Petit théorème de Fermat

Soit p un nombre premier,
Si M n'est pas divisible par p alors $a^{p-1} \equiv 1 (\mathbf{mod}\ p)$.

exemple : 5 n'est pas divisible par 3 (premier) et $5^2 = 25 \equiv 1 (\text{mod } 3)$.

demonstration : Montrons par recurrence sur a que $a^p \equiv a (\text{mod } p)$.

initialisation : $1^p = 1$ donc vrai.

hérédité : Supposons que $a^p \equiv a (\text{mod } p)$ pour un p.
$(a+1)^p = a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k + 1$
Or pour k compris entre 1 et $p-1$, $\binom{p}{k} = \frac{p(p-1)...(p-k+1)}{k!}$ est un entier.
Or p est premier donc aucun facteur de $k!$ ne peut diviser p donc c'est que $k!$ divise $(p-1)...(p-k+1)$.
$\frac{(p-1)...(p-k+1)}{k!}$ est donc un entier donc p divise $\binom{p}{k}$.
donc $(a+1)^p \equiv a^p + 1 (\text{mod } p)$
donc $(a+1)^p \equiv a + 1 (\text{mod } p)$ par hypothèse de recurrence.
La propriété se transmet.

Conclusion : pour tout $a \in \mathbb{N}^*$, $a^p \equiv a (\text{mod } p)$ donc p divise $a^p - a = a(a^{p-1} - 1)$.
Si p premier ne divise pas a, p divise $a^{p-1} - 1$.

Si $n = pq$ p et q premiers, $\phi(n) = (p-1)(q-1)$
p et q étant premiers, les seuls facteurs communs possibles de n avec des entiers inférieurs à n sont p et q.
Tous les nombres entre 1 et $n-1$ sont donc premiers avec n sauf les multiples de p ($1p$, $2p$, $3p$, ... , $(q-1)p$) et les multiples de q ($1q$, $2q$, $3q$, ... $(p-1)q$).
Il y en a donc : $pq - 1 - (q-1) - (p-1) = (p-1)(q-1)$.

Décryptage du RSA
p et q sont premiers, M est suffisament petit pour être inférieur à p et q et donc premier avec p et q.
$M^{p-1} \equiv 1 (\text{mod } p)$ et $M^{q-1} \equiv 1 (\text{mod } q)$.

Or $C^d \equiv (M^e)^d \equiv M^{ed} (\text{mod } n)$.

Mais $ed \equiv 1 \text{ mod } \phi(n) = (p-1)(q-1)$
donc $ed = 1 + k(p-1)(q-1)$, k entier.
$M^{ed} = M^{1+k(p-1)(q-1)} = M \times (M^{p-1})^{k(q-1)} \equiv M \ (\text{mod } p)$ c'est à dire p divise $M^{ed} - M$.

de même, $M^{ed} \equiv M (\text{mod } q)$ c'est à dire q divise $M^{ed} - M$.

comme p et q sont premiers entre eux, $pq = n$ divise $M^{ed} - M$.

Donc $M^{ed} \equiv M (\text{mod } n)$.