Beispiel zu Pohlig-Hellmann:

Sei $G := (\mathbb{Z}/2017\mathbb{Z})^{\times}$. Dann ist $n = |G| = 2016 = 2^5 3^2 7$. Es gilt $\langle 5 \rangle = G$. Dies kann man mit KASH nachprüfen durch

```
Length(Set(List([1..2016], i-> 5ˆi mod 2017))) = 2016
```

oder

```
FFEltToInt(FFPrimitiveElt(FF(2017,1)))=5.
```

Gesucht ist $x \in \{1, ..., n\}$ mit $5^x = 3 \mod 2017$. Es ist $\alpha = 3$ und $\gamma = 5$.

1. **p=2**

   (i) $n_2 = 3^2 7 = 63$,
   $\gamma_2 = \gamma^{n_2} = 5^{63} \equiv 500 \mod 2017$,
   $\alpha_2 = \alpha^{n_2} = 913 \mod 2017$

   (ii) Gesucht ist $x(2) \in \mathbb{N}$ mit $\gamma_2^{x(2)} = \alpha_2$, d.h. also $500^{x(2)} \equiv 913 \mod 2017$

   (iii) $x(2) = x_0 + x_1 \cdot 2 + x_2 \cdot 2^2 + x_3 \cdot 2^3 + x_4 \cdot 2^4$

   (iv) $\beta_0 := 913, \quad \beta_i = \beta_{i-1} \cdot \gamma_2^{-(x_0+x_1p+\ldots+x_{i-1}p^{i-1})}$ für $i = 1, \ldots, 4$

   (v) Allgemein gilt: $\left(500^{2^4}\right)^{x_i} \equiv 2016^{x_i} \equiv \beta_i^{2^{5-i-1}}$ für $i = 0, \ldots, 4$, also

   $$\begin{array}{llll}
   2016^{x_0} & \equiv 913^{2^4} & \equiv 1 \mod 2017, & \text{also } x_0 = 0 \text{ und } \beta_1 = 913. \\
   2016^{x_1} & \equiv 913^{2^3} & \equiv 2016 \mod 2017, & \text{also } x_1 = 1 \text{ und } \beta_2 = 913 \cdot 691 \quad \equiv 1579 \mod 2017 \\
   2016^{x_2} & \equiv 1579^{2^2} & \equiv 2016 \mod 2017, & \text{also } x_2 = 1 \text{ und } \beta_3 = 1579 \cdot 1469 \quad \equiv 1 \mod 2017 \\
   2016^{x_3} & \equiv 1^{2^1} & \equiv 1 \mod 2017, & \text{also } x_3 = 0 \text{ und } \beta_4 \equiv 1 \mod 2017 \\
   2016^{x_4} & \equiv 1 & \mod 2017 & \text{also } x_4 = 0.
   \end{array}$$

   Damit erhalten wir $x(2) = 1 \cdot 2 + 1 \cdot 2^2 = 6$

2. **p=3**

   (i) $n_3 = 2^5 7 = 224$
   $\gamma_3 = \gamma^{n_3} \equiv 576 \mod 2017$
   $\alpha_3 = \alpha^{n_3} \equiv 1933 \mod 2017$

   (ii) Gesucht ist $x(3) \in \mathbb{N}$ mit $\gamma_3^{x(3)} = \alpha_3$, d.h. also $576^{x(3)} = 1933 \mod 2017$

   (iii) $x(3) = x_0 + x_1 \cdot 3$

   (iv) $\beta_0 := 1933, \quad \beta_1 = \beta_0 \gamma_3^{-x_0}$

   (v) Also: $(576^3)^{x_0} = 294^{x_0} \equiv 1933^3 = 294$, d.h. also $x_0 = 1$ und $\beta_1 = 1933 \cdot 576^{-1} = 1933 \cdot 1005 \equiv 294 \mod 2017$. Aus $294^{x_1} \equiv \beta_1^{3^0} \equiv 294 \mod 2017$ folgt dann $x_1 = 1$.

   Damit erhalten wir $x(3) = 1 + 1 \cdot 3 = 4$.

3. **p=7**

   (i) $n_7 = 2^5 3^2 = 288$
   $\gamma_7 = 5^{n_7} \equiv 1879 \mod 2017$
   $\alpha_7 = 3^{n_7} \equiv 1879 \mod 2017$

   (ii) Gesucht ist $x(7) \in \mathbb{N}$ mit $\gamma_7^{x(7)} \equiv \alpha_7$, d.h. also $1879^{x(7)} \equiv 1879$.

   Daraus folgt sofort $x(7) = 1$.

Mit dem Hauptsatz der simultanen Kongruenzen berechnet man $x = 6 \cdot (-1) \cdot 63 + 4 \cdot (-1) \cdot 224 + 1 \cdot 1 \cdot 288 = -986 \equiv 1030 \mod 2017$.