Corollary. *If a is not divisible by p and if $n \equiv m \ mod\ (p-1)$, then $a^n \equiv a^m \ mod\ p$.*

Proof of corollary. Say $n > m$. Since $p-1 | n-m$, we have $n = m + c(p-1)$ for some positive integer c. Then multiplying the congruence $a^{p-1} \equiv 1 \ mod\ p$ by itself c times and then by $a^m \equiv a^m \ mod\ p$ gives the desired result: $a^n \equiv a^m \ mod\ p$.

Example 2. Find the last base–7 digit in $2^{1000000}$.

Solution. Let $p = 7$. Since 1000000 leaves a remainder of 4 when divided by $p - 1 = 6$, we have $2^{1000000} \equiv 2^4 = 16 \equiv 2 \ mod\ 7$, so 2 is the answer.

Proposition I.3.3 (Chinese Remainder Theorem). *Suppose that we want to solve a system of congruences to different moduli:*

$$\begin{aligned} x &\equiv a_1 \ mod\ m_1, \\ x &\equiv a_2 \ mod\ m_2, \\ &\cdots \qquad \cdots \\ x &\equiv a_r \ mod\ m_r. \end{aligned}$$

Suppose that each pair of moduli is relatively prime: $g.c.d.(m_i, m_j) = 1$ for $i \neq j$. Then there exists a simultaneous solution x to all of the congruences, and any two solutions are congruent to one another modulo $M = m_1 m_2 \cdots m_r$.

Proof. First we prove uniqueness modulo M (the last sentence). Suppose that x' and x'' are two solutions. Let $x = x' - x''$. Then x must be congruent to 0 modulo each m_i, and hence modulo M (by Property 5 at the beginning of the section). We next show how to construct a solution x.

Define $M_i = M/m_i$ to be the product of all of the moduli *except for* the i-th. Clearly $g.c.d.(m_i, M_i) = 1$, and so there is an integer N_i (which can be found by means of the Euclidean algorithm) such that $M_i N_i \equiv 1 \ mod\ m_i$. Now set $x = \sum_i a_i M_i N_i$. Then for each i we see that the terms in the sum other than the i-th term are all divisible by m_i, because $m_i | M_j$ whenever $j \neq i$. Thus, for each i we have: $x \equiv a_i M_i N_i \equiv a_i \ mod\ m_i$, as desired.

Corollary. *The Euler phi-function is "multiplicative", meaning that $\varphi(mn) = \varphi(m)\varphi(n)$ whenever $g.c.d.(m,n) = 1$.*

Proof of corollary. We must count the number of integers between 0 and $mn - 1$ which have no common factor with mn. For each j in that range, let j_1 be its least nonnegative residue modulo m (i.e., $0 \leq j_1 < m$ and $j \equiv j_1 \ mod\ m$) and let j_2 be its least nonnegative residue modulo n (i.e., $0 \leq j_2 < n$ and $j \equiv j_2 \ mod\ n$). It follows from the Chinese Remainder Theorem that for each pair j_1, j_2 there is one and only one j between 0 and $mn-1$ for which $j \equiv j_1 \ mod\ m$, $j \equiv j_2 \ mod\ n$. Notice that j has no common factor with mn if and only if it has no common factor with m — which is equivalent to j_1 having no common factor with m — and it has no common factor with n — which is equivalent to j_2 having no common factor with n. Thus, the j's which we must count are in 1-to-1 correspondence with the pairs j_1, j_2 for which $0 \leq j_1 < m$, $g.c.d.(j_1, m) = 1$; $0 \leq j_2 < n$,