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

JOACHIM VON ZUR GATHEN, OLAF MÜLLER, MICHAEL NÜSKEN

Abgabe bis Freitag, 12. Dezember 2003, 11^{11}
in den jeweils richtigen grünen oder roten Kasten auf dem D1-Flur.

Aufgabe 7.1 (Symmetrischer EEA). (9 Punkte)

Ziel dieser Aufgabe ist es zu zeigen, was man gewinnt, wenn man bei der Division mit Rest auch negative Reste zulässt.

Seien a und b zwei ganze Zahlen. Man kann leicht zeigen, dass es immer zwei ganze Zahlen q und r gibt, so dass $a = qb + r$ und $-\frac{1}{2}|b| \leq r < \frac{1}{2}|b|$. Wir nennen dies *symmetrische Division mit Rest* und schreiben $q = a \operatorname{squo} b$. (*Idee:* Verwende normale Divison mit Rest und korrigiere das Ergebnis.)

(i) Berechne entsprechende q und r für $a = 100$ und $b = 53$.

(ii) Berechne entsprechende q und r für $a = 807\,959$ und $b = 219\,215$.

Wir betrachten nun den Erweiterten Euklidischen Algorithmus mit symmetrischen Resten.

Algorithmus. Symmetrischer EEA.
Eingabe: $a, b \in \mathbb{Z}$.
Ausgabe: $\ell \in \mathbb{N}$, $r_i, s_i, t_i \in \mathbb{Z}$ für $0 \leq i \leq \ell + 1$, und $q_i \in \mathbb{Z}$ für $1 \leq i \leq \ell$, wie unten berechnet.

1. $r_0 \leftarrow a, \quad r_1 \leftarrow b$.
2. $s_0 \leftarrow 1, \quad t_0 \leftarrow 0$.
3. $s_1 \leftarrow 0, \quad t_1 \leftarrow 1$.
4. $i \leftarrow 1$.
5. While $r_i \neq 0$ do 6–10
6. $\quad q_i \leftarrow r_{i-1} \operatorname{squo} r_i$. // Hier symmetrische Division mit Rest.
7. $\quad r_{i+1} \leftarrow r_{i-1} - q_i r_i$.
8. $\quad s_{i+1} \leftarrow s_{i-1} - q_i s_i$.
9. $\quad t_{i+1} \leftarrow t_{i-1} - q_i t_i$.
10. $\quad i \leftarrow i + 1$.
11. $\ell \leftarrow i - 1$.
12. Return ℓ, r_i, s_i, t_i für $0 \leq i \leq \ell + 1$, und q_i für $1 \leq i \leq \ell$.

(iii) Benutze diesen Algorithmus, um einen ggT von $a = F_{10} = 55$ und $b = F_9 = 34$ zu berechnen.

(iv) Benutze diesen Algorithmus, um einen ggT von $a = 219\,215$ und $b = 807\,959$ zu berechnen.

(v) Vergleiche die Anzahl der Schleifendurchläufe aus (iii) und (iv) mit dem normalen euklidischen Algorithmus. [Beide Angaben zum normalen EA sind bekannt!]

(vi) Zeige, dass ab $i = 1$ der Betrag jedes Restes r_{i+1} höchstens halb so groß ist wie der Betrag des vorangehenden Restes r_i. Genauer gesagt: $|r_{i+1}| \leq \frac{1}{2}|r_i|$, falls $1 \leq i \leq \ell$.

(vii) Schließe, dass $|r_i| \leq \frac{1}{2^{i-1}}|b|$ für $2 \leq i \leq \ell + 1$ gilt.

(viii) Zeige, dass diese Variante des Euklidischen Algorithmus für $b \neq 0$ höchstens $\log_2 |b| + 1$ Schritte (also Durchläufe von Schritt 5–10 im Algorithmus) braucht.

Aufgabe 7.2 (Modulare Arithmetik). (6 Punkte)

(i) Löse $x \equiv 271\,828 + 314\,159 \mod 125$ geschickt.

(ii) Löse $x \equiv 271\,828 - 314\,159 \bmod 125$ geschickt.

(iii) Löse $x \equiv 271\,828 \cdot 314\,159 \bmod 125$ geschickt.

(iv) Löse $5(x + 27) \equiv 4x \bmod 31$.

(v) Löse $5(x + 27) \equiv 25 \bmod 31$.

(vi) Löse $13(5 - x) \equiv 17x \bmod 31$.

(vii) Berechne $s, t \in \mathbb{Z}$ mit $1 = 5s + 17t$.

(viii) Löse $5x \equiv 1 \bmod 17$.

(ix) Finde alle Lösungen von $3x \equiv 0 \bmod 15$.

(x) Finde alle Lösungen von $3x \equiv 2 \bmod 1\,011$.

Aufgabe 7.3 (Modular Potenzieren). (2 Punkte)

(i) Berechne 3^{16} rem 17 (von Hand!).

(ii) Berechne $3^{10\,000}$ rem 85 (von Hand!).

Aufgabe 7.4 (Teilbarkeitsregeln). (5 Punkte)

Du kennst bestimmt einige Teilbarkeitsregeln. Zum Beispiel ist eine Zahl durch 2 teilbar, wenn ihre Dezimaldarstellung auf 2, 4, 6, 8 oder 0 endet. Und eine Zahl ist durch 3 teilbar genau dann, wenn auch ihre Quersumme durch 3 teilbar ist. Woher kommen diese Regeln? Wir wollen einige interessante anschauen, die in Deiner Sammlung vielleicht noch fehlen:

(i) Beweise die Teilbarkeitsregel für 9:

Satz. *Wenn die Quersumme einer Zahl x durch 9 teilbar ist, dann ist auch x durch 9 teilbar.*

Tipp: Betrachte $x = \sum_{0 \le j < k} x_j 10^j$ modulo 9.

(ii) Leite eine Teilbarkeitsregel für 3 ab.

(iii) Finde und zeige eine Teilbarkeitsregel für 11.

(iv) Finde und zeige eine Teilbarkeitsregel für $1\,001$.

(v) Leite eine Teilbarkeitsregel für 7 und 13 ab. [*Tipp*: $1\,001 = 7 \cdot 11 \cdot 13$.]

Aufgabe 7.5 (Von großen zu kleinen Moduln). (1 Punkt)

Zeige:

Sei n ein Teiler von m. Sind zwei Zahlen a, b modulo m kongruent, $a \equiv b \bmod m$, dann sind sie auch modulo des Teilers n kongruent, $a \equiv b \bmod n$.

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

JOACHIM VON ZUR GATHEN, OLAF MÜLLER, MICHAEL NÜSKEN

Mündliche Aufgabe 7.6 (Symmetrischer EEA).

Die Voraussetzungen seien wie in Aufgabe 7.1.

(i) Berechne den Quotienten $q = a \operatorname{squo} b$ und den symmetrischen Rest r für $a = 80$ und $b = 41$.

(ii) Berechne den Quotienten $q = a \operatorname{squo} b$ und den symmetrischen Rest r für $a = 767\,702$ und $b = 193\,764$.

(iii) Benutze den symmetrischen EEA, um den ggT von $a = F_9 = 34$ und $b = F_8 = 21$ zu berechnen.

(iv) Benutze diesen Algorithmus, um den ggT von $a = 47\,248$ und $b = 83\,740$ zu berechnen.

(v) Vergleiche die Anzahl der Operationen aus (iii) und (iv) mit dem normalen euklidischen Algorithmus. [Beide Angaben zum normalen EA sollten bekannt sein!]

Mündliche Aufgabe 7.7 (Modulare Arithmetik).

(i) Löse $x \equiv 217\,288 + 341\,195 \bmod 99$ geschickt.

(ii) Löse $x \equiv 217\,288 - 341\,195 \bmod 99$ geschickt.

(iii) Löse $x \equiv 217\,288 \cdot 341\,195 \bmod 99$ geschickt.

(iv) Löse $4(x + 25) \equiv 3x \bmod 29$.

(v) Löse $4(x + 25) \equiv 21 \bmod 29$.

(vi) Löse $13(5 - x) \equiv 17x \bmod 29$.

(vii) Berechne $s, t \in \mathbb{Z}$ mit $1 = 7s + 11t$.

(viii) Löse $7x \equiv 1 \bmod 11$.

(ix) Finde alle Lösungen von $7x \equiv 0 \bmod 21$.

(x) Finde alle Lösungen von $9x \equiv 2 \bmod 333$.

Mündliche Aufgabe 7.8 (Modular Potenzieren).

(i) Berechne 5^{10} rem 11 (von Hand!).

(ii) Berechne $5^{10\,000}$ rem 33 (von Hand!).

Mündliche Aufgabe 7.9 (Modulare Nullteiler).

Definition (Nullteiler). *Eine ganze Zahl a heißt* Nullteiler modulo m*, wenn* $a \not\equiv 0 \bmod m$ *gilt und es eine ganze Zahl* $b \not\equiv 0 \bmod m$ *gibt mit* $ab \equiv 0 \bmod m$*.*

(i) Finde Nullteiler modulo 12.

(ii) Zeige, dass es keine Nullteiler modulo p gibt, wenn p eine Primzahl ist.

(iii) Entscheide, ob es Nullteiler modulo p^2 gibt, wenn p eine Primzahl ist.

Mündliche Aufgabe 7.10 (Modulare Arithmetik).

Seien $m, n \in \mathbb{N}_{\geq 1}$. Dann gilt:

$$(\forall a, b \in \mathbb{Z} \quad (a \equiv b \bmod m \Rightarrow a \equiv b \bmod n)) \Rightarrow n | m.$$