Eine Kürzungsregel für Kongruenzgleichungen:

> Für $b, c, d \in \mathbb{Z}$, $n \in \mathbb{N}$ mit $c \neq 0$ und $\mathrm{ggT}(c, n) = 1$ gilt
> $$bc \equiv dc \mod n \iff b \equiv d \mod n$$

Beweis:

$$bc \equiv dc \mod n \iff \exists k \in \mathbb{Z} : bc = dc + kn \iff \exists k \in \mathbb{Z} : b = d + \frac{kn}{c}$$

Weil b und d ganze Zahlen sind, muss auch $\frac{kn}{c}$ eine ganze Zahl sein.
Dazu muss aber, weil c und n teilerfremd sind, k ein Vielfaches von c sein, d.h. es muss eine ganze Zahl k' mit $k = k' \cdot c$ existieren. Dann ist $\frac{k}{c} = k'$. Also

$$\begin{aligned} bc \equiv dc \mod n &\iff \exists k \in \mathbb{Z} : bc = dc + kn \iff \exists k \in \mathbb{Z} : b = d + \frac{kn}{c} \\ &\iff \exists k' \in \mathbb{Z} : b = d + k'n \iff b \equiv d \mod n \end{aligned}$$

q.e.d.

Übung: Löse die Kongruenzen a) $45x \equiv 15 \mod 4$, b) $27x \equiv 18 \mod 5$.

Der kleine Satz von Fermat

> Für jede Primzahl p und alle $a \in \mathbb{Z}$ gilt: $a^p \equiv a \mod p$.

Falls a kein Vielfaches von p ist, (dann ist a auch nicht 0), können wir die Kürzungsregel anwenden und die zweite Formulierung des kleinen Satzes von Fermat ableiten:

> Für jede Primzahl p und alle $a \in \mathbb{Z}$, die nicht Vielfaches von p sind, gilt: $a^{p-1} \equiv 1 \mod p$.

Für kleine Primzahlen p kann man den kleinen Satz von Fermat durch Aufstellen von "Restetabellen" für das Teilen von Potenzen von a durch p überprüfen. Damit fangen wir an und stellen uns Tabellen für $p = 2, 3, 5, 7, 11$ auf.

$p = 2$:

$a \mod 2$	0	1
$a^2 \mod 2$	0	1

$p = 3$:

$a \mod 3$	0	1	2
$a^2 \mod 3$	0	1	1
$a^3 \mod 3$	0	1	2

$p = 5$:

$a \mod 5$	0	1	2	3	4
$a^2 \mod 5$	0	1	4	4	1
$a^4 \mod 5$	0	1	1	1	1
$a^5 \mod 5$	0	1	2	3	4

$p = 7$:

$a \mod 7$	0	1	2	3	4	5	6
$a^2 \mod 7$	0	1	4	2	2	4	1
$a^3 \mod 7$	0	1					1
$a^6 \mod 7$	0	1	1	1	1	1	1
$a^7 \mod 7$	0	1	2	3	4	5	6

$\boxed{p = 11:}$

$a \mod 11$	0	1	2	3	4	5	6	7	8	9	10
$a^2 \mod 11$	0	1	4	9	5	3	3	5	9	1	1
$a^4 \mod 11$	0	1									1
$a^5 \mod 11$	0	1									1
$a^{10} \mod 11$	0	1	1	1	1	1	1	1	1	1	1
$a^{11} \mod 11$	0	1	2	3	4	5	6	7	8	9	10

Wie man sieht, ist der kleine Satz von Fermat zumindest für die ersten Primzahlen richtig. Das ist natürlich kein Beweis für alle Primzahlen p. Obwohl erst Euler den ersten Beweis angegeben hat, kennt man heute mehrere Möglichkeiten diesen Satz zu beweisen. Wir wollen eine davon kennenlernen. Wir beginnen mit einem Hilfssatz.

Hilfssatz: Es sei p eine Primzahl und a eine ganze Zahl, die kein Vielfaches von p ist. Dann lassen die ersten $(p-1)$ Vielfachen von a, d. h. die Zahlen $a, 2a, 3a, \ldots, (p-1)a$ beim Teilen durch p jeden der Reste $1, 2, 3, \ldots, p-1$ genau einmal.

Ehe wir diesen Hilfssatz beweisen,sehen uns an, was bei $p = 5$ und $p = 7$ passiert.

$\boxed{p = 5:}$

$a \mod 5$	1	**2**	3	**4**
$2a \mod 5$	2	**4**	1	**3**
$3a \mod 5$	3	**1**	4	**2**
$4a \mod 5$	4	**3**	2	**1**

$\boxed{p = 7:}$

$a \mod 7$	1	**2**	3	**4**	5	**6**
$2a \mod 7$	2	**4**	6	**1**	3	**5**
$3a \mod 7$	3	**6**		**5**		**4**
$4a \mod 7$	4	**1**		**2**		**3**
$5a \mod 7$	5	**3**		**6**		**2**
$6a \mod 7$	6	**5**	4	**3**	2	**1**

In jeder Spalte kommen alle Reste von 1 bis 4 bzw. von 1 bis 6 genau einmal vor. Das Produkt in jeder Spalte ist immer gleich, nämlich $1 \cdot 2 \cdot 3 \cdot 4 = 4!$ für $p = 5$ bzw. $6!$ für $p = 7$.

Beweis des Hilfssatzes:
Es genügt zu zeigen, dass es unter den Vielfachen $a, 2a, 3a, \ldots, (p-1)a$ von a keine zwei verschiedenen gibt, die beim Teilen durch p den gleichen Rest lassen.
Wir beweisen dies indirekt, d.h. wir nehmen an, es gebe doch zwei solche Vielfache von a mit dem gleichen Rest und führen das zum Widerspruch.
Angenommen, es ist $1 \leq i < j \leq (p-1)$ und $i \cdot a$ und $j \cdot a$ lassen den gleichen Rest beim Teilen durch p. Dann folgt

$$(j-i)a \equiv 0 \mod p \iff \exists k \in \mathbb{Z} : (j-i)a = kp \iff \exists k \in \mathbb{Z} : \frac{(j-i)a}{p} = k$$

Da a und p teilerfremd sind, muss dann $j - i$ ein Vielfaches von p sein. Das ist aber nach unseren Voraussetzungen nicht möglich, also war die Annahme falsch[2]. q.e.d.

[2]Man könnte genausogut die Kürzungsregel anwenden.Da a und p teilerfremd sind, kann ich $(j-i)a \equiv 0 \mod p$ durch a kürzen. Und $(j-i) \equiv 0 \mod p$ ist falsch.