EFREI

Mathématiques discrètes
TD 5
Congruences, Théorème de Bézout, Théorème de Fermat

Exercice 1

Résoudre les congruences suivantes :

1. $3x \equiv 7 \pmod{16}$
2. $4x \equiv 9 \pmod{13}$
3. $5x + 7 \equiv 6 \pmod{23}$
4. $2x + 8 \equiv 5 \pmod{33}$
5. $3x + 9 \equiv 8x + 61 \pmod{64}$
6. $4x + 3 \equiv 7x + 12 \pmod{11}$

Exercice 2

Le théorème de Bézout affirme que le PGCD d de deux entiers a et b est une combinaison linéaire (à coefficients entiers) de a et b :

$$d = au + bv.$$

Une modification simple de l'algorithme d'Euclide (qu'on appelle alors algorithme d'Euclide *étendu*) permet de calculer ces coefficients u et v.

Dans chacun des cas suivants déterminer des nombres u et v vérifiant l'identité de Bézout $ua + vb = a \wedge b$:

46	16
21	56
124	64
3450	331
65432	876
453675	9876
1111111111	111111
10000000000001	100000001

Exercice 3

a) Calculer u et v pour $47u + 111v = 1$

b) Déterminer le pgcd(1482,1428) et trouver deux entiers u_0 et v_0 tels que : $d = 1482u_0 + 1428v_0$

c) Ecrire un algorithme d'Euclide étendu.

d) Adopter un algorithme d'Euclide étendu au calcul de l'inverse de b modulo n s'il existe. Rappelons que l'inverse modulo b^{-1} de b est le nombre entier tel que $b \cdot b^{-1} \pmod{n} = 1$. Par exemple 7 est l'inverse modulo 9 de 4, car $4 \cdot 7 \pmod{9} = 1$.

e) Trouver 15^{-1} modulo 26, trouver 5^{-1} modulo 8.

Exercice 4

Trouver le reste de $(57383)^{40}$ par 19 en utilisant le théorème de Fermat.