9. Übungsblatt zu Mathematik für Informatiker I, WS 2003/04

JOACHIM VON ZUR GATHEN, OLAF MÜLLER, MICHAEL NÜSKEN

Abgabe bis Freitag, 9. Januar 2004, 11^{11}
in den jeweils richtigen grünen oder roten Kasten auf dem D1-Flur.

Frohe Weihnachten und ein Gutes Neues Jahr

wünscht Euch
Euer MfI1-Team.

Die mit * gekennzeichneten Aufgabenteile und Aufgaben sind freiwillig. Die dort erworbenen Punkte werden als Weihnachtszusatzpunkte gutgeschrieben.

Aufgabe 9.1 (Modulares Rechnen). (4+3 Punkte)

(i) Finde alle Lösungen x von $3(x+3) = 7$ in $\mathbb{Z}_{13}$.

(ii) Finde alle Lösungen x von $17(2-x)x = 4x^2 - x + 7$ in $\mathbb{Z}_{21}$.

(iii) Finde alle Lösungen x von $x + 1/x = 1 - 5x$ in $\mathbb{Z}_6$.

(iv) Finde alle Lösungen x von $3x = 9$ in $\mathbb{Z}_{105}$. *Tipp*: Verwende den Chinesischen Restsatz.

(v*) Finde alle Lösungen von $x^2 + x + 4 = 0$ in $\mathbb{Z}_{19}$. *Tipp*: Eine Gleichung der Form $u^2 = c$ hat höchstens zwei Lösungen modulo einer Primzahl.

(vi*) Finde alle Lösungen x von $x \equiv 2 \bmod 7$ und $x^2 \equiv 1 \bmod 11$.

Aufgabe 9.2 (RSA durchführen). (4+1 Punkte)

Wir wollen einmal das RSA Verfahren an Zahlen durchführen.

(i) Sei $p = 251$ und $q = 263$. Bestimme den Modul N sowie $\varphi(N)$.

(ii) Sei $e = 17$. Bestimme den Entschlüsselungsexponenten d.

(iii) Sei x die geheime Nachricht, die dem ASCII-Zeichenpaar „`Ok`“ entspricht. Berechne deren Verschlüsselung y.

(iv) Sei $y = 3263$ die verschlüsselte Nachricht. Berechne deren Entschlüsselung z.

(v*) Programmiere RSA in MAPLE. *Tipp*: Verwende die Hilfe, um mehr über `mod` sowie `nextprime` zu erfahren.

Aufgabe 9.3 (Ansatz für einen Primtest). (4+2 Punkte)

Sei n ungerade.

(i) Berechne $2^{n-1} \operatorname{rem} n$ für alle ungeraden n mit $3 \leq n \leq 20$ sowie für $n = 1105$.

(ii) Prüfe, für welche dieser n

(a) die Gleichung $2^{n-1} \equiv 1 \bmod n$ gilt.

(b) die Zahl n prim ist.

Vergleiche.

(iii) Gilt „n prim $\implies 2^{n-1} \equiv 1 \bmod n$“? Begründe.

(iv) Gilt „$2^{n-1} \equiv 1 \bmod n \implies n$ prim“? Begründe.

(v*) Verwende beispielsweise MUPAD oder MAPLE, um alle Zahlen n zwischen 3 und 1000 zu finden, für die Primheit und $2^{n-1} \equiv 1 \bmod n$ nicht äquivalent sind. Gib außer der Lösung auch Dein Mapleprogramm an. *Hilfe*: Schleifen und Bedingungen in Maple gibt man wie im folgenden Beispiel ein:

```
> for n from 3 to 100 do
    A:=(n mod 10=1);
    B:=isprime(2*n+1);
    if A and B then print( n, A, B ); end if;
  end do:
```

Erläuterung des MAPLE-*Codes*: Die Schleife läuft hier von 3 bis 100. Es wird jeweils geprüft, ob die Schleifenvariable n der 1 modulo 10 entspricht (A) und danach, ob $2n+1$ prim ist (B). Wenn beides zutrifft, werden n, A und B ausgegeben.

Der Doppelpunkt anstelle eines Semikolons am Ende verhindert, dass jedes Zwischenergebnis ausgegeben wird. Mit `print(...)` kann man trotzdem etwas ausgeben; MAPLEs Hilfe dazu erhält man mit `?print`. MAPLE kennt den logischen Operator `xor` und das Prädikat `isprime`. Möchtest Du `A` ein wenig anders sehen, schlag doch mal unter `evalb` nach.

***Aufgabe 9.4** (Modulare quadratische Gleichung). (0+6 Punkte)

Wir betrachten hier die Gleichung

$$x^2 \equiv 1 \bmod m.$$

Die entsprechende Gleichung über den reellen (oder komplexen) Zahlen hat genau zwei Lösungen, und jede Gleichung der Form $ax^2 + bx + c = 0$ hat jedenfalls höchstens zwei reelle (komplexe) Lösungen. Wir wollen untersuchen, was modulo einer Zahl m passiert.

Wir beginnen mit dem Fall, dass $m = p$ eine Primzahl ist.

(i*) Sei $ab \equiv 0 \bmod p$. Zeige, dass dann $a \equiv 0 \bmod p$ oder $b \equiv 0 \bmod p$ ist. *Bemerkung*: Über den reellen (oder komplexen) Zahlen gilt das: Ist $ab = 0$ für zwei reelle (oder komplexe) Zahlen, dann ist $a = 0$ oder $b = 0$.

(ii*) Gib zwei Lösungen der Gleichung $x^2 \equiv 1 \bmod p$ an.

(iii*) Zeige, dass es keine weiteren Lösungen gibt. *Tipp*: Schreibe $x^2 - 1$ als Produkt und verwende (i*).

Nun wollen wir untersuchen, was für ein Produkt $m = pq$ zweier unterschiedlicher Primzahlen p, q geschieht.

(iv*) Seien $s, t \in \mathbb{Z}$ mit $1 = sp + tq$. Zeige, dass $\pm sp \pm tq$ Lösungen von $x^2 \equiv 1 \bmod pq$ sind.

(v*) Zeige, dass es modulo m höchstens vier Lösungen gibt. *Tipp*: Kombiniere den chinesischen Restsatz und (iii*).

Faktorisierungsalgorithmen versuchen zu einer natürlichen Zahl m ihre Primfaktorzerlegung zu berechnen. Einige beruhen darauf, dass sie (mehr oder minder geschickt) zwei Zahlen finden mit

$$u^2 \equiv v^2 \bmod m, \qquad u \not\equiv \pm v \bmod m.$$

(vi*) Zeige, dass (und wie) man für $m = pq$ aus solchen u und v ganz leicht p und q berechnen kann.

***Aufgabe 9.5** (Rabin Entschlüsselung). (0+5 Punkte)

Das Rabin-Verfahren arbeitet mit einem Produkt N zweier Primzahlen p und q, die beide kongruent 3 modulo 4 sind. Die zu verschlüsselnde Zahl wird dann modulo N quadriert. Wir wollen hier sehen, wie man diesen Quadrierungsschritt modulo der Primzahl p rückgängig machen kann.

(i*) Zeige, dass $\frac{p+1}{4}$ eine ganze Zahl ist.

(ii*) Zeige $a^{p+1} \equiv a^2 \bmod p$.

(iii*) Schließe, $a^{\frac{p+1}{2}} \equiv \pm a \bmod p$. *Tipp*: Verwende (ii*) und *Aufgabe 9.4(iii*).

(iv*) Sei $b = a^2$ und $w = b^{\frac{p+1}{4}}$. Zeige $a \equiv \pm w \bmod p$. Mit anderen Worten: w ist eine Wurzel aus b.

Damit können wir also modulo einer Primzahl, die kongruent 3 modulo 4 ist, Wurzeln ziehen aus einer Zahl, die ein Quadrat ist.

Mit Hilfe des chinesischen Restsatzes lassen sich Wurzeln auch modulo N ziehen. Sei $b \equiv a^2 \bmod N$.

(v*) Seien $s, t \in \mathbb{Z}$ mit $1 = sp + tq$ und $c = \pm spb^{\frac{q+1}{4}} \pm tqb^{\frac{p+1}{4}}$. Zeige, dass in jedem der vier Fälle $c^2 \equiv b \bmod N$ gilt.

Nach *Aufgabe 9.4(v*) kann es nicht mehr Lösungen geben, wir haben also alle gefunden. Aus diesen vier Lösungen muss man zur Rabin-Entschlüsselung die richtige raten, was leicht möglich ist, wenn natürlicher Text verschlüsselt wurde wie in Aufgabe 5.3. (Beachte, dass $N = 66013$ den oben genannten Anforderungen genügt.)

9. Übungsblatt zu Mathematik für Informatiker I, WS 2003/04, Mündlicher Teil

JOACHIM VON ZUR GATHEN, OLAF MÜLLER, MICHAEL NÜSKEN

Mündliche Aufgabe 9.6 (Modulares Rechnen).

(i) Finde alle Lösungen x von $3(x+3) = 7$ in $\mathbb{Z}_{17}$.

(ii) Finde alle Lösungen x von $47(2-x)x = 8x^2 + 6x - 11$ in $\mathbb{Z}_{55}$.

(iii) Finde alle Lösungen x von $8x + 2/x = 1 - 7x$ in $\mathbb{Z}_{15}$.

(iv) Finde alle Lösungen x von $5x = 35$ in $\mathbb{Z}_{110}$.

(v*) Finde alle Lösungen von $x^2 + x + 5 = 0$ in $\mathbb{Z}_{23}$. *Tipp*: Eine Gleichung der Form $u^2 = c$ hat höchstens zwei Lösungen modulo einer Primzahl.

(vi*) Finde alle Lösungen x von $x \equiv 2 \bmod 5$ und $x^2 \equiv 1 \bmod 7$.

Mündliche Aufgabe 9.7 (RSA durchführen).

Wir wollen einmal das RSA Verfahren an Zahlen durchführen.

(i) Sei $p = 31$ und $q = 41$. Bestimme den Modul N sowie $\varphi(N)$.

(ii) Sei $e = 17$. Bestimme den Entschlüsselungsexponenten d.

(iii) Sei $x = 1234$ die geheime Nachricht. Berechne deren Verschlüsselung y.

(iv) Sei $y = 1214$ die verschlüsselte Nachricht. Berechne deren Entschlüsselung z.

Mündliche Aufgabe 9.8 (Ansatz für einen Primtest).

Sei n nicht durch 3 teilbar.

(i) Berechne 3^{n-1} rem n für einige nicht durch drei teilbare n mit $2 \leq n \leq 30$ sowie für $n = 91$.

(ii) Prüfe, für welche dieser n

(a) die Gleichung $3^{n-1} \equiv 1 \bmod n$ gilt.

(b) die Zahl n prim ist.

Vergleiche.

(iii) Gilt „n prim $\implies 3^{n-1} \equiv 1 \bmod n$“? Begründe.

(iv) Gilt „$3^{n-1} \equiv 1 \bmod n \implies n$ prim“? Begründe.