MAT 2440 : Théorie des nombres

Théorème d'Euler

Exercice 1 Déterminer les 2 derniers chiffres en écriture décimale de 22^{2006}.

Exercice 2 Déterminer le dernier chiffre en écriture décimale de 7^{355}.

Exercice 3 Déterminer les 2 derniers chiffres en écriture décimale de 7^{355}.

Exercice 4 Chercher les n tels que $\varphi(n) = 4$.

Exercice 5 Montrer que $\varphi(n) = 14$ n'a pas de solution.

Exercice 6

$$1+2=\tfrac{3}{2}\varphi(3),\ \ 1+3=\tfrac{4}{2}\varphi(4),\ \ 1+2+3+4=\tfrac{5}{2}\varphi(5),\ \ 1+5=\tfrac{6}{2}\varphi(6),$$
$$1+2+3+4+5+6=\tfrac{7}{2}\varphi(7),\quad 1+3+5+7=\tfrac{8}{2}\varphi(8)$$

Deviner et prouver un théorème.

Exercice 7 On dit que q est pseudo-premier si $a^{q-1} \equiv 1 \bmod q$ pour tout a premier à q. Montrer que $561 = 3 \times 11 \times 17$ est pseudo-premier. Comment trouver d'autres nombres pseudo-premiers ?

Exercice 8 Voici le procédé de codage RSA. Soit $n = pq$ avec p et q deux nombres premiers distincts et soit e un entier premier à $\varphi(n) = (p-1)(q-1)$. On code un message m modulo n en envoyant $c \equiv m^e \bmod n$. Montrer que pour connaître m modulo n à partir de c, il suffit de connaître d tel que $ed \equiv 1 \bmod n$.

Exercice 9 Soit p et q des nombres premiers impairs distincts tels que $p-1$ divise $q-1$. Montrer que $m^{q-1} \equiv 1 \bmod pq$ pour tout m premier à pq.