Exercise (1.19b of Permutation Groups by P. J. Cameron)**.** *Let q be a prime power, and n a positive integer. Suppose that every prime divisor of n divides $q-1$, and that, if $q \equiv 1 \pmod 4$, then n is not divisible by 4. Let $m(k) = (q^k - 1)/(q-1)$. Prove that*

- *n divides $m(n)$*
- *the numbers $m(0) = 0, m(1) = 1, m(2), \ldots, m(n-1)$ form a complete set of residues modulo n.*

Remark. $q \equiv 1 \pmod 4$ is a typo in the statement and should be replaced by $q \equiv -1 \pmod 4$. (For $q = 3$, $n = 4$ the conclusion of the second part is not true.)

Remark. In the exceptional case it is enough to assume a slightly weaker (and necessary) condition, see below. The assumption of q being a prime power can be dropped (obviously it is needed for (c)).

Exercise (Suggested correction[1])**.** *Let q and and n a positive integers such that every prime divisor of n divides $q-1$. Let $m(k) = \sum_{i=0}^{k-1} q^i$.*

- *Prove that n divides $m(n)$.*
- *If n is even and $q \equiv -1 \pmod 4$, suppose further that n is not divisible by 4. Prove that the numbers $m(0) = 0, m(1) = 1, m(2), \ldots, m(n-1)$ form a complete set of residues modulo n.*

Proof.

- Let $m_q(k) := m(k)$. Observe that $m_q(n) = m_q(d) \cdot m_{q^d}(n/d)$ for any $d \mid n$. Let p be an arbitrary prime divisor of n and let $n = p^a r$ where $p \nmid r$. Apply the observation a times each time separating a divisor p to get
$$m_q(n) = \prod_{j=0}^{a-1} m_{q^{p^j}}(p) \cdot m_{q^{p^a}}(r).$$
By the assumption $q^{p^j} = 1 + P_j$ for some multiple P_j of p for any j, so $m_{q^{p^a}}(r) \equiv r \not\equiv 0 \pmod p$ and $m_{q^{p^j}}(p) = \sum_{k=0}^{p-1}(1+P_j)^k = \sum_{k=0}^{p-1}\sum_{l=0}^{k}\binom{k}{l}P_j^l = \sum_{l=0}^{p-1}\sum_{k=l}^{p-1}\binom{k}{l}P_j^l = \sum_{l=0}^{p-1}\binom{p}{l+1}P_j^l$, hence $m_{q^{p^j}}(p) \equiv p + \binom{p}{2}P_j \pmod{p^2}$. More explicitly
$$m_{q^{p^j}}(p) \equiv \begin{cases} 0, & \text{if } p = 2, q \equiv -1 \pmod 4, j = 0 \\ p, & \text{otherwise} \end{cases}$$
modulo p^2. Thus $p^a \mid m_q(n)$, but since p was an arbitrary prime divisor of n, we have $n \mid m_q(n)$ as stated.

  Even more, this argument shows that $\gcd(m_q(n)/n, n) = 1$ unless both $2 \mid n$ and $q \equiv -1 \pmod 4$ in which case $\gcd(m_q(n)/n, n) = \gcd(n, (q+1)/2)$, a positive power of 2.

- Note that from the condition, n and q are relative primes, i.e. q is invertible modulo n, and that $m_q(k+l) = m_q(k) + q^k m_q(l)$ for natural numbers k and l. Then $m_q(k+l) \equiv m_q(k) \pmod n$ if and only if $n \mid m_q(l)$. Choose $l > 0$ be minimal such that $n \mid m_q(l)$. Assume for contradiction that $l \neq n$, otherwise the conclusion is true.

  Let $n = hl + l'$ where $0 \leq l' < l$. Then from the observation and the previous note $m_q(n) = m_q(l)m_{q^h}(h) + q^{hl}m_q(l')$. Form the first part $n \mid m_q(n)$, by assumptions $\gcd(n,q) = 1$ and $n \mid m_q(l)$, so $n \mid m_q(l')$. Then minimality of l forces $l' = 0$, i.e. $l \mid n$. Then the previous equation simplifies to $m_q(n) = m_q(l)m_{q^l}(n/l)$, so $\frac{m_q(n)}{n} = \frac{m_q(l)}{n}m_{q^l}(n/l)$, so $m_{q^l}(n/l) \mid \frac{m_q(n)}{n}$. On the other hand, from the first part $\frac{n}{l} \mid m_{q^l}(n/l)$, thus $\frac{n}{l} \mid m_{q^l}(n/l) \mid \frac{m_q(n)}{n}$ and hence $\frac{n}{l} \mid \gcd(m_q(n)/n, n)$. By (the contrapositive) assumption $1 < \frac{n}{l}$, so $1 < \gcd(m_q(n)/n, n)$. Comparing this with the last sentence of the first part yields $2 \mid n$ and $q \equiv -1 \pmod 4$ (i.e. the exceptional case of this part is satisfied) and that n/l is a positive power of 2. Then $2 \mid n \mid m_q(l)$ and $m_q(l) = \sum_{i=0}^{l-1} q^i \equiv (-1)^i \pmod 4$, which is only possible if $2 \mid l$. But then $n = l \cdot \frac{n}{l}$ is a product of two even numbers, so $4 \mid n$. This contradicts the exceptional assumption of the exercise. □

Remark. Note that in the extra case the assumption $4 \nmid n$ is necessary to obtain a complete set of residues, i.e. if $4 \mid n$ and $q \equiv -1 \pmod 4$ then the numbers are not pairwise incongruent: Pick a with $2^a \mid n$ but $2^{a+1} \nmid n$. Consider $m_q(n) = n_q(n/2) \cdot (1 + q^{n/2})$. The term $(1 + q^{n/2})$ is relative prime to all the odd prime divisors of n. Now $(1 + q^{n/2}) \equiv 2 \pmod 4$ from the assumptions on n and q. In the first part we proved that $2^{a+1} \mid m_q(n)$. These imply $2^n \mid m_q(n/2)$. But also from the first part $\frac{n}{2} \mid n_q(n/2)$, and these together imply that $n \mid n_q(n/2)$. Then $m_q(0) \equiv m_q(n/2) \pmod n$ so the listed elements do not form a complete set of residues.

[1] Dávid Szabó, Central European University, Budapest, 2016, `Szabo_David@phd.ceu.edu`