❑ Rotasjonssykler

La n være et positivt heltall og k et heltall med $0 \le k < n$. La d være største felles divisor for n og k, og m og l heltallene definert ved $n = md$ og $k = ld$.

Setning 1 La a være et heltall slik at $0 \le a < d$.

1. Hvis $0 \le s < m$, $0 \le t < m$ og $s \ne t$, vil $(a + sk) \bmod n \ne (a + tk) \bmod n$.
2. $a = (a + mk) \bmod n$

Bevis: I 1. kan vi anta (eventuelt ved å bytte om) at $s < t$ og dermed at $0 < t - s < m$. Anta så at $(a + sk) \bmod n = (a + tk) \bmod n$, det vil si at n går opp i $(t - s)k$. Det betyr at m går opp i $(t - s)l$. Men siden d er største felles divisor for n og k, må m og l være relativt primiske. Hvis m går opp i $(t - s)l$, må derfor m gå opp i $t - s$. Men det er umulig siden $0 < t - s < m$. Dermed er 1. bevist. Påstanden i 2. kan omformuleres til at n går opp i mk og det stemmer siden $mk = mdl = nl$.

Setning 2 La a og b være to heltall slik at $a \ne b$, $0 \le a < d$ og $0 \le b < d$. La s være et vilkårlig heltall. Da er $b \ne (a + sk) \bmod n$.

Bevis: Anta at $b = (a + sk) \bmod n$ og siden $b < n$ betyr det at n går opp i $a - b + sk$, dvs. at det finnes heltall t slik at $a - b + sk = tn$. Dette betyr igjen at d går opp i $a - b$ siden d går opp i både n og k. Umulig siden $-d < a - b < d$.

La $A = \{0, 1, 2, \ldots, d - 1\}$ og la M_a for hver $a \in A$ være mengden definert ved $M_a = \{(a + sk) \bmod n \mid s = 0, 1, 2, \ldots, m - 1\}$. Setning 1 og 2 gir at

(1) $\quad a = (a + mk) \bmod n,\ a \in A$

(2) $\quad M_a \cap M_b = \varnothing,\ a \ne b$

(3) $\quad \bigcup (M_a, a \in A) = \{0, 1, 2, \ldots, n - 1\}$