UNIVERSITÉ DE RENNES 1
UFR Mathématiques

Licence STS-1ère année

NOMBRES ENTIERS ET RATIONNELS, CONGRUENCES (A02)

Lundi 3 décembre 2007

Documents, notes de cours ou de TD, téléphones portables, calculatrices sont interdits.
Justifiez toutes vos réponses

NOM :
PRENOM :

EXERCICE 1
Soit p un nombre premier impair et soit a un entier non multiple de p.
Donner (sans la justifier) une condition nécessaire et suffisante sur a et p pour que a soit un carré modulo p.
3 est-il un carré modulo 17 ?

EXERCICE 2
Calculer $\varphi(91)$.
Calculer un inverse de 29 modulo 72.
Soraya souhaite transmettre un message m à Matthieu. En utilisant le principe du cryptosystème RSA, elle le chiffre en un message M. Sachant que la clé publique de Matthieu est $(91, 29)$ et que le message reçu est $M = 3$, retrouver le message initial m.