm{ggT}(a,b)$*"), wenn*

$$g|a \;\wedge\; g|b \;\wedge\; \big(\forall c :\; c|a \wedge c|b \;\Rightarrow\; c|g\big) \;.$$

Beispiel 6 *i)* $6|7182, \quad 6|7410$
ii) $7182 \bmod 228 = 114$
iii) $5^{16} \bmod 17 = 1$
iv) $3|a_0 + 10\cdot a_1 + 100\cdot a_2 + \cdots + 10^n \cdot a_n \quad\Leftrightarrow\quad 3|a_0 + a_1 + a_2 + \cdots + a_n$
iv) $\mathrm{ggT}(91686,19362) = 42$
v) $6 = \mathrm{ggT}(4812,2430) = 301\cdot 2430 - 152\cdot 4812$

Lemma 7 *i)* $a|b \Rightarrow a\cdot c|b\cdot c$.
ii) $z|x \wedge z|y \Rightarrow z|a\cdot x+b\cdot y$.
iii) Es gilt $(x+y) \bmod z = \big((x \bmod z)+(y \bmod z)\big) \bmod z$
und $(x\cdot y) \bmod z = \big((x \bmod z)\cdot(y \bmod z)\big) \bmod z$.
iv) Für p Primzahl und $k \in \mathbb{N}$ *gilt:* $p \big| \binom{p}{k}$.
v) $\mathrm{ggT}(a, c\cdot a) = a$.
vi) $\mathrm{ggT}(b,a) = \mathrm{ggT}(a,b) = \mathrm{ggT}(a-q\cdot b, b)$.
vii) $\forall a,b \in \mathbb{Z}\ \exists x,y \in \mathbb{Z}: \quad \mathrm{ggT}(a,b) = x\cdot a + y\cdot b$.

Theorem 8. *i) x ist Einheit in* $\mathbb{Z}_n$ *wenn* $\mathrm{ggT}(x,n) = 1$,
andernfalls ist x Nullteiler.
ii) In $\mathbb{Z}_n$ *besitzt jedes* $x \neq 0$ *ein Inverses genau dann, wenn n Primzahl ist.*
iii) Sind p,q *verschiedene Primzahlen, so gilt* $|\mathbb{Z}^{\times}_{p\cdot q}| = (p-1)\cdot(q-1)$.
iv) Für p,q *wie in iii) und* $0 \leq m < p\cdot q$ *und* d,e *mit* $d\cdot e = 1 \bmod (p-1)\cdot(q-1)$ *gilt:*
$m^{d\cdot e} = m \bmod (pq)$.

Algorithmus 9 (Rivest/Shamir/Adleman 1973)

Schlüsselpaargenerierung: *Wähle verschiedene Primzahlen* p,q *(mit typischerweise um die tausend Binärstellen) sowie* $e \in \mathbb{N}$ *teilerfremd zu* $(p-1)\cdot(q-1)$.
Veröffentliche $p\cdot q$ *und e, halte* $p,q,(p-1)\cdot(q-1)$ *sowie d geheim,*
für $d = e^{1} \bmod (p-1)\cdot(q-1)$ *gemäß Theorem 8a).*
Verschlüsselung: *Eine Zahl* $1 < m < pq$ *wird verschlüsselt als* $\hat{m} := m^e \bmod pq$.
Entschlüsselung: *Die Zahl* $\hat{m}$ *wird entschlüsselt als* $m = \hat{m}^d \bmod pq$.
Signieren: *Eine Zahl* $1 < m < p\cdot q$ *wird signiert als* $\tilde{m} := m^d \bmod pq$.

Prof. Dr. Martin Ziegler Ausgabe am 24.4./8.5.2013

Praktikum Wissenschaftswelt Mathematik 2012

Rechnen in Restklassenringen mit Anwendungen in der Kryptografie,

24.April + 8.Mai 2013

AUFGABEN:

i) Geben Sie die Multiplikationstabelle (Verknüpfungstafel bzgl. $\times$) an für $\mathbb{Z}_6$.

ii) Lesen Sie die Nullteiler von $\mathbb{Z}_6$ ab und für jedes andere Element sein Inverses.
Überprüfen Sie Lemma 3 v) am Beispiel $R = \mathbb{Z}_6$.

iii*) Verifizieren Sie, dass die Menge $\{0,1,\alpha,\beta\}$ mit den folgenden Verknüpfungen einen kommutativen Ring bildet, in dem jedes Element $\neq 0$ invertierbar ist:

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\times$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

iv) Welches sind die invertierbaren Elemente von $\mathbb{Z}_{17}$, von $\mathbb{Z}_{18}$ und von $\mathbb{Z}_{256}$?

v) Berechnen Sie die Inverse von 5 in $\mathbb{Z}_{18}$ und jene von 111 in $\mathbb{Z}_{256}$.

vi) Berechnen Sie die Wertetabelle von $(2-X+4X^2+X^3)/X$ in $\mathbb{Z}_5$.

vii) Beweisen Sie die schöne Formel $(x+y)^p = x^p + y^p$ in $\mathbb{Z}_p$ für p Primzahl.
(Hinweis: benutzen Sie den binomischen Lehrsatz und Lemma 7 iv)

viii) Wie kann man einer Binärzahl leicht ansehen, ob sie durch 3 teilbar ist oder nicht?

xi) Berechnen Sie $x^2, x^4, x^8, x^{16}, x^{32}, x^{64}$ und x^{75} in $\mathbb{Z}_{18}$ für $x := 13$. (Tipp: $75 = 1+2+8+64$)

x) Berechnen Sie die Wertetabelle von $1+x+x^2+x^3+x^4+x^5+x^6$ in $\mathbb{Z}_7$.

xi) Berechnen Sie das Produkt der Polynome $2X^2+3X+4$ und $3X+3$ über $\mathbb{Z}_5$.

xii) Was ist der Rest des Polynoms $X^3+X+1 \in \mathbb{Z}_5[X]$ bei Division durch $3X^2+2X+4 \in \mathbb{Z}_5[X]$?

xiii) Seien $a := X^3+X+1 \in \mathbb{Z}_5[X]$ und $b := 3X^2+2X+4 \in \mathbb{Z}_5[X]$.
Bestimmen Sie Polynome $p,q \in \mathbb{Z}_5[X]$ mit $a \cdot p + b \cdot q = 2$ in $\mathbb{Z}_5[X]$.
Finden Sie auch p', q' mit $a \cdot p' + b \cdot q' = 1$?

xiv) Ein öffentlicher Schlüssel laute $(3953, 1337)$. Verschlüsseln Sie damit die Nachricht $m = 42$.

xv) Entschlüsseln Sie mit dem öffentlichen Schlüssel aus xiv) die signierte Nachricht $\tilde{m} = 3073$.

xvi) Können Sie den privaten Schlüssel knacken? Wer es schafft, sende die Antwort per Email an `ziegler@mathematik.tu-darmstadt.de`): kodiert mit meinem öffentlichen PGP-Schlüssel, *fingerprint* `AF37 ECD4 AEBE 3D4E 76EB 4445 227F 4D27 4A4B E6FE`.

*Fleißaufgabe, ggf. besser am Computer durchführen