Zu Blatt 6:

(1.) a) Teilbarkeitsregel für 7:

Beispiel:

verkleinernde Zahl → 864 ← letzte Stelle streichen
− 6 ← −2 × 3 (letzte Stelle)
verkleinernde Zahl → 85 ← letzte Stelle streichen
− 16 ← −2 × 8
69 ← nicht durch 7 teilbar

⇒ 8643 ist nicht durch 7 teilbar

kurz:

8643
− 6
858
− 16
69

entspricht:

8643
− 63 ← 3 · 21
858 *
− 168 ← 8 · 21
69 *

7427
− 14 ← 2 · 7
728
− 16 ← 2 · 8
56 ← durch 7 tb.!
(−12 / −7)

$7 \cdot 1 = 7 \quad 7 \cdot 2 = 14 \quad 7 \cdot 3 = \underline{\underline{21}}$

⇒ 3 ist die 1. Zahl, die mit 7 multipliziert eine 1 an letzter Stelle des Produkts erzeugt!

$7 \cdot 3 = \underline{\underline{21}}$

Das 2-fache der letzten Ziffer muss von der verkleinernden Zahl abgezogen werden!!!

Grund!

- 21 ist durch 7 teilbar!
- Wenn man von einer durch 7 teilbaren Zahl eine durch 7 teilbare Zahl (also insbesondere 21 & jedes Vielfache von 21) abzieht, bleibt die Zahl durch 7 teilbar!
- Bei 21 ist die Zehnerziffer (nämlich 2) doppelt so groß wie die Einerziffer (nämlich 1)!

⇒ Damit das, was in jedem Schritt insgesamt abgezogen wird (Streichung der Einerziffer & Subtraktion) ein Vielfaches von 21 ist, muss der Subtrahend doppelt so groß wie die Einerziffer die gestrichen wird sein!

* (Streichen einer 0 (≙ Teilen durch 10) ändert nichts an der Teilbarkeit durch 7!)

b) Teilbarkeitsregel für 13:

$13 \cdot 1 = 13,\ 13 \cdot 2 = 26,\ 13 \cdot 3 = 39,\ 13 \cdot 4 = 52,\ 13 \cdot 5 = 65,\ 13 \cdot 6 = 78,$

$13 \cdot 7 = \underline{\underline{91}}$ ← 1. Produkt von 13 mit Einerziffer 1

Das 9-Fache der Einerziffer muss von der verkleinernden Zahl abgezogen werden!!!

(analog zu a)) → Grund:

- 91 ist durch 13 teilbar!
- Bei 91 ist die Zehnerziffer 9 mal so groß wie die Einerziffer!

⇒ Damit das, was in jedem Schritt insgesamt abgezogen wird (Streichung & Subtraktion) ein Vielfaches von 91 ist, muss der Subtrahend 9x so groß wie die Einerziffer sein!!! (die gestrichen wird)

Teilbarkeitsregel für 17:

c) $17 \cdot 1 = 17$, $17 \cdot 2 = 34$, $17 \cdot 3 = \underline{51}$ ← 1. Produkt von 17 mit Einerziffer 1!

Das 5-Fache der Einerziffer muss von der verbleibenden Zahl abgezogen werden !!!

(analog zu a) → **Grund:**
- 51 ist durch 17 teilbar!
- Bei 51 ist die Zehnerziffer 5x so groß wie die Einerziffer!

⇒ Damit das, was in jedem Schritt insgesamt abgezogen wird (Streichung & Subtraktion) ein Vielfaches von 5x ist, muss der Subtrahend 5x so groß wie die Einerziffer sein, die gestrichen wird !!!

2.) a) Modulo 12 rechnen !!!

$200 = \underbrace{12 \cdot 16}_{192} + \underline{8}$ ⇒ $200 \bmod 12 = \underline{8}$

⇒ 3 Uhr + 8 Stunden = **11 Uhr** !

(oder Modulo 24:

$200 = \underbrace{24 \cdot 8}_{192} + \underline{8}$

⇒ $200 \bmod 24 = 8$

⇒ 3 Uhr + 8 Std. = 11 Uhr!)

b) Modulo **24** rechnen !!!

$300 = \underbrace{24 \cdot 12}_{288} + \underline{12}$ ⇒ $300 \bmod 24 = \underline{12}$

⇒ 15 Uhr + 12 Stunden = **3 Uhr** !
(3 Uhr Nachmittags) (3 Uhr **Nachts**)

c) Modulo 7 rechnen !!!

$100 = \underbrace{7 \cdot 14}_{98} + \underline{2}$ ⇒ $100 \bmod 7 = \underline{2}$

⇒ Montag + 2 Tage = **Mittwoch** !!!

d) Modulo 7 rechnen !!! (denn es gibt 7 versch. Wochentage)

1.) kein Schaltjahr → d.h. **365** Tage:

$365 = \underbrace{7 \cdot 52}_{364} + \underline{1}$ ⇒ $365 \bmod 7 = \underline{1}$

⇒ Sonntag + 1 Tag = **Montag** !!!

2.) Schaltjahr → d.h. **366** Tage:

$366 = \underbrace{7 \cdot 52}_{364} + \underline{2}$ ⇒ $366 \bmod 7 = \underline{2}$

⇒ Sonntag + 2 Tage = **Dienstag** !!!

3.) a) $3 \cdot x = 7k + 1 \quad (0 \leq x < 7)$

$3 \cdot 0 = 0$
$3 \cdot 1 = 3$
$3 \cdot 2 = 6$
$3 \cdot 3 = 9 = 7 + 2$
$3 \cdot 4 = 12 = 7 + 5$

$3 \cdot \underline{5} = 15 = 2 \cdot 7 + \underline{1} \quad \Rightarrow$ Lösung: $x = 5$

b) $2 \cdot x = 8k + 1 \quad (0 \leq x < 8)$

Es gibt keine Lösung, denn 2 und 8 sind nicht teilerfremd!
$(ggT(2,8) = 2 \neq 1)$

c) $7 \cdot x = 10k + 1 \quad (0 \leq x < 10)$

$7 \cdot 0 = 0$
$7 \cdot 1 = 7$
$7 \cdot 2 = 14 = 10 + 4$
$7 \cdot \underline{3} = 21 = 2 \cdot 10 + \underline{1} \quad \Rightarrow$ Lösung: $x = 3$

d) $4 \cdot x = 12k + 1 \quad (0 \leq x < 12)$

Es gibt keine Lösung, denn $ggT(4,12) = 4 \neq 1$!

e) $4 \cdot x = 15k + 1 \quad (0 \leq x < 15)$

$4 \cdot 0 = 0$
$4 \cdot 1 = 4$
$4 \cdot 2 = 8$
$4 \cdot 3 = 12$

$4 \cdot \underline{4} = 16 = 1 \cdot 15 + \underline{1} \quad \Rightarrow$ Lösung: $x = 4$

f) Behauptung:

Damit die Gleichung $a \cdot x = m \cdot k + 1$ (mit $0 \leq x < m$) genau ein Lösung besitzt, muss gelten: $ggT(a,m) = 1$, d.h. a und m müssen teilerfremd sein!

$(\exists!\ x$ mit $0 \leq x < m$, so dass $a \cdot x = m \cdot k + 1) \Leftrightarrow ggT(a,m) = 1.$

Beweis zu 3.) f):

"⇒" Es gebe ein x mit $0 \le x < m$, so dass $a \cdot x = m \cdot k + 1$. ($\Leftrightarrow ax - mk = 1$)

zu zeigen: $ggT(a, m) = 1$.

Beweis durch Widerspruch:

A: $ggT(a, m) = q > 1$.

$\Rightarrow q \mid a$ und $q \mid m \Rightarrow q \mid \underbrace{(ax - mk)}_{=1 \text{ nach Voraus.}} \Rightarrow q \mid 1$ ↯ Widerspruch zu $q > 1$

$\Rightarrow$ Die Annahme ist also falsch, d.h. $ggT(a, m) = 1$.

"⇐" siehe nächster Zettel!

"⇐" Beweis mit euklidischem Algorithmus:

Es gelte: $ggT(a,m) = 1$.

zu zeigen: Es gibt genau ein x mit $0 \le x < m$, so dass $a \cdot x = m \cdot k + 1$.

Euklidischer Algorithmus zur Bestimmung des ggT von a und m:

(1) $a = q_1 \cdot m + r_1$
(2) $m = q_2 \cdot r_1 + r_2$
(3) $r_1 = q_3 \cdot r_2 + r_3$
(4) $r_2 = q_4 \cdot r_3 + r_4$
$\vdots$
(5) $r_{n-4} = q_{n-2} \cdot r_{n-3} + r_{n-2}$
(6) $r_{n-3} = q_{n-1} \cdot r_{n-2} + r_{n-1}$
(7) $r_{n-2} = q_n \cdot r_{n-1} + \boxed{r_n}$
(8) $r_{n-1} = q_{n+1} \cdot r_n + \underbrace{r_{n+1}}_{=0}$ $\Rightarrow$ r_n ist $ggT(a,m) \Rightarrow r_n = 1$ nach Voraussetzung!

Rückwärtseinsetzen:

(7) $\Rightarrow r_n = r_{n-2} - q_n r_{n-1}$
(6) $\Rightarrow r_{n-1} = r_{n-3} - q_{n-1} r_{n-2}$
$\Rightarrow r_n = r_{n-2} - q_n \overbrace{(r_{n-3} - q_{n-1} r_{n-2})}^{r_{n-1}}$

$= r_{n-2} - q_n r_{n-3} + q_n q_{n-1} r_{n-2}$

$= r_{n-2} \underbrace{(1 + q_n q_{n-1})}_{=: A_{n-2,2}} - \underbrace{q_n}_{=: A_{n-3,1}} r_{n-3}$

(5) $\Rightarrow r_{n-2} = r_{n-4} - q_{n-2} r_{n-3}$ $\Rightarrow r_n = \overbrace{(r_{n-4} - q_{n-2} r_{n-3})}^{r_{n-2}}(1 + q_n q_{n-1}) - q_n r_{n-3}$

$= r_{n-4} + r_{n-4} q_n q_{n-1} - q_{n-2} r_{n-3} - q_{n-2} r_{n-3} q_n q_{n-1} - q_n r_{n-3}$

$= r_{n-3} \underbrace{(-q_{n-2} - q_{n-2} q_n q_{n-1} - q_n)}_{=: A_{n-3,2}} + r_{n-4} \underbrace{(1 + q_n q_{n-1})}_{=: A_{n-4,1}}$

$\vdots$

$\Rightarrow r_n = r_2 \cdot A_{2,2} + r_1 \cdot A_{1,1}$

$\Rightarrow r_n = r_1 \cdot A_{1,2} + m \cdot A_{m,1}$

$\Rightarrow r_n = m \cdot A_{m,2} + a \cdot A_{a,1}$, (*)

wobei die A's irgendwelche ganzzahligen Faktoren sind & $r_n = 1$ nach Voraussetzung (siehe oben).

(*) $\Rightarrow a \cdot A_{a,1} = m \cdot (-A_{m,2}) + \underbrace{r_n}_{=1}$

$\Rightarrow$ Gleichung $a \cdot x = m \cdot k + 1$ besitzt eine Lösung [mit $x = A_{a,1}$ (und $k = -A_{m,2}$)].

Fortsetzung: Beweis zu 3f) "⇐"

noch zu zeigen: 1.) $0 \leq x < m$, und

2.) x ist eindeutig!

zu 1.):

Annahme: $x \geq m$ (oder $x < 0$), z.B. $x = n \cdot m + e$ mit $0 \leq e < m$ und mit $ax = mk + 1$.

Dann gilt: $a(n \cdot m + e) = mk + 1 \quad (\Leftrightarrow anm + ae = mk + 1 \Leftrightarrow ae = \underbrace{mk - anm}_{m(k-an)} + 1)$

$\Leftrightarrow \quad a \cdot e = m\tilde{k} + 1 \quad$ mit $\tilde{k} = k - an$

D.h. dann gibt es ein $\tilde{x}$ (hier: $\tilde{x} = e$), welches die Gleichung $a\tilde{x} = m\tilde{k} + 1$ erfüllt und zwischen 0 und m liegt ($0 \leq \tilde{x} = e < m$).

Zu 2.):

Annahme: Es gibt x und x' mit $0 \leq x, x' < m$, $x \neq x'$ und

$ax = mk + 1$, sowie $ax' = mk' + 1$.

Dann gilt: $ax - ax' = mk + 1 - (mk' + 1)$

$\Leftrightarrow a(x - x') = m(k - k')$

$\Rightarrow m \mid a(x - x')$

Wegen $ggT(a, m) = 1$ nach Voraus. muss also gelten: $m \mid (x - x')$ ↯

Dies ist aber ein Widerspruch zu $0 \leq x, x' < m$, also $x - x' < m$!

$\Rightarrow$ Annahme falsch, d.h. $x = x'$, also x ist eindeutig!

($x - x' = 0$, $m \mid 0$ ✓)

□

Alternativ-Beweis zu Aufg. 3 f) • "⇐": (ohne euklidischen Algorithmus)

Es gelte: $ggT(a,m) = 1$.

zu zeigen: Es gibt genau ein x mit $0 \le x < m$, so dass $a \cdot x = mk + 1$.

Betrachte auf der Menge $M := \{0, 1, 2, \dots, m-1\}$ die Funktion

$$\varphi : M \to M, \quad x \mapsto (ax) \bmod m.$$

Es gilt: φ ist injektiv, d.h. für alle $x_1, x_2 \in M$ mit $x_1 \neq x_2$ gilt $\varphi(x_1) \neq \varphi(x_2)$,

denn: Seien $x_1, x_2 \in M$ mit $x_1 \neq x_2$.

A: $\varphi(x_1) = \varphi(x_2)$.

$\Leftrightarrow (ax_1) \bmod m = (ax_2) \bmod m$

$\Leftrightarrow \exists k_1, k_2 \in \mathbb{Z}: ax_1 - k_1 m = ax_2 - k_2 m$

$\Leftrightarrow ax_1 - ax_2 = k_1 m - k_2 m$

$\Leftrightarrow a\underbrace{(x_1 - x_2)}_{\neq 0, \text{ da } x_1 \neq x_2} = m(k_1 - k_2)$

Wegen $ggT(a,m) = 1$ nach Vorauss., muss gelten $m \mid (x_1 - x_2)$ ↯

Dies ist ein Widerspruch zu $x_1, x_2 \in M = \{0, 1, 2, \dots, m-1\}$.

⇒ Annahme widerlegt, d.h. φ ist injektiv.

Wenn es also ein x mit $0 \le x < m$ (und ein!) gibt, so dass $ax = mk + 1$ ($\hat{=} (ax) \bmod m = 1$), dann ist dieses x eindeutig.

Weiterhin gilt: φ ist surjektiv, denn die injektive Abbildung einer endlichen Menge (hier M) auf sich selbst ist immer surjektiv!

D.h. also $\forall y \in M: \exists x \in M: \varphi(x) = y$.

⇒ Insbesondere gilt also für $y = 1 \in M$:

$\exists x \in M: \varphi(x) = 1$, d.h. $(ax) \bmod m = 1$,

d.h. $\exists k \in \mathbb{Z}: ax = mk + 1$.

□

(2, 4)

$f_1 \cdot f_2 \equiv 1 \bmod 15 \Rightarrow$ Kreisdiagramme gleich

$f = 0$ macht keinen Sinn!
→ Landet alles auf 0:

$1 \cdot 0 = 0 \quad 0 \bmod 15 = 0$
$2 \cdot 0 = 0 \quad 0 \bmod 15 = 0$
$\vdots$
$14 \cdot 0 = 0 \quad 0 \bmod 15 = 0$

$f = 1$ macht keinen Sinn!
→ Landet alles auf sich selbst:

$1 \cdot 1 = 1 \quad 1 \bmod 15 = 1$
$2 \cdot 1 = 2 \quad 2 \bmod 15 = 2$
$\vdots$
$14 \cdot 1 = 14 \quad 14 \bmod 15 = 14$

$f = 2 \triangleq f = 8$, denn: $2 \cdot 8 = 16$, $16 \bmod 15 = 1$

$f = 3$

$f = 4$

$f = 5$

$f = 6$

$f = 7 \triangleq f = 13$, denn: $7 \cdot 13 = 91$, $91 \bmod 15 = 1$
($91 = 6 \cdot 15 + 1$)

$f = 9$

$f = 10$

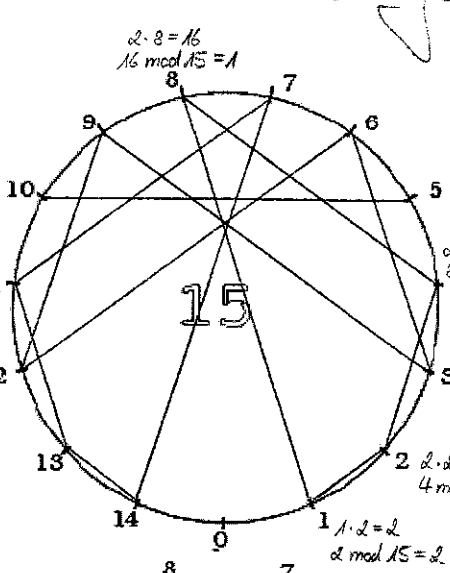
$f = 11$

$f = 12$

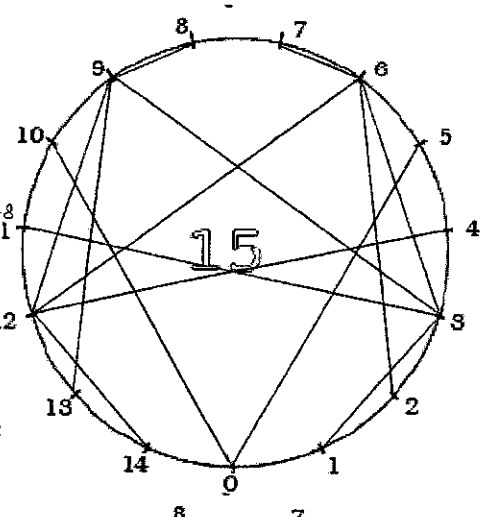
$f = 14$

$\Rightarrow$ 11 verschiedene Kreisdiagramme !!!

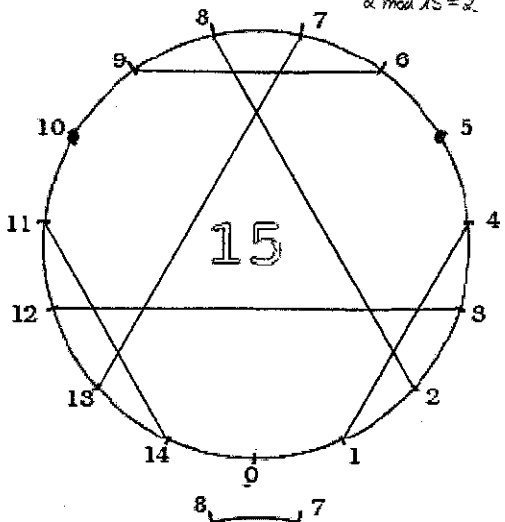
Die Diagramme müssen symmetrisch sein!!



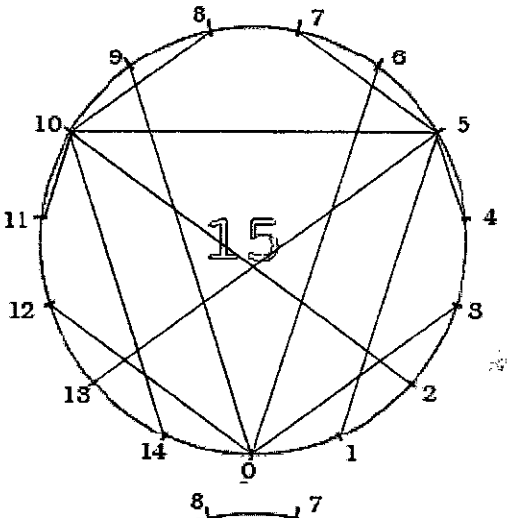
$f = 2$ bzw. 8
$\rightarrow \cdot 2 \bmod 15$
bzw.
$\cdot 8 \bmod 15$



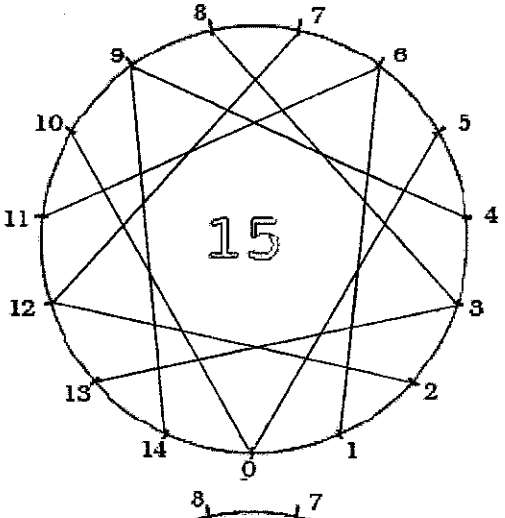
$f = 3$
$\rightarrow \cdot 3 \bmod 15$



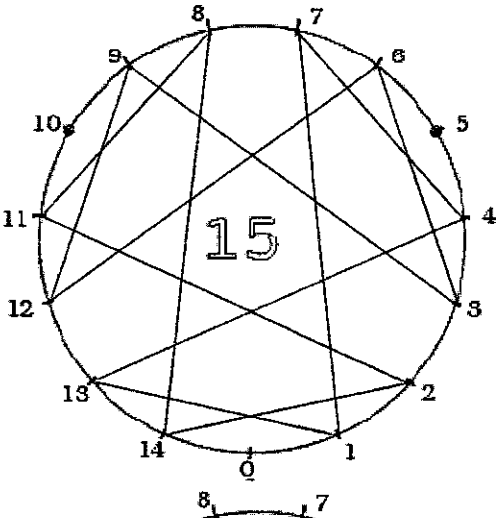
$f = 4$
$\rightarrow \cdot 4 \bmod 15$



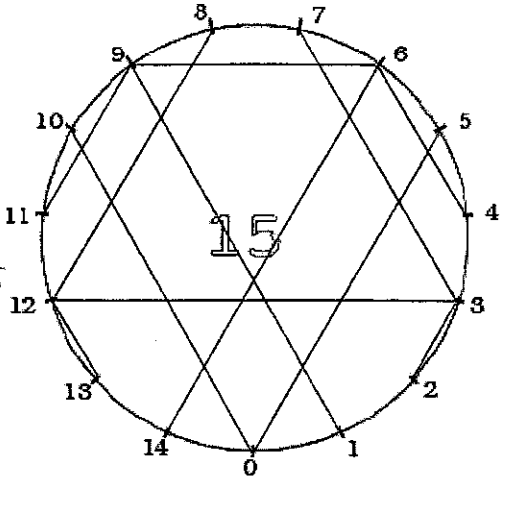
$f = 5$
$\rightarrow \cdot 5 \bmod 15$



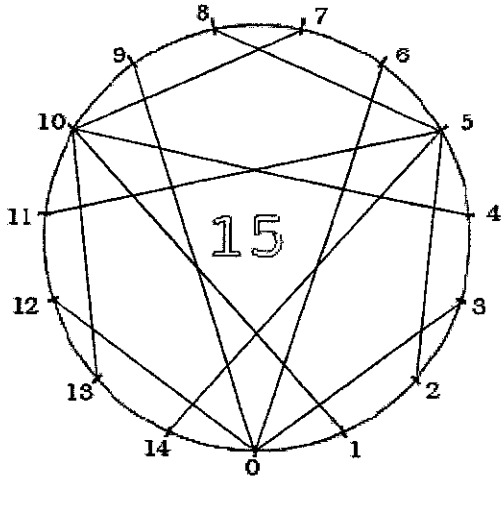
$f = 6$
$\rightarrow \cdot 6 \bmod 15$



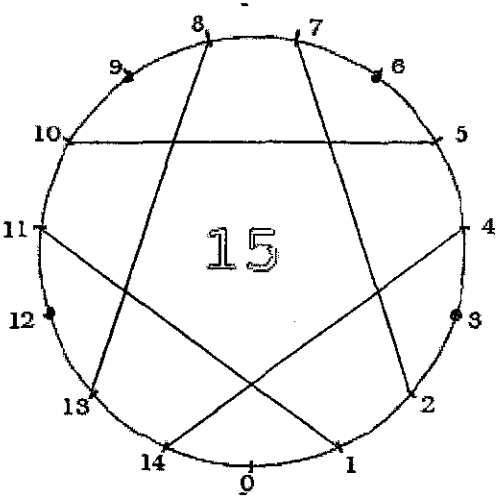
$f = 7$ bzw. 13
$\rightarrow \cdot 7 \bmod 15$
bzw.
$\cdot 13 \bmod 15$



$f = 9$
$\rightarrow \cdot 9 \bmod 15$

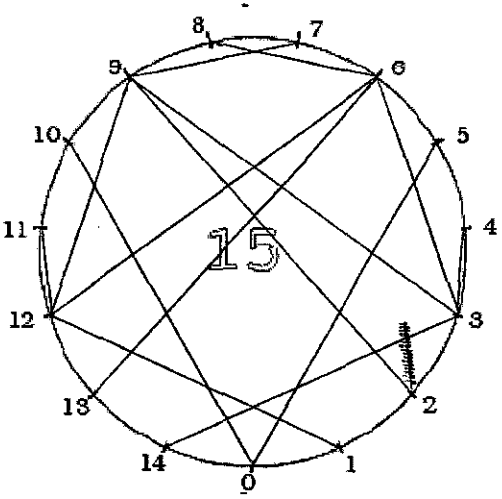


$f = 10$
$\rightarrow \cdot 10 \bmod 15$



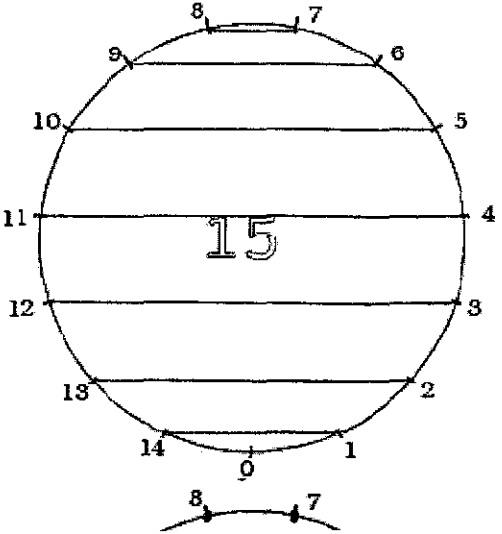
$f = 11$

$\rightarrow \cdot 11 \bmod 15$



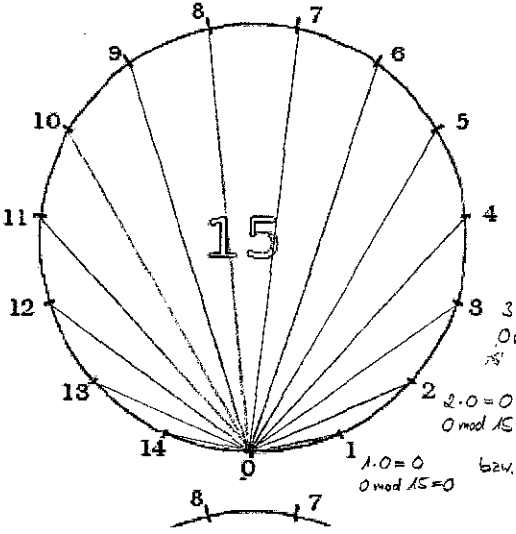
$f = 12$

$\rightarrow \cdot 12 \bmod 15$



$f = 14$

$\rightarrow \cdot 14 \bmod 15$



$f = 0$ bzw. 15

$3 \cdot 0 = 0$ bzw. $3 \cdot 15 = 45$

$0 \bmod 15 = 0$ $45 \bmod 15 = 0$

$2 \cdot 0 = 0$ bzw. $2 \cdot 15 = 30$

$0 \bmod 15 = 0$ $30 \bmod 15 = 0$

$1 \cdot 0 = 0$ bzw. $1 \cdot 15 = 15$

$0 \bmod 15 = 0$ $15 \bmod 15 = 0$