ÜE6

Donnerstag, 22. Dezember 2022 08:03

Aufgabe P 1. *Modulare Arithmetik*

Wir betrachten ganzzahlige Division durch 13.

(a) Bestimmen Sie $42 \mod 13$ sowie $18 \mod 13$. Wählen Sie hierzu jeweils die Darstellung

$$x = a \cdot 13 + r \quad \text{mit} \quad 0 \le r < 13.$$

(b) Listen Sie einige negative und positive Elemente der Restklassen $[42]_{\equiv_{13}}$ und $[18]_{\equiv_{13}}$ auf, darunter jeweils das Element, das im Bereich von 0 bis 12 liegt.

a)

42=3*13+3
18=1*13+5

$42 \mod 13 = 3$

$18 \mod 13 = 5$

b) $[42]_{\equiv_{13}} = \{\ldots, -23, -10, 3, 16, 29, \ldots\}$ (+13, +13, +13, +13)

$[18]_{\equiv_{13}} = \{\ldots, -21, -8, 5, 18, 31, 44, \ldots\}$ (+13, +13, +13, +13, +13)

(c) Die Zahl 16 liegt in der Restklasse $[3]_{\equiv_{13}}$, die Zahl 18 liegt in der Restklasse $[5]_{\equiv_{13}}$. Berechnen Sie $16 \cdot 18$ und überzeugen Sie sich davon, dass $(16 \cdot 18) \mod 13 = 2$ gilt.

(d) Verfizieren Sie, dass $225 \underset{13}{\equiv} 4$ sowie $225 \underset{13}{\equiv} 264$ gilt.

(e) Bestimmen Sie $(42 \cdot 18)^2 \mod 13$.

c) $16 \cdot 18 = 16(10+8) = 160 + 128 = 288$

$288 \mod 13 = 2$

1. $288 = 22 \cdot 13 + 2$

2. $(16 \cdot 18) \mod 13 = (16 \mod 13) \cdot (18 \mod 13) \mod 13$

$= (3 \cdot 5) \mod 13 = 15 \mod 13 = 2$

d) $225 - 4 = 221 = 13 \cdot 17$

221 ist teilbar durch 13

$264 - 225 = 39 = 13 \cdot 3$

39 ist teilbar durch 13

e) $(42 \cdot 18)^2 \mod 13 = ((42 \cdot 18)(42 \cdot 18)) \mod 13$

$= ((3 \cdot 5)(3 \cdot 5)) \mod 13 = (2 \cdot 2) \mod 13 = 4$

Aufgabe P 2. *Eulersche φ-Funktion*

(a) Ermitteln Sie die Menge $E(30)$ derjenigen ganzen Zahlen x im Bereich $\{1, 2, 3, \ldots, 29, 30\}$, die zu 30 teilerfremd sind (für die also $\text{ggT}(x, 30) = 1$ gilt), sowie deren Elementeanzahl $|E(30)|$ „von Hand".

(b) Lesen Sie den folgenden, in der Vorlesung behandelten **Satz:**

Wenn p, q und r drei (paarweise) voneinander verschiedene Primzahlen sind, so gilt

$$\varphi(p \cdot q) = (p-1) \cdot (q-1)$$
$$\varphi(p \cdot q \cdot r) = (p-1) \cdot (q-1) \cdot (r-1).$$

(c) Verwenden Sie die jeweils einschlägige Formel zur Berechnung der folgende Werte:

(i) $\varphi(30)$ (ii) $\varphi(91)$ (iii) $\varphi(1001)$

a)

$E(30) = \{1, 7, 11, 13, 17, 19, 23, 29\}$

$|E(30)| = \varphi(30) = 8$

c) $\varphi(30) = \varphi(2 \cdot 3 \cdot 5) = (2-1)(3-1)(5-1)$

$= 2 \cdot 4 = 8$

$\varphi(91) = \varphi(7 \cdot 13) = (7-1)(13-1)$

$= 6 \cdot 12 = 72$

$\varphi(1001) = \varphi(7 \cdot 13 \cdot 11) = 6 \cdot 12 \cdot 10$

$= 720$

P3

(a) **Berechnen Sie** $87^{27} \mod 103$.
Hinweis: Sie können z.B. ausnutzen, dass $87 \underset{103}{\equiv} -16$ *ist.*

Wir schreiben 27 als Summe von 2er Potenzen

Lookup-Tabelle 2-er Potenzen

n	0	1	2	3	4	5	6	7
2^n	1	2	4	8	16	32	64	128

$27 = 16 + 11 = 16 + 8 + 2 + 1$

$87^{27} = 87^{16} \cdot 87^{8} \cdot 87^{2} \cdot 87$

d.h. $87^{27} \mod 103 = \left((87^{16} \mod 103) \cdot (87^{8} \mod 103) \cdot (87^{2} \mod 103) \cdot (87 \mod 103) \right) \mod 103$

$87 \underset{103}{\equiv} -16$

$87^2 \underset{103}{\equiv} (-16)^2 = 256 \underset{103}{\equiv} 50$

$87^4 = (87^2)^2 \underset{103}{\equiv} 50^2 \underset{103}{\equiv} 28$

$87^8 = (87^4)^2 \underset{103}{\equiv} 28^2 \underset{103}{\equiv} 63$

$87^{16} = (87^8)^2 \underset{103}{\equiv} 63^2 \underset{103}{\equiv} 55$

$87^{27} \mod 103 = (55 \cdot 63 \cdot 50 \cdot 87) \mod 103$
$= 39$

(b) Berechnen Sie $87^{43} \mod 103$.

$43 = 32 + 11 = 32 + 8 + 2 + 1$

$87^{32} = (87^{16})^2 \underset{103}{\equiv} 55^2 \underset{103}{\equiv} 38$

$87^{43} \mod 103 = (38 \cdot 63 \cdot 50 \cdot 87) \mod 103$
$= 85$