§3. Polynomiale Kongruenzen, Primitivwurzeln und quadratische Reste

Systeme von linearen Kongruenzengleichungen sind eindeutig lösbar.
(wo haben wir das gezeigt?)

Wie sieht es mit Lösbarkeit polynomialer Gleichungen aus, z.B. quadratischer Gleichungen?

3.1 Proposition: Sei p eine Primzahl. Die quadratische Kongruenz $x^2 \equiv -1 \pmod p$ ist lösbar $\Leftrightarrow p \not\equiv 3 \pmod 4$

Für $p=2$ ist 1 die einzige Lösung modulo 2.

Für $p \equiv 1 \bmod 4$ gibt es modulo p genau zwei verschiedene Lösungen, $\left(\frac{p-1}{2}\right)!$ und $-\left(\frac{p-1}{2}\right)!$ probieren Sie einige p aus

Beweis: p gerade, also $p=2$: 1 ist Lösung, wie jede ungerade Zahl, und es kann keine gerade Lösung geben

Sei nun p ungerade und x eine Lösung. $1 \equiv x^{p-1} \pmod p$ warum?

p ungerade $\Rightarrow \frac{p-1}{2}$ ganze Zahl, $\underset{\substack{\text{\tiny{III}}(\bmod p) \\ 1}}{x^{p-1}} = x^{2\cdot\frac{p-1}{2}} = (x^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod p$

$\Rightarrow 1 \equiv (-1)^{\frac{p-1}{2}} \pmod p$

Jetzt unterscheiden wir die beiden Fälle $p \equiv 1 \pmod 4$ und $p \equiv 3 \pmod 4$

Falls $p \equiv 3 \pmod 4$: $\exists n: p = 4n+3$, $\frac{p-1}{2} = \frac{4n+2}{2} = 2n+1$ ungerade

$\Rightarrow (-1)^{\frac{p-1}{2}} = -1 \Rightarrow 1 \equiv -1 \pmod p \Rightarrow 2 \equiv 0 \pmod p$ ↯ Widerspruch wozu?

Bleibt also $p \equiv 1 \pmod 4$: $\frac{p-1}{2}$ ist gerade, hier entsteht kein Widerspruch

Es gilt $(p-1)! \equiv -1 \pmod p$ warum?

$$\overset{\shortparallel}{1\cdot 2\cdot \ldots \cdot \tfrac{p-1}{2}}\cdot\left(\tfrac{p-1}{2}+1\right)\cdots(p-1) = \left(\tfrac{p-1}{2}\right)!\cdot\prod_{j=1}^{\frac{p-1}{2}}(p-j) \equiv$$

warum?

$$\equiv (-1)^{\frac{p-1}{2}}\cdot\left(\tfrac{p-1}{2}\right)!\cdot\left(\tfrac{p-1}{2}\right)!$$

$$\equiv 1\cdot\left(\left(\tfrac{p-1}{2}\right)!\right)^2 \pmod p \Rightarrow \left(\tfrac{p-1}{2}\right)! \text{ ist eine Lösung und}$$

$-\left(\frac{p-1}{2}\right)!$ daneben

Kann es noch weitere Lösungen geben? Nein, denn $\mathbb{Z}/p\mathbb{Z}$ ist ein Körper □

warum hat ein quadratisches Polynom $\underset{\ne 0}{f(x)} \in K[x]$ höchstens 2 Nullstellen? K Körper

Wie sieht es allgemein bei polynomialen Gleichungen aus?
Sei $f(x) \in \mathbb{Z}[x]$. Gleichung: $f(x) \equiv 0 \pmod m$
Darf man mit Restklassen rechnen?
$x_1 \equiv x_2 \Rightarrow x_1^j \equiv x_2^j \; \forall j$. Daraus folgt: x_1 Lösung $\Rightarrow x_2 \equiv x_1$ auch, d.h. die ganze Restklasse von x_1 besteht aus Lösungen. Also fragen wir: Welche und wieviele Restklassen sind Lösungen?
Hier ist m noch eine beliebige Zahl. Im Spezialfall f linear wissen wir:

$x - a \equiv 0 \pmod m$ ist äquivalent zu
$$\begin{array}{l} x-a \equiv 0 \pmod{p_1^{a_1}} \\ x-a \equiv 0 \pmod{p_2^{a_2}} \\ \vdots \\ x-a \equiv 0 \pmod{p_l^{a_l}} \end{array}$$
falls $m = p_1^{a_1} \cdots p_l^{a_l}$

und es gibt genau eine Lösung.

Für allgemeine f suchen wir: $\rho_f(m) := \{x \in \mathbb{Z}/m\mathbb{Z} : f(x) \equiv 0 \pmod m\}$
Auch hier kann man $m = p_1^{a_1} - p_l^{a_l}$ nutzen:
<u>3.2 Proposition:</u> Sei $f(x) \in \mathbb{Z}[x]$, $m = p_1^{a_1} \cdots p_l^{a_l}$. Dann gilt:
$$\rho_f(m) = \prod_{k=1}^{l} \rho_f(p_k^{a_k})$$
Beweis: $f(x) \equiv 0 \pmod m$ bedeutet $m \mid f(x)$

$\overset{\text{warum?}}{\Rightarrow} f(x) \equiv 0 \pmod{p_k^{a_k}} \; \forall k$

Sei y eine Lösung von $f(x) \equiv 0 \pmod m$ $\Rightarrow$ y ist eine Lösung des Systems
$$\begin{array}{l} f(x_1) \equiv 0 \pmod{p_1^{a_1}} \\ \vdots \\ f(x_l) \equiv 0 \pmod{p_l^{a_l}} \end{array}$$
Umgekehrt sei eine Lösung dieses Systems gegeben, d.h. ein l-Tupel $y_1, \ldots, y_l$ mit $y_j \in \mathbb{Z}/p_j^{a_j}\mathbb{Z}$. Gesucht ist y mit $f(y) \equiv 0 \pmod m$.

y muß erfüllen:
$$\begin{array}{l} y \equiv y_1 \pmod{p_1^{a_1}} \\ \vdots \\ y \equiv y_l \pmod{p_l^{a_l}} \end{array}$$
Es gibt genau ein solches y. □
warum?

$f(x) \equiv 0 \pmod m$ unlösbar bedeutet also: mindestens eine Gleichung $f(x) \equiv 0 \pmod{p_i^{a_i}}$ ist unlösbar

Damit ist das Problem reduziert auf den Fall von m = Primzahlpotenz. Wir wissen aber noch nicht, wie man die Gleichung in diesem Fall lösen kann.

Kann man den Exponenten induktiv verkleinern und damit auf den Fall reduzieren, daß p eine Primzahl ist?

$\rightsquigarrow$ Wir wollen also zwei Gleichungen betrachten und ihre Lösungen vergleichen: (a) $f(x) \equiv 0 \pmod{p^{a-1}}$ mit Lösungen $y_1, -, y_s$ $(s \geq 0)$

(b) $f(x) \equiv 0 \pmod{p^a}$ mit Lösungen $z_1, -, z_t$ $(t \geq 0)$

Können wir s und t vergleichen und die y_i mit den z_j?

$f(z_j) \equiv 0 \pmod{p^a} \Rightarrow p^a \mid f(z_j) \Rightarrow p^{a-1} \mid f(z_j)$

$\underset{\text{in } \mathbb{Z}/p^a\mathbb{Z}}{z_j \in \mathbb{Z}/p^a\mathbb{Z} \text{ Nullstelle}} \Rightarrow \underset{\text{Restklasse}}{\bar{z}_j} \in \mathbb{Z}/p^{a-1}\mathbb{Z}$ Nullstelle in $\mathbb{Z}/p^{a-1}\mathbb{Z}$

Die Restklassen der z_j sind also bei den y_i beteiligt.

Umgekehrt hat $y_i \in \mathbb{Z}/p^{a-1}\mathbb{Z}$ Urbilder in $\mathbb{Z}/p^a\mathbb{Z}$ (das surjektiv auf $\mathbb{Z}/p^{a-1}\mathbb{Z}$ abbildet: $\underbrace{y_i, y_i + p^{a-1}, y_i + 2p^{a-1}, -, y_i + (p-1)p^{a-1}}_{\text{Repräsentanten in } \mathbb{Z}/p^a\mathbb{Z}}$ liefern alle dasselbe y_i in $\mathbb{Z}/p^{a-1}\mathbb{Z}$

Jeder davon kann ein z_j sein (oder auch nicht).

Die Aufgabe ist also, die z_j unter diesen Zahlen zu finden, und sie zu zählen. Das ist mit etwas Aufwand verbunden.

Zunächst eine Definition: Sei $f(x) \in \mathbb{Z}[x]$, $f(x) = \sum_{i \geq 0} a_i x^i$, dann setzen wir $f'(x) = \sum_{i \geq 1} i \cdot a_i \cdot x^{i-1}$ (formale Ableitung), und mit $f^{(1)} = f'$ dann induktiv weiter.

$\rightsquigarrow$ Für $\ell \in \mathbb{N}$ ist $f^{(\ell)}(x) = \sum_{i \geq \ell} \ell! \binom{i}{\ell} a_i x^{i-\ell}$ nachprüfen

$\Rightarrow \frac{1}{\ell!} f^{(\ell)}(x) \in \mathbb{Z}[x]$

Es gilt auch eine "Taylor-Formel"

$$f(x+y) = \sum_{\ell \geq 0} \frac{1}{\ell!} f^{(\ell)}(x) y^\ell \quad \text{Beweis?}$$

In die Taylorformel setzen wir die Kandidaten für z ein, d.h.

$y+dp^{a-1}$ mit $d \in \{0, \ldots, p-1\}$:

$$f(y+dp^{a-1}) = \sum_{e\geq 0} \underbrace{\frac{1}{e!} f^{(e)}(y)}_{\in \mathbb{Z}} d^e p^{(a-1)e}$$ warum?

$a \geq 2$, also $a-1 \geq 1$, für $e \geq 2$ ist also p^a ein Teiler von $p^{(a-1)e}$

(denn: $(a-1)e = a + a(e-1) - e \geq a + 2(e-1) - e \geq a$)

$\Rightarrow$ modulo p^a verschwinden alle Terme mit $e \geq 2$

$$\Rightarrow f(y+dp^{a-1}) \equiv f(y) + f'(y)dp^{a-1} \pmod{p^a}$$

$$\Rightarrow f(z) \equiv 0 \pmod{p^a} \Leftrightarrow f(y) + f'(y)dp^{a-1} \equiv 0 \pmod{p^a}$$

Die Voraussetzung an y war: $f(y) \equiv 0 \pmod{p^{a-1}}$, d.h. $p^{a-1} \mid f(y)$

$\Rightarrow$ durch p^{a-1} darf geteilt werden: $-\dfrac{f(y)}{p^{a-1}} \equiv f'(y)d \pmod p$

warum mod p?

Gesucht ist ein passendes d:

d muß die Gleichung $f'(y)d \equiv -\dfrac{f(y)}{p^{a-1}} \pmod p$ erfüllen — das ist eine lineare Gleichung,

lösbar $\Leftrightarrow$ $ggT(f'(y), p) \mid \dfrac{f(y)}{p^{a-1}}$ warum?

Für $ggT(f'(y), p)$ gibt es nur zwei Möglichkeiten: 1 oder p

Erster Fall: $p \nmid f'(y)$, d.h. $ggT(f'(y), p) = 1 \Rightarrow$ es gibt eine eindeutige Lösung d

Zweiter Fall: $p \mid f'(y)$, d.h. $f'(y) \equiv 0 \pmod p$, die Gleichung wird zu

$$0 \cdot d \equiv -\frac{f(y)}{p^{a-1}} \pmod p$$

Das ist lösbar genau dann, wenn $p \mid \dfrac{f(y)}{p^{a-1}}$, d.h. $p^a \mid f(y)$, und dann kann man d beliebig wählen $\rightsquigarrow$ p Lösungen

Damit erhalten wir:

<u>3.3 Proposition:</u> Sei $f(x) \in \mathbb{Z}[x]$, p prim, $a \in \mathbb{N}$, $a \geq 2$ und $y \in \mathbb{Z}$ mit $f(y) \equiv 0 \pmod{p^{a-1}}$. Dann gilt:

(a) Falls $p \mid f'(y)$ und $f(y) \not\equiv 0 \pmod{p^a}$, dann gibt es kein z mit $f(z) \equiv 0 \pmod{p^a}$ und $z \equiv y \pmod{p^{a-1}}$.

(b) Falls $p \mid f'(y)$ und $f(y) \equiv 0 \pmod{p^a}$, dann gibt es genau p viele z mit $f(z) \equiv 0 \pmod{p^a}$ und $z \equiv y \pmod{p^{a-1}}$.

(c) Falls $p \nmid f'(y)$, dann gibt es genau ein z mit $f(z) \equiv 0 \pmod{p^a}$ und $z \equiv y \pmod{p^{a-1}}$. z hat die Form $z = y + dp^{a-1}$, wobei d die eindeutige Lösung von $f'(y)d \equiv -\frac{f(y)}{p^{a-1}} \pmod{p}$ ist.

Wir haben gesehen, daß ein quadratisches Polynom über $\mathbb{Z}/p\mathbb{Z}$ höchstens zwei verschiedene Lösungen haben kann. Allgemein hat ein Polynom $f(x) \in K[x]$, K Körper, mit Grad $\deg f = n > 0$ höchstens n viele Nullstellen.
Verwenden Sie den euklidischen Algorithmus für Polynome, um dies zu zeigen.
Was bedeutet das für Nullstellen modulo p von $f(x) \in \mathbb{Z}[x]$?
Über $\mathbb{Z}/p^a\mathbb{Z}$ $(a > 1)$ stimmt das nicht mehr. Was sagt 3.3 dazu?
Wieviele Lösungen z hat $f(x) = p \cdot x$ modulo p^2?
Quadratische Polynome in einer Variablen müssen keine Nullstelle haben.
Finden Sie ein Beispiel modulo 3?
Ein Polynom, das jedes Element als Nullstelle hat, muss nicht das Nullpolynom sein. Verwenden Sie den kleinen Satz von Fermat, um so ein Polynom zu finden.
Bei Polynomen mit mehreren Variablen gibt es, unter Voraussetzungen, allgemeine Aussagen über die Existenz von Lösungen, z.B.:

<u>3.4 Theorem</u> (Chevalley): Sei $n \geq 2$, $f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ mit $\deg f < n$ und $f(0) = 0$. Sei p eine Primzahl. Dann hat die Kongruenz $f(x_1, \ldots, x_n) \equiv 0 \pmod{p}$ neben dem Nullvektor noch mindestens eine weitere Lösung.

Beweis: $f(0,0,\dots,0)=0$ bedeutet f hat Konstanten Term 0.
Der totale Grad $\deg f$ ist für ein Monom (nur ein Term) die Summe der Grade in den x_i, und allgemein das ~~Ma~~ Maximum dieser Grade. Also z.B. $\deg(x_1^2x_2^3+x_2^4+x_1^3)=5$.

Angenommen, der Satz ist falsch, der Nullvektor ist die einzige Lösung.
Um einen Widerspruch zu erreichen, betrachten wir eine andere Kongruenz:

$$(*)\quad 1-(f(x_1,\dots,x_n))^{p-1} \equiv (1-x_1^{p-1})\cdots(1-x_n^{p-1}) \pmod p$$

Für $x_1,\dots,x_n=0$ steht links und rechts 1.
Sei nun $x_i \not\equiv 0 \pmod p$ für ein i. Also ist $x_i^{p-1}\equiv 1 \pmod p$ warum?
und $f(x_1,\dots,x_n)^{p-1}\equiv 1 \pmod p$ warum?
$\Rightarrow$ $(x_1,\dots,x_n)$ löst diese Kongruenz $(*)$, d.h. Nullstellen von $1-(f(x_1,\dots,x_n))^{p-1}-(1-x_1^{p-1})\cdots(1-x_n^{p-1})$. Das gilt für alle $x_1,\dots,x_n$, was schon verdächtig wirkt.

Wir können noch $(f(x_1,\dots,x_n))^{p-1}$ ausmultiplizieren und $\underbrace{(1-x_1^{p-1})\cdots(1-x_n^{p-1})}_{\text{das hat Totalgrad } n\cdot(p-1)}$ auch.

$\deg f<n \Rightarrow \deg(f(x_1,\dots,x_n)^{p-1}) < n(p-1)$
$\Rightarrow$ der Term $\pm x_1^{p-1}\cdots x_n^{p-1}$ mit dem höchsten Grad kann nicht weggekürzt werden, und p teilt nicht den Koeffizienten ± 1.
In $f(x_1,\dots,x_n)^{p-1}$ können manche x_i noch mit Grad $\geq p$ vorkommen. Aber wenn das passiert können ~~x~~ wir x_i^p durch x_i ersetzen warum?
und erhalten insgesamt ein Polynom, in dem in jeden Term jedes x_i höchstens $p-1$ mal vorkommt, und bei dem der Höchst Koeffizient nicht durch p teilbar, das aber alle $(x_1,\dots,x_n)$ ~~als~~ als Nullstellen hat. Wir zeigen, daß es so was nicht gibt. D.h. wir zeigen die folgende Behauptung:
Behauptung: Sei $g(x_1,\dots,x_n)\in\mathbb{Z}[x_1,\dots,x_n]$ ein Polynom, in ~~z~~ dem jedes x_i nur mit Grad $<p$ vorkommt. Dann gilt: Alle $(x_1,\dots,x_n)$ sind Nullstellen modulo p $\Leftrightarrow$ alle Koeffizienten von g sind durch p teilbar.

(Daraus folgt dann der gesuchte Widerspruch.)

Beweis der Behauptung: Falls p | alle Koeffizienten $\Rightarrow g = 0$ modulo p. ✓

Zunächst der Fall $n=1$, d.h. g ist ein Polynom in einer Variablen, nicht 0 modulo p. $\deg g < p \Rightarrow g$ kann keine p Nullstellen haben, es muß Restklassen geben, die keine Nullstellen sind. ✓ (Damit beginnt Induktion nach n.)

Jetzt der Fall $n > 1$: Wir schreiben

$$g(x_1, \dots, x_n) = h_{p-1}(x_2, \dots, x_n) x_1^{p-1} + h_{p-2}(x_2, \dots, x_n) x_1^{p-2} + \dots$$

Falls $h_i(x_2, \dots, x_n) \equiv 0 \pmod p \ \forall x_2, \dots, x_n$ müssen nach Induktion alle seine Koeffizienten durch p teilbar sein. $\Rightarrow$ Es bleibt nur der Fall, daß $\exists i: \exists x_2, \dots, x_n$ mit $h_i(x_2, \dots, x_n) \not\equiv 0 \pmod p$. Wenn wir solche $x_2, \dots, x_n$ fest wählen ist $g(x_1, x_2, \dots, x_n)$ ein Polynom in der einen Variablen x_1 und der Induktionsanfang ist anwendbar. wie?

$\Rightarrow$ Behauptung □

Das wird zunehmend kompliziert und vor allem technisch. Um theoretische Fortschritte zu machen, müssen wir spezialisieren. Bei Quadratwurzeln gab es in 3.1 ein überzeugendes Ergebnis. Also betrachten wir jetzt k-te Wurzeln genauer. Gesucht: Lösungen von $ax^k \equiv b \pmod p$

$a \equiv 0$ uninteressant, $a \not\equiv 0$ bedeutet $\exists a': aa' \equiv 1 \pmod p$, also kann man die Gleichung auch ~~so~~ schreiben

$$x^k \equiv c \pmod p$$

Wann gibt es überhaupt eine Lösung? Wieder ist 0 uninteressant, sei also $c \not\equiv 0$.

<u>3.5 Definition:</u> Ein c mit $(c,p) = 1$, für das ein x existiert mit $x^k \equiv c \pmod p$ heißt <u>k-ter Potenzrest modulo p.</u>

Wenn es kein solches x gibt, heißt c <u>k-ter Potenz-Nichtrest modulo p.</u>

Für $k = 2$ redet man von <u>quadratischen Resten</u> bzw. von <u>quadratischen Nichtresten.</u>

Beispiele für $k=2$ oder $k=3$

$p=2$	x	x^2	x^3
	1	1	1

$p=3$	x	x^2	x^3
	1	1	1
	2	1	2

Was sind nun die Reste bzw Nichtreste?

$p=5$	x	x^2	x^3
	1	1	?
	2	4	?
	3	4	?
	4	1	?

quadratische Nichtreste? (zwei Stück)
kubische Nichtreste?

$p=11$?   quadratische Nichtreste: 2, 6, 7, 8, 10?
kubische Nichtreste: ?

$p=13$?   (6 quadratische Nichtreste, 8 kubische Nichtreste)

Sehen Sie ein Muster bei quadratischen oder kubischen Nichtresten?

Kann man $x^k \equiv c$ lösen, indem man "Logarithmen" betrachtet?

Zur Vorbereitung betrachten wir eine andere, aber verwandte Frage.
Sei $x \neq 0$, $x \in \mathbb{Z}/p\mathbb{Z}$. Die Ordnung von x definiert als
$$\operatorname{ord}(x) := \min\{k : x^k \equiv 1 \pmod p\}$$
Für alle x gilt $x^{p-1} \equiv 1 \pmod p$ nach dem kleinen Satz von Fermat.
$\Rightarrow$ Außer $c \equiv 1 \pmod p$ gibt es keine $p-1$-ten Potenzreste.
Im Allgemeinen ist $\operatorname{ord}(x) \leq p-1$ (sogar ein Teiler). Falls $\operatorname{ord}(x) = p-1$, sind $\underbrace{x, x^2, \ldots, x^{p-1} \equiv 1}_{\text{verschieden}}$, d.h. $(\mathbb{Z}/p\mathbb{Z})^* = \{x, x^2, \ldots, x^{p-2}, 1\}$.   was heißt das für die mult. Gruppe $(\mathbb{Z}/p\mathbb{Z})^*$?
$\rightsquigarrow$ es gibt quadratische Reste $x^2, x^4, x^6, \ldots$
und kubische Reste $x^3, x^6, x^9, \ldots$ usw.
Kann x oder x^3 auch ein quadratischer Rest sein?
Falls $x \equiv (x^j)^2$ für ein $j \in \{1, \ldots, p-1\}$ ein quadratischer Rest ist, also $x \equiv x^{2j}$
Die x^k, $1 \leq k \leq p-1$, sind alle verschieden $\Rightarrow 2j > p-1$, aber auch $2j < 2(p-1)$.
$p=2$ uninteressant, also p ungerade, d.h. $p-1$ gerade
$2j > p-1 \Rightarrow \underbrace{2j-p-1}_{\text{gerade}} > 0$, $\underset{x}{\underset{|||}{x^{2j}}} \equiv x^{2j-p-1} \Rightarrow x \in \{x^2, x^4, \ldots\}$ ↯
$\Rightarrow x$ ist kein quadratischer Rest

Analog: x_i^3, x_i^5 – kein quadratischer Rest. nachprüfen

In diesem Fall sind also die quadratischen Reste von den quadratischen Nichtresten getrennt: $x_i^2, x_i^4 - \leftrightarrow x, x_i^3 -$

Das geht nur, wenn es ein x mit $\mathrm{ord}(x) = p-1$ gibt. vergleiche mit den obigen Beispielen.

3.6 Definition: Sei p prim und $x \in \mathbb{N}$. x heißt Primitivwurzel modulo p :$\Leftrightarrow$ $\mathrm{ord}(x) = p-1$.

Ist $x = 2$ eine Primitivwurzel für $p = 11$?

3.7 Theorem: Zu jeder Primzahl p existiert eine Primitivwurzel.

Beweis: (von Legendre, den Satz hatte schon Euler gefunden, dessen Beweis aber nicht korrekt war)

Strategie: $p-1 = q_1^{a_1} q_2^{a_2} \ldots q_\ell^{a_\ell}$ mit $q_1, \ldots, q_\ell$ paarweise verschiedene Primzahlen. In einem Teil des Beweises finden wir x_i mit Ordnung $q_i^{a_i}$, im anderen Teil machen wir aus den x_i $(i = 1, \ldots, \ell)$ das gesuchte ~~x_n~~ x.

Wir fangen mit dem zweiten Teil an, d.h. wir nehmen an, daß wir $x_1, \ldots, x_\ell$ mit Ordnung $q_1^{a_1}, \ldots, q_\ell^{a_\ell}$ schon gefunden haben.

Sei $x := x_1 \cdot \ldots \cdot x_\ell$ das Produkt. Zz $\mathrm{ord}(x) = p-1 = q_1^{a_1} \ldots q_\ell^{a_\ell}$. Das folgt mit Induktion aus der Behauptung: $\mathrm{ggT}(\mathrm{ord}(a), \mathrm{ord}(b)) = 1 \Rightarrow \mathrm{ord}(ab) = \mathrm{ord}(a) \cdot \mathrm{ord}(b)$

Denn: $(a \cdot b)^{\mathrm{ord}(a) \cdot \mathrm{ord}(b)} = a^{\mathrm{ord}(a)} \cdot b^{\mathrm{ord}(b)} \equiv 1 \cdot 1 = 1 \pmod p$

$\Rightarrow \mathrm{ord}(ab) \mid \mathrm{ord}(a) \cdot \mathrm{ord}(b)$, also $\mathrm{ord}(ab) = a_1 \cdot b_1$ mit $a_1 \mid \mathrm{ord}(a)$, $b_1 \mid \mathrm{ord}(b)$

d.h. $\mathrm{ord}(a) = a_1 \cdot a_2$, $\mathrm{ord}(b) = b_1 \cdot b_2$

$(ab)^{a_1 b_1} \equiv 1 \pmod p$ nach Wahl von a_1, b_1

Aber auch $(a \cdot b)^{a_1 a_2 b_1} = \underbrace{(a^{a_1 a_2})^{b_1}}_{\equiv 1} \cdot b^{a_1 a_2 b_1}$

$$\begin{array}{l} \| \\ ((ab)^{a_1 b_1})^{a_2} \equiv 1^{a_2} = 1 \end{array} \quad \Rightarrow \left. \begin{array}{l} b^{a_1 a_2 b_1} \equiv 1 \\ \| \\ b^{\mathrm{ord}(a) \cdot b_1} \end{array} \right\} \Rightarrow \mathrm{ord}(b) \mid \mathrm{ord}(a)\, b_1$$

Aber $\mathrm{ggT}(\mathrm{ord}(a), \mathrm{ord}(b)) = 1 \Rightarrow \mathrm{ord}(b) \mid b_1$, also $\mathrm{ord}(b) = b_1$

Analog $\mathrm{ord}(a) = a_1 \quad \Rightarrow$ Behauptung

was passiert, wenn $\mathrm{ggT}(\mathrm{ord}(a), \mathrm{ord}(b)) \neq 1$?

Also genügt es, die Existenz der x_i mit $\operatorname{ord}(x_i) = q_i^{a_i}$ zu zeigen.
Ein solches x_i muß (*) $x^{q^a} \equiv 1 \pmod p$ erfüllen, für $q = q_i$, $a = a_i$, aber die Ordnung darf auch nicht kleiner sein, d.h. x darf nicht

$$(**)\ \cancel{q}\ x^{q^{a-1}} \equiv 1 \pmod p \text{ erfüllen}$$

Das bedeutet: wir müssen zeigen, daß (*) mehr Lösungen hat als (**).

$\mathbb{Z}/p\mathbb{Z}$ Körper $\overset{\text{warum?}}{\Rightarrow}$ (*) hat höchstens q^a viele Lösungen
(**) hat höchstens q^{a-1} viele Lösungen

Wir zeigen: (*) hat genau q^a viele Lösungen
(**) hat genau q^{a-1} viele Lösungen

Daraus folgt dann: es gibt $q^a - q^{a-1}$ viele x_i's, also mindestens eines.

Allgemeiner zeigen wir:

Behauptung: Sei d ein Teiler von $p-1$. Dann hat $x^d \equiv 1 \pmod p$ genau d viele verschiedene Lösungen.

Beweis der Behauptung: $\mathbb{Z}/p\mathbb{Z}$ Körper $\Rightarrow$ höchstens d viele Lösungen

$X^d - 1 \mid X^{p-1} - 1$, denn: $p-1 = d \cdot e \Rightarrow x^{p-1} - 1 = (x^d)^e - 1 =$

$$= (x^d - 1)\underbrace{\left((x^d)^{e-1} + (x^d)^{e-2} + \dots + 1\right)}_{f(x)} \text{ mit } \deg f(x) = p-1-d$$

$x^{p-1} - 1 \equiv 0 \pmod p$ hat ganz $(\mathbb{Z}/p\mathbb{Z})^*$ als Lösungsmenge

Für eine Lösung y gilt manchmal sogar $y^d \equiv 1$. Wenn nicht, muß $f(y) \equiv 0$ gelten. Angenommen $y^d \equiv 1$ und $f(y) = 0$: $f(y) = (y^d)^{e-1} + \dots + 1 \equiv$
$\equiv 1 + 1 + \dots + 1 = e \not\equiv 0 \pmod p$, weil $e < p$ ↯ $\Rightarrow$ y erfüllt entweder $y^d \equiv 1$ oder $f(y) \equiv 0$, aber nicht beides.

höchstens d viele Lösungen

höchstens $\deg f = p-1-d$ viele Lösungen

Insgesamt $p-1$ viele Lösungen $\Rightarrow$ über "=" statt "höchstens" $\Rightarrow$ $x^d - 1$ hat genau d viele Lösungen
$\Rightarrow$ Behauptung $\square$

Laut Beweis gibt es für x_i gerade $\underbrace{q_i^{a_i} - q_i^{a_i - 1}}_{=\varphi(q_i^{a_i})}$ viele Wahlen, also $\varphi(q_i^{a_i})$ viele (φ = Eulersche φ-Funktion)

Insgesamt also $\varphi(p-1) = \varphi(q_1^{a_1}) \cdot \ldots \cdot \varphi(q_e^{a_e})$ viele Möglichkeiten. Sind die warum? alle verschieden? Anders gefragt: Gibt es $\varphi(p-1)$ viele verschiedene Primitivwurzeln oder weniger?

Sei x eine Primitivwurzel, d.h. $(\mathbb{Z}/p\mathbb{Z})^* = \{x, x^2, \ldots, x^{p-1} = 1\}$, welche x^i sind selbst Primitivwurzeln?

Sei $j = \text{ord}(x^i) \Rightarrow x^{ij} = (x^i)^j \equiv 1 \pmod p \overset{\text{warum?}}{\Rightarrow} p-1 \mid ij$

Falls $\text{ggT}(i, p-1) = 1$: $p-1 \mid j \Rightarrow p-1 = j$

Falls $\text{ggT}(i, p-1) \neq 1$: $j := \frac{p-1}{\text{ggT}(i,p-1)}$ funktioniert nachprüfen

Konsequenz: Die Anzahl der Primitivwurzeln modulo p ist $\varphi(p-1)$

Die Existenz von Primitivwurzeln hilft, mit Kongruenzen zu rechnen. Sei g eine Primitivwurzel modulo p. Dann ist $\{1, \ldots, p-1\} = \{g, g^2, \ldots, g^{p-1}\}$ und $g^a \cdot g^b = g^{a+b}$. Damit wird Multiplikation / Division zu Addition / Subtraktion – wie beim Logarithmus.

3.8 Definition: Sei g eine Primitivwurzel modulo p und $x = g^a$. a heißt der Index von x (bezüglich der Primitivwurzel g).

Bezeichnung: $\text{ind}_p x$. (Wir ignorieren g in dieser Notation.)

Zurück zu unserem Ausgangsproblem:

Gelöst werden soll die Kongruenz $x^k \equiv a \pmod p$, mit $a \not\equiv 0$, also $x \not\equiv 0$.

Falls eine Lösung x existiert, sei $\xi := \text{ind}_p x$ und $\alpha := \text{ind}_p a$.

$x^k \equiv a \pmod p$ bedeutet nicht $k\xi = \alpha$, sondern $k\xi \equiv \alpha \pmod{p-1}$

nachprüfen   kann größer als $p-1$ sein   kann $\leq p-1$ gewählt werden

Das ist eine lineare Kongruenz! ξ ist die Unbekannte.

Solche Kongruenzen haben wir schon betrachtet.

$k\xi \equiv \alpha \pmod{p-1} \iff \exists y: k\xi = \alpha + y(p-1)$
Lösbar nur, wenn $ggT(k, p-1) \mid \alpha$.
Sei $ggT(k,p-1) \mid \alpha \Rightarrow$ Euklidischer Algorithmus garantiert die Existenz einer Lösung. Genauer: sei $c := ggT(k,p-1)$, $k = c \cdot k'$, $\alpha = c\beta$
$\Rightarrow ck'\xi \equiv c\beta \pmod{p-1}$
$\Rightarrow k'\xi \equiv \beta \pmod{\frac{p-1}{c}}$, $ggT(k', \frac{p-1}{c}) = 1$, also ist k' invertierbar und es gibt genau eine Lösung ξ_0. Diese Lösung ξ_0 ist auch eine Lösung für $k\xi \equiv \alpha \pmod{p-1}$ nachprüfen
Aber $\xi_0 + \frac{p-1}{c}$, $\xi_0 + \frac{2(p-1)}{c}$ usw sind auch Lösungen und modulo $p-1$ voneinander verschieden. Zu der einen Lösungen modulo $\frac{p-1}{c}$ entsprechen also c viele Lösungen modulo $p-1$.
Ergebnis:
3-9 Theorem: Sei p prim. Die k-ten Potenzreste modulo p sind genau die $a \in \{1, .., p-1\}$ für die gilt: $ggT(k,p-1) \mid \mathrm{ind}_p\, a$.
Es gibt genau $\frac{p-1}{ggT(k,p-1)}$ viele k-te Potenzreste. Beweis daraufhin durchgehen

Spezialfall: $k=2$, $p>2$, also $ggT(2,p-1)=2 \Rightarrow$ die quadratischen Reste a haben geraden Index $\mathrm{ind}_p a$, die quadratischen Nichtreste haben ungeraden Index $\mathrm{ind}_p a$. Das sind jeweils $\frac{p-1}{2}$ viele Zahlen. Für einen quadratischen Rest a hat $x^2 \equiv a \pmod p$ genau zwei Lösungen. warum?

Zu den Zahlenbeispielen von oben:

p	k	ggT(k, p-1)	Anzahl quadratische Reste / kubische Reste
5	2	2	4/2
	3	1	4
11	2	?	?
	3	?	?
13	2	2	?
	3	3	4

Quadratische Reste verhalten sich "besser". Im nächsten Kapitel konzentrieren wir uns auf sie.