Alabama Journal of Mathematics

Alabama Journal of Mathematics
Volume 46 (1) (2023), 6 – 11

ORIGINAL ARTICLE

A Shifty Approach to Little Theorems

T. J. Kepka*[1], J. D. Phillips[2]

[1] *Department of Algebra, MFF UK, Sokolovská 83, 186 75 Praha 8, Czech Republic*

[2] *Department of Mathematics & Computer Science, Northern Michigan University, Marquette, MI 49855 USA*

Abstract

Herein, we offer a gentle yet rigorous introduction to both modular arithmetic and the elementary combinatorics of the common shift mapping, culminating in self-contained and accessible proofs of various cases of a general Euler Totient Function Theorem, Fermat's Little Theorem included. The reader may consider this an homage to T.P. Kirkman and W.S.B. Woolhouse for their pioneering work in elementary combinatorics [2], [3]. We recommend [1] both as a primer on the shift mapping and as an engaging example of elementary mathematics transmogrified.

Keywords. Fermat's Little Theorem, Euler's totient function
Mathematics Subject Classification (2020). 11A99

0A. The Shift Mapping

A1. Let $q \geq 2$ be a (fixed) positive integer. Define a transformation π of the interval $Q = \{1, 2, 3, \ldots, q\}$ by $\pi(i) = i + 1$ for every $i, 1 \leq i < q$, and $\pi(q) = 1$. For example, if $q = 6$, then $\pi(1) = 2, \pi(2) = 3, \pi(3) = 4, \pi(4) = 5, \pi(5) = 6, \pi(6) = 1$. This *shift mapping*, π, is fixed for the balance of this paper.

A2. We claim that $q \mid (\pi^j(i) - i - j)$ for all $i, 1 \leq i \leq q$, and all positive integers j. We proceed by induction on $j \geq 1$. We observe immediately that $\pi(i) - i - 1 = 0$ for $i \neq q$ and $\pi(q) - q - 1 = -q$. This settles the case $j = 1$. Using this and the induction hypothesis, we see that $q \mid (\pi(\pi^j(i)) - \pi^j(i) - 1)$ and $q \mid (\pi^j(i) - i - j)$. It follows easily that $q \mid (\pi(\pi^j(i)) - i - j - 1)$. But since $\pi(\pi^j(i)) = \pi^{j+1}(i)$ this completes the proof.

A3. We now show that $\pi^q(i) = i$ for each $i, 1 \leq i \leq q$. By A2, $q \mid (\pi^q(i) - i - q)$; hence, $q \mid (\pi^q(i) - i)$. Finally, since $0 \leq |\pi^q(i) - i| < q$, we have $|\pi^q(i) - i| = 0$, and hence, $\pi^q(i) = i$.

A4. We also note that $\pi^j(q) = j$ for every $j, 1 \leq j \leq q$. Indeed, by A2, $q \mid (\pi^j(q) - q - j)$, and so $q \mid (\pi^j(q) - j)$; hence, $\pi^j(q) = j$.

A5. The assertions A3 and A4 assure us that the transformation π of Q is, in fact, a permutation of Q, whose order is just q. That is, q is the smallest positive integer such that $\pi^q(i) = i$, for all $i \in Q$. While this fact is intuitive, a rigorous proof is still a rigorous proof.

*Corresponding Author.
Email addresses: kepka@karlin.mff.cuni.cz,
jophilli@nmu.edu

A6. Let $1 \le s \le q$. Define a binary relation λ_s on the interval Q by $(i,j) \in \lambda_s$ if and only if $j = \pi^{st}(i)$ for some $t \ge 0$. We claim that λ_s is an equivalence relation on Q, i.e., λ_s is reflexive, symmetric and transitive.

Reflexivity is clear, since $i = \pi^0(i)$ $(i.e., t = 0)$. For transitivity, note that if $j = \pi^{st}(i)$ and $k = \pi^{sr}(j)$, then $\pi^{s(t+r)}(i) = \pi^{sr}(\pi^{st}(i)) = \pi^{sr}(j) = k$. For symmetry, let $j = \pi^{st}(i)$ and choose any $u \ge 1$ such that $q \mid (t+u)$ (for example, $u = vq - t$ with v the smallest positive integer such that $vq \ge t$). Thus, $\pi^{su}(j) = \pi^{su}(\pi^{st}(i)) = \pi^{s(u+t)}(i) = \pi^{svq}(i) = i$.

A7. Let $1 \le s \le q$ and let $r = \gcd(s,q)$. Then $1 \le r \le q, r|s$, and $r|q$. Moreover—and this will be vital down the road—we have $\lambda_s = \lambda_r$, as we shall now prove. Firstly, since $r|s, s = ur$, for some u, and it follows easily from the definition of the equivalences that $\lambda_s \subseteq \lambda_r$. Secondly, we must show that $\lambda_r \subseteq \lambda_s$. This will take more effort.

Denote by N the set of all sums $xs + yq$, for arbitrary integers x and y. Clearly, N contains infinitely many positive integers; let t be the smallest. Since r divides both s and q, r divides any integer from N; in particular $r|t$. We have $1 \le r \le t \le s \le q$, where $s = lt + f, l \ge 0, 0 \le f < t, q = gt + h, g \ge 0, 0 \le h < t$, and $t = x_1 s + y_1 q$, where x_1, y_1 are suitable integers. Rearranging a bit gives $lt = lx_1 s + ly_1 q, f = s - lt = (1 - lx_1)s + (-ly_1)q, gt = gx_1 s + gy_1 q, h = q - gt = (-gx_1)s + (1 - gy_1)q$. Thus, $f, h \in N$. Now, using the minimality of t, we get $f = 0 = h$. That is, $t|s$ and $t|q$. But then $t|\gcd(s,q)$, where $\gcd(s,q) = r$. Thus, $t = r$, and so $r = x_1 s + y_1 q$. Next, find a positive integer k such that $ks > y_1$ and $kq > -x_1$ (there are, again, infinitely many choices). We write $x_2 = kq + x_1 > 0$ and $y_2 = ks - y_1 > 0$, and so $x_2 s - y_2 q = kqs + x_1 s - ksq + y_1 q = x_1 s + y_1 q = r$, and thus $x_2 s = r + y_2 q$, with x_2 and y_2 positive integers. Finally, if $(i,j) \in \lambda_r$ with $j = \pi^{rx}(i)$, then $\pi^{sx_2 x}(i) = \pi^{rx + xy_2 q}(i) = \pi^{rx}(\pi^{xy_2 q}(i)) = \pi^{rx}(i) = j$, and therefore $(i,j) \in \lambda_s$. Thus, $\lambda_r \subseteq \lambda_s$, which completes the proof.

A8. Let $1 \le s \le q$. The equivalence λ_s determines a partition of the interval Q. This interval is the disjoint union of the (pair-wise different) blocks (or cosets modulo λ_s) of the equivalence λ_s. The number of these blocks is the cardinality of the corresponding factor-set Q/λ_s. We now show that this common divisor is not just great, it is the greatest common divisor $\gcd(s,q)$!

In view of A7, we can assume without loss of generality that $s|q$. We show that $(i,j) \notin \lambda_s$ whenever $1 \le i < j \le s$. Proceeding by contradiction, assume that $(i,j) \in \lambda_s$. Then $j = \pi^{st}(i)$ for a non-negative integer t, and it follows from A2 that $q|(j - i - st)$. Since $s|q$, we get $s|(j - i - st), s|(j - i)$ and $2 \le s \le j - i \le s - 1$, a contradiction. The numbers $1, 2, \ldots, s$ are pair-wise nonequivalent modulo λ_s, which means that λ_s possesses at least s different blocks (this fact is, of course, trivial for $s = 1$).

In order to show that λ_s has at most s blocks, it suffices to find for every $i, 1 \le i \le q$, a number j such that $1 \le j \le s$ and $(i,j) \in \lambda_s$. If $i \le s$, then put $j = i$. Thus, we can restrict ourselves to the case $s + 1 \le i \le q$ (then $s < q$). Since $s|q$, we have $q = us$ where $2 \le u \le q$. Moreover, $i = ks + l, 1 \le k \le u, 0 \le l < s$. Put $v = u - k$, so that $0 \le v \le u - 1, i + vs = us + l$. By A2, $q|(\pi^{vs}(i) - us - l)$. Consequently, $q|(\pi^{vs}(i) - l)$. On the other hand, we clearly have $-q < -s < 1 - s < 1 - l \le \pi^{vs}(i) - l \le q$.

If $\pi^{vs}(i) = l$ then certainly $1 \le l \le s$ and $(i,l) \in \lambda_s$ and we can put $j = l$. If $\pi^{vs}(i) \ne l$ then $l = 0, \pi^{vs}(i) = q, i = ks, 2 \le k \le u$. Put $w = u - k + 1, 1 \le v \le u - 1 \le q - 1$. By A2, $q|(\pi^{ws}(i) - (ws + i))$. As $ws + i = (u+1)s$ and $q = us$, we see that $q|(\pi^{ws}(i) - s)$. However, $-s < 1 - s \le \pi^{ws}(i) - s \le q - s = (u-1)s$, and we conclude that $\pi^{ws}(i) = s$. That is, $(i,s) \in \lambda_s$, and we put $j = s$.

A9. Let $1 \le s \le q$. If follows directly from A8 that $\lambda_s = \mathrm{id}_Q$ (the identity equivalence possessing precisely q one-element blocks) if and only if $\gcd(s,q) = q$, i.e., $s = q$. However, to show this, we need not make use of the somewhat laborious results of A7 and A8; instead, we proceed directly. The equality $\lambda_q = \mathrm{id}_Q$ follows from A3. Conversely, if $\lambda_s = \mathrm{id}_Q$, then $\pi^s(i) = i$ for each $i, 1 \le i \le q$ and it follows directly from A4 that $s = q$.

Another consequence of A8 is the following: $\lambda_s = Q \times Q$ (the total equivalence possessing only one block) if and only if the numbers s and q are coprime. It seems doubtful that this assertion can be proven in a simpler way.

Finally, and locally, let us observe that each block of the equivalence λ_s contains just $\dfrac{q}{\gcd(s,q)}$ different numbers. As usual, we can restrict ourselves to the case when $s|q, q = rs, 1 \le r \le q$. For $1 \le i \le q$ the block $\{j | 1 \le j \le q, (i,j) \in \lambda_s\}$ containing i equals the set $\{\pi^{st}(i) | 0 \le t < r\}$. The latter set contains exactly r numbers.

0B. Two Scholia

B1. Let $q \ge 2$ be a positive integer. Let A be any finite set containing $m \ge 2$ elements. Denote by $\underline{A}$ $(= A^q)$ the set of ordered q-tuples $\underline{a} = (\underline{a}(1), \underline{a}(2), \dots, \underline{a}(q))$ of elements from A. We see easily that $|\underline{A}| = m^q$ (≥ 4)

B2. Define a transformation α of $\underline{A}$ by $\alpha(\underline{a}) = \underline{a}(\pi(i))$; that is, $\alpha(\underline{a}) = (\underline{a}(2), \underline{a}(3), \dots \underline{a}(q), \underline{a}(1))$.

B3. We now show that $\alpha^j(\underline{a})(i) = \underline{a}(\pi^j(i))$ for all $j \ge 0$ and $1 \le i \le q$. We proceed by induction on j. The case $j = 0$ is clear, since $\alpha^0 = \mathrm{id}_{\underline{A}}$. The case $j = 1$ is just the definition of the transformation α. Next, we write $\alpha^{j+1}(\underline{a})(i) = \alpha(\alpha^j(\underline{a}))(i) = \alpha^j(\underline{a})(\pi(i)) = \underline{a}(\pi^j(\pi(i))) = \underline{a}(\pi^{j+1}(\underline{a}))$.

B4. Combining A3 and B3, we obtain $\alpha^q(\underline{a}) = \underline{a}$ for every $\underline{a} \in \underline{A}$.

B5. Let $1 \le j < q$. Our goal is to show that there exists at least one q-tuple $\underline{a}$ with $\alpha^j(\underline{a}) \ne \underline{a}$. Indeed, denote by r the smallest positive integer such that $\alpha^r(\underline{a}) = \underline{a}$ for every $\underline{a} \in \underline{A}$. We know from B4 that r exists and that $1 \le r \le q$. We show that $r = q$. We proceed by contradiction, and assume $r < q$. The set A contains at least two elements and we take $a, b \in A$ such that $a \ne b$. Now, define $\underline{a} \in A$ by $\underline{a}(i) = a$ for $1 \le i < q$ and $\underline{a}(q) = b$ $(\underline{a} = (a, a, \dots, a, b))$. By B3 and A4 we have $\alpha^j(\underline{a})(q) = \underline{a}(\pi^j(q)) = \underline{a}(j) = a \ne b = \underline{a}(q)$. Thus, $\alpha^j(\underline{a}) \ne \underline{a}$.

B6. B4 and B5 together show that α is a permutation of the set $\underline{A}$ of ordered q-tuples and that the order of α is, again, q.

B7. For every $\underline{a} \in \underline{A}$, let $\rho(\underline{a})$ designate the smallest positive integer such that $\alpha^{\rho(\underline{a})}(\underline{a}) = \underline{a}$. As we know from B6, $\rho(\underline{a})$ exists and $1 \le \rho(\underline{a}) \le q$.

B8. Next, we show that $\rho(\underline{a})|q$. Since $1 \le \rho(\underline{a}) \le q$, we can write $q = r\rho(\underline{a}) + s$, where $r \ge 1$ and $0 \le s < \rho(\underline{a})$. Of course, $\alpha^{r\rho(\underline{a})}(\underline{a}) = \alpha^{(r-1)\rho(\underline{a})}(\alpha^{\rho(\underline{a})}(\underline{a})) = \alpha^{(r-1)\rho(\underline{a})}(\underline{a}) = \cdots = \alpha^{\rho(\underline{a})}(\underline{a}) = \underline{a}$, and therefore $\alpha^s(\underline{a}) = \alpha^s(\alpha^{r\rho(\underline{a})}(\underline{a})) = \alpha^{s+r\rho(\underline{a})}(\underline{a}) = a^{\alpha}(\underline{a}) = \underline{a}$. Using the minimality of $\rho(\underline{a})$, we get $s = 0$. That is, $q = r\rho(\underline{a})$.

B9. If the ordered q-tuples $\underline{a}, \alpha(\underline{a}), \dots, \alpha^{q-1}(\underline{a})$ are pair-wise different, then in particular, $\underline{a} \ne \alpha^j(\underline{a})$ for every $j, 1 \le j \le q-1$, and it is clear that $\rho(\underline{a}) = q$. On the other hand, if $\alpha^j(\underline{a}) = \alpha^k(\underline{a})$ for some $j, k, 0 \le j < k \le q-1$, then $\alpha^{k-j}(\underline{a}) = \underline{a}$, so that $\rho(\underline{a}) \le k - j \le q - 1, \rho(\underline{a}) < q$.

We have shown that $\rho(\underline{a}) = q$ if and only if the q-tuples $\alpha^j(\underline{a}), 0 \le j \le q-1$, are pair-wise different.

B10. In what follows, for ease of reference, a q-tuple $\underline{a}$ will be called *aeptic* when $\rho(\underline{a}) = q$.

B11. Choose two different elements $a, b \in A$ and set $\underline{a} = (a, b, b, \dots, b)$ $(\underline{a} = (a, b)$ for $q = 2, \underline{a} = (a, b, b)$ for $q = 3$, etc.). It is easy to see that the q-tuple $\underline{a}$ is aeptic.

B12. Let $2 \le r < q, r|q, q = rs$, so that $2 \le s < q$ and $q \ge 4$. Consider the q-tuple $\underline{a} \in \underline{A}$ where $\underline{a}(kr+1) = a$ for $k, 0 \le k \le s-1$ and $\underline{a}(i) = b$ otherwise $(a, b \in A, a \ne b)$. That is, $\underline{a} = (a, b, b, \dots, b, a, b, b, \dots, b, \dots, a, b, b, \dots, b)$ where the element a occurs s-times and the element b occurs $(q-s)$-times $(q - s = s(r-1))$. Put $\underline{b} = \alpha^r(\underline{a})$. Since $\pi^r(1) = r+1, \pi^{2r}(1) = 2r+1, \dots, \pi^{(s-1)r}(1) = (s-1)r+1$ and $\pi^{rs}(1) = \pi^q(1) = 1$, we see that $\underline{b}(kr+1) = a$ for all $k, 0 \le k \le s-1$. This means that $\underline{a}(kr+1) = a = \underline{b}(kr+1)$ and the number of occurrences of the element a in both $\underline{a}$ and $\underline{b}$ is the same. It is now easy to see that $\underline{b} = \underline{a}$ and $\rho(\underline{a}) = r$.

B13. It is self-evident that $\rho(\underline{a}) = 1$ if and only if $\underline{a}$ is a *constant* q-tuple (i.e., $\underline{a}(1) = \underline{a}(2) = \cdots = \underline{a}(q)$). The number of such q-tuples is exactly m $(= |A|)$.

B14. The following observation will be useful: $\rho(\underline{a}) = |\{\alpha^i(\underline{a}) | 0 \le i\}|$. Indeed, denote by r the number on the right side of the equality. The q-tuples $\underline{a}, \alpha(\underline{a}), \ldots, \alpha^{\rho(\underline{a})-1}(\underline{a})$ are pairwise different; consequently, $r \ge \rho(\underline{a})$. Conversely, $\alpha^{\rho(\underline{a})+j}(\underline{a}) = \alpha^j(\underline{a})$ for every $j \ge 0$, and hence, $r \le \rho(\underline{a})$.

B15. Let $1 \le s \le q$ and $\underline{a} \in \underline{A}$. Then $\alpha^s(\underline{a}) = \underline{a}$ if and only if $\underline{a}(i) = \underline{a}(j)$ whenever $(i,j) \in \lambda_s$. In view of B3, $\alpha^s(\underline{a}) = \underline{a}$ if and only if $\underline{a}(\pi^s(i)) = \underline{a}(i)$ for every $i, 1 \le i \le q$. The rest is clear from the definition of the equivalence λ_s (see A6).

B16. For every $\underline{a} \in \underline{A}$, put $w(\underline{a}) = |\{\underline{a}(i) | 1 \le i \le q\}|$. The number $w(\underline{a})$ is just the number of (different) elements from A appearing as components of the ordered q-tuple $\underline{a}$. Clearly, $1 \le w(\underline{a}) \le \min(m, q)$.

B17. For every $\underline{a} \in \underline{A}$ define a binary relation $\sigma(\underline{a})$ on the interval $Q = \{1, 2, \ldots, q\}$ by $(i,j) \in \sigma(\underline{a})$ if and only if $\underline{a}(i) = \underline{a}(j)$. Obviously, $\sigma(\underline{a})$ is a well-defined equivalence relation on Q. Moreover, it is straightforward to see that $\sigma(\underline{a})$ has exactly $w(\underline{a})$ different blocks.

B18. We show that $\lambda_{\rho(\underline{a})} \subseteq \sigma(\underline{a})$ for every $\underline{a} \in \underline{A}$. As we know (see B7), $\rho(\underline{a})$ is the smallest positive integer satisfying the equality $\alpha^{\rho(\underline{a})}(\underline{a}) = \underline{a}$. Now, from B15, if $(i,j) \in \lambda_{\rho(\underline{a})}$, then $\underline{a}(i) = \underline{a}(j)$, which is the same as $(i,j) \in \sigma(\underline{a})$ (see B17).

B19. We have now arrived at our first scholium: $w(\underline{a}) \le \min(\rho(\underline{a}), m)$ for every $\underline{a} \in \underline{A}$. Let's prove it! By B8, $\rho(\underline{a})|q$. By A8, the equivalence $\lambda_{\rho(\underline{a})}$ has exactly $\rho(\underline{a})$ blocks. By B17, the equivalence $\sigma(\underline{a})$ has exactly $w(\underline{a})$ blocks. By B18, $\lambda_{\rho(\underline{a})} \subseteq \sigma(\underline{a})$, and this inclusion implies that $w(\underline{a}) \le \rho(\underline{a})$. The inequality $w(\underline{a}) \le m$ is trivial.

B20. And now, the second scholium: Put $r(q) = q/p$, where p is the smallest prime number dividing q. Clearly, $r(q)$ is just the greatest integer properly dividing q $(r(q)|q, r(q) \ne q, -q)$. Now, if $\underline{a} \in \underline{A}$ is such that $w(\underline{a}) > r(q)$, then, with respect to B19, we get $r(q) \le \rho(\underline{a})$, and since $\rho(\underline{a})|q$, the equality $\rho(\underline{a}) = q$ is clear. *The ordered q-tuple $\underline{a}$ is thus aeptic.*

As an illustration, we present a handy tablette of the values $r(q) + 1$ for $2 \le q \le 28$:

q	2	3	4	5	6	7	8	9	10
r(q) + 1	2	2	3	2	4	2	5	4	6
q	11	12	13	14	15	16	17	18	19
r(q) + 1	2	7	2	8	6	9	2	10	2
q	20	21	22	23	24	25	26	27	28
r(q) + 1	11	8	12	2	13	6	14	10	15

Apparently, if q is a prime number, then $r(q) + 1 = 2$. If $q = p^k$, where p is a prime and $k \ge 1$, then $r(q) = p^{k-1} + 1$ $(r(p^2) = p + 1)$.

Another example: Let $\underline{a} \in \underline{A}$ be a q-tuple such that $w(\underline{a}) = r(q) - 1$. Since $w(\underline{a}) \ge 1$, we see that $r(q) \ge 2$ and q is not a prime number. Of course, $q = pr(q)$, where p is the smallest prime number dividing q and $2 \le p < q$. Furthermore, by B19, we see that $r(q) - 1 \le \rho(\underline{a})$.

Assume, for a moment, that $\rho(\underline{a}) = r(q) - 1$. By B8, $q = u\rho(\underline{a}) = u(r(q) - 1)$ for some $u, 1 \le u \le q$. Thus, $ur(q) - u = q = vr(q), (v - u)r(q) = -u < 0, u > v, u - v \ge 1, u = (u - v)r(q) \ge r(q)$. Since $u|q$, we have either $u = q$ or $u = r(q)$. If $u = q$, then $\rho(\underline{a}) = 1 = w(\underline{a})$ by (B13), $r(q) = 2 = p, q = 4$ and $\underline{a} = (a, a, a, a)$ for some $a \in A$. Suppose, therefore, that $u = r(q)$. Then $\rho(\underline{a}) = p, r(q) = p + 1, w(\underline{a}) = p, q = p^2 + p$, where q is an even number, $p = 2, q = 6, \rho(\underline{a}) = 2 = w(\underline{a})$ and $\underline{a} = (a, b, a, b, a, b)$ for some $a, b \in A, a \neq b$.

Next, assume that $\rho(\underline{a}) > r(q) - 1$. That is, $\rho(\underline{a}) \geq r(q)$ and thus, either $\rho(\underline{a}) = r(q)$ or $\rho(\underline{a}) = q$ ($\underline{a}$ is aeptic in the latter case).

Consider the case $\rho(\underline{a}) = r(q)$. Thus, we have $w(\underline{a}) = r(q) - 1$. Since $\rho(\underline{a}) = r(q) \geq 2$, we get $w(\underline{a}) \geq 2$ and $r(q) \geq 3, q \geq 6$. It is not difficult to see that $\underline{a} = (\underline{b}, \underline{b}, \dots, \underline{b})$ ($\underline{b}$ repeated p-times), where $\underline{b} = (a_1, a_2, \dots, a_r), r = r(q), a_1, a_2, \dots a_r \in A$, and $|\{a_1, a_2, \dots, a_r\}| = r - 1$. As a consequence of the latter equality, we see that there is a (uniquely determined) pair (k, l) of indices, $1 \leq k < l \leq r$, such that $a_k = a_l$ and $a_i \neq a_j$ whenever $1 \leq i < j \leq r$ and $(i, j) \neq (k, l)$. For instance, if $q = 6$, then $r(q) = 3$ and $\underline{b} = (a, a, b), (a, b, a), (a, b, b)$. If $q = 8$, then $r(q) = 4$ and $\underline{b} = (a, a, b, c), (a, b, a, c), (a, b, c, a), (a, b, b, c)(a, b, c, b), (a, b, c, c)$.

One final example: let $\underline{a} \in \underline{A}$ be a q-tuple such that $w(\underline{a}) = r(q) = r$. If $r = 1$, then q is a prime. Assume, therefore, $r \geq 2, q = pr$, with p the smallest prime dividing q. Furthermore, $r \leq \rho(\underline{a})$. If $\rho(\underline{a}) > r$ then $\rho(\underline{a}) = q$ and the q-tuple $\underline{a}$ is aeptic. So, let $\rho(\underline{a}) = r$. It is routine to observe that then $\underline{a} = (a_1, a_2, \dots, a_r, a_1, a_2, \dots a_r, \dots, a_1, a_2, \dots, a_r)$.

The moral of the story: Given $q \geq 2$ first establish the number $r(q)$, although it might be (hopelessly) difficult. Then, given a q-tuple $\underline{a}$, establish the number $w(\underline{a})$ (by, alas, a fatigueant calculation). If, by chance, it happens that $w(\underline{a}) \geq r(q) - 1$, then, up to (relatively) few more or less easily recognizable exceptions, we know that the q-tuple $\underline{a}$ is aeptic.

0C. Fermat's Little Theorem and an Euler Theorem

C1. Define a binary relation τ on the set $\underline{A}$ by $(\underline{a}, \underline{b}) \in \tau$ if and only if $\underline{b} = \alpha^k(\underline{a})$ for some $k \geq 0$. We check that τ is an equivalence (on $\underline{A}$).

The reflexivity of τ is trivial since $\underline{a} = \alpha^0(\underline{a})$. For transitivity, note that if $\underline{b} = \alpha^k(\underline{a})$ and $\underline{c} = \alpha^l(\underline{b})$, then $c = \alpha^{k+l}(\underline{a})$. Finally, for symmetry, let $b = \alpha^k(\underline{a}), r = \rho(\underline{a})$, so that $\alpha^{k(r-1)}(\underline{b}) = \alpha^{k(r-1)}(\alpha^k(\underline{a})) = \alpha^{kr}(\underline{a}) = \underline{a}$.

C2. For $\underline{a} \in \underline{A}$, let $[\underline{a}]_\tau$ denote the block of the equivalence τ that is determined by $\underline{a}$. This means that $\underline{a} \in [\underline{a}]_\tau, [\underline{a}]_\tau = \{\underline{b} | (\underline{a}, \underline{b}) \in \tau\}$.

By the definition of τ, we have $[\underline{a}]_\tau = \{\alpha^k(\underline{a}) | k \geq 0\}$. Thus, by B14, we see that the block $[\underline{a}]_\tau$ contains precisely $\rho(\underline{a})$ different q-tuples.

C3. If $(\underline{a}, \underline{b}) \in \tau$, then $\rho(\underline{a}) = \rho(\underline{b})$.

C4. For every $r, 1 \leq r, r|q$, let $\kappa(r)$ be the number of those ordered q-tuples $\underline{a}$ that satisfy the equality $\rho(\underline{a}) = r$. If follows easily from B8 that $(|A| =)\ m^q = \sum_{r=k, r|q}^{q} \kappa(r)$. By B13, B11, and B12, we have that $\kappa(1) = m$ and $\kappa(r) \geq 1$ for every $r, r|q$.

We show that $r|\kappa(r)$. Indeed, we have $\kappa(r) = |\underline{A}_r|, \underline{A}_r = \{\underline{a} | \rho(\underline{a}) = r\}, \kappa(r) \geq 1$. By C3, $\underline{A}_r$ is the disjoint union of distinct blocks of the equivalence τ. By C2, each such block contains precisely r q-tuples. It follows that $r|\kappa(r)$.

C5. Consider the following basic set-up: Let $q = p^t$, where p is a prime and t is a positive integer. What could be simpler! In view of C4, we obtain the equality $m^q - m = \sum_{s=1}^{t} \kappa(p^s)$. Since $\kappa(p^s) = p^s \cdot \mu(p^s)$, we get $m^q - m = \sum_{s=1}^{t} p^s \cdot \mu(p^s) = p \sum_{s=1}^{t} p^{s-1} \cdot \mu(p^s)$. That is, $p|(m^q - m)$. In particular, for $t = 1$ we get $p|(m^p - m = m(m^{p-1} - 1))$. And we have proved Fermat's Little Theorem!

More generally, a routine check shows that $\kappa(p) = m^p - m$ for $t \geq 1$ and $\kappa(p^2) = m^{p^2} - m^p = m^p(m^{p(p-1)} - 1)$ for $t \geq 2$. If, moreover, $p \nmid m$, then $p^2 | (m^{p(p-1)} - 1)$ and this assertion is a subcase of a well-known Euler Theorem; $p(p-1) = \varphi(p)$, where φ is the Euler totient function.

As an example, choose $p = 3$ and $t = 2$. If $m = 2$, then $\kappa(1) = 6$ $(= 2 \cdot 3)$ and $\kappa(9) = 504$ $(= 2^3 \cdot 3^2 \cdot 7)$. If $m = 3$, then $\kappa(3) = 24$ $(= 2^3 \cdot 3)$ and $\kappa(9) = 19,656$ $(= 2^3 \cdot 3^2 \cdot 7 \cdot 13)$.

Choose $p = 1093, t \geq 1, m \geq 2$, and, as an exercise, check that 1093 is a prime number such that $1093^2 | \kappa(1093)$ (so that $1093^2 | (2^q - 2)$). Show all your work; no calculators, please!

Finally, in the general case, we get $\kappa(p^s) = m^{p^s} - m^{p^{s-1}} = m^{p^{s-1}}(m^{p^{s-1}(p-1)} - 1)$ for $1 \leq s \leq t$ ($p \nmid m$ implies $p^s | m^{p^{s-1}(p-1)} - 1, \varphi(p^s) = p^{s-1}(p-1)$).

The foregoing approach may be used for a proof of the above-mentioned Euler Theorem.

C6. Let $A = \{a_1, a_2, \ldots, a_m\}$. For all $\underline{a} \in \underline{A}$ and $j, 1 \leq j \leq m$, let $v_j(\underline{a}) = |\{i | 1 \leq i \leq q, \underline{a}(i) = a_j\}|$. Clearly $0 \leq v_j(\underline{a}) \leq q$ and $q = \sum_{j=1}^{m} v_j(\underline{a})$. Moreover, $w(\underline{a}) = |\{j | 1 \leq j \leq m, v_j(\underline{a}) \neq 0\}| \leq \min(m, q)$ and $w(\underline{a})v(\underline{a}) \leq q$, where $v(\underline{a}) = \min\{v_j(\underline{a}) | 1 \leq j \leq m, v_j(\underline{a}) \neq 0\}, 1 \leq v(\underline{a}) \leq q$.

We now show that $q \leq \rho(\underline{a})v(\underline{a})$. Put $r = \rho(\underline{a})$. By B15, $\underline{a}(i_1) = \underline{a}(i_2)$, for every pair $(i_1, i_2) \in \lambda_r$. If R is a block of λ_r, then we know that $|R| = q/r$ (A9) and $\underline{a}(i_1) = \underline{a}(i_2) = j$ for all $i_1, i_2 \in R$ and some $1 \leq j \leq m$. Thus, $v_j(\underline{a}) \geq q/r$. This is true for any j and consequently, $v(\underline{a}) \geq q/r$.

So $w(\underline{a})v(\underline{a}) \leq q \leq \rho(\underline{a})v(\underline{a})$ which implies that $w(\underline{a}) \leq \rho(\underline{a})$ (see B18 and B19).

Finally, define a binary relation ξ on $\underline{A}$ as $(\underline{a}, \underline{b}) \in \xi$ if and only if $v_j(\underline{a}) = v_j(\underline{b})$ for every $j, 1 \leq j \leq m$. Then ξ is an equivalence and $\tau \subseteq \xi$.

There is more to say, but *hanc marginis exiguitas non caperet*. Perhaps others can continue these lines. Perhaps *you* can!

References

[1] P. Dehornoy, Algebraic Properties of the Shift Mapping, *Proc. Amer. Math. Soc.*, **106**(1989), 617–623.

[2] T. P. Kirkman, Query VI, *The Lady's and Gentleman's Diary*, 1850, pg.48.

[3] W. S. B. Woolhouse, XV. Prize Question (1733), *Lady's and Gentleman's Diary*. 1844, pg.84.