Prof. Dr. M. Helbig
Mathematik – Übung

Hochschule **Rosenheim**
University of Applied Sciences

Satz von Euler/Fermat
Chinesischer Restsatz (CRS)

Fragen?

Satz von Euler.

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

Lösung.

$ggT(7;360)=1$: $7^{\varphi(360)} \equiv 1 \pmod{360}$

$\varphi(360) = \underbrace{\varphi(2^3)}_{2^3-2^2} \cdot \underbrace{\varphi(3^2)}_{3^2-3} \cdot \underbrace{\varphi(5)}_{5-1} = 96$

$4 \cdot 6 \cdot 4$

$7^{\varphi(360)} = 7^{96} \equiv 1 \mod 360$

$7^{193} = 7^{2\cdot 96+1} = (7^{96})^2 \cdot 7 = 7 \mod 360$

$(\ldots)$

1

2.) $19^{1683} \equiv ? \pmod{24}$

$ggT(19;24)=1$ ✓ $\qquad 19^8 \equiv 1 \mod 24$

$\varphi(24) = \varphi(2^3 \cdot 3) = 8 \qquad 19^{1683} = 19^{210\cdot 8+3} = (19^8)^{210} \cdot 19^3$

$\underbrace{2^3-2^2}_{4} \quad \underbrace{3-1}_{2}$

$\equiv 1^{210} \cdot \underbrace{19^3}_{361} : 19 = 1$

$1 \cdot 1$

1

Eigener Lösungsversuch.

3) $68^{1152} \equiv ?$ (mod 127)

$\gcd(68;127) = 1$ ✓

$\varphi(127) = 126$

$68^{1152} = (68^{126})^8 \cdot 68^{124} \equiv 68^{124} = (68^2)^{62} = \underbrace{(4624)}_{52}^{62} = (2704)^{31} = (37^2)^{15} \cdot 37$

$= (33)^{15} \cdot 37 = 22^7 \cdot 99 \cdot 37 = 22 \cdot 99 \cdot 37 \cdot 10\,648 = \ldots$ mod (127)

Chinesischer Restsatz. Lösen Sie folgendes Kongruenzsystem:

- $x \equiv 2 \mod 3$
- $x \equiv 7 \mod 10$

$ggT(3;10) = 1$ ✓

Lösung.

$10x_1 \equiv 1 \mod 3$

$3x_2 \equiv 1 \mod 10$

$x_1 = 1$

$x_2 \equiv 7$

$x = 2 \cdot 10 \cdot 1 + 7 \cdot 7 \cdot 3$

$= 167$

$167 + z \cdot 3 \cdot 10$

$k_1 = 3 \cdot 10$

$k_2 = 3 \cdot 10$

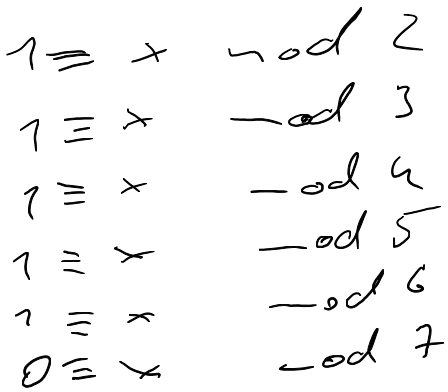
$10 \cdot x_1 \equiv 1 \mod 3 \quad x_1 = 1$

$3 \cdot x_2 \equiv 1 \mod 10 \quad x_2 = 7$

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?

Lösung.



Eigener Lösungsversuch.