Eventually constant modulo m. Prove that for any positive integer m and any sequence of positive integers $a_1, a_2, a_3, \ldots$, the following sequence is eventually constant modulo m:

$$a_1, \quad a_1^{a_2}, \quad a_1^{a_2^{a_3}}, \quad a_1^{a_2^{a_3^{a_4}}}, \ \ldots$$

Solution. The result is trivial if $a_n = 1$ for some n, or if $m = 1$, so we may assume that $a_n \geq 2$ for all n and that $m \geq 2$.

We will use the following result.

Euler's theorem. If $\gcd(a, m) = 1$, then

$$a^{\varphi(m)} \equiv 1 \pmod{m},$$

where φ denotes Euler's totient function.

In particular, if $\gcd(a, m) = 1$ and $b \geq 1$, then

$$a^b \equiv a^{\,b \bmod \varphi(m)} \pmod{m}.$$

where $b \bmod \varphi(m)$ denotes the remainder in $\{0, 1, \ldots, \varphi(m) - 1\}$.[1]

We prove the result by strong induction on m. For $1 \leq k \leq n$, let

$$T_{k,n} = a_k^{\cdot^{\cdot^{a_n}}}$$

denote the power tower starting at a_k and ending at a_n.

Basic step. For $m = 2$ the sequence is constant, since

$$T_{1,n} \equiv \begin{cases} 0 \pmod 2 & \text{if } a_1 \text{ is even,} \\ 1 \pmod 2 & \text{if } a_1 \text{ is odd,} \end{cases}$$

for all n.

Induction step. Assume the result holds for all moduli $d < m$, and we prove it for m.

Case 1: $\gcd(a_1, m) = 1$. Write $T_{1,n} = a_1^{T_{2,n}}$. By Euler's theorem and the congruence above,

$$T_{1,n} \equiv a_1^{\,T_{2,n} \bmod \varphi(m)} \pmod{m}.$$

Since $\varphi(m) < m$, the induction hypothesis implies that $T_{2,n}$ is eventually constant modulo $\varphi(m)$, hence so is $T_{2,n} \bmod \varphi(m)$. Therefore $T_{1,n}$ is eventually constant modulo m.

Case 2: $\gcd(a_1, m) = g > 1$. Write $m = m_1 m_2$, where $\gcd(m_1, m_2) = 1$, every prime divisor of m_1 divides a_1, and $\gcd(a_1, m_2) = 1$.

[1]Note: If $b \equiv 0 \pmod{\varphi(m)}$, then the right-hand side is $a^0 = 1$, and Euler's theorem gives $a^b \equiv 1 \pmod m$ as well, so the congruence is numerically correct. However, authors may prefer to avoid the zero exponent by choosing instead a representative in $\{1, 2, \ldots, \varphi(m)\}$ congruent to b modulo $\varphi(m)$. This is a matter of formal convention rather than a substantive issue in the present argument.

For each prime $p \mid m_1$, let $p^e \parallel m_1$ and $p^f \parallel a_1$ with $f \geq 1$. Then

$$v_p(T_{1,n}) = v_p(a_1^{T_{2,n}}) = f\, T_{2,n} \xrightarrow[n\to\infty]{} \infty,$$

since $T_{2,n}$ is strictly increasing (because all $a_k \geq 2$). Thus, for all sufficiently large n, we have $p^e \mid T_{1,n}$. Doing this for every prime divisor of m_1 shows that

$$T_{1,n} \equiv 0 \pmod{m_1}$$

for all sufficiently large n.

If $m_2 = 1$, we are done. Otherwise, $1 < m_2 < m$ and $\gcd(a_1, m_2) = 1$. By the induction hypothesis applied to modulus m_2, the sequence $T_{1,n} \bmod m_2$ is eventually constant; say

$$T_{1,n} \equiv c \pmod{m_2}$$

for all n large enough.

By the Chinese Remainder Theorem, the system

$$\begin{aligned} x &\equiv 0 \pmod{m_1}, \\ x &\equiv c \pmod{m_2} \end{aligned}$$

has a unique solution modulo $m = m_1 m_2$. Hence $T_{1,n}$ is eventually constant modulo m.

This completes the induction and the proof. □

Miguel A. Lerma - 12/11/2025