Eventually constant modulo m. Prove that for any two positive integers a and m, the following sequence is eventually constant modulo m: $a, a^a, a^{a^a}, a^{a^{a^a}}, \dots$.

Solution. The result is trivial if $a = 1$ or $m = 1$, so we may assume that $a \geq 2$ and $m \geq 2$.

For convenience we use Donald Knuth's arrow notation for the iterated power:

$$a \uparrow\uparrow n = \overbrace{a^{a^{\cdot^{\cdot^{\cdot^{a}}}}}}^{n \text{ levels}}.$$

Its recursive definition is the following: $a \uparrow\uparrow 0 = 1$, $a \uparrow\uparrow (n+1) = a^{a\uparrow\uparrow n}$.

So we must prove that $a \uparrow\uparrow n$ is eventually constant modulo m. The proof works by induction on m.

(1) Basic Step: If $m = 2$ then obviously $a \uparrow\uparrow n \equiv a \pmod 2$ for every $n > 0$, because $a \uparrow\uparrow n$ has the same parity has a.

(2) Induction Step: Assume that the result is true for every modulo up to $m - 1$. We will prove that it is also true for modulo m.

   (a) Case 1: If $\gcd(a, m) = 1$, by Euler's theorem
   $$a \uparrow\uparrow (n+1) = a^{a\uparrow\uparrow n} \equiv a^{(a\uparrow\uparrow n) \bmod \phi(m)} \pmod m,$$
   where ϕ = Euler's phi function and $x \bmod y$ = "x reduced modulo y". Since $\phi(m) < m$, by induction hypothesis $(a \uparrow\uparrow n) \bmod \phi(m)$ is eventually constant, hence $\{a \uparrow\uparrow (n+1)\} \bmod m$ is eventually constant.

   (b) Case 2: If $\gcd(a, m) = g > 1$ then we write $m = m_1 m_2$, were $\gcd(m_1, m_2) = 1$ and m_1 contains exactly the same prime factors as g, perhaps raised to different exponents. Clearly $a \uparrow\uparrow n \equiv 0 \pmod{m_1}$ for n large enough. If $m_2 = 1$ then we are done, otherwise $1 < m_2 < m$ and $\gcd(a, m_2) = 1$, so by induction hypothesis $(a \uparrow\uparrow n) \bmod m_2$ is eventually constant, say $k = (a \uparrow\uparrow n) \bmod m_2$ for all n large enough. According to the Chinese Remainder Theorem, the following system of congruences
   $$\begin{cases} x \equiv 0 \pmod{m_1} \\ x \equiv k \pmod{m_2} \end{cases}$$
   has a unique solution $x = r$ modulo $m = m_1 m_2$, hence $a \uparrow\uparrow n \equiv r \pmod m$ for all n large enough. This completes the proof.

Remark: The result can be generalized to any tower of exponents with an increasing number of levels, even if the exponents are not all the same: $a_1, a_1^{a_2}, a_1^{a_2^{a_3}}, a_1^{a_2^{a_3^{a_4}}}, \dots$.

Corollary (graduate level): $a \uparrow\uparrow n$ has a p-adic limit as $n \to \infty$ for every p.

Miguel A. Lerma - 2/3/2003