

6.4 Considérons les classes de congruence associées aux puissances de a :
 $\overline{a}, \overline{a^2}, \overline{a^3} \dots$

Il existe une infinité de puissances positives de a , mais seulement m classes de congruence.

C'est pourquoi, deux de ces puissances doivent appartenir à la même classe de congruence, c'est-à-dire être congrues modulo m .