DM 07-B (HA) zum 07.11.2012

Paul Bienkowski, Jascha Andersen, Benedikt Bushart

5. Dezember 2012

1. a) Die Zahl 473 ist in $\mathbb{Z}_{2413}$ invertierbar, da 473 und 2413 teilerfremd sind. Es gilt:
$ggT(2413, 473) = 1$

$$\begin{array}{rcrcrcl} 2413 & = & 473 & \cdot & 5 & + & 48 \\ 473 & = & 48 & \cdot & 9 & + & 41 \\ 48 & = & 41 & \cdot & 1 & + & 7 \\ 41 & = & 7 & \cdot & 5 & + & 6 \\ 7 & = & 6 & \cdot & 1 & + & 1 \end{array}$$

Durch Rückwärtseinsetzen lässt sich das Inverse ermitteln:

$$\begin{array}{rcllcl} 1 & = & 7 - 6 \cdot 1 & & & \\ & = & 7 - (41 - 7 \cdot 5) & & = & 6 \cdot 7 - 41 \\ & = & 6 \cdot (48 - 41 \cdot 1) - 41 & & = & 6 \cdot 48 - 7 \cdot 41 \\ & = & 6 \cdot 48 - 7 \cdot (473 - 48 \cdot 9) & & = & 69 \cdot 48 - 7 \cdot 473 \\ & = & 69 \cdot (2413 - 473 \cdot 5) - 7 \cdot 473 & & = & \underbrace{-352 \cdot 473} + 69 \cdot 2413 \end{array}$$

Es lässt sich ablesen, dass $-352 \cdot 473 \equiv 1 \pmod{2413}$ gilt. Dies lässt sich umformen zu

$$-352 \cdot 473 \equiv 2061 \cdot 473 \equiv 1 \pmod{2413}$$

Also ist 2061 das Multiplikative Inverse von 473 in $\mathbb{Z}_{2413}$.

b) Die Zahl 1672 ist in $\mathbb{Z}_{2413}$ nicht invertierbar, da 19 ein gemeinsamer Teiler ist.
$ggT(2413, 1672) = 19$

$$\begin{array}{rcrcrcl} 2413 & = & 1672 & \cdot & 1 & + & 741 \\ 1672 & = & 741 & \cdot & 2 & + & 190 \\ 741 & = & 190 & \cdot & 3 & + & 171 \\ 190 & = & 171 & \cdot & 1 & + & 19 \\ 171 & = & 19 & \cdot & 9 & + & 0 \end{array}$$

c) Da $2412 \equiv -1 \pmod{2413}$ gilt, ist 2412 sein eigenes Inverses in $\mathbb{Z}_{2413}$:

$$2412 \cdot 2412 = (-1) \cdot (-1) = 1 \qquad (\text{in } \mathbb{Z}_{2413})$$

2. Nach dem Satz von Fermat gilt $3^{18} = 1$ in $\mathbb{Z}_{19}$. Damit lässt sich ermitteln:

$$3^{1000} = (3^{18})^{55} \cdot 3^{10} = 1^{55} \cdot 3^{10} = 3 \cdot (3^3)^3 = 3 \cdot 8^3 = 16 \qquad (\text{in } \mathbb{Z}_{19})$$

3. a) $\pi = (1, 7, 6)(2, 10, 8, 5, 11, 13)(3, 4)(9, 12)$

b) $\pi = (1, 6) \circ (1, 7) \circ (2, 12) \circ (2, 11) \circ (2, 5) \circ (2, 8) \circ (2, 10) \circ (3, 4) \circ (9, 12)$

c) $\operatorname{sign} \pi = -1$ (ungerade)

4. a) Es gibt 3 Möglichkeiten, das erste Element des Tupels (mit Elementen aus A) zu belegen, dazu jeweils 5 Möglichkeiten für das zweite und 2 Möglichkeiten für das dritte Element. Da es auf die Reihenfolge der Elemente ankommt, gilt die Multiplikationsregel:

$$3 \cdot 5 \cdot 2 = 30$$

b) Eine ternäre Relation wird immer aus 3 Mengen gebildet. Da 3 Mengen zur Auswahl stehen, es auf die Reihenfolge der Mengen im kartesischen Produkt ankommt, und eine Menge auch mehrfach verwendet werden darf (z.B. $A \times A \times B$), gilt für die Anzahl der möglichen Relationen (nach dem Prinzip „ziehen mit Zurücklegen, geordnet"):

$$3^3 = 27$$

Hier sind auch Relationen einbezogen, in denen eine Menge mehrfach vorkommt, und somit mindestens eine der Mengen A, B und C nicht vorkommt. Man könnte demnach argumentieren, dies sei keine Relation über die drei Mengen. Um diese Möglichkeiten auszuschließen, muss das Prinzip „ziehen ohne Zurücklegen, geordnet" gewählt werden. Dann gilt:

$$3^{\underline{3}} = 3! = 3 \cdot 2 \cdot 1 = 6$$