Beweis des kleinen Fermatschen Satzes für $\mathbb{Z}/pq\mathbb{Z}$.

In $\mathbb{Z}/n\mathbb{Z}$ bedeutet $[a] = [r]$, dass es ein ganzzahliges k gibt, sodass $a = kn + r$ ist. Das sollte man stets im Hinterkopf behalten.

Wir nehmen uns ein x, **das weder durch p noch durch q teilbar ist**. Jetzt müssen wir zeigen, dass $[x]^{(p-1)(q-1)} = [1]$ gilt, und zwar in $\mathbb{Z}/pq\mathbb{Z}$, d. h. wir müssen zeigen, dass es ein ganzzahliges k gibt, sodass

$$x^{(p-1)(q-1)} = kpq + 1$$

ist. Dafür reicht es zu zeigen, dass pq die Zahl $x^{(p-1)(q-1)} - 1$ teilt[1]. Dafür wiederum reicht es zu zeigen, ...

1. ... dass p die Zahl $x^{(p-1)(q-1)} - 1$ teilt und ...
2. ... dass auch q die Zahl $x^{(p-1)(q-1)} - 1$ teilt.

Warum teilt das Produkt pq dann automatisch schon die Zahl $x^{(p-1)(q-1)} - 1$?[2]

1. **Weil x nicht durch p teilbar sein soll**, können wir das zweite Lemma anwenden, d.h.

   $$\left[x^{p-1}\right] = [1] \text{ in } \mathbb{Z}/p\mathbb{Z} \qquad \text{d.h. es gibt ein ganzzahliges } k_1, \text{ sodass } x^{p-1} = k_1 p + 1$$

   Das bedeutet, dass p die Zahl d.h. $x^{p-1} - 1$ teilt[3]. Wir müssen aber zeigen, dass p die Zahl $x^{(p-1)(q-1)} - 1$ teilt. Weiter geht's also:

   Es ist $x^{(p-1)(q-1)} - 1 = \left(x^{p-1}\right)^{q-1} - 1$. Mit dem Teleskopsummentrick[4] (also doch, Julius!) zeigt man, dass

   $$x^{(p-1)(q-1)} - 1 = \left(x^{p-1}\right)^{q-1} - 1 = \left(\left(x^{p-1}\right)^{q-1-1} + \left(x^{p-1}\right)^{q-1-2} + \ldots + \left(x^{p-1}\right) + 1\right)\left(x^{p-1} - 1\right)$$

   Das zeigt, dass p die Zahl $x^{(p-1)(q-1)} - 1$ teilt (Warum?).

2. **Weil x nicht durch q teilbar sein soll**, ...

   ... [könnt ihr euch selber denken] ...

   Das zeigt, dass q die Zahl $x^{(p-1)(q-1)} - 1$ teilt.

---

[1] Dann kann man nämlich das ganzzahlige(!) $k = \left(x^{(p-1)(q-1)} - 1\right)/pq$ wählen

[2] Hinweis: eindeutige Primfaktorzerlegung und $p \neq q$ sind *verschiedene(!)* Primzahlen. Ggf. nochmals Aufgabe 4(a) aus der vorletzten Stunde anschauen.

[3] nach Division kommt die ganze Zahl k_1 raus

[4] Es gilt $z^e - 1 = \left(z^{e-1} + z^{e-2} + \ldots + z + 1\right)(z - 1)$. Bei uns sind $z = x^{p-1}$ und $e = q - 1$.