...

Wir sehen, daß die maximale Ordnung in $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ höchstens $2^{\alpha-2}$ ist. $\boxed{/\!/}$

Bem: $(\mathbb{Z}/2\mathbb{Z})^*$ und $(\mathbb{Z}/4\mathbb{Z})^*$ sind zyklisch.

Beob: Ist p eine ungerade Primzahl, so sei $\bar{g}$ ein primitives Element von $(\mathbb{Z}/p^\alpha)^*$ und g sei ein ungerader Representant von $\bar{g}$ in $\mathbb{Z}$.

Die Potenzen von g sind alle ungerade und durchlaufen sämtliche zu $2p^\alpha$ teilerfremden Restklassen mod $2p^\alpha$. Insbesondere ist g primitiv mod $2p^\alpha$. $\square$

Damit haben wir die Antwort:

Satz: Die Einheitengruppe $(\mathbb{Z}/m\mathbb{Z})^*$ ist genau dann zyklisch, wenn $m = 1, 2, 4,$ p^α oder $2p^\alpha$ ist, wobei p eine ungerade

Primzahl ist.

<u>Bew</u>: Wir haben gesehen, daß für alle aufgezählten Moduli m die Einheitengruppe $(\mathbb{Z}/m\mathbb{Z})^*$ zyklisch ist.

Höhere Potenzen von 2 haben wir schon ausgeschlossen.

Sei nun $m = m_1 m_2$ mit

$$\left.\begin{array}{l} ggT(m_1, m_2) = 1 \\ m_1 > 2 \\ m_2 > 2 \end{array}\right. \qquad (*)$$

Setze $k := kgV(\varphi(m_1), \varphi(m_2))$.

Ist nun g teilerfremd zu m, so ist g teilerfremd zu m_1 und zu m_2. Also ist

$$g^{\varphi(m_i)} \equiv 1 \mod m_i \qquad i = 1, 2$$

$$\Rightarrow \quad g^k \equiv 1 \mod m \quad \forall \bar{g} \in (\mathbb{Z}/m\mathbb{Z})^*$$

Es reicht also $k < \varphi(m)$ zu zeigen.

Nun sind $\varphi(m_1)$ und $\varphi(m_2)$ beide gerade:

Hat n einen ungeraden Primfaktor p, so ist $\varphi(n)$ Vielfaches der geraden Zahl $p-1$.
Ist $n = 2^{\alpha}$ mit $\alpha \geq 2$, so ist $\varphi(n) = 2^{\alpha-1}$.

Also ist $2k \mid m_1 m_2 = m$.

Darum: Im Fall $(*)$ ist $(\mathbb{Z}/m\mathbb{Z})^*$ nicht zyklisch.

Inspektion: Alle Fälle sind abgedeckt. $\square$

Potenzreste

Def: Sei p eine Primzahl und a teilerfremd zu p. Wir nennen a einen <u>Potenzrest der Ordnung n</u>, wenn die Kongruenz

$$x^n \equiv a \mod p$$

lösbar ist.

Potenzreste der Ordnung 2 heißen <u>quadratische Reste</u>. Ist a teilerfremd zu p aber kein quadratischer Rest, so heißt a <u>quadratischer Nichtrest</u>.

Prop: p: prim, $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^*$. Die Gleichung

$$(*) \qquad \bar{x}^n = \bar{a} \quad \text{in } \mathbb{Z}/p\mathbb{Z}$$

hat keine Lösung, es sei denn:

$$(\Delta) \qquad \bar{a}^{\left(\frac{p-1}{\text{ggT}(p-1,n)}\right)} = \bar{1} \quad \text{in } \mathbb{Z}/p\mathbb{Z}$$

In diesem Fall hat $(*)$ genau $\text{ggT}(p-1, n)$ Lösungen.

<u>Bew:</u> Sei $\bar{g}$ ein primitives Element von $(\mathbb{Z}/p\mathbb{Z})^*$ und $\bar{a} = \bar{g}^{k}$.

Dann hat $(*)$ eine Lösung $\bar{x} \in \mathbb{Z}/p\mathbb{Z}$ genau dann, wenn

$$(\square) \qquad nx \equiv k \mod p-1$$

eine Lösung in $\mathbb{Z}/(p-1)\mathbb{Z}$ hat.

Nun ist die Lösbarkeit von $(\square)$ gleichbedeutend mit

$$k \in \mathbb{Z}n + \mathbb{Z}(p-1) = \mathbb{Z}\,ggT(n, p-1)$$

$$\iff ggT(n, p-1) \mid k$$

$$\iff p-1 \;\Big|\; \frac{k\,(p-1)}{ggT(n, p-1)}$$

$$\iff \left(\bar{g}^{k}\right)^{\frac{p-1}{ggT(n,p-1)}} = \bar{1} \text{ in } (\mathbb{Z}/p\mathbb{Z})^*$$

$$\iff (\Delta)$$

Ist nun (Δ) erfüllt, so gibt es mod $(p-1)$, so ist $(\square)$ äquivalent zu

$$\underbrace{\frac{n}{ggT(n,p-1)}}_{n'} x \equiv \underbrace{\frac{k}{ggT}}_{k'} \mod \underbrace{\frac{p-1}{ggT}}_{m'}$$

wobei n' und m' teilerfremd sind. Es gibt also genau eine Lösung mod m'. Darüber liegen $ggT(n, p-1)$ Lösungen mod $(p-1)$. $\boxtimes$

<u>Bsp</u>: $X^5 \equiv 6 \mod 101$ hat 5 Lösungen:

1) $5 = ggT(n=5, \; p-1 = 100)$

2) $\frac{100}{5} = 20$. Also müssen wir zeigen:

$$6^{20} \equiv 1 \mod 101$$

$$6^2 \equiv 36$$

$$6^4 = 36 \cdot 36 = 1225 + 70 + 1 = 1296$$
$$\equiv 286 \mod 101$$
$$\equiv 84 \mod 101$$

$$6^8 \equiv 84^2 = 7225 - 170 + 1 = 7056$$
$$\equiv -14 \mod 101$$

$$6^{16} \equiv (-14)^2 = 196 \equiv 95 \mod 101$$

$$6^{20} = 6^4 \cdot 6^{16} \equiv \frac{84 \times 95}{\begin{array}{r} 756 \\ 420 \\ \hline 7980 \end{array}} \equiv \underline{\underline{1 \mod 102}} \qquad \frac{79 \times 101}{7979}$$

Kor (Eulerkriterium)

Sei p eine Primzahl $\neq 2$ und $p \nmid a$. Dann ist a quadratischer Rest mod p genau dann, wenn gilt:

$$a^{\frac{p-1}{2}} \equiv 1 \mod p$$

Andernfalls ist $a^{\frac{p-1}{2}} \equiv -1 \mod p$.

Bew. $\left(a^{\frac{p-1}{2}}\right)^2 \equiv 1 \mod p$. Die Gleichung

$$x^2 = \overline{1}$$

hat die beiden Lösungen ± 1 in $\mathbb{Z}/p\mathbb{Z}$. $\boxtimes$

Quadratische Kongruenzen mod p

Wir wollen

$$(*) \quad ax^2 + bx + c \equiv 0 \mod p$$

lösen. Zunächst: ist $p | a$, so ist $(*)$ äquivalent zur linearen Kongruenz $bx + c \equiv 0$.

Also: O.B.d.A.: $p \nmid a$

D.h.: $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^*$

Modulo p können wir also durch $\bar{a}$ teilen, und $(*)$ ist äquivalent zu

$$(\square) \qquad x^2 + px + q \equiv 0 \mod p$$

$$\Leftrightarrow \quad x^2 + px \equiv -q$$

$$\Leftrightarrow \quad \left(x + \frac{p}{2}\right)^2 \equiv \left(\frac{p}{2}\right)^2 - q \qquad \Big| \ \underline{\underline{p \neq 2}}$$

Also: $(\square)$ ist lösbar genau dann, wenn $\left(\frac{p}{2}\right)^2 - q$ ein quadratischer Rest ist.

Mit $y := x + \frac{p}{2}$ $\quad d := \left(\frac{p}{2}\right)^2 - q$ ist $(\square)$ äquivalent zu:

$$(\Delta) \qquad y^2 \equiv d \mod p$$

Beob: Ist $d \equiv 0 \mod p$, so hat (Δ) genau eine Lösung mod p, nämlich $y \equiv 0$.
Ist d quadratischer Nichtrest, so hat (Δ) keine Lösung.

Ist d quadratischer Rest und ist y eine Lösung, so ist $-y \not\equiv y$ die zweite Lösung von (Δ). (Hier geht wieder $p \neq 2$ ein.)

Quadratwurzeln in $\mathbb{Z}/p\mathbb{Z}$:

Wir wollen (Δ) lösen. Wir nehmen an, daß $p \neq 2$ ist und daß d ein quadratischer Rest ist.

Erinnerung: Ein Rest $\bar{d} \in (\mathbb{Z}/p\mathbb{Z})^*$ ist quadratischer Rest, wenn:

$$\bar{d}^{\frac{p-1}{2}} = \bar{1}$$

und quadratischer Nichtrest, wenn:

$$\bar{d}^{\frac{p-1}{2}} = -\bar{1}$$

Bem: Die Hälfte aller Reste in $(\mathbb{Z}/p\mathbb{Z})^*$ sind quadratische Reste, die andere Hälfte sind quadratische Nichtreste.

$\Rightarrow$ Ein quadr. Nichtrest läßt sich leicht durch Raten finden.

Lemma: Sei p eine ungerade Primzahl, und seien $\bar{a}, \bar{b} \in (\mathbb{Z}/p\mathbb{Z})^*$ Elemente der Ordnung 2^k mit $k \geq 1$. Dann hat das Produkt $\bar{a}\bar{b}$ Ordnung 2^j mit $j < k$.

Bew: $(\bar{a}\bar{b})^{2^k} = \bar{a}^{2^k} \bar{b}^{2^k} = 1$

$\Rightarrow \operatorname{ord}(\bar{a}\bar{b}) \mid 2^k$

$\Rightarrow \operatorname{ord}(\bar{a}\bar{b}) = 2^j$ mit $j \leq k$.

Da a Ordnung 2^k hat, hat $a^{2^{k-1}}$ die Ordnung 2, d.h.

$$\bar{a}^{2^{k-1}} = -1$$

$\ulcorner (\mathbb{Z}/p\mathbb{Z})^*$ hat $\varphi(2) = 1$ El. der Ord. 2 $\lrcorner$

Analog $\bar{b}^{2^{k-1}} = -1$.

Also: $(\bar{a}\bar{b})^{2^{k-1}} = \bar{a}^{2^{k-1}} \bar{b}^{2^{k-1}} = (-1)(-1) = 1$.

Also $\operatorname{ord}(\bar{a}\bar{b}) \mid 2^{k-1}$. $\boxtimes$

Verfahren: Vorbereitungsschritt:

1) Bestimme m und k mit:

$$p-1 = 2^k m \qquad \begin{array}{l} m: \text{ungerade} \\ k \geq 1 \end{array}$$

2) Rate einen quadratischen Nichtrest z mod p.

Nun setze:

$$\left.\begin{array}{l} r := d^{\frac{m+1}{2}} \\ n := d^{m} \end{array}\right\} \Rightarrow r^2 \equiv dn \mod p$$

Einfacher Fall: $n \equiv 1 \mod p$

Dann ist $x = \pm r$.

Anderer Fall: $n \not\equiv 1 \mod p$

Beob: $n^{2^k} = d^{2^k m} = d^{p-1} \equiv 1 \mod p$

$$\Rightarrow \operatorname{ord}(n) \mid 2^k$$

Beob: $n^{2^{k-1}} = d^{\frac{p-1}{2}} \equiv 1 \mod p$

weil d ein quadratischer Rest ist.

<u>Also</u>: $\operatorname{ord}(n) = 2^j$ mit $j < k$.

Bestimme j durch wiederholtes Quadrieren.

<u>Analog</u>: $c := z^m$ hat Ordnung 2^k.

$\ulcorner$ $c^{2^k} = z^{2^k m} = z^{p-1} \equiv 1 \mod p$

$c^{2^{k-1}} = z^{\frac{p-1}{2}} \equiv -1 \mod p$, denn

z ist quadratischer Nichtrest. $\lrcorner$

<u>Also</u>: $c^{2^{k-j}}$ hat Ordnung 2^j.

Lemma $\Rightarrow$ $n c^{2^{k-j}}$ hat kleinere Ordnung.

<u>Iteration</u>:

$b := c^{2^{k-j-1}}$ | hat Ordnung 2^{j+1}

$c' := b^2$ | hat Ordnung 2^j

$n' := c'n$ | hat Ordnung 2^i mit $i < j$ (Lemma)

$r' := br$

$\Rightarrow$ $r'^2 = b^2 r^2 = c'nd = dn' \mod p$