Pontificia Universidad Católica de Chile
Facultad de Matemáticas
Departamento de Matemática

Ayudante: Nicholas Mc-Donnell
Email: namcdonnell@uc.cl

Solución Ayudantía 6

Álgebra I - MAT2227

Fecha: 2019/09/10

1) 1) Se nota que $(3, 11) = 1$ y que $\varphi(11) = 10$ por lo que $3^{200} \equiv (3^{10})^2 0 \equiv 1 \mod 11$.
   2) Se nota que $(7, 12) = 1$ y que $\varphi(12) = 4$, por lo que $7^{256} \equiv (7^4)^{64} \equiv 1 \mod 12$.
   3) Se nota que $(4, 9) = 1$ y $\varphi(9) = 6$, como $6 \mid 9072$, se tiene que $4^{9072} \equiv 1 \mod 9$.

2) Se nota que ver el dígito de la unidad de un número es equivalente a ver el número modulo 10.
   1) Como $(3, 10) = 1$ y $\varphi(10) = 4$, entonces $3^{90} \equiv 3^{88} \cdot 3^2 \equiv 9 mod 10$, por lo que el dígito de la unidad es 9.
   2) Como $(17, 10) = 1$ y $4 \mid 212$, entonces $17^{212} \equiv 1 \mod 10$.
   3) Se escribe $9! = 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$, y se nota que $10 \mid 9!$, por lo que su dígito de la unidad es 0.
   4) Se escribe el producto modulo 10: $2 \cdot 3 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \equiv 2 \cdot 3^3 \cdot 7^2 \cdot 9 \equiv 3^5 \cdot (-3)^2 \equiv 3^7 \equiv 3^3 \equiv 27 \equiv 7 \mod 10$.

3) Sea n minimal tal que $a^n \equiv 1 \mod 36$, con a fijo y coprimo con 36. Luego se nota que $\varphi(36) = 12$, por lo que $n \leq 12$. Ahora se asume que $n \nmid 12$, por lo $12 = n \cdot q + r$, donde $0 < r < n$, luego $a^{12} \equiv a^{n \cdot q + r} \equiv (a^n)^q \cdot a^r \equiv a^r \equiv 1 \mod 36$, por lo que n no es minimal. Se nota que esta demostración implica que los n minimales tal que $a^n \equiv 1 \mod m$ para algún a fijo coprimo con m, cumplen que $n \mid \varphi(m)$.

4) Como $p \mid m$, se tiene que $a^{m-1} \equiv 1 \mod p$, como p primo, se tiene que el mínimo n tal que $a^n \equiv 1 \mod p$ es $p - 1$, por lo que $p - 1 \mid m - 1$. Similarmente se tiene que $\varphi(p^r) \mid m - 1$, pero se nota que $(m - 1, m) = 1$, y como $p \mid m$, se tiene que $r = 1$[1] y más aún se tiene que $p \neq 2$, por lo mismo.

[1] $\varphi(p^r) = p^{r-1}(p - 1)$