Elementare Zahlentheorie

P. Amrein, A. Lägeler, M. Schwagenscheidt

ETH Zürich D-MATH / Ubique Innovation AG

Studienwoche ETH 2022

8. Juni 2022

Der Fundamentalsatz der Arithmetik

Seien a, b zwei ganze Zahlen. Wir sagen, dass "a die Zahl b teilt", wenn eine ganze Zahl c existiert, so dass

$$b = ac.$$

Wir schreiben $a|b$ für "a teilt b".

Der Fundamentalsatz der Arithmetik

Seien a, b zwei ganze Zahlen. Wir sagen, dass "a die Zahl b teilt", wenn eine ganze Zahl c existiert, so dass

$$b = ac.$$

Wir schreiben $a|b$ für "a teilt b".

Eine Primzahl $p \geq 2$ ist eine ganze Zahl, die nur von 1 und p geteilt wird.

Der Fundamentalsatz der Arithmetik

Seien a, b zwei ganze Zahlen. Wir sagen, dass "a die Zahl b teilt", wenn eine ganze Zahl c existiert, so dass

$$b = ac.$$

Wir schreiben $a|b$ für "a teilt b".

Eine Primzahl $p \geq 2$ ist eine ganze Zahl, die nur von 1 und p geteilt wird. In abstrakter Notation schreiben wir:

$$a|p \Rightarrow a = 1 \text{ oder } a = p$$

für alle $a \in \mathbb{Z}$ und $a \geq 1$ ($\mathbb{Z}$: die Menge der ganzen Zahlen, also $..., -2, -1, 0, 1, 2, ...$).

Der Fundamentalsatz der Arithmetik

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20

Der Fundamentalsatz der Arithmetik

~~1~~	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20

Der Fundamentalsatz der Arithmetik

~~1~~	2	3	~~4~~	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20

Die Zahl 4 kann keine Primzahl sein, da sie von 2 geteilt wird.

Der Fundamentalsatz der Arithmetik

~~1~~	2	3	~~4~~	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20

Die Zahl 4 kann keine Primzahl sein, da sie von 2 geteilt wird. Genauso können wir alle Mehrfachen von 2 streichen.

Der Fundamentalsatz der Arithmetik

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~
11	~~12~~	13	~~14~~	15	~~16~~	17	~~18~~	19	~~20~~

Die Zahl 4 kann keine Primzahl sein, da sie von 2 geteilt wird. Genauso können wir alle Mehrfachen von 2 streichen.

Der Fundamentalsatz der Arithmetik

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~
11	~~12~~	13	~~14~~	15	~~16~~	17	~~18~~	19	~~20~~

Da 2 nur von 1 und 2 geteilt wird, ist 2 sicherlich eine Primzahl! Die Zahl 3 ist ebenfalls keine Primzahl, da sie von keiner kleineren Zahl geteilt wird (ansonsten wäre sie durchgestrichen).

Der Fundamentalsatz der Arithmetik

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~
11	~~12~~	13	~~14~~	15	~~16~~	17	~~18~~	19	~~20~~

Der Fundamentalsatz der Arithmetik

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~
11	~~12~~	13	~~14~~	15	~~16~~	17	~~18~~	19	~~20~~

Wir können nun ebenfalls die Mehrfachen von 3 streichen, da das sicherlich keine Primzahlen sind.

Der Fundamentalsatz der Arithmetik

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~

Wir können nun ebenfalls die Mehrfachen von 3 streichen, da das sicherlich keine Primzahlen sind.

Der Fundamentalsatz der Arithmetik

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~

Diese Methode ist als *Sieb des Erathostenes* bekannt und liefert einen Algorithmus, um alle Primzahlen zwischen 1 und $n \geq 1$ zu finden.

Der Fundamentalsatz der Arithmetik

Jede ganze Zahl a kann eindeutig als Produkt von Primzahlen geschrieben werden:

Theorem 1 (Fundamentalsatz der Arithmetik)

Sei $a \in \mathbb{Z}$ und $a > 1$. Dann existieren eindeutige $n \geq 1$, $k_1, ..., k_n \geq 1$ und Primzahlen $p_1 < p_2 < ... < p_n$, so dass

$$a = p_1^{k_1} p_2^{k_2} \cdot p_n^{k_n}.$$

Der Fundamentalsatz der Arithmetik

Jede ganze Zahl a kann eindeutig als Produkt von Primzahlen geschrieben werden:

Theorem 1 (Fundamentalsatz der Arithmetik)

Sei $a \in \mathbb{Z}$ und $a > 1$. Dann existieren eindeutige $n \geq 1$, $k_1, ..., k_n \geq 1$ und Primzahlen $p_1 < p_2 < ... < p_n$, so dass

$$a = p_1^{k_1} p_2^{k_2} \cdot p_n^{k_n}.$$

Existenz: Jede Zahl $a > 1$ hat eine Primfaktorisierung.
Eindeutig: Eine Zahl a kann nicht zwei verschiedene Primfaktorisierungen haben.

Fundamentalsatz der Arithmetik

Beispiel für eine Primfaktorisierung:

$$4200 = 2^3 \cdot 3 \cdot 5^2 \cdot 7.$$

Aufgabe: Wie viele Teiler hat die Zahl 4200?

Fundamentalsatz der Arithmetik

Beispiel für eine Primfaktorisierung:

$$4200 = 2^3 \cdot 3 \cdot 5^2 \cdot 7.$$

Aufgabe: Wie viele Teiler hat die Zahl 4200?

Die Anzahl Teiler einer Zahl $a = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$ ergeben sich direkt aus den Exponenten der Primfaktorisierung! Jeder Teiler von a hat nämlich die Form $p_1^{l_1} p_2^{l_2} \cdots p_n^{l_n}$ mit $0 \leq l_i \leq k_i$ für $i = 1, 2, ..., n$.

Fundamentalsatz der Arithmetik

Beispiel für eine Primfaktorisierung:

$$4200 = 2^3 \cdot 3 \cdot 5^2 \cdot 7.$$

Aufgabe: Wie viele Teiler hat die Zahl 4200?

Die Anzahl Teiler einer Zahl $a = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$ ergeben sich direkt aus den Exponenten der Primfaktorisierung! Jeder Teiler von a hat nämlich die Form $p_1^{l_1} p_2^{l_2} \cdots p_n^{l_n}$ mit $0 \leq l_i \leq k_i$ für $i = 1, 2, ..., n$.

Z.B. sind $2^2 \cdot 3 = 12$ und $2 \cdot 3 \cdot 5 \cdot 7 = 210$ Teiler von 4200.

Fundamentalsatz der Arithmetik

Beispiel für eine Primfaktorisierung:

$$4200 = 2^3 \cdot 3 \cdot 5^2 \cdot 7.$$

Aufgabe: Wie viele Teiler hat die Zahl 4200?

Die Anzahl Teiler einer Zahl $a = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$ ergeben sich direkt aus den Exponenten der Primfaktorisierung! Jeder Teiler von a hat nämlich die Form $p_1^{l_1} p_2^{l_2} \cdots p_n^{l_n}$ mit $0 \leq l_i \leq k_i$ für $i = 1, 2, ..., n$.

Z.B. sind $2^2 \cdot 3 = 12$ und $2 \cdot 3 \cdot 5 \cdot 7 = 210$ Teiler von 4200.

Insgesamt hat $a = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$ also $(k_1 + 1)(k_2 + 1) \cdots (k_n + 1)$ Teiler. Für $a = 4200$ sind das

$$(3 + 1) \cdot (1 + 1) \cdot (2 + 1) \cdot (1 + 1) = 48$$

Teiler.

Der euklische Algorithmus

Seien $a, b \geq 1$ zwei ganze Zahlen. Der *grösster gemeinsame Teiler* $d = \mathrm{ggT}(a, b)$ ist die grösste Zahl $d \geq 1$, so dass $d|a$ und $d|b$ gilt.

Der euklische Algorithmus

Seien $a, b \geq 1$ zwei ganze Zahlen. Der *grösster gemeinsame Teiler* $d = \mathrm{ggT}(a, b)$ ist die grösste Zahl $d \geq 1$, so dass $d|a$ und $d|b$ gilt.

Wenn wir die Primfaktorisierungen von $a = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$ und $b = q_1^{r_1} q_2^{r_2} \cdots q_m^{r_m}$ kennen, ist es einfach den ggT zu finden: Nehme alle Primzahlen p, die in beiden Primfaktorisierungen vorkommen mit dem kleineren der beiden Exponenten.

Der euklische Algorithmus

Seien $a, b \geq 1$ zwei ganze Zahlen. Der *grösster gemeinsame Teiler* $d = \mathrm{ggT}(a, b)$ ist die grösste Zahl $d \geq 1$, so dass $d|a$ und $d|b$ gilt.

Wenn wir die Primfaktorisierungen von $a = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$ und $b = q_1^{r_1} q_2^{r_2} \cdots q_m^{r_m}$ kennen, ist es einfach den ggT zu finden: Nehme alle Primzahlen p, die in beiden Primfaktorisierungen vorkommen mit dem kleineren der beiden Exponenten.

Beispiel: Wir wollen den ggT von $4200 = 2^3 \cdot 3 \cdot 5^2 \cdot 7$ und $10780 = 2^2 \cdot 5 \cdot 7 \cdot 11$ finden. Dann ist

$$\mathrm{ggT}(4200, 10780) = 2^2 \cdot 5 \cdot 7 = 140.$$

Der euklische Algorithmus

Seien $a, b \geq 1$ zwei ganze Zahlen. Der *grösster gemeinsame Teiler* $d = \mathrm{ggT}(a, b)$ ist die grösste Zahl $d \geq 1$, so dass $d|a$ und $d|b$ gilt.

Wenn wir die Primfaktorisierungen von $a = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$ und $b = q_1^{r_1} q_2^{r_2} \cdots q_m^{r_m}$ kennen, ist es einfach den ggT zu finden: Nehme alle Primzahlen p, die in beiden Primfaktorisierungen vorkommen mit dem kleineren der beiden Exponenten.

Beispiel: Wir wollen den ggT von $4200 = 2^3 \cdot 3 \cdot 5^2 \cdot 7$ und $10780 = 2^2 \cdot 5 \cdot 7 \cdot 11$ finden. Dann ist

$$\mathrm{ggT}(4200, 10780) = 2^2 \cdot 5 \cdot 7 = 140.$$

Problem: Wenn a und b sehr gross sind, dann ist es sehr aufwändig die Primfaktorisierung von a und b zu berechnen!

Euklidische Division

Seien n und q eine ganze Zahlen. In der Schule haben wir womöglich die Division mit Rest gelernt. In abstrakter Sprache heisst das: Es gibt ganze Zahlen a, r mit $0 \leq r < |q|$, so dass

$$n = a \cdot q + r.$$

Beispiel: Sei $n = 23$ und $q = -12$. Dann ist

$$23 = -1 \cdot (-12) + 11,$$

das heisst $a = -1$ und $r = 11$ sind die gesuchten Zahlen.

Euklidische Division

Seien n und q eine ganze Zahlen. In der Schule haben wir womöglich die Division mit Rest gelernt. In abstrakter Sprache heisst das: Es gibt ganze Zahlen a, r mit $0 \leq r < |q|$, so dass

$$n = a \cdot q + r.$$

Beispiel: Sei $n = 23$ und $q = -12$. Dann ist

$$23 = -1 \cdot (-12) + 11,$$

das heisst $a = -1$ und $r = 11$ sind die gesuchten Zahlen.

Aufgabe: Beweise die euklidische Division!

Euklidische Division

Algorithmus für $\mathrm{ggT}(a, b)$ mit $a > b$:

1. Schreibe $a = q \cdot b + r$ mit $q \in \mathbb{Z}$ und $0 \leq r < b$.
2. $a \leftarrow b$ und $b \leftarrow r$.
3. Wiederhole das so lange, bis $r \mid b$.
4. Dann ist $r = \mathrm{ggT}(a, b)$.

Euklidische Division

Beispiel: Wir berechnen $\mathrm{ggT}(1547, 560)$.

$$\begin{aligned} 1547 &= 2 \cdot 560 + 427, \\ 560 &= 1 \cdot 427 + 133, \\ 427 &= 3 \cdot 133 + 28, \\ 133 &= 4 \cdot 28 + 21, \\ 28 &= 1 \cdot 21 + 7. \end{aligned}$$

Wir bemerken, dass $7|21$, also sind wir fertig. Die Lösung ist $7 = \mathrm{ggT}(1547, 560)$.
Aufgabe: Implementiere diesen Algorithmus!

ggT

Eigenschaften des ggT:

1. Für eine Primzahl p gilt $\mathrm{ggT}(a, p) = 1 \text{ oder } p$.
2. Es gibt ganze Zahlen u, v, so dass $u \cdot a + v \cdot b = \mathrm{ggT}(a, b)$.

Die Zahlen u, v erhalten wir, wenn wir den euklidischen Algorithmus rückwärts anwenden!

ggT

Wir illustrieren das wieder an unserem Beispiel $7 = \mathrm{ggT}(1547, 560)$.
Vorhin hatten wir:

$$\begin{aligned} 1547 &= 2 \cdot 560 + 427, \; 560 = 1 \cdot 427 + 133, \\ 427 &= 3 \cdot 133 + 28, \; 133 = 4 \cdot 28 + 21, \\ 28 &= 1 \cdot 21 + 7. \end{aligned}$$

Rückwärts:

$$\begin{aligned} 7 &= 28 - 1 \cdot 21 = 28 - 1 \cdot (133 - 4 \cdot 28) \\ &= 5 \cdot 28 - 1 \cdot 133 = 5 \cdot (427 - 3 \cdot 133) - 1 \cdot 133 \\ &= 5 \cdot 427 - 16 \cdot 133 = 5 \cdot 427 - 16 \cdot (560 - 1 \cdot 427) \\ &= 21 \cdot 427 - 16 \cdot 560 = 21 \cdot (1547 - 2 \cdot 560) - 15 \cdot 560 \\ &= 21 \cdot 1547 - 58 \cdot 560. \end{aligned}$$

Eulersche φ-Funktion

Für eine ganze Zahl $n \geq 1$, sei $\varphi(n)$ die Anzahl Zahlen $1 \leq b < n$, so dass $\mathrm{ggT}(b, n) = 1$ gilt. In abstrakter Notation:

$$\varphi(n) := |\{1 \leq b < n : \mathrm{ggT}(b, n) = 1\}| .$$

Beispiele: $\varphi(1) = 1$ und für eine Primzahl p gilt $\varphi(p) = p - 1$.

Aufagbe: Finde $\varphi(p^k)$ für ein $k > 1$.

Kongruenzen

Kongruenzen

Zwei ganze Zahlen a, b heissen "kongruent modulo m", falls $m|(a-b)$. Wir schreiben

$$a \equiv b \pmod{m}.$$

Kongruenzen

Zwei ganze Zahlen a, b heissen "kongruent modulo m", falls $m|(a-b)$. Wir schreiben

$$a \equiv b \pmod{m}.$$

Falls $a \equiv b \pmod{m}$, so ist $a = b + k \cdot m$ für ein $k \in \mathbb{Z}$.

Kongruenzen

Zwei ganze Zahlen a, b heissen "kongruent modulo m", falls $m|(a-b)$. Wir schreiben

$$a \equiv b \pmod{m}.$$

Falls $a \equiv b \pmod{m}$, so ist $a = b + k \cdot m$ für ein $k \in \mathbb{Z}$.

Beispiel: $160 \equiv 21 \pmod{139}$ oder $64 \equiv 2 \pmod{31}$.

Kongruenzen

Für jede ganze Zahl $a \in \mathbb{Z}$ gibt es ein $b = 0, 1, 2, ..., m-1$, so dass

$$a \equiv b \pmod{m}$$

(Euklidische Division!). Wir bezeichnen die Menge $\{0, 1, 2, ..., m-1\}$ mit $\mathbb{Z}/m\mathbb{Z}$.

Kongruenzen

Für jede ganze Zahl $a \in \mathbb{Z}$ gibt es ein $b = 0, 1, 2, ..., m-1$, so dass

$$a \equiv b \pmod{m}$$

(Euklidische Division!). Wir bezeichnen die Menge $\{0, 1, 2, ..., m-1\}$ mit $\mathbb{Z}/m\mathbb{Z}$.

Wir können auf $\mathbb{Z}/m\mathbb{Z}$ die Addition definieren, nämlich wenn $a_1, a_2 \in \mathbb{Z}/m\mathbb{Z}$, dann wählen wir $b \in \mathbb{Z}/m\mathbb{Z}$, so dass $a_1 + a_2 \equiv b \pmod{m}$. Also ist $a_1 + a_2$ gleich b in $\mathbb{Z}/m\mathbb{Z}$.

Kongruenzen

Für jede ganze Zahl $a \in \mathbb{Z}$ gibt es ein $b = 0, 1, 2, ..., m-1$, so dass

$$a \equiv b \pmod{m}$$

(Euklidische Division!). Wir bezeichnen die Menge $\{0, 1, 2, ..., m-1\}$ mit $\mathbb{Z}/m\mathbb{Z}$.

Wir können auf $\mathbb{Z}/m\mathbb{Z}$ die Addition definieren, nämlich wenn $a_1, a_2 \in \mathbb{Z}/m\mathbb{Z}$, dann wählen wir $b \in \mathbb{Z}/m\mathbb{Z}$, so dass $a_1 + a_2 \equiv b \pmod{m}$. Also ist $a_1 + a_2$ gleich b in $\mathbb{Z}/m\mathbb{Z}$.

Genauso können wir Subtraktion und Multiplikation auf $\mathbb{Z}/m\mathbb{Z}$ definieren, z.B. $a_1 \cdot a_2 \equiv b \pmod{m}$ für ein $b \in \mathbb{Z}/m\mathbb{Z}$.

Kongruenzen

Für jede ganze Zahl $a \in \mathbb{Z}$ gibt es ein $b = 0, 1, 2, ..., m-1$, so dass

$$a \equiv b \pmod{m}$$

(Euklidische Division!). Wir bezeichnen die Menge $\{0, 1, 2, ..., m-1\}$ mit $\mathbb{Z}/m\mathbb{Z}$.

Wir können auf $\mathbb{Z}/m\mathbb{Z}$ die Addition definieren, nämlich wenn $a_1, a_2 \in \mathbb{Z}/m\mathbb{Z}$, dann wählen wir $b \in \mathbb{Z}/m\mathbb{Z}$, so dass $a_1 + a_2 \equiv b \pmod{m}$. Also ist $a_1 + a_2$ gleich b in $\mathbb{Z}/m\mathbb{Z}$.

Genauso können wir Subtraktion und Multiplikation auf $\mathbb{Z}/m\mathbb{Z}$ definieren, z.B. $a_1 \cdot a_2 \equiv b \pmod{m}$ für ein $b \in \mathbb{Z}/m\mathbb{Z}$.

Was ist mit der Division?

Kongruenzen

Aufgabe: Zeige, dass für jedes $a \in \mathbb{Z}/m\mathbb{Z}$ ein $b \in \mathbb{Z}/m\mathbb{Z}$ existiert, so dass $a \cdot b \equiv \mathrm{ggT}(a, m) \pmod{m}$.

Kongruenzen

Aufgabe: Zeige, dass für jedes $a \in \mathbb{Z}/m\mathbb{Z}$ ein $b \in \mathbb{Z}/m\mathbb{Z}$ existiert, so dass $a \cdot b \equiv \mathrm{ggT}(a, m) \pmod{m}$.

Lösung: Wir haben gesehen, dass Zahlen $u, v \in \mathbb{Z}$ existieren, so dass $u \cdot a + v \cdot m = \mathrm{ggT}(a, m)$, also

$$u \cdot a \equiv \mathrm{ggT}(a, m) \pmod{m}.$$

Kongruenzen

Aufgabe: Zeige, dass für jedes $a \in \mathbb{Z}/m\mathbb{Z}$ ein $b \in \mathbb{Z}/m\mathbb{Z}$ existiert, so dass $a \cdot b \equiv \mathrm{ggT}(a, m) \pmod{m}$.

Lösung: Wir haben gesehen, dass Zahlen $u, v \in \mathbb{Z}$ existieren, so dass $u \cdot a + v \cdot m = \mathrm{ggT}(a, m)$, also

$$u \cdot a \equiv \mathrm{ggT}(a, m) \pmod{m}.$$

Schreibe $u = k \cdot m + r$ mit $0 \leq r < m$ (Euklidische Division). Dann ist

$$r \cdot a = (u - k \cdot m) \cdot a = u \cdot a - k \cdot m \cdot a \equiv u \cdot a \equiv \mathrm{ggT}(a, m) \pmod{m}$$

Kongruenzen

Falls $m = p$ eine Primzahl ist, dann gilt für alle $a = 1, 2, ..., p-1$, dass $\mathrm{ggT}(a, p) = 1$. Also existiert für jedes $0 \neq a \in \mathbb{Z}/p\mathbb{Z}$ ein "multiplikatives Inverses" $0 \neq \overline{a} \in \mathbb{Z}/p\mathbb{Z}$, so dass

$$a \cdot \overline{a} \equiv 1 \pmod{p}.$$

Kongruenzen

Falls $m = p$ eine Primzahl ist, dann gilt für alle $a = 1, 2, ..., p-1$, dass $\mathrm{ggT}(a, p) = 1$. Also existiert für jedes $0 \neq a \in \mathbb{Z}/p\mathbb{Z}$ ein "multiplikatives Inverses" $0 \neq \overline{a} \in \mathbb{Z}/p\mathbb{Z}$, so dass

$$a \cdot \overline{a} \equiv 1 \pmod{p}.$$

Insbesondere gilt also für $a, b, c \in \mathbb{Z}/p\mathbb{Z}$, dass

$$a \cdot c \equiv b \cdot c \pmod{p} \Rightarrow a \equiv b \pmod{p} \tag{1}$$

(multipliziere beide Seiten mit $\overline{c}$).

Kongruenzen

Falls $m = p$ eine Primzahl ist, dann gilt für alle $a = 1, 2, ..., p-1$, dass $\mathrm{ggT}(a, p) = 1$. Also existiert für jedes $0 \neq a \in \mathbb{Z}/p\mathbb{Z}$ ein "multiplikatives Inverses" $0 \neq \overline{a} \in \mathbb{Z}/p\mathbb{Z}$, so dass

$$a \cdot \overline{a} \equiv 1 \pmod{p}.$$

Insbesondere gilt also für $a, b, c \in \mathbb{Z}/p\mathbb{Z}$, dass

$$a \cdot c \equiv b \cdot c \pmod{p} \Rightarrow a \equiv b \pmod{p} \tag{1}$$

(multipliziere beide Seiten mit $\overline{c}$).
Die Regel (1) stimmt im Allgemeinen nicht, wenn m keine Primzahl ist! Z.B. $m = 6$. Dann ist

$$2 \cdot 4 \equiv 2 \cdot 1 \pmod{6} \text{ und } 4 \not\equiv 1 \pmod{6}.$$

Kongruenzen

Falls $m = p$ eine Primzahl ist, dann gilt für alle $a = 1, 2, ..., p-1$, dass $\mathrm{ggT}(a, p) = 1$. Also existiert für jedes $0 \neq a \in \mathbb{Z}/p\mathbb{Z}$ ein "multiplikatives Inverses" $0 \neq \overline{a} \in \mathbb{Z}/p\mathbb{Z}$, so dass

$$a \cdot \overline{a} \equiv 1 \pmod{p}.$$

Insbesondere gilt also für $a, b, c \in \mathbb{Z}/p\mathbb{Z}$, dass

$$a \cdot c \equiv b \cdot c \pmod{p} \Rightarrow a \equiv b \pmod{p} \tag{1}$$

(multipliziere beide Seiten mit $\overline{c}$).
Die Regel (1) stimmt im Allgemeinen nicht, wenn m keine Primzahl ist! Z.B. $m = 6$. Dann ist

$$2 \cdot 4 \equiv 2 \cdot 1 \pmod{6} \text{ und } 4 \not\equiv 1 \pmod{6}.$$

Aufgabe: Schreibe eine Funktion $\mathrm{inv}(a, p)$, die $\overline{a} \in \mathbb{Z}/p\mathbb{Z}$ ausgibt.

Theorem 2 (Fermat)

Sei p eine Primzahl und $0 \neq a \in \mathbb{Z}/p\mathbb{Z}$. Dann gilt

$$a^{p-1} \equiv 1 \pmod{p}.$$

Beispiel: $3^6 = 729 \equiv 1 \pmod 7$. Der Satz von Fermat kann auch angewendet werden, um hohe Potenzen in $\mathbb{Z}/p\mathbb{Z}$ schnell zu berechnen, etwa:

$$3^{31} = 3^{5\cdot 6+1} = (3^6)^5 \cdot 3 \equiv 3 \pmod 7.$$

Fermats Kleiner Satz

Sei p eine Primzahl und $0 \neq a \in \mathbb{Z}/p\mathbb{Z}$. Wir betrachten die Funktion $f : \{1, 2, ..., p-1\} \to \{1, 2, ..., p-1\}$, die durch $f(x) = a \cdot x \pmod{p}$ definiert ist.

Fermats Kleiner Satz

Sei p eine Primzahl und $0 \neq a \in \mathbb{Z}/p\mathbb{Z}$. Wir betrachten die Funktion $f : \{1, 2, ..., p-1\} \to \{1, 2, ..., p-1\}$, die durch $f(x) = a \cdot x \pmod{p}$ definiert ist.

Bemerke, dass für $x, y \in \{1, 2, ..., p-1\}$ mit $f(x) = f(y)$ auch folgendes gilt:

$$a \cdot x \equiv a \cdot y \pmod{p} \Rightarrow x \equiv y \pmod{p}.$$

Fermats Kleiner Satz

Sei p eine Primzahl und $0 \neq a \in \mathbb{Z}/p\mathbb{Z}$. Wir betrachten die Funktion $f : \{1, 2, ..., p-1\} \to \{1, 2, ..., p-1\}$, die durch $f(x) = a \cdot x \pmod{p}$ definiert ist.

Bemerke, dass für $x, y \in \{1, 2, ..., p-1\}$ mit $f(x) = f(y)$ auch folgendes gilt:

$$a \cdot x \equiv a \cdot y \pmod{p} \Rightarrow x \equiv y \pmod{p}.$$

Also ist für $x \not\equiv y \pmod{p}$ auch $f(x) \neq f(y)$.

Fermats Kleiner Satz

Sei p eine Primzahl und $0 \neq a \in \mathbb{Z}/p\mathbb{Z}$. Wir betrachten die Funktion $f : \{1, 2, ..., p-1\} \to \{1, 2, ..., p-1\}$, die durch $f(x) = a \cdot x \pmod{p}$ definiert ist.

Bemerke, dass für $x, y \in \{1, 2, ..., p-1\}$ mit $f(x) = f(y)$ auch folgendes gilt:

$$a \cdot x \equiv a \cdot y \pmod{p} \Rightarrow x \equiv y \pmod{p}.$$

Also ist für $x \not\equiv y \pmod{p}$ auch $f(x) \neq f(y)$.

Jeder Wert $1, 2, ..., p-1$ ist unter $f(1) = a \cdot 1 \pmod{p}$, $f(2) = a \cdot 2 \pmod{p}$, ..., $f(p-1) = a \cdot (p-1) \pmod{p}$ genau einmal zu finden!

Fermats Kleiner Satz

Sei p eine Primzahl und $0 \neq a \in \mathbb{Z}/p\mathbb{Z}$. Wir betrachten die Funktion $f : \{1, 2, ..., p-1\} \to \{1, 2, ..., p-1\}$, die durch $f(x) = a \cdot x \pmod{p}$ definiert ist.

Bemerke, dass für $x, y \in \{1, 2, ..., p-1\}$ mit $f(x) = f(y)$ auch folgendes gilt:

$$a \cdot x \equiv a \cdot y \pmod{p} \Rightarrow x \equiv y \pmod{p}.$$

Also ist für $x \not\equiv y \pmod{p}$ auch $f(x) \neq f(y)$.

Jeder Wert $1, 2, ..., p-1$ ist unter $f(1) = a \cdot 1 \pmod{p}$, $f(2) = a \cdot 2 \pmod{p}$, ..., $f(p-1) = a \cdot (p-1) \pmod{p}$ genau einmal zu finden! Also

$$1 \cdot 2 \cdots (p-1) \equiv f(1) \cdot f(2) \cdots f(p-1) = a^{p-1} \cdot (1 \cdot 2 \cdots (p-1)) \pmod{p}.$$

Fermats Kleiner Satz

Sei p eine Primzahl und $0 \neq a \in \mathbb{Z}/p\mathbb{Z}$. Wir betrachten die Funktion $f : \{1, 2, ..., p-1\} \to \{1, 2, ..., p-1\}$, die durch $f(x) = a \cdot x \pmod{p}$ definiert ist.

Bemerke, dass für $x, y \in \{1, 2, ..., p-1\}$ mit $f(x) = f(y)$ auch folgendes gilt:

$$a \cdot x \equiv a \cdot y \pmod{p} \Rightarrow x \equiv y \pmod{p}.$$

Also ist für $x \not\equiv y \pmod{p}$ auch $f(x) \neq f(y)$.

Jeder Wert $1, 2, ..., p-1$ ist unter $f(1) = a \cdot 1 \pmod{p}$, $f(2) = a \cdot 2 \pmod{p}$, ..., $f(p-1) = a \cdot (p-1) \pmod{p}$ genau einmal zu finden! Also

$$1 \cdot 2 \cdots (p-1) \equiv f(1) \cdot f(2) \cdots f(p-1) = a^{p-1} \cdot (1 \cdot 2 \cdots (p-1)) \pmod{p}.$$

Inbesondere ist

$$b \equiv b \cdot a^{p-1} \pmod{p},$$

wenn wir $b \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}$ wählen.

Fermats Kleiner Satz

Sei p eine Primzahl und $0 \neq a \in \mathbb{Z}/p\mathbb{Z}$. Wir betrachten die Funktion $f : \{1, 2, ..., p-1\} \to \{1, 2, ..., p-1\}$, die durch $f(x) = a \cdot x \pmod{p}$ definiert ist.

Bemerke, dass für $x, y \in \{1, 2, ..., p-1\}$ mit $f(x) = f(y)$ auch folgendes gilt:

$$a \cdot x \equiv a \cdot y \pmod{p} \Rightarrow x \equiv y \pmod{p}.$$

Also ist für $x \not\equiv y \pmod{p}$ auch $f(x) \neq f(y)$.

Jeder Wert $1, 2, ..., p-1$ ist unter $f(1) = a \cdot 1 \pmod{p}$, $f(2) = a \cdot 2 \pmod{p}$, ..., $f(p-1) = a \cdot (p-1) \pmod{p}$ genau einmal zu finden! Also

$$1 \cdot 2 \cdots (p-1) \equiv f(1) \cdot f(2) \cdots f(p-1) = a^{p-1} \cdot (1 \cdot 2 \cdots (p-1)) \pmod{p}.$$

Inbesondere ist

$$b \equiv b \cdot a^{p-1} \pmod{p},$$

wenn wir $b \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}$ wählen. Also ist auch

$$a^{p-1} \equiv 1 \pmod{p}.$$

Satz von Euler

Theorem 3 (Euler)

Sei $m \geq 1$ eine ganze Zahl und $0 \neq a \in \mathbb{Z}/m\mathbb{Z}$ mit $\mathrm{ggT}(a, m) = 1$. Dann gilt

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Der Satz von Fermat ist ein Spezialfall vom Satz von Euler, da $\varphi(p) = p - 1$.