Diskrete Mathematik WS 09\10
Lösungsblatt 6

1

Chinesicher Restsatz, $m = m_1 \cdot m_2 \cdot m_3$ mit $m_1 = 5, m_2 = 7$ und $m_3 = 13$.

(a) Man suche ein x mit: $x \equiv 31 \mod 5, x \equiv 10 \mod 7$ und $x \equiv 52 \mod 13$.

(b) Man berechne in $(\mathbb{Z}_m, +, \cdot)$ was $12 \cdot 36$ liefert direkt und über den Umweg über die Zerlegung von $\mathbb{Z}_m$ in $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \mathbb{Z}_{m_3}$.

Lösung:
a) $m = m_1 \cdot m_2 \cdot m_3 = 5 \cdot 7 \cdot 13 = 455$

$m \equiv \underbrace{31}_{a_1} \mod \underbrace{5}_{m_1}$
$m \equiv \underbrace{10}_{a_2} \mod \underbrace{7}_{m_2}$
$m \equiv \underbrace{52}_{a_3} \mod \underbrace{13}_{m_3}$
$M_1 = m_2 \cdot m_3 = 7 \cdot 13 = 91$
$M_2 = m_1 \cdot m_3 = 5 \cdot 13 = 65$
$M_3 = m_1 \cdot m_2 = 5 \cdot 7 = 35$

$y_1 \cdot M_1 \equiv 1 \mod m_1$
$y_1 \cdot 91 \equiv 1 \mod 5$
$y_1 \cdot 1 \equiv 1 \mod 5$

$y_2 \cdot M_2 \equiv 1 \mod m_2$
$y_2 \cdot 65 \equiv 1 \mod 7$
$y_2 \cdot 2 \equiv 1 \mod 7$

$y_3 \cdot M_3 \equiv 1 \mod m_3$
$y_3 \cdot 35 \equiv 1 \mod 13$
$y_3 \cdot 9 \equiv 1 \mod 13$

$x = \sum_{i=1}^{3} a_i y_i M_i = 31 \cdot 1 \cdot 91 + 10 \cdot 4 \cdot 65 + 52 \cdot 3 \cdot 35 = 2821 + 2600 + 5460 = \underline{10881}$
$x = 10881 \equiv \boxed{416} \mod 455$

b)
Direkt: $12 \cdot 36 = \boxed{432}$

$(\underbrace{12}_{\text{mod } 5}, \underbrace{12}_{\text{mod } 7}, \underbrace{12}_{\text{mod } 13}) = (2, 5, 12)$
$(\underbrace{36}_{\text{mod } 5}, \underbrace{36}_{\text{mod } 7}, \underbrace{36}_{\text{mod } 13}) = (1, 1, 10)$
$(2, 5, 12) \cdot (1, 1, 10) = \underline{(2, 5, 3)}$

Zurück mit chinesischen Restsatz
$x \equiv 2 \mod 5$
$x \equiv 5 \mod 7$
$x \equiv 3 \mod 13$

$x = \sum_{i=1}^{3} a_i y_i M_i = 2 \cdot 1 \cdot 91 + 5 \cdot 4 \cdot 65 + 3 \cdot 3 \cdot 35 = 182 + 1300 + 315 = 1797$
$1797 \equiv \boxed{432} \mod 455 \surd$

2

Berechne $\phi(13013)$ (Eulersche Phi-Funktion).

Lösung:
$13013 = 13^2 \cdot 11 \cdot 7$
$\phi(m) = \prod_{i=1}^{n} p_i^{a_i - 1} \cdot (p_i - 1)$
$\phi(13013) = 13 \cdot (13-1) \cdot (11-1) \cdot (7-1) = 13 \cdot 12 \cdot 10 \cdot 6 = \boxed{9360}$

3

Wir rechnen in $(\mathbb{Z}_{21}, +, \cdot)$.

(a) Man gebe die von 15 erzeugte Untergruppe von $(\mathbb{Z}_{21}, +)$ an.

(b) Welche Elemente erzeugt $(\mathbb{Z}_{21}, +)$?

(c) Welche Elemente von $(\mathbb{Z}_{21}, \cdot)$ haben ein Inverses?

(d) Man bestimme die Ordnung einiger Elemente von $(\mathbb{Z}_{21}^*, \cdot)$.

Lösung:
a)
Wir rechnen in $\mathbb{Z}_{21}$
$15, 30 = 9, 24 = 3, 18, 33 = 12, 27 = 6, 21 = 0$
Also von 15 erzeugte Untergruppe in $(\mathbb{Z}_{21}, +) : \{15, 9, 3, 18, 12, 6, 0\}$
7 Elemente (ist Teiler von 21) $\surd$

b)

1 ist erzeugendes Element

Satz: $(G, \cdot)$ endliche zyklische Gruppe der Ordnung n und a erzeugendes Element. Dann: a^k erzeugendes Element $\iff ggT(a,n) = 1$ für $1 \leq k \leq n$

Hier: $a = 1$
und $a^k \underbrace{\widehat{=}}_{\text{wegen + Verknüpfung}} k \cdot a \widehat{=} k \cdot 1 \widehat{=} k$
Also k erzeugendes Element von $(\mathbb{Z}_n, +) \iff ggT(k,n) = 1$
Hier $n = 21 = 3 \cdot 7$. Also erzeugende Elemente:
$\{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$ 12 Elemente
$\phi(21) = \phi(3 \cdot 7) = 2 \cdot 6 = 12 \surd$

c)
x hat Inverses bez. $\cdot$, falls $ggT(x,n) = 1$
Also $\mathbb{Z}_2 1^* = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$

d)
Durch Probieren:
$2, 4, 8, 16, 32 = 11, 22 = 1$ nein
$5, 25 = 4, 20, 100 = 16, 80 = 17, 85 = 1$
$11, 121 = 16, 176 = 8, 88 = 4, 44 = 2, 22 = 1$
$13, 169 = 1$
$19, 361 = 4, 76 = 13, 247 = 16, 304 = 10, 190 = 1$
von 19 erzeugte Untergruppe: $\{19, 4, 13, 16, 10, 1\} = U$
Ordnung $n = 6$
$ord\ 13 = ord\ 19^3 = \frac{n}{ggT(n,k)} = \frac{6}{ggT(6,3)} = \frac{6}{3} = 2 \surd$
$ord\ 10 = ord\ 19^5 = \frac{6}{ggT(6,5)} = 6$
Also 10 erzeugende Elemente von Untegruppe U. Test:
$10, 100 = 16, 160 = 13, 130 = 4, 40 = 19, 190 = 1 \surd$

4 Eulersche ϕ-Funktion

Es sei eine natürliche Zahl n mit $n > 1$ gegeben. Finden Sie die Anzahl der natürlichen Zahlen aus $1, 2, 3, ..., n$, die teilerfremd zu n sind. Das ist die Eulersche Phi-Funktion, die so definiert ist: $\phi : \mathbb{N} \to \mathbb{N}, \phi(n) =$ die Anzahl der natürlichen Zahlen von 1 bis n, die teilerfremd zu n sind.

Lösung:
Siehe Buch[2], Seite 86.

5 Wieviele sind es mindestens?

Wir haben eine gewisse Anzahl von Gummibärchen, wissen aber nicht, wieviele es sind. Wenn wir die Bärchen in Tüten verpacken, in die je m_1 Bärchen passen, bleiben a_1 Bärchen übrig. Wenn wir sie in Tüten verpacken, die jeweils eine Kapazität von m_2 Bärchen besitzen, bleiben a_2 übrig. ... Wenn wir sie in Tüten füllen, die je m_k Bärchen aufnehmen, bleiben a_k übrig. Wieviele Gummibärchen sind es mindestens, wenn die $m_1, m_2, \ldots, m_k$ mit $m_k < 100$ untereinander teilerfremd sind? Eingabe: In der Datei baerchen.in befinden sich die Paare (a_i, m_i)

mit $0 \leq a_i < m_i$; ein Paar pro Zeile. Das Produkt $m_1 \cdot m_2 \cdot \ldots \cdot m_k$ passt in den Typ unsigned. Ausgabe: Geben Sie die minimale Anzahl der Gummibärchen in die Ausgabedatei baerchen.out aus.

Lösung:
Siehe Buch[2], Seiten 134-135.

References

[1] Albrecht Beutelspacher, Marc-Alexander Zschiegner, Diskrete Mathematik für Einsteiger. Mit Anwendungen in Technik und Informatik, 3. Auflage, Vieweg Verlag, 2007.

[2] Doina Logofătu, Algorithmen und Problemlösungen mit C++, Vieweg+Tebuner Verlag, 2010.