Der Fall $a < 0$ kann auf den bereits behandelten Fall zurückgeführt werden.

(9.43) FOLG: (Kleiner) Satz von Fermat, 1640

Für $p \in \mathbb{P}$ und $a \in \mathbb{Z}$ mit $p \not| a$ gilt er erfüllt $x = 6j$

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

Bew: : Nach (9.42) gilt $a^p \equiv a \pmod{p}$ oder umgeschrieben

$$(\star) \quad [a]_p^p = [1]_p$$

Wegen $p \not| a$ sind p und a teilerfremd, so daß $[a]_p$ nach (9.40) invertierbar ist. Multiplikation von $(\star)$ mit dem Inversen auf beiden Seiten ergibt die Behauptung.

Beispiel: $24^{12} \equiv 1 \pmod{13}$

$24^{12} = 36520347436056576$ ist eine 17–stellige Zahl.

	$24 \equiv -2 \pmod{13}$	|^2
	$24^2 \equiv 4 \pmod{13}$	|^2
$(\star)$	$24^4 \equiv 3 \pmod{13}$	|^2
$(\star\star)$	$24^8 \equiv 9 \pmod{13}$	Multiplikation von $(\star)$ und $(\star\star)$
	$24^{12} \equiv 1 \pmod{13}$	

Eine Verallgemeinerung des Satzes von Fermat hat Euler 1760 gefunden:

(9.44) SATZ: **Euler** Für $a \in \mathbb{Z}$ und $m \in \mathbb{N}$ mit $\mathrm{ggT}(a, m) = 1$ gilt

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

Beispiel: $4^{10} = 4^{\varphi(15)} \equiv 1 \pmod{15}$.

Wegen $\varphi(p) = p - 1$ für eine Primzahl p ist der Satz von Fermat in dem Satz von Euler enthalten. Die Sätze von Fermat und Euler sind Grundlage für eine Reihe von Primzahltests, die leistungsfähiger als die bisher erwähnten sind.

Primzahltest Es gilt: p Primzahl $\implies$ $2^p \equiv 2 \pmod{p}$

Die Umkehrung gilt i.a. nicht: Es ist

$2^{341} \equiv 2 \pmod{341}$ aber $341 = 11 \cdot 31$ ist zusammengesetzt.

Wir nennen 341 eine **Pseudoprimzahl (zur Basis 2)**.

Gilt also $2^n \equiv 2 \pmod{n}$ für eine natürliche Zahl n, so können wir nicht schließen, daß n eine Primzahl ist. Gilt jedoch $2^n \not\equiv 2 \pmod{n}$, so ist n **keine** Primzahl. Ersetzen wir 2 durch eine beliebige Zahl b, so gilt für eine Primzahl p immer $b^p \equiv b \pmod{p}$ und auch hier gilt nicht die Umkehrung. Gilt dagegen $b^n \not\equiv b \pmod{n}$ für eine Zahl $n \in \mathbb{N}$,so ist n wieder keine Primzahl.

Es gilt $3^{341} \not\equiv 3 \pmod{341}$, woraus folgt, daß 341 keine Primzahl ist.

Testverfahren: Es soll untersucht werden, ob eine Zahl $n \in \mathbb{N}$ eine Primzahl ist.

Dazu wählen wir uns eine "Testmenge" $B \subseteq \mathbb{N}$ und testen, ob für jedes $b \in B$ die Kongruenz $b^n \equiv b \pmod{n}$ gilt. Ist dies für ein $b \in B$ nicht erfüllt, so ist n **keine** Primzahl, gilt dies jedoch für alle $b \in B$, so ist n **mit einiger Wahrscheinlichkeit** eine Primzahl. Es gibt jedoch Zahlen, die sich diesem Test vollständig entziehen. Dies sind zusammengesetzte Zahlen n (sog. **Carmichael–Zahlen**) mit $b^n \equiv b \pmod{n}$ für alle $b \in \mathbb{Z}$, z.B. $n = 561$.

Es handelt sich hierbei um einen **probabilistischen Primzahltest**.

Zum Abschluß wollen wir noch kurz den Chinesischen Restsatz behandeln. Es geht um das Problem, eine ganze Zahl zu bestimmen, die bei Division durch gewisse Zahlen vorgeschriebene Reste hat, z.B. ist $x \in \mathbb{Z}$ gesucht mit

$$x \equiv 1 \pmod{5} \quad , \quad x \equiv 2 \pmod{4}$$

Hier erfüllt $x = 6$ beide Kongruenzen, aber auch $26 = 6 + 4 \cdot 5$ und allgemein $6 + k \cdot 6 \quad (k \in \mathbb{Z})$

(9.45) SATZ: Chinesischer Restsatz (CRS)

Gegeben seien ganze Zahlen $b_1, \ldots, b_r$ und paarweise teilerfremde natürliche Zahlen $m_1, \ldots, m_r$. Dann gibt es eine ganze Zahl $x_0 \in \mathbb{Z}$, die das folgende System von Kongruenzen simultan erfüllt:

$$(\star) \quad \begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \qquad \vdots \\ x \equiv b_r \pmod{m_r} \end{cases}$$

Sind x_0 und x_0' zwei Lösungen von $(\star)$, so folgt $x \equiv x' \pmod{m}$, wobei $m := m_1 \cdot m_2 \cdot \ldots \cdot m_r$ ist. Außerdem ist jedes Element aus der Restklasse $[x_0]_m$ eine Lösung von $(\star)$.

Bew: Es sei $n_k := \dfrac{m}{m_k}$. Es folgt $n_k \in \mathbb{N}$ und $\mathrm{ggT}(m_k, n_k) = 1$ für alle $k = 1, 2, \ldots, r$. Dann gibt es $c_k, d_k \in \mathbb{Z}$ mit $1 = m_k c_k + n_k d_k$ (EEA), und es ist

$$x_0 := \; b_1 n_1 d_1 + b_2 n_2 d_2 + \ldots + b_r n_r d_r \in \mathbb{Z}$$

eine Lösung von $(\star)$. Für $i \neq k$ gilt nämlich $n_i \equiv 0 \pmod{m_k}$, also $x_0 \equiv b_k n_k d_k \equiv b_k \pmod{m_k}$ für alle k , da sich aus $1 = m_k c_k + n_k d_k$ die Kongruenz $n_k d_k \equiv 1 \pmod{m_k}$ ergibt.

Der CRS ist die Grundlage für die **modulare Arithmetik**.

Modulare Addition

Wir wollen die beiden Zahlen $a = 37$ und $b = 56$ nach einem Verfahren addieren, das für große Zahlen schneller ist als die "normale Addition". Dieses Beispiel soll nur das Verfahren erklären:

Wir wählen dazu eine Zahl $m > a + b$, hier etwa $m = 140$, und stellen m als ein Produkt von paarweise teilerfremden Zahlen dar: $m = 4 \cdot 5 \cdot 7$. Wir bilden nun die Restklassen von 37 (bzw. 56) modulo 4,5 und 7 und addieren die entsprechenden Restklassen

$$
\begin{array}{lll}
37 & \longrightarrow & ([37]_4, [37]_5, [37]_7) \;=\; ([1]_4, [2]_5, [2]_7) \\
 & & \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad + \\
56 & \longrightarrow & ([56]_4, [56]_5, [56]_7) \;=\; ([0]_4, [1]_5, [0]_7) \\
\hline
93 & \longleftarrow & (\star) \qquad\qquad\qquad\qquad\qquad\qquad ([1]_4, [3]_5, [2]_7)
\end{array}
$$

($\star$) Mit dem CRS bestimmen wir eine Lösung $x_0 \in \{0, 1, \ldots, 139\}$ des Systems

$$
\begin{cases}
x \equiv 1 \pmod 4 \\
x \equiv 3 \pmod 5 \\
x \equiv 2 \pmod 7
\end{cases}
$$

Das ergibt hier $x_0 = 93$, und dies ist auch die Summe von 37 und 56.

Berechnung von x_0:

Mit der Bezeichnungsweise von (9.45) gilt:

$m_1 = 4\ ,\ m_2 = 5\ ,\ m_3 = 7\ \ ,\ \ b_1 = 1\ ,\ b_2 = 3\ ,\ b_3 = 2\ \ ,$

$n_1 = \frac{m}{m_1} = \frac{140}{4} = 35\ ,\ n_2 = \frac{m}{m_2} = \frac{140}{5} = 28\ ,\ n_3 = \frac{m}{m_3} = \frac{140}{7} = 20$

$\mathrm{ggT}(4, 35) = 1 \qquad 1 = 9 \cdot 4 + (-1) \cdot 35 \qquad d_1 = -1$

$\mathrm{ggT}(5, 28) = 1 \qquad 1 = (-11) \cdot 5 + 2 \cdot 28 \qquad d_2 = 2$

$\mathrm{ggT}(7, 20) = 1 \qquad 1 = 3 \cdot 7 + (-1) \cdot 20 \qquad d_3 = -1$

$x_0 = b_1 n_1 d_1 + b_2 n_2 d_2 + b_3 n_3 d_3 \;=\; 1 \cdot 35 \cdot (-1) + 3 \cdot 28 \cdot 2 + 2 \cdot 20 \cdot (-1) = -35 + 168 - 40 = 93$

Probe: $93 \equiv 1 \pmod 4\ ,\ 93 \equiv 3 \pmod 5\ ,\ 93 \equiv 2 \pmod 7$

Modulare Multiplikation

Berechne das Produkt $37 \cdot 56$. Wähle dazu $m = 3465 = 5 \cdot 7 \cdot 9 \cdot 11$.

$$
\begin{array}{lll}
37 & \longrightarrow & ([37]_5, [37]_7, [37]_9, [37]_{11}) \;=\; ([2]_5, [2]_7, [1]_9, [4]_{11}) \\
 & & \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \times \\
56 & \longrightarrow & ([56]_5, [56]_7, [56]_9, [56]_{11}) \;=\; ([1]_5, [0]_7, [2]_9, [1]_{11}) \\
\hline
2072 & \longleftarrow & \qquad\qquad\qquad\qquad\qquad\qquad ([2]_5, [0]_7, [2]_9, [4]_{11}) \quad (\star)
\end{array}
$$

($\star$) Mit dem CRS bestimmen wir eine Lösung $x_1 \in \{0, 1, \ldots, 3464\}$ des Systems

$$
\begin{cases}
x \equiv 2 \pmod 5 \\
x \equiv 0 \pmod 7 \\
x \equiv 2 \pmod 9 \\
x \equiv 4 \pmod{11}
\end{cases}
$$

Das ergibt hier $x_1 = 2072$, und dies ist auch das Produkt von 37 und 56.