Wir wollen jetzt die Struktur der Gruppe

$$G = G_\nu = (\mathbb{Z}/p^\nu\mathbb{Z})^\times \quad , \quad p \text{ Primzahl}, \nu \in \mathbb{N} \ [\nu > 1]$$

untersuchen. (Prime Restklassengruppe mod p^ν)

$\mathrm{ord}(G) = \varphi(p^\nu)$

$$\varphi(p^\nu) = \#\{\underset{\uparrow}{0} \le a < p^\nu \mid p \nmid a\} = p^\nu - \#\{0 \le a < p^\nu \mid p \mid a\}$$
$$\mathbb{Z} \qquad\qquad a = pb,\ 0 \le b < p^{\nu-1}$$

also $$\varphi(p^\nu) = p^\nu - p^{\nu-1} = (p-1)p^{\nu-1} \qquad (\nu \ge 1)$$

Damit gilt für jedes $n \in \mathbb{N}$

$$\varphi(n) = \varphi\Big(\prod_{p|n} p^{w_p(n)}\Big) = \prod_{p|n} \varphi\big(p^{w_p(n)}\big) = \prod_{p|n}\big(p^{w_p(n)} - p^{w_p(n)-1}\big)$$

$$= \prod_{p|n} p^{w_p(n)}\Big(1 - \frac{1}{p}\Big) = n \prod_{p|n}\Big(1 - \frac{1}{p}\Big)$$

F3: Für jedes $n \in \mathbb{N}$ gilt

$$\varphi(n) = \prod_{p|n}\big(p^{w_p(n)} - p^{w_p(n)-1}\big) = n \cdot \prod_{p|n}\Big(1 - \frac{1}{p}\Big)$$

Def. Sei $G_\nu = (\mathbb{Z}/p^\nu)^\times$ wie oben. Der Kern $G_\nu^{(1)}$ des Homomorphismus

$$(\mathbb{Z}/p^\nu)^\times \longrightarrow (\mathbb{Z}/p)^\times$$
$$a \bmod p^\nu \longmapsto a \bmod p$$

heißt die Gruppe der 1-Einheiten von $(\mathbb{Z}/p^\nu)^\times$. Sie besteht aus den Elementen $a \bmod p^\nu$ von $(\mathbb{Z}/p^\nu)^\times$ mit $a \equiv 1 \bmod p$.*) Es ist

(*) $$\mathrm{ord}(G_\nu^{(1)}) = p^{\nu-1}$$

*) Für $p = 2$ ist $G_\nu = G_\nu^{(1)}$, denn: $2 \nmid a \Rightarrow a \equiv 1 \bmod 2$.

Bew. von (*). leichtes Abzählen: $0 \le 1+jp < p^\nu$ genau für $0 \le j \le p^{\nu-1}-1$;
also nach Homomorphiesatz: $\operatorname{ord}(G_\nu) = \operatorname{ord}(G_\nu^{(1)}) \cdot \operatorname{ord}((\mathbb{Z}/p)^\times)$,
also $\operatorname{ord}(G_\nu^{(1)}) = (p-1)p^{\nu-1} : (p-1) = p^{\nu-1}$.

Lemma 2: p Primzahl, $j \in \mathbb{N}$, $a \in \mathbb{Z}$. Es gelte

(1) $a \equiv 1 \bmod p^j$, aber $a \not\equiv 1 \bmod p^{j+1}$

Dann folgt – außer für $\boxed{p=2 \text{ und } j=1}$ –

(2) $a^p \equiv 1 \bmod p^{j+1}$, aber $a^p \not\equiv 1 \bmod p^{j+2}$ *)

Bew. w. u.

*) die erste Beh. von (2) gilt auch für $p=2$ und $j=1$.

F4: Sei $\nu > 1$.

(i) Im Falle $p \neq 2$ ist für jedes a der Gestalt $a = 1+cp$ mit $p \nmid c$ die Restklasse $a \bmod p^\nu$ ein Element der Ordnung $p^{\nu-1}$ in der 1-Einheitengruppe von $(\mathbb{Z}/p^\nu)^\times$. Insbesondere gilt dies für $a = 1+p$.
Die 1-Einheitengruppe von $(\mathbb{Z}/p^\nu)^\times$ ist also für $p \neq 2$ zyklisch (mit kanonischem Erzeuger $1+p \bmod p^\nu$).

$5 = 1+2^2$

(ii) Im Falle $p=2$ gilt: Für $\nu \ge 3$ ist $5 \bmod 2^\nu$ ein Element der Ordnung $2^{\nu-2}$ in $(\mathbb{Z}/2^\nu)^\times$.
Für $\nu = 2$: $(\mathbb{Z}/4\mathbb{Z})^\times$ ist zyklisch mit $-1 \bmod 4$ als Erzeuger.

Bew. 1) $p \neq 2$. $a \equiv 1 \bmod p$, $a \not\equiv 1 \bmod p^2$. Induktiv mit Lemma 2:

$$a^{p^j} \equiv 1 \bmod p^{j+1}, \quad a^{p^j} \not\equiv 1 \bmod p^{j+2},$$

also $a^{p^j} \not\equiv 1 \bmod p^\nu$ für alle $1 \le j \le \nu-2$ (und natürlich $a^{p^{\nu-1}} \equiv 1 \bmod p^\nu$). $\Rightarrow \operatorname{ord}(a \bmod p^\nu) = p^{\nu-1}$.

2) $p=2$. $5 \equiv 1 \bmod 2^2$, $5 \not\equiv 1 \bmod 2^3$. Mit Lemma 2 folgt Beh.

Bew. des Lemmas: Es gilt

(*) $\binom{p}{j} \equiv 0 \bmod p$ für $1 \le j \le p-1$

(vgl. Aufgabe 23 oder: p teilt Zähler, aber nicht Nenner von $\binom{p}{j} = \frac{p(p-1)\cdots}{1\cdot 2\cdots j} \in \mathbb{N}$)

bei Vor. (1) bedeutet $a = 1 + xp^j$ mit $p \nmid x$.

$2j \ge j+1$ für $j \in \mathbb{N}$

$a^p = (1+xp^j)^p = 1 + \binom{p}{1}xp^j + \binom{p}{2}x^2p^{2j} + \dots + x^pp^{pj}$, $\Rightarrow$

$a^p \equiv 1 + xp^{j+1} + x^pp^{pj} \bmod p^{j+2}$ [$\Rightarrow a^p \equiv 1 \bmod p^{j+1}$]

$pj \ge j+2$ bis auf Fall: $p=2$ und $j=1$. Also:

$a^p \equiv 1 + xp^{j+1} \bmod p^{j+2}$ bis auf den Ausnahmefall.

$\Downarrow$

(2).

Satz 2: Sei $p \ne 2$. Auch für $\nu \ge 2$ ist dann $(\mathbb{Z}/p^\nu\mathbb{Z})^\times$ zyklisch.

Mit anderen Worten: $(\mathbb{Z}/p^\nu\mathbb{Z})^\times$ besitzt eine Primitivwurzel.

Es existiert also ein $g \in \mathbb{Z}$, so daß es zu jedem $a \in \mathbb{Z}$ mit $(a,p)=1$ genau ein $i \in \mathbb{Z}$ gibt mit

$$a \equiv g^i \bmod p^\nu \quad \text{und} \quad 0 \le i < \varphi(p^\nu)$$

Es gibt genau $\varphi(\varphi(p^\nu)) = \varphi((p-1)p^{\nu-1}) = \varphi(p-1)\,\varphi(p^{\nu-1})$ Primitivwurzeln von $(\mathbb{Z}/p^\nu)^\times$.

Zusatz: Ist schon eine Primitivwurzel $g_0 \bmod p$ bekannt, so findet man eine Primitivwurzel $\bmod p^\nu$ wie folgt: Ist $g_0^{p-1} \ne 1 \bmod p^2$, so ist $g = g_0$ eine Primitivwurzel $\bmod p^\nu$. Ist $g_0^{p-1} \equiv 1 \bmod p^2$, so ist $g = g_0 + p$ eine Primitivwurzel $\bmod p^\nu$.

Beweis: 1) Ist g eine Primitivwurzel mod p mit $g^{p-1} \not\equiv 1 \bmod p^2$, so ist g auch eine Primitivwurzel mod p^ν. Denn:

Nach Fermat ist $g^{p-1} = 1 + cp$ mit einem $c \in \mathbb{Z}$, und nach Vor. ist $p \nmid c$. Nach F4 gilt dann für $\alpha := g \bmod p^\nu$

$$\operatorname{ord}(\alpha^{p-1}) = p^{\nu-1}$$

*) $\operatorname{ord}(g \bmod p) = p-1$

Sei $k := \operatorname{ord}(\alpha)$. $\Rightarrow g^k \equiv 1 \bmod p^\nu$, $\Rightarrow g^k \equiv 1 \bmod p$, $\overset{*)}{\Rightarrow}$ $p-1 \mid k$. Damit

$$p^{\nu-1} = \operatorname{ord}(\alpha^{p-1}) = \frac{k}{(k, p-1)} = \frac{k}{p-1}, \text{ also } k = (p-1)p^{\nu-1} = \varphi(p^\nu),$$

und es folgt die Beh.

2) Sei g_0 eine bel. Primitivwurzel mod p. Ist $g_0^{p-1} \not\equiv 1 \bmod p^2$, so fertig nach 1).

Sei also $g_0^{p-1} \equiv 1 \bmod p^2$. Betrachte nun $g := g_0 + p$.

[$p-1 \geq 2$]

Es ist $g^{p-1} = (g_0 + p)^{p-1} \equiv g_0^{p-1} + (p-1) g_0^{p-2} p \bmod p^2$.

Also $g^{p-1} \equiv 1 - g_0^{p-2} p \bmod p^2$, $\overset{p \nmid g_0}{\Longrightarrow}$

$g^{p-1} \not\equiv 1 \bmod p^2$, $\overset{1)}{\Longrightarrow}$ g ist Prim.wurzel mod p^ν.

q. e. d.

Bem. Gibt es überhaupt eine Primitivwurzel g_0 mit $0 < g_0 < p$, für die $g_0^{p-1} \equiv 1 \bmod p^2$ gilt?

Kleinstes Bsp. ist $p = 29$ mit $g_0 = 14$. Doch g_0 ist nicht die kleinste Prim. wurzel mod 29. Diese ist 2, und für sie gilt $2^{p-1} \not\equiv 1 \bmod p^2$ für $p = 29$. Also Problem:

Kann $g_0^{p-1} \equiv 1 \bmod p^2$ für die kleinste Primitivwurzel $g_0 \bmod p$ gelten? Kleinstes Beispiel?

Computer: Für die 4244-te Primzahl $p = 40487$ ist $g_0 = 5$ die kleinste Primitivwurzel $\bmod p$ und es gilt

$$g_0^{p-1} \equiv 1 \bmod p^2.$$

Bem. Nach Satz 2 (mit Zusatz) ist klar, daß folgende Aussagen für $p \neq 2$ und $g \in \mathbb{Z}$ äquivalent sind:

(i) g ist Primitivwurzel $\bmod p$ und $g^{p-1} \not\equiv 1 \bmod p^2$.

(ii) g ist Primitivwurzel $\bmod p^n$ für alle $n \in \mathbb{N}$.

(iii) g ist Primitivwurzel $\bmod p^2$.

Satz 3: Sei $\nu \in \mathbb{N}$, $\nu \geq 3$. Zu jeder ungeraden Zahl $a \in \mathbb{Z}$ gibt es eindeutig bestimmte $k \in \{0,1\}$ und $j \in \{0,1,\dots,2^{\nu-2}-1\}$ mit

$$a \equiv (-1)^k 5^j \bmod 2^\nu$$

Mit anderen Worten: Die Abbildung

$$(*) \qquad \begin{aligned} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\nu-2}\mathbb{Z} &\longrightarrow (\mathbb{Z}/2^\nu)^\times \\ (k \bmod 2,\ j \bmod 2^{\nu-2}) &\longmapsto (-1 \bmod 2^\nu)^k \cdot (5 \bmod 2^\nu)^j \end{aligned}$$

ist ein Isomorphismus von Gruppen. Es ist also

$$(\mathbb{Z}/2^\nu\mathbb{Z})^\times = \langle -1 \bmod 2^\nu \rangle \times \langle 5 \bmod 2^\nu \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\nu-2}\mathbb{Z}$$

Insbesondere ist $(\mathbb{Z}/2^\nu\mathbb{Z})^\times$ nicht zyklisch.

Bew. 1) Die Abb. (*) ist wohldefiniert (!)*) und ein Homomorphismus.

*) beachte: nach F4(ii) ist $\operatorname{ord}(5 \bmod 2^\nu) = 2^{\nu-2}$.

2) Da Definitions- und Bildbereich von (*) gleichviel Elemente haben,

z.z.z. (*) ist injektiv, d.h. $\operatorname{Kern}(*)$ trivial.

Sei also $(-1)^k 5^j \equiv 1 \bmod 2^\nu$, $\overset{\nu \geq 3}{\Rightarrow} (-1)^k \equiv 1 \bmod 2^2$,

$\Rightarrow k$ gerade, $\Rightarrow k \bmod 2 = 0$. Jetzt folgt

$$5^j \equiv 1 \bmod 2^\nu \xrightarrow[\text{nach F4(i)}]{\operatorname{ord}(5 \bmod 2^\nu) = 2^{\nu-2}} 2^{\nu-2} \mid j \Rightarrow j \bmod 2^{\nu-2} = 0$$

3) $G := \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\nu-2}\mathbb{Z}$ nicht zyklisch, denn offenbar ist

$e(G) = 2^{\nu-2}$ $(< \operatorname{ord}(G) = 2^{\nu-2})$.

(Dass G nicht zyklisch ist, folgt auch aus Eindeutigkeitsaussage des Hauptsatzes über endliche abelsche Gruppen)

Anderer Beweis: $G := (\mathbb{Z}/2^\nu\mathbb{Z})^\times$

$G^{(2)} := \{ a \bmod 2^\nu \mid a \equiv 1 \bmod 4 \}$ 1-Einheitengruppe 2-te Stufe von $(\mathbb{Z}/2^\nu\mathbb{Z})^\times$

$\|$

$\mathrm{Kern}\left((\mathbb{Z}/2^\nu\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/2^2\mathbb{Z})^\times \right)$. Offenbar ist $G = \langle -1 \rangle \times G^{(2)}$

z.z. $G^{(2)} = \langle \bar{5} \rangle$, $\bar{5} = 5 \bmod 2^\nu$.

$\mathrm{ord}(G^{(2)}) = 2^{\nu-2}$. Nach F4 gilt aber $\mathrm{ord}(5 \bmod 2^\nu) = 2^{\nu-2}$,

$\Rightarrow G^{(2)} = \langle \bar{5} \rangle$.

Satz 2': Sei p Primzahl mit $p \neq 2$. $\nu \in \mathbb{N}$, $\nu \geq 2$. Dann existiert eine Primitivwurzel $g \bmod p$, so daß die Abbildung

$$(*) \quad \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{\nu-1}\mathbb{Z} \longrightarrow (\mathbb{Z}/p^\nu)^\times$$
$$(i \bmod (p-1),\ j \bmod p^{\nu-2}) \longmapsto g^i (1+p)^j \bmod p^\nu$$

wohldefiniert und ein Isomorphismus von Gruppen ist. Insbesondere ist $(\mathbb{Z}/p^\nu\mathbb{Z})^\times$ zyklisch (d.h. wir erhalten von neuem Satz 2).

Bew. Sei zunächst $a \bmod p$ eine beliebige Prim.wurzel $\bmod p$. Nach Euler-Fermat gilt $a^{(p-1)p^\mu} \equiv 1 \bmod p^\nu$ für $\mu = \nu - 1$. Setze nun $g = a^{p^\mu}$. Dann $\mathrm{ord}(g \bmod p) = \frac{\mathrm{ord}(a \bmod p)}{(p-1, p^\mu)} = p-1$, also ist g Prim.wurzel $\bmod p$. Aber g erfüllt jetzt

$$(**) \quad g^{p-1} \equiv 1 \bmod p^\nu$$

Damit ist $(*)$ wohldefiniert und ein Homomorphismus.