Exercices - Feuille C

`Texte distribué le 19 Mars 2004, à rendre le 22 ou le 24`
`(des indications seront données le 22 mars)`

Exercice C1. Calculer le pgcd d des deux nombres a et b et déterminer deux entiers x et y satisfaisant $ax + by = d$ dans chacun des cas suivants:

$$(i)\ a = 841,\ b = 160 \qquad (ii)\ a = 2613,\ b = 2171 \qquad (iii)\ a = 8991,\ b = 3293.$$

Exercice C2. Soient b et n des entiers > 1 et soit p un diviseur premier de $b^n - 1$. Montrer que l'une au moins des deux propriétés suivantes est vraie:
(i) $p \equiv 1 \pmod{n}$
(ii) il existe un diviseur d de n, distinct de n, tel que p divise $b^d - 1$.
En utilisant cette remarque, factoriser chacun des nombres suivants:

$$2^{11} - 1 = 2047, \quad 3^{12} - 1 = 531\ 440, \quad 2^{35} - 1 = 34\ 359\ 738\ 367.$$

Exercice C3.

a) Trouver le plus petit entier positif x satisfaisant simultanément

$$x \equiv 2 \pmod{3}, \qquad x \equiv 3 \pmod{5}, \qquad x \equiv 4 \pmod{11}, \qquad x \equiv 5 \pmod{16}.$$

b) Trouver le plus petit entier positif x satisfaisant simultanément

$$19x \equiv 103 \pmod{900}, \qquad 10x \equiv 511 \pmod{841}.$$

Exercice C4. Montrer que -2 est une racine primitive modulo 23. Déterminer toutes les solutions de la congruence

$$x^7 \equiv 17 \pmod{23}$$

puis celles de la congruence

$$x^{26} \equiv 10 \pmod{23}.$$

Exercice C5. Soit A le groupe $(\mathbf{Z}/65\ 520\mathbf{Z})^\times$. Déterminer le plus petit entier $n > 0$ tel que $g^n = 1$ pour tout $g \in A$.

http://www.math.jussieu.fr/~miw/enseignement.html