Aufgabe 3, Übungsblatt 2, Der Satz von Wilson

Ulrich Görtz

Lineare Algebra 1, WS 20/21

UNIVERSITÄT
DUISBURG
ESSEN

Sei p eine Primzahl. Zeigen Sie: Es existiert $k \in \mathbb{Z}$ mit

$$(p-1)! = kp - 1.$$

Äquivalent:
$(p-1)! + 1$ wird von p geteilt.

Notation: $a \in \mathbb{N}$

"a Fakultät" $a! := \prod_{i=1}^{a} i = 1 \cdot 2 \cdot \ldots \cdot a$

$0! := 1$
$1! = 1$
$2! = 1 \cdot 2 = 2$
$3! = 1 \cdot 2 \cdot 3 = 2! \cdot 3 = 6$
$4! = 24$
$\vdots$

$p = 2$: $(p-1)! + 1 = 2$ ✓
$p = 3$: $= 3$ ✓
$p = 5$: $= 25$ ✓

Übersetzung in Aussage über endlichen Körper $\mathbb{F}_p$:

$(p-1)!+1$ wird von p geteilt

$$(p-1)! + 1 = 0 \quad \text{in } \mathbb{F}_p$$

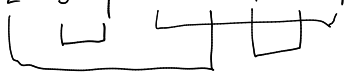
mit anderen Worten: $\bar{1} \cdot \bar{2} \cdot \bar{3} \cdot \ldots \cdot \overline{(p-1)} + \bar{1} = \bar{0}$ in $\mathbb{F}_p$

Äquivalent: $1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) = -1$ in $\mathbb{F}_p$

Beispiel $p = 11$.

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 = -1 = 10$$

$$\Leftrightarrow \quad 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 = 1 \quad \checkmark$$



zz: $1 \cdot 2 \cdot \ldots \cdot (p-1) = -1$ in $\mathbb{F}_p$, äquivalent: $2 \cdot \ldots \cdot (p-2) = 1$

(Hier und im folgenden sei $p > 2$.)

Idee: Fasse die Faktoren im Produkt auf der linken Seite zu Paaren a, a^{-1}

Dann: Das Produkt hat $p-3$ Faktoren, also eine gerade Zahl.

Müssen ausschließen: $a = a^{-1}$ für a Faktor im Produkt $2 \cdot \ldots \cdot (p-2)$.

In jedem Körper gilt ($a \neq 0$)

$$a = a^{-1} \iff a^2 = 1 \iff a^2 - 1 = 0$$
$$\iff (a-1)(a+1) = 0 \iff a-1 = 0 \text{ oder } a+1 = 0$$
$$\iff a = 1 \text{ oder } a = -1.$$

In dem Produkt $2 \cdot \ldots \cdot (p-2)$ in $\mathbb{F}_p$ haben also alle Faktoren a die Eigenschaft $a \neq a^{-1}$.

Wir finden also Elemente $a_1, a_2, \dots, a_{\frac{p-3}{2}} \in \mathbb{F}_p$,

so dass $\mathbb{F}_p = \{0, 1, -1, a_1, a_1^{-1}, a_2, a_2^{-1}, \dots, a_{\frac{p-3}{2}}, a_{\frac{p-3}{2}}^{-1}\}$

($-1 = p-1$)

Dann gilt $2 \cdot \dots \cdot (p-2) = \prod_{\substack{a \in \mathbb{F}_p \\ a \neq 0,1,-1}} a = a_1 a_1^{-1} \cdot a_2 a_2^{-1} \cdot \dots \cdot a_{\frac{p-3}{2}} a_{\frac{p-3}{2}}^{-1} = 1.$