Nom :
Prénom :

Université de Rennes 1
M1 MEFF Maths (2014-2015)
Algèbre, Géométrie, Algorithmique II
Contôle continu 6 (15 à 30 minutes)

On compose de préférence sur cette feuille en soignant la rédaction et sans document ni appareil électronique.

Exercice 1. (6 points) Montrer que les solutions dans $\mathbf{Z}^3$ de l'équation $a^2+b^2=c^2$ avec a,b,c tous non nuls et sans facteur commun sont, quitte à permuter a et b, de la forme $a=2rs$, $b=r^2-s^2$ et $c=r^2+s^2$ avec $r,s\in\mathbf{Z}$ de partiés différentes.

Exercice 2. (6 points) On rappelle que si $n\in\mathbf{Z}$ est premier et $a\in\mathbf{Z}$ est non divisible par n alors $a^{n-1}\equiv_n 1$. Soient p et q deux nombres premiers différents. On pose $n=pq$. Soient aussi $c,d\in\mathbf{N}$ strictement inférieurs à $(p-1)(q-1)$ et $k\in\mathbf{Z}$ vérifiant $cd=1+k(p-1)(q-1)$. Soit enfin $a\in\mathbf{N}$ premier avec p et q.
Vérifier les égalités $a^{cd}\equiv_p a$ et $a^{cd}\equiv_q a$ et en déduire que $(a^c)^d\equiv_n a$.

Exercice 3. (8 points) Construire à la règle et au compas dans le plan affine euclidien
- l'image d'un point par une similitude dont on connaît l'action sur deux points différents,
- les tangentes à un cercle qui passent par un point donné du plan et hors du disque bordé par le cercle,
- un point quelconque d'une ellipse dont on connait les deux foyers et le grand diamètre,
- la tangente à une ellipse en un point donné, supposés connus les deux foyers.