

Donc, il y aura autant de générateurs de G_d qu'il y a de nombre $a_d \leq d_d$ (2)

tels que $a_d, n d_d = 1$. ($a_d \leq d_d$ car $a \leq n \Leftrightarrow a, d \leq d_d d$), d'où le résultat.

$\forall a \in \mathbb{Z}/n\mathbb{Z}$, (c) engendre un et un seul G_d et donc $\{N_d, d|n\}$ partitionne $\mathbb{Z}/n\mathbb{Z}$.

D'où: $\text{card}(\mathbb{Z}/n\mathbb{Z}) = \sum_{d|n} \text{card}(N_d)$ (formule des classes). (2)

$$\Rightarrow n = \sum_{d|n} \varphi(d) = \sum_{d|n} \varphi(d) \quad (d, d=n)$$

3°) a). (2)

$U(A)$ s.g. et $x^{\varphi(n)} = 1$ cf cours. (2)

Si $k \equiv 1 [\varphi(n)]$: $k = 1 + d \cdot \varphi(n)$ et $x^k = x \cdot (x^{\varphi(n)})^d = x \in (1)$

b). $n \equiv 1 [p-1] \Leftrightarrow n = 1 + d(p-1)$ et $x^n = x \cdot x^{d(p-1)} = x \cdot (x^{p-1})^d = x \cdot 1^d = x$ (car $p \mid x^p - x$) (2)

c). $\varphi(k) = (p_1-1)(p_2-1)\dots(p_r-1)$.

$n \equiv 1 [\varphi(k)] \Rightarrow n \equiv 1 [p_i-1]$ donc: $p_i \mid x^n - x \quad x \in [1, n]$.

par conséquent: $k = \prod_{i=1}^r p_i \mid x^n - x$ (Et ceci pour tout x)

d). On a: $\omega(\phi(T)) = T^{\varphi(k)} [K] = T \Rightarrow \omega(\phi(T)) = T$.

de même $\phi(\omega(T)) = T$ donc ϕ et ω sont des fonctions réciproques l'une de l'autre. (2)

e). $K = 311 \times 313 \Rightarrow \varphi(K) = 96720$ (2)

$$36720 = 7 \times 13817 + 1 \Rightarrow 7 \times 13817 \equiv -1 [96720]$$

$$\text{donc } 7(96720 - 13817) \equiv 1 [96720]$$

$$T = 82903 \leftarrow (1)$$

$$\phi(T) \equiv T^7 \equiv 183^7 \equiv 1666 [97343] \leftarrow (2)$$

$$\omega(T) \equiv T^{82903} \equiv 1970^{82903} \equiv -110 [97343] \equiv 97233 \leftarrow (3)$$

Pour faire ces calculs, cf le programme.

```

10 PRINT "Calcul de A^B[C]"
20 INPUT "Valeur de A"; A
30 INPUT "Valeur de B"; B
40 INPUT "Valeur de C"; C
50 K = INT(LOG(B)/LOG(2))
60 DIM B(K), A(K)
70 FOR I = 0 TO K
80 B(I) = INT(B - INT(B/2)*2)
90 B = INT(B/2)
100 NEXT I
110 A(0) = A - INT(A/C)*C
120 FOR I = 1 TO K
130 D = A(I-1)*A(I-1)
140 A(I) = D - INT(D/C)*C
150 NEXT I
160 AB = 1
170 FOR I = K TO 0 STEP -1
180 IF B(I) = 0 THEN 200
190 AB = INT(AB*A(I)) - INT(AB*A(I)/C)*C
200 NEXT I
210 PRINT "A^B[C] = "; AB

```

écriture de B en base 2.

Calcul de $A^{2^i} [C] \rightarrow A(i)$