

# Aufgaben zur Zahlentheorie und Kryptologie WS 2004/05, Blatt 1

Michael Hortmann

## Aufgabe 1

a) Man finde ein erzeugendes Element von  $\mathbb{Z}_{29}^*$ , also ein Element  $x \in \mathbb{Z}_{29}^*$  der Ordnung 28.

Ist  $x \in \mathbb{Z}_{29}^*$ , so ist jedenfalls  $\text{ord}(x)$  ein Teiler von 28, also 1, 2, 4, 7, 14 oder 28.

Man muß also nur testen, ob nicht schon  $x^k \equiv 1 \pmod{29}$  für  $k=4$  oder  $k=14$ . Dieser Test ist für  $x=2$  sofort erfolgreich. Der Pari-Befehl `znorder(Mod(2,29))` wirft sofort das Ergebnis 28 aus, während der Befehl `znprimroot(29)` ebenfalls 2 als Erzeuger vorschlägt.

b) Man finde eine 4-elementige und eine 7-elementige Untergruppe von  $\mathbb{Z}_{29}^*$ .

$2^7 \equiv 12 \pmod{29}$  sollte eine 4-elementige,  $2^4 \equiv 16 \pmod{29}$  eine 7-elementige Untergruppe erzeugen. Es ergibt sich über die Potenzen von 12 die Untergruppe  $\{1, 12, 28, 17\}$  und über die Potenzen von 16 die Untergruppe  $\{1, 16, 24, 7, 25, 23, 20\}$

## Aufgabe 2

Seien  $m \in \mathbb{Z}, n \in \mathbb{N}$ . Dann gibt es eindeutig bestimmte Elemente  $q \in \mathbb{Z}, r \in \mathbb{N}$  mit  $0 \leq r < n$  und  $m = qn + r$  (Division mit Rest). Man schreibt  $r := m \% n$ .

a) Man zeige durch explizite Rechnung, daß die Abbildung  $\mathbb{Z} \rightarrow \mathbb{Z}_n$ ,  $m \rightarrow m \% n$  ein surjektiver Ringhomomorphismus ist.

b)  $m, n \in \mathbb{N}$  seien teilerfremd. Man zeige durch explizite Rechnung, daß die Abbildung  $\mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$ ,  $k \rightarrow (k \% m, k \% n)$  ein **Ringisomorphismus** ist.

## Aufgabe 3

Für eine Primzahl  $p \in \mathbb{N}$  und einen Exponenten  $\alpha \in \mathbb{N}, \alpha \geq 2$  setze man  $n = p^\alpha$  und betrachte die multiplikative Gruppe  $\mathbb{Z}_n^*$ . Man zeige:

a) Ist  $p > 2$  und  $g$  ein erzeugendes Element von  $\mathbb{Z}_p^*$ , so ist  $g$  oder  $(p+1)g$  ein erzeugendes Element von  $\mathbb{Z}_n^*$ .

Die multiplikative Gruppe  $\mathbb{Z}_{p^\alpha}^*$  besteht aus den zu  $p^\alpha$  und damit zu  $p$  teilerfremden Elementen von  $\mathbb{Z}_{p^\alpha}$ , sie besitzt also die Ordnung bzw. Elementzahl  $p^\alpha - p^{\alpha-1} = (p-1)p^{\alpha-1}$ . Setzen wir

$U_1 := \{x \in \mathbb{Z}_{p^\alpha}^* \mid x \equiv 1 \pmod{p}\}$  so erhalten wir eine  $p^{\alpha-1}$ -elementige Menge (wie man leicht nachzählt), die offenbar multiplikativ abgeschlossen ist. Eine multiplikativ abgeschlossene Teilmenge einer endlichen Gruppe bildet aber, wie man sich wieder leicht überlegt, immer eine

Unterguppe<sup>1</sup>. Für  $2 \leq k \leq \alpha$  definieren wir weitere Mengen  $U_k := \{x \in \mathbb{Z}_{p^\alpha}^* \mid x \equiv 1 \pmod{p^k}\}$ , die jeweils  $p^{\alpha-k}$  Elemente enthalten, multiplikativ abgeschlossen und daher Untergruppen sind. Wir haben also eine Kette von echt kleiner werdenden Untergruppen  $\mathbb{Z}_{p^\alpha}^* \supset U_1 \supset \dots \supset U_\alpha = \{1\}$ .

Nun nehmen wir einen Erzeuger  $g \in \mathbb{Z}_{p^\alpha}^*$ . Die Ordnung von  $g$  in  $\mathbb{Z}_{p^\alpha}^*$  muß ein Vielfaches von  $p-1$  sein, denn ist  $g^m = 1$  in  $\mathbb{Z}_{p^\alpha}^*$ , so auch in  $\mathbb{Z}_p^*$ . Da  $(p-1)p^{\alpha-1}$  die Ordnung von  $\mathbb{Z}_{p^\alpha}^*$  ist, folgt  $\text{ord } g = (p-1)p^\beta$  mit  $\beta \leq \alpha-1$ . Wir bilden also  $b_1 = g^{p-1}$  in  $\mathbb{Z}_{p^\alpha}^*$ . Offenbar ist  $b_1 \equiv 1 \pmod{p}$ , und wir nehmen zunächst an, daß  $b_1 \not\equiv 1 \pmod{p^2}$ . Damit ist  $b_1 \in U_1 - U_2$ , und man hat  $b_1 = mp + 1$  mit  $m \not\equiv 0 \pmod{p}$ . Man errechnet mit der binomischen Formel  $b_1^p = (mp+1)^p \equiv pmp + 1 \pmod{p^2}$ , was bedeutet, daß  $b_2 = b_1^p \in U_2 - U_3$ . So geht es weiter, bis schließlich erst im letzten Schritt  $b_{\alpha-1} = b_{\alpha-2}^p \in U_\alpha = \{1\}$ . Damit ist offenbar  $\text{ord}(b_1) = p^{\alpha-1}$  in  $\mathbb{Z}_{p^\alpha}^*$  und somit insgesamt  $\text{ord } g = (p-1)p^{\alpha-1}$ .

Nun zum oben übersprungenen Fall  $g^{p-1} \equiv 1 \pmod{p^2}$ . Diese Kongruenz wäre ein seltener Zufall, wie man sich mit Hilfe von Pari an Beispielen klarmacht. In diesem Fall bilden wir  $\tilde{g} := (p+1)g$  in  $\mathbb{Z}_{p^\alpha}^*$ . Dann ist in offenbar wieder  $\tilde{g}^{p-1} \equiv 1 \pmod{p}$ , während dieselbe Potenz in  $\mathbb{Z}_{p^\alpha}^*$   $\tilde{g}^{p-1} = (p+1)^{p-1} g^{p-1} \equiv ((p-1)p+1) \cdot 1 \equiv -(p-1) \pmod{p^2}$  ergibt. Jetzt funktioniert mit  $\tilde{g}$  statt mit  $g$  dasselbe Argument wie im vorigen Abschnitt, d.h. wir bilden  $b_1 = \tilde{g}^{p-1}$ , etc.

### Kurzfassung:

Man hat eine natürliche Folge von Untergruppen  $\mathbb{Z}_{p^\alpha}^* \supset U_1 \supset \dots \supset U_\alpha = \{1\}$

Man beschaffe sich ein  $g \in \mathbb{Z}_{p^\alpha}^*$ , welches mod  $p$  ein Erzeuger von  $\mathbb{Z}_p^*$  ist, und für welches in  $\mathbb{Z}_{p^\alpha}^*$  gilt:  $b_1 := g^{p-1} \in U_1 - U_2$ . Mit  $b_k := b_{k-1}^p$  für  $2 \leq k \leq \alpha$  gilt  $b_k = g^{(p-1)p^{k-1}} \in U_k - U_{k-1}$  für  $1 \leq k \leq \alpha-1$  und schließlich  $b_\alpha = g^{(p-1)p^{\alpha-1}} = 1$ ,  $g$  ist damit ein Erzeuger von  $\mathbb{Z}_{p^\alpha}^*$

b) Ist  $p=2$  und  $\alpha > 2$ , so ist  $\mathbb{Z}_n^*$  nicht zyklisch, besitzt also kein erzeugendes Element. Jedoch ist 5 Erzeuger einer Untergruppe vom Index 2, also einer Untergruppe, welche die Hälfte der Elemente von  $\mathbb{Z}_n^*$  enthält, nämlich derjenigen Elemente von  $\mathbb{Z}_n^*$ , welche bei Division durch 4 den Rest 1 lassen.

Zunächst ein Beispiel:

$\mathbb{Z}_8^* = \{1, 3, 5, 7\}$ . Jedes der 3 Elemente  $\neq 1$  erzeugt eine zweielementige Untergruppe. Also ist  $\mathbb{Z}_8^*$  nicht zyklisch.

3 könnte eine ähnliche Rolle spielen wie  $\tilde{g}$  oben. Benutzen wir für dieses Element die 2-adische Darstellung 11, so ist  $11^2 = 1001$ . Oben hätten wir aber benötigt  $11^2 = x01$  mit  $x \neq 0$ .

Deshalb spielt für  $p=2$  die Untergruppe  $U_1$  keine Rolle. Es gilt aber  $5 \in U_2 - U_0$ ,

- 1 Ist  $G$  eine endliche Gruppe und  $U$  eine multiplikativ abgeschlossene Teilmenge, und  $\alpha \in U$  besitze die Ordnung  $m \geq 1$  in  $G$ . Offenbar ist  $\alpha^m \in U$  und  $\alpha^m \equiv 1 \pmod{m}$ , so daß auch  $\alpha \in U$ .
- 2 Genau dies ist falsch für  $p=2$ !
- 3 Die ist in der  $p$ -adischen Darstellung eine zweistellige Zahl, im Gegensatz zum einstelligen  $g$ .

$5^2 \in U_3 - U_2$  bis schließlich  $5^{2^{\alpha-2}} \in U_\alpha = \{1\}$ . Damit erzeugt 5 die Untergruppe  $U_2$ , und diese besitzt die Ordnung  $2^{\alpha-2}$  und umfaßt die Hälfte der Elemente von  $\mathbb{Z}_{2^\alpha}^*$ . Es ist bereits  $U_1 = \mathbb{Z}_{2^\alpha}^*$ , im Unterschied zu der Situation für  $p \neq 2$ . Gäbe es einen Erzeuger  $x$  von  $U_1$ , der natürlich in  $U_1 - U_2$  liegen müßte, so könnten die Elemente von  $U_2 - U_3$  nur ungerade Potenzen von  $x$  sein, denn die geraden Potenzen sind als Quadrate in  $\mathbb{Z}_{2^\alpha}^*$  ist ja kongruent zu 1 mod 8 und liegen damit in  $U_3$ . Die ungeraden Potenzen von  $x$  liegen aber offenbar in  $U_1 - U_2$ ! Daher kommen keine Elemente von  $U_2 - U_3$  unter den Potenzen von  $x$  vor,  $x$  kann also kein Erzeuger von  $U_1 = \mathbb{Z}_{2^\alpha}^*$  sein.

#### Aufgabe 4

Eine Carmichael Zahl  $n \in \mathbb{N}$  ist dadurch charakterisiert, daß für jeden Primfaktor  $p$  von  $n$  gilt:

$(p-1) | (n-1)$ . Wir haben in der Vorlesung gesehen, daß dann gilt:  $\forall x \in \mathbb{Z}_n^*: x^{n-1} = 1$ , und wir haben gesehen, daß 561 eine Carmichael Zahl ist.

Die obige Aussage ist nicht ganz korrekt, in der Übung wurde ja auch eine entsprechende Bemerkung gemacht: die Bedingung ist zwar notwendig, aber nicht hinreichend. Hinreichend wird sie erst, wenn man zusätzlich voraussetzt, daß  $n$  quadratfrei ist, daß also in der Primfaktorzerlegung von  $n$  keine Primzahlpotenzen mit Exponenten größer als 1 auftreten.

Es ist interessant, ein entsprechende Gegenbeispiel zu konstruieren: dies gelingt nach Anregung durch den Aufgabenteil a):

```
for(m=1,100,\
  p=6*m+1;\
  q=12*m+1;\
  r=18*m+1;\
  \
  if(isprime(p) && isprime(q) && isprime(r), print(m," Primzahlen"););\
  if(matsize(factor(p))[1]==1 && matsize(factor(q))[1]==1 && matsize(factor(r))[1]==1,\
    print(m," Primzahlpotenzen"););\
)
```

Damit erhalten wir in der Formel  $(6m+1)(12m+1)(18m+1)$  z.B. für  $m=1$  die Carmichael Zahl  $7*13*19=1729$ , aber schon für  $m=2$  das Produkt  $n=13*25*37=12025$ . Offenbar gilt für jeden Primteiler  $p$  von  $n$ , also für 13, 5, 37, daß  $p-1 | n-1$ , aber 12025 ist keine Carmichael Zahl, denn man erhält z.B. sofort  $2^{12024} \equiv 7216 \pmod{12025}$ .

Hier noch einmal der Beweis der Tatsache, daß eine Carmichael-Zahl quadratfrei sein muß:

Sei  $n = p^\alpha r$  mit  $p \geq 3, \alpha \geq 2, \text{ggT}(p, r) = 1$ . Wir haben nach dem chinesischen Restesatz den Ringisomorphismus  $\mathbb{Z}_n \simeq \mathbb{Z}_{p^\alpha} \times \mathbb{Z}_r$ , nehmen einen Erzeuger  $g \in \mathbb{Z}_{p^\alpha}^*$  und finden  $b \in \mathbb{Z}_n$  mit  $b \rightarrow (g, 1)$ , so daß  $\text{ggT}(b, n) = 1$  und somit  $b \in \mathbb{Z}_n^*$ . Wäre  $n$  eine Carmichael-Zahl, so hätte man  $b^{n-1} \equiv 1 \pmod{n}$  und wegen  $p^2 | n$  auch  $b^{n-1} \equiv 1 \pmod{p^2}$ . Weil  $b$  ein Erzeuger auch der Reste modulo  $p^2$  ist und die Anzahl dieser Reste gleich  $(p-1)p$  ist, muß daher auch gelten:  $(p-1)p$  teilt  $n-1$ , d.h. wir haben gleichzeitig:  $p$  teilt  $n$  und  $p$  teilt  $n-1$ , was natürlich nicht geht.

a) Sei nun  $m \in \mathbb{N}$  und jede der drei Zahlen  $(6m+1), (12m+1), (18m+1)$  sei prim. Man zeige, daß dann das Produkt  $(6m+1)(12m+1)(18m+1)$  eine Carmichael Zahl ist.

b) Man benutze Pari<sup>4</sup>, um auf diese Weise mit dem eingebauten Primzahltest weitere Carmichael-Zahlen zu finden.

Mit obigem Code ergeben sich Carmichael-Zahlen für  $m = 1, 6, 35, 45, 51, 55, 56, 100$

Natürlich gibt es zwischendurch Carmichael-Zahlen, die von dieser Formel nicht erfaßt werden.

c) Man zeige zusätzlich, daß jede Carmichael-Zahl mindestens drei verschiedene Primfaktoren besitzt.

Man nehme an,  $n = pq$  sei eine Carmichael-Zahl mit  $p, q$  als einzigen Primfaktoren.

Sei o.B.d.A.  $p < q$ .

Wir wissen bereits, daß  $q-1$  ein Teiler von  $n-1 = p(q-1+1)q-1 = p(q-1) + (p-1)$  sein muß, daher auch von  $p-1$ . Wegen  $p < q$  geht das aber nicht.

---

<sup>4</sup> Man kann natürlich auch andere Computeralgebra- oder Arithmetik-Programme benutzen. In den meisten derartigen Systemen gibt es eine Funktion `isprime(n)`.