Seminarvortrag aus Reiner Mathematik

Zweierpotenzen als Moduln
und Satz von Wilson

Stefan Rosenberger

November 16, 2009

1 Notationen und Vorbemerkungen

1.1 Erinnerung an bekannte Definitionen

a) Für alle natürlichen n bezeichnet man
$\varphi(n) = |\{l \in \{0, ..., n-1\} : ggT(l, n) = 1\}| = |(\mathbb{Z}/n\mathbb{Z})^\times|$
als **EULERsche Phifunktion**.

b) Die Einheitengruppe $(\mathbb{Z}/m\mathbb{Z})^\times = \{a+m\mathbb{Z} | a \in \{1, ..., m\}, ggT(a, m) = 1\}$ nennt man **prime Restklassengruppe modulo m**.

c) Jede Menge von m ganzen Zahlen, die paarweise inkongruent modulo m sind, nennt man **ein vollstandiges Restsystem modulo m**.

d) Nach der Definition der Eulerschen Funktion gibt es genau $\varphi(m)$ zu m teilerfremde Zahlen. Damit gibt es genau $\varphi(m)$ verschiedene prime Restklassen modulo m. Diese können von jedem System von $\varphi(m)$ paarweise modulo m inkongruenten, zu m teilerfremden ganzen Zahlen repräsentiert werden.
Ein solches System heißt ein **primes Restsystem modulo m**.
z.B.: modulo 8 bildet die Menge $\{-3, -1, 1, 3\}$ ein primes Restsystem.

1.2 Zitierte Sätze

Die hier angeführten Sätze werden nur zitiert, da diese bereits in vorangegangenen Präsentationen bzw. in der Vorlesung erwähnt und bewiesen wurden.

Satz von Gauß: Modulo $m \in \mathbb{N}$ existieren genau dann Primitivwurzeln,wenn m gleich $1, 2, 4, p^\alpha, 2p^\alpha$ mit ungerader Primzahl p und natürlichem α ist.

Satz 2.3.2)7) aus der Vorlesung)
Sei G eine Gruppe, H eine Untergruppe von G und R ein Repräsentantensystem von G/H dann gilt $G = \bigcup_{r \in R} r \cdot H$ und $\forall r, r' \in R$ mit $r \neq r'$ gilt $rH \cap r'H = \emptyset$
(analog für die Rechtsnebenklasse)

Satz 2.5.10)2)(ii) aus der Vorlesung)
Sei G eine additiv geschriebene zyklische Gruppe und $g \in G :< g >= G$
Ist $|G| = n \in \mathbb{N}^+$ und ist $\pi_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ der kanonische Homomorphismus.
$\Rightarrow \exists! \varphi : \mathbb{Z}/n\mathbb{Z} \to G$ isomorph mit $\varphi(\pi_n(1)) = g$.
Notation: $\pi_n(x) = \overline{x}$

2 Zweierpotenzen als Moduln

2.1 Lemma

Seien $a, b \in \mathbb{Z},\ n \in \mathbb{N}^+$ falls $a \equiv b\ mod(2^n)$ ist, dann gilt $\forall m \in \mathbb{N}^+ :\ a^{2^m} \equiv b^{2^m}\ mod(2^{n+m})$

Beweis:
Seien $a, b \in \mathbb{Z},\ n \in \mathbb{N}^+$ sodass $a \equiv b\ mod(2^n)$.
d.h.: $\exists c \in \mathbb{Z} : 2^n c = a - b$ und da $a - b$ gerade ist, gilt auch dass $\exists \tilde{c} \in \mathbb{Z} : 2\tilde{c} = a + b$

Induktion über m) Sei $m = 1$.
$a^2 - b^2 = (a-b)(a+b) = 2^n c \cdot 2\tilde{c} = 2^{n+1} c\tilde{c}$
Daher gilt dass $2^{n+1} | a^2 - b^2$ und somit $a^2 \equiv b^2\ mod(2^{n+1})$

Gelte nun für $m \in \mathbb{N}$ dass $a^{2^m} \equiv b^{2^m}\ mod(2^{n+m})$ ist.
d.h.: $\exists d \in \mathbb{Z} : 2^{n+m} d = a^{2^m} - b^{2^m}$ und wieder da $a^{2^m} - b^{2^m}$ gerade ist, gilt dass $\exists \tilde{d} \in \mathbb{Z} : 2\tilde{d} = a^{2^m} + b^{2^m}$

$m \to m+1)\ \ a^{2^{m+1}} - b^{2^{m+1}} = (a^{2^m} - b^{2^m})(a^{2^m} + b^{2^m}) = 2^{n+m} d \cdot 2\tilde{d} = 2^{n+m+1} d\tilde{d}$
Daher gilt dass $2^{n+m+1} | a^{2^{m+1}} - b^{2^{m+1}}$ und somit $a^{2^{m+1}} \equiv b^{2^{m+1}}\ mod(2^{n+m+1})$

2.2 Lemma

Bei ungeradem ganzen u gilt:
i) $\forall \alpha \geq 3 :\ u^{2^{\alpha-2}} \equiv 1\ mod(2^\alpha)$
ii) $u \equiv \pm 3\ mod(8) \Rightarrow \forall \alpha \geq 3 : ord_{2^\alpha}(u) = 2^{\alpha-2}$
iii) $u \equiv \pm 1\ mod(8) \Rightarrow \forall \alpha \geq 4 : ord_{2^\alpha}(u) | 2^{\alpha-3}$

Bemerkung: Da u ungerade ist kann nur gelten $u \equiv \pm 3\ mod(8)$ oder $u \equiv \pm 1\ mod(8)$ womit jeder Fall betrachtet wird.

Beweis:
i) Nach 2.1 genügt es die Aussage für $\alpha = 3$ zu zeigen.
Sei $x \in \mathbb{Z}$ sodass $u = 2x + 1$ (Existiert da u ungerade).
$u^2 - 1 = (2x+1)^2 - 1 = 4x^2 - 4x = 2^2 x(x+1)$
Da $x(x+1)$ gerade ist gilt dass $2^3 | u^2 - 1$ und somit $u^2 \equiv 1\ mod(2^3)$

ii) Hierbei zeigen wir zuerst die Hilfsaussage
$u \equiv \pm 3\ mod(2^3)\ \Rightarrow \forall \beta \in \mathbb{N}^+\ \exists \nu_\beta \in \mathbb{Z}\backslash 2\mathbb{Z}\ : u^{2^\beta} - 1 = 2^{\beta+2} \nu_\beta$.

Sei $u \equiv \pm 3\ mod(8)$. d.h.: $\exists c \in \mathbb{Z} :\ u = 8c \pm 3$
Induktion über β)
Sei $\beta = 1$. $\quad u^2 - 1 = (8c \pm 3)^2 - 1 = 64c^2 \pm 48c + 8 = 8(8c^2 \pm 6c + 1)$
Daher gilt $u^2 - 1 = 2^3 \nu_1$ mit $\nu_1 = (8c^2 \pm 6c + 1) \in \mathbb{Z} \setminus 2\mathbb{Z}$

Gelte nun $u^{2^\beta} - 1 = 2^{\beta+2} \nu_\beta$ mit $\nu_\beta \in \mathbb{Z}\backslash 2\mathbb{Z}$ für ein $\beta \in \mathbb{N}$.
$\beta \to \beta+1)\ u^{2^{\beta+1}} - 1 = (u^{2^\beta})^2 - 1 = (2^{\beta+2}\nu_\beta + 1)^2 - 1 = 2^{2\beta+4}\nu_\beta^2 + 2^{\beta+3}\nu_\beta = 2^{\beta+3}(2^{\beta+1}\nu_\beta^2 + \nu_\beta)$
d.h.: $u^{2^{\beta+1}} - 1 = 2^{(\beta+1)+2} \nu_{\beta+1}$ mit $\nu_{\beta+1} = (2^{\beta+1}\nu_\beta^2 + \nu_\beta) \in \mathbb{Z}\backslash 2\mathbb{Z}$.

Die Aussage (i) heißt insbesondere dass $ord_{2^\alpha}(u) | 2^{\alpha-2}$.
Sei daher nun $ord_{2^\alpha}(u) := 2^\gamma$ mit $\gamma \in \mathbb{N}$ womit gilt $u^{2^\gamma} \equiv 1\ mod(2^\alpha)$.
d.h.: $2^\gamma | 2^{\alpha-2}$ und somit muss gelten: $\gamma \leq \alpha - 2$
Andererseits gilt nach der eben gezeigen Hilfsaussage dass:
$2^\alpha | u^{2^\gamma} - 1 = 2^{\gamma+2}\nu_\beta$ mit $\beta \in \mathbb{Z} \setminus 2\mathbb{Z}$. d.h.: $2^\alpha | 2^{\gamma+2}$ und somit muss gelten: $\gamma \geq \alpha - 2$
Und somit gilt :$ord_{2^\alpha}(u) = 2^{\alpha-2}$

iii) Sei $u \equiv \pm 1 \ mod(2^3)$
Nach (2.1) gilt dass $u^{2^\alpha} \equiv 1 \ mod(2^{3+\alpha})$ und somit gilt wenn $\alpha \geq 4$ ist dass $u^{2^{\alpha-3}} \equiv 1 \ mod(2^\alpha)$ und damit $ord_{2^\alpha}(u) | 2^{\alpha-3}$ $\square$

2.3 Satz

Bei ganzem $\alpha \geq 3$ und $u \equiv \pm 3 \ mod(8)$ sind die folgenden $\varphi(2^\alpha) = 2^{\alpha-1}$ Zahlen paarweise inkongruent modulo 2^α
$u, u^2, u^3, ..., u^{2^{\alpha-2}}, -u, -u^2, ..., -u^{2^{\alpha-2}}$

Beweis: Sei $A_1 = \{u, u^2, ..., u^{2^{\alpha-2}}\}$ und $A_2 = \{-u, -u^2, ..., -u^{2^{\alpha-2}}\}$.
Nach 2.2(ii) gilt: $ord_{2^\alpha}(u) = 2^{\alpha-2}$ womit alle Elemente in A_1 paarweise inkongruent sind, und daher auch die Elemente aus A_2.

Da $u \equiv \pm 3 \ mod(8) \Rightarrow 8 | u \pm 3$ daher ist u ungerade und somit sind alle Elemente in A_1 und A_2 ungerade.

Zeige dass auch jedes der Elemente in A_1 inkongruent zu jedem der Elementen in A_2 ist.
Angenommen $u^i \equiv -u^j \ mod(2^\alpha)$ für $1 \leq i, j \leq 2^{\alpha-2}$
o.B.d.A.: $j \leq i$ dann gilt:
$u^i + u^j = u^j(u^{i-j} + 1)$ und da $2^\alpha | u^i + u^j$ sowie u ungerade ist $\Rightarrow 2^\alpha | u^{i-j} + 1$
d.h.: $u^{i-j} \equiv -1 \ mod(2^\alpha)$ mit (2.1) gilt nun $u^{2(i-j)} \equiv 1 \ mod(2^{\alpha+1})$
Aus 2.2(ii) folgt $ord_{2^{\alpha+1}}(u) = 2^{\alpha-1}$
$2^{\alpha-1} | 2(i-j) \Rightarrow 2^{\alpha-2} | i-j$ und da gilt $0 \leq i-j < 2^{\alpha-2} \Rightarrow i-j = 0 \Rightarrow i = j$
$\Rightarrow u^i \equiv -u^i \ mod(2^\alpha)$ und daher gilt $2^\alpha | u^i + u^i = 2u^i \Rightarrow 2^{\alpha-1} | u^i$ und da $\alpha \geq 3$ ist, steht dies im Widerspruch zu u ist ungerade. $\square$

Bemerkung: Sei $a \in A_1 \cup A_2$. Da u ungerade ist gilt $ggT(a, 2^\alpha) = 1$, und da diese $\varphi(2^\alpha) = 2^{\alpha-1}$ Zahlen paarweise inkongruent modulo 2^α sind, bildet die Menge $A_1 \cup A_2$ ein primes Restsystem modulo 2^α.

2.4 Korollar

Sei $u \in \mathbb{Z}$ ungerade, $u \equiv \pm 3 \ mod(8)$ sowie $\alpha \in \mathbb{N}_{\geq 3}$. Dann gibt es einen Gruppenisomorphismus
$\varphi : \ (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{\alpha-2}\mathbb{Z}) \longrightarrow (\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ mit $\varphi(\bar{i}, \bar{j}) = (\overline{-1})^i \cdot \overline{u}^j \ \forall i, j \in \mathbb{Z}$.

Beweis:
Es gilt nach (2.2) dass $ord(\overline{u}) = 2^{\alpha-2}$, $ord(\overline{-1}) = 2$ und $|(\mathbb{Z}/2^\alpha\mathbb{Z})^\times| = \varphi(2^\alpha) = 2^{\alpha-1}$. Nach dem "Struktursatz für zyklische Gruppen" (2.5.10.2(ii)) gibt es Isomorphismen φ und $\tilde{\varphi}$ sodass:

$$\varphi = \begin{cases} (\mathbb{Z}/2\mathbb{Z}) \longrightarrow < \overline{-1} > \\ \bar{i} \longmapsto (-1)^i \end{cases}$$

$$\tilde{\varphi} = \begin{cases} (\mathbb{Z}/2^{\alpha-2}\mathbb{Z}) \longrightarrow < \overline{u} > \\ \bar{j} \longmapsto (u)^j \end{cases}$$

Betrachte nun:

$$\psi = \begin{cases} (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{\alpha-2}\mathbb{Z}) \longrightarrow (\mathbb{Z}/2^\alpha\mathbb{Z})^\times \\ (\bar{i}, \bar{j}) \longmapsto \varphi(i)\tilde{\varphi}(j) \end{cases}$$

Für $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ betrachte das prime Restsystem $A_1 \cup A_2$ von 2.3. Und für $(\mathbb{Z}/2\mathbb{Z})$ betrachte $\{0, \overline{1}\}$ sowie für $(\mathbb{Z}/2^{\alpha-2}\mathbb{Z})$ die Menge $\{1, ..., \overline{2^{\alpha-2}}\}$.
Dann gilt für $(-1)^i u^j \in (A_1 \cup A_2)$ existiert $(\bar{i}, \bar{j}) \in (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{\alpha-2}\mathbb{Z}) \ : \ \psi(\bar{i}, \bar{j}) = (-1)^i u^j$. Und daher ist ψ surjektiv.
Nach (2.2) gilt dass $ord(\overline{u}) = 2^{\alpha-2}$, $ord(\overline{-1}) = 2$ und $|(\mathbb{Z}/2^\alpha\mathbb{Z})^\times| = \varphi(2^\alpha) = 2^{\alpha-1}$. Daher ist $|(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{\alpha-2}\mathbb{Z})| = |(\mathbb{Z}/2^\alpha\mathbb{Z})^\times|$ und somit ist ψ injektiv.
Seien $(i, j), (k, l) \in (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{\alpha-2}\mathbb{Z})$. Dann gilt $\psi((i, j)(k, l)) = \psi(ik, jl) = \varphi(ik)\tilde{\varphi}(jl) = \varphi(i)\varphi(k)\tilde{\varphi}(j)\tilde{\varphi}(l) =$

$\varphi(i)\tilde{\varphi}(j)\varphi(k)\tilde{\varphi}(l) = \psi(i,j)\psi(k,l)$ somit ist ψ homomorph.
Und daher ist ψ ein Isomorphismus.

3 Satz von Wilson und die Verallgemeinerung nach Gauß

3.1 Vorbemerkung

Sei G eine endliche abelsche Gruppe (multiplikativ geschrieben).
Definiere:
$\pi(G) := \prod_{g\in G} g,\ \ G_2 := \{g \in G | g^2 = 1\},\ \ G(2) := \{g \in G_2 | ord(g) = 2\} \subset G_2.$

G_2 ist eine Untergruppe von G denn $1 \in G_2$, für $g_1, g_2 \in G_2$ gilt $g_1g_2 \cdot g_1g_2 = g_1g_2g_2g_1 = g_1g_1 = 1$ und somit ist $g_1 \cdot g_2 \in G_2$ und jedes Element in G_2 ist zu sich selbst invers, somit ist G_2 eine Untergruppe von G.

3.2 Lemma

Sei G eine endliche abelsche Gruppe. Dann gilt:

$$\pi(G) = \begin{cases} 1 & \text{wenn } |G(2)| = 0 \text{ oder } |G(2)| \geq 2 \\ g & \text{wenn } |G(2)| = 1 \text{ und } G(2) = \{g\} \end{cases}$$

Beweis: Es gilt:

$$\pi(G) = \prod_{g\in G} g = \prod_{g\in G_2} g \cdot \prod_{g\in G\setminus G_2} g$$

Falls $g \in G \setminus G_2$

$$\Rightarrow g^2 \neq 1 \Rightarrow g \neq g^{-1} \text{und } g^{-1} \in G \setminus G_2 \text{ und natürlich gilt } g \cdot g^{-1} = 1$$

$$\text{Also gilt: } \prod_{g\in G\setminus G_2} g = 1$$

Und daher kann o.E. angenommen werden dass $G = G_2$ d.h.: $g^2 = 1\ , \forall g \in G$.
1.Fall) $|G(2)| = 0 \Rightarrow G = \{1\} \Rightarrow \pi(G) = 1$.
2.Fall) $|G(2)| = 1 \Rightarrow G(2) = \{g\} \Rightarrow G = \{1, g\} \Rightarrow \pi(G) = g$.
3.Fall) $|G(2)| \geq 2$.
Seien nun $g_1, g_2 \in G(2)$ mit $g_1 \neq g_2$, sowie $H := \{1, g_1, g_2, g_1g_2\}$, wiederum ist H eine Untergruppe von G denn $1 \in H,\ \ ord(g_i) = 2\ , i \in \{1, 2\}$ und daher sind alle g_i selbstinvers und natürlich gilt H ist abgeschlossen.

Sei nun $R \subset G$ ein Repräsentantensystem für G/H, dann hat jedes $g \in G$ eine eindeutige Darstellung der Form $g = r \cdot h$ mit $r \in R, h \in H$.
Die Existenz und Eindeutigkeit der Darstellung folgt unmittelbar aus 2.3.2)7) der Vorlesung Einführung in die Algebra.

Nun gilt $\forall x \in 2\mathbb{Z}\ \forall r \in R :\ r^x = 1$

$$\pi(G) = \prod_{g\in G} g = \prod_{r\in R}\prod_{h\in H}(r\cdot h) = \prod_{r\in R}\prod_{h\in H} r\cdot\prod_{r\in R}\prod_{h\in H} h = \prod_{r\in R} r^{|H|}\cdot(\pi(H))^{|R|} = (\prod_{r\in R} 1)\cdot(1\cdot g_1\cdot g_2\cdot g_1g_2)^{|R|} = 1$$

Was zu zeigen war. □

3.3 Verallgemeinerung von Gauß

Sei $m \in \mathbb{N}$. Dann gilt:

$$\prod_{\substack{i=1 \\ ggT(i,m)=1}}^{m-1} i \equiv \begin{cases} -1 & \text{mod(m) existiern Primitivwurzeln} \\ 1 & \text{mod(m) existieren keine Primitivwurzeln} \end{cases}$$

Beweis: Es gilt:

$$\pi(\prod_{\substack{i=1 \\ ggT(i,m)=1}}^{m-1} i) = \prod_{g \in (\mathbb{Z}/m\mathbb{Z})^\times} g$$

Zeige daher:

$$\prod_{g \in (\mathbb{Z}/m\mathbb{Z})^\times} g = \begin{cases} -1 & \text{mod(m) existiern Primitivwurzeln} \\ 1 & \text{mod(m) existieren keine Primitivwurzeln} \end{cases}$$

1.Fall) $m = 1$, dann gilt $(\mathbb{Z}/m\mathbb{Z})^\times = (\mathbb{Z}/\mathbb{Z})^\times = \{0\} = \{1\} = \{-1\}$.
Womit gilt dass $\prod_{(g \in \mathbb{Z}/\mathbb{Z})^\times} = -1$. Nach dem Satz von Gauß ist somit die Aussage wahr. ✓
2.Fall) $m = 2$, dann gilt $(\mathbb{Z}/m\mathbb{Z})^\times = (\mathbb{Z}/2\mathbb{Z})^\times = \{\overline{0}, 1\}^\times = \{1\} = \{-1\}$.
Womit gilt dass $\prod_{(g \in \mathbb{Z}/2\mathbb{Z})^\times} = -1$. Und widerum ist die Aussage mit dem Satz von Gauß wahr. ✓
3.Fall) Sei $m \geq 3$.
Hierbei müssen wir zwei verschiedene Fälle betrachten.
Zum Einen: Gibt es mod(m) Primitivwurzeln, so ist nach dem vorangegangenen Lemma zu zeigen: $-1 \in (\mathbb{Z}/m\mathbb{Z})^\times$ ist das einzige Element der Ordnung 2.
Gebe es nun mod(m) Primitivwurzeln ,dann gilt $(\mathbb{Z}/m\mathbb{Z})^\times \cong (\mathbb{Z}/\varphi(m)\mathbb{Z})$. Also ist zu zeigen dass in $(\mathbb{Z}/\varphi(m)\mathbb{Z})$ existiert genau ein Element der Ordnung 2.
"Existenz"
Da $m \geq 3$ gilt dass $\varphi(m)$ gerade ist.
Sei daher $\varphi(m) = 2k$ mit $k \in \mathbb{N}^+$. Sei $\pi : \mathbb{Z} \to \mathbb{Z}/2k\mathbb{Z}$ der Restklassen Homomorphismus.
$2\pi(k) = \pi(2k) = 0$, $\pi(k) \neq 0 \Rightarrow \pi(k)$ ist ein Element der Ordnung 2.
"Eindeutigkeit"
Sei $l \in [0, 2k-1]$ und $ord(\pi(l)) = 2 \Rightarrow l \neq 0$, und $0 = 2\pi(l) = \pi(2l)$ und daher gilt $2k|2l \Leftrightarrow k|l \Rightarrow k = l$.

Zum Anderen: Gebe es nun mod(m) keine Primitivwurzeln. z.z.: in $(\mathbb{Z}/m\mathbb{Z})^\times$ gibt es mindestens zwei ungleiche Elemente der Ordung 2. Nach dem Satz von Gauß sind zwei Fälle zu betrachten
a) Sei $m = 2^\alpha,\ \alpha \geq 3$. Wie bereits gezeigt gilt:
$(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/\overline{2^{\alpha-2}}\mathbb{Z}) =: G$.
Es gilt die Restklassen $(\overline{0}, \overline{2^{\alpha-3}}), (\overline{1}, \overline{0}) \in (\mathbb{Z}/2\mathbb{Z})$. Und daher gilt $|G(2)| \geq 2 \Rightarrow \pi(G) = 1$.
b) Sei $m = p^\beta \cdot m'$, mit $m' \in \mathbb{N}^+_{\geq 3}, p \in \mathbb{P}_{\geq 3}$ und $p \nmid m'$
$G := (\mathbb{Z}/m\mathbb{Z})^\times \cong (\mathbb{Z}/p^\beta\mathbb{Z})^\times \times (\mathbb{Z}/m'\mathbb{Z})^\times$ gilt nach dem Chinesischen Restsatz.
Weiters gilt $(-1, 1), (1, -1) \in G(2)$ womit gilt $|G(2)| \geq 2 \Rightarrow \pi(G) = 1$.
(Bemerkung: da $m' \geq 3 \Rightarrow 1 \neq -1$ in $(\mathbb{Z}/m'\mathbb{Z})^\times \Rightarrow (1, -1) \neq (-1, 1)$) □

3.4 Satz von Wilson

Für $m \in \mathbb{N}_{\geq 2}$ ist m genau dann eine Primzahl wenn gilt $(m-1)! \equiv -1\ mod(m)$.

Beweis:
Sei $m \in \mathbb{P}$.
Nach der Verallgemeinerung von Gauss und da $\forall k \in \mathbb{N}^+, p \in \mathbb{P}\ k < p : ggT(k, p) = 1$ und es modulo einer Primzahl Primitivwurzeln gibt, gilt $(m-1)! \equiv -1\ mod(m)$.
Sei nun andererseits $(m-1)! \equiv -1\ mod(m)$
Angenommen m ist keine Primzahl, dann gibt es ein $p \in \mathbb{P}$ sodass $m = px$ mit $x \in \mathbb{N}_{\geq 2}$ und $1 < p < m$.
Dann gilt $p|m$ und $p|(m-1)!$ Daraus folgt $p|m|(m-1)!$ und $p|(m-1)! + 1$
Daher teilt p die Differenz, also $p|1$. Was im Widerspruch zu $p \in \mathbb{P}$ steht.□