Satz von Euler/Fermat
Chinesischer Restsatz (CRS)

Fragen?

paarw. teilerfremd: ggT(2,3) = 1, ggT(2,5) = 1, ggT(3,5) = 1

Ü

$x \equiv 1 \mod 2$
$x \equiv 2 \mod 3$
$x \equiv 3 \mod 5$

Lösen Sie das Kongruenzsystem, indem Sie folgende Schritte durchführen:

(0.) Berechnen Sie
$k_1 = \cancel{2} \cdot 3 \cdot 5 = 15$
$k_2 = 2 \cdot \cancel{3} \cdot 5 = 10$
$k_3 = 2 \cdot 3 \cdot \cancel{5} = 6$

(1.) Berechnen Sie die Inversen x_i von k_i mod m_i:

$15 \cdot x_1 = k_1 x_1 \equiv 1 \pmod 2 \Rightarrow x_1 = 1$
$10 \cdot x_2 = k_2 x_2 \equiv 1 \pmod 3 \Rightarrow x_2 = 1$
$6 \cdot x_3 = k_3 x_3 \equiv 1 \pmod 5 \Rightarrow x_3 = 1$

(2.) Berechnen Sie $x = 1 \cdot 15 \cdot 1 + 2 \cdot 10 \cdot 1 + 3 \cdot 6 \cdot 1$
$= 15 + 20 + 18$
$= 53$

(3.) Allgemeine Lösung $y = x + z \cdot \underbrace{m}_{= m_1 m_2 m_3 = \underbrace{2 \cdot 3 \cdot 5}_{30}} = 53 + z \cdot 30 = 23 + z \cdot 30 = \ldots, -7, 23, 53, 83, 113, \ldots \quad z \in \mathbb{Z}$

Satz von Euler.

* 1. $7^{193} \equiv ?\ (\text{mod } 360)$
  2. $19^{1683} \equiv ?\ (\text{mod } 24)$
  3. $68^{1132} \equiv ?\ (\text{mod } 127)$

⚠ Voraussetzung prüfen!

Lösung. Euler: $\operatorname{ggT}(a,n) = 1$: $a^{\varphi(n)} \equiv 1 \ (\text{mod } n)$

1. $\operatorname{ggT}(7, \underbrace{360}_{2^3\cdot 3^2\cdot 5}) = 1$ (Voraussetzung erfüllt ✓). $\varphi(360) = \underbrace{\varphi(2^3)}_{\underbrace{2^3-2^2}_{4}} \cdot \underbrace{\varphi(3^2)}_{\underbrace{3^2-3}_{6}} \cdot \underbrace{\varphi(5)}_{\underbrace{5-1}_{4}} = 96.$

Euler: $\underbrace{7^{\varphi(360)}}_{7^{96}} \equiv 1 \quad (\text{mod } 360)$

$$7^{193} = 7^{2\cdot 96+1} = (\underbrace{7^{96}}_{\equiv 1})^2 \cdot 7 \equiv 7 \quad (\text{mod } 360)$$

2. Voraussetzung Euler: $\operatorname{ggT}(\underbrace{19}_{\text{prim}}, \underbrace{24}_{2^3\cdot 3}) = 1$ ✓. $\varphi(24) = \underbrace{\varphi(2^3)}_{\underbrace{2^3-2^2}_{4}} \cdot \underbrace{\varphi(3)}_{2} = 8$

Euler: $19^8 \equiv 1 \ (\text{mod } 24)$.

$$19^{1683} = 19^{210\cdot 8+3} = (\underbrace{19^8}_{\equiv 1})^{210} \cdot 19^3 \equiv 19^3 = \underbrace{19^2}_{\substack{361 \\ \equiv \\ 1}} \cdot 19 \equiv 19 \quad (\text{mod } 24)$$

3. Voraussetzung: $\operatorname{ggT}(\underbrace{68}_{2^2\cdot 17}, \underbrace{127}_{\text{prim, teste bis } \sqrt{127} \approx 11,\dots}) = 1$ ✓. $\varphi(127) = 126$

$\cancel{2}, \cancel{3}, \cancel{5}, \cancel{7}, \cancel{11}$

Schnelles Potenzieren

$$68^{1132} = 68^{8\cdot 126 + 124} = (\underbrace{68^{126}}_{\substack{\equiv \text{ Euler} \\ 1}})^8 \cdot 68^{124} \equiv 68^{124} = (\underbrace{68^2}_{\substack{4624 \\ \equiv \\ 52}})^{62} \equiv (\underbrace{52^2}_{\substack{2704 \\ \equiv \\ 37}})^{31}$$

$$\equiv 37^{2\cdot 15+1} = (\underbrace{37^2}_{\substack{\equiv \\ 99}})^{15} \cdot 37 \equiv (\underbrace{99^3}_{\substack{970.299 \\ \equiv \\ 19}})^5 \cdot 37 \equiv \underbrace{19^5}_{\substack{\equiv \\ 107}} \cdot 37 \equiv 22 \quad (\text{mod } 127)$$

Eigener Lösungsversuch.

Chinesischer Restsatz. Lösen Sie folgendes Kongruenzsystem:

- $x \equiv 2 \mod 3$ $\qquad k_1 = \cancel{3} \cdot 10$ $\qquad \overset{1 \overset{?}{\equiv} 10}{\tilde{k}_1} \cdot x_1 \equiv 1 \pmod{3} \Rightarrow x_1 = 1$
- $x \equiv 7 \mod 10$ $\qquad k_2 = 3 \cdot \cancel{10}$ $\qquad \underbrace{k_2}_{3} \cdot x_2 \equiv 1 \pmod{10} \Rightarrow x_2 = 7$

$$x = 2 \cdot 10 \cdot 1 + 7 \cdot 3 \cdot 7 = 20 + 147 = 167$$

Lösung.

⚠ Voraussetzung CRS: Moduln müssen paarweise teilerfremd sein: $ggT(3, \underset{2 \cdot 5}{10}) = 1$ ✓

Allg. Lösung: $y = \underbrace{x}_{167} + z \cdot \underbrace{(3 \cdot 10)}_{30} = 167 + z \cdot 30, \quad z \in \mathbb{Z}$

$\ldots, 17, \ldots, 137, 167, 197, \ldots, \ldots$

Eigener Lösungsversuch.

Eieraufgabe des Brahmagupta. Eine alte Frau geht über den Marktplatz. Ein Pferd tritt auf ihre Tasche und zerbricht die gekauften Eier. Der Besitzer des Pferdes möchte den Schaden ersetzen und fragt die alte Frau, wie viele Eier in ihrer Tasche waren. Sie weiß die exakte Zahl nicht mehr, aber sie erinnert sich, dass genau ein Ei übrig bleibt, wenn sie beim Auspacken die Eier immer zu zweit aus der Tasche nimmt. Das Gleiche geschieht, wenn sie die Eier immer zu dritt, zu viert, zu fünft und zu sechst aus der Tasche nimmt. Nur wenn sie die Eier zu siebt aus der Tasche nimmt, bleibt kein Ei übrig. Was ist die kleinste Zahl an Eiern, welche die alte Frau in ihrer Tasche haben kann?

$x = q \cdot 2 + 1$

Lösung. x = Anzahl Eier.

$$
\begin{aligned}
&(I) && \cancel{x \equiv 1 \pmod{2}} \\
&(II) && \cancel{x \equiv 1 \pmod{3}} \\
& && \cancel{x \equiv 1 \pmod{4}} \\
& && x \equiv 1 \pmod{5} \\
&(V) && x \equiv 1 \pmod{6} \\
& && x \equiv 0 \pmod{7}
\end{aligned}
$$

Voraussetzung CRS: Nicht erfüllt! z.B. $ggT(2,4) = 2 \neq 1$.

Idee: Werfe zuerst ein paar Kongruenzen raus, damit man CRS darauf anwenden kann. Dann betracht ich die fehlenden Kongruenzen...

$x = 1 + q \cdot \underbrace{6}_{2\cdot 3} \equiv 1 \pmod{2}$, $\equiv 1 \pmod{3}$ d.h. Gleichung (I)/(II) folgen aus (V)

CRS: $5, 6 = 2\cdot 3, 7$ sind paarweise teilerfremde Moduln, da keine gemeinsamen Primfaktoren.

$$
\begin{aligned}
x &\equiv 1 \pmod{5} & k_1 &= \cancel{5}\cdot 6 \cdot 7 = 42 & \overset{2}{\overset{\rotatebox{90}{$\equiv$}}{42}} \cdot x_1 &\equiv 1 \pmod{5} \Rightarrow x_1 = 3 \\
x &\equiv 1 \pmod{6} & k_2 &= 5 \cdot \cancel{6} \cdot 7 = 35 & \overset{5}{\overset{\rotatebox{90}{$\equiv$}}{35}} \cdot x_2 &\equiv 1 \pmod{6} \Rightarrow x_2 = 5 \\
x &\equiv 0 \pmod{7} & k_3 &= 5 \cdot 6 \cdot \cancel{7} = 30 & \overset{2}{\overset{\rotatebox{90}{$\equiv$}}{30}} \cdot x_3 &\equiv 1 \pmod{7} \Rightarrow x_3 = 4
\end{aligned}
$$

$$x = 1 \cdot 42 \cdot 3 + 1 \cdot 35 \cdot 5 + 0 \cdot 30 \cdot 4 = 126 + 175 + 0 = \underline{301}$$

Allg. Lösung: $\underline{y} = 301 + z \cdot (\underbrace{5 \cdot 6 \cdot 7}_{210}) = \underline{301 + z \cdot 210}$, $z \in \mathbb{Z}$

Muss $x \equiv 1 \pmod{4}$ erfüllen; d.h. $\underset{1}{301} + z \cdot \underset{2}{210} \equiv 1 \pmod{4}$

$$
\begin{aligned}
&\Leftrightarrow & 1 + 2z &= 1 + q \cdot 4 \\
&\overset{-1}{\Leftrightarrow} & 2z &= q \cdot 4 \\
&\overset{:2}{\Leftrightarrow} & \underline{z} &\underline{= q \cdot 2}, \text{ d.h. } z \text{ gerade}
\end{aligned}
$$

ODER: mit dioph. Gl.:

$301 + z \cdot 210 = 1 + q \cdot 4$

$\Leftrightarrow 210 \cdot \underbrace{z}_{x} + 4 \cdot \underbrace{(-q)}_{y} = -300$

$$\Rightarrow \underline{y} = 301 + q \cdot 2 \cdot 210 = \underline{301 + q \cdot 420,\ q \in \mathbb{Z}} \qquad \ldots, -119, 301, 721, \ldots$$

kleinste positive Anzahl an Eiern ist $\underline{301}$.

Eigener Lösungsversuch.