Université Paris 7 - Denis Diderot 2018-2019

UFR de Mathématiques M1 - Arithmétique

Corrigé feuille d'exercices 2

Exercice 1 Trivialement vrai si $a = 1$. Si $a > 1$, par construction $a^n = 1 \mod n$, et si $k < n$ alors $0 < a^k - 1 < a^n - 1$ donc $a^k \neq 1 \mod n$. Donc a est d'ordre n, donc par Lagrange n divise $\phi(a^n - 1)$.

Exercice 2 On adapte la preuve classique d'Euclide. Si on a une liste finie $p_1, \ldots, p_n$ de premiers égaux à $3 = -1 \mod 4$, posons $N = \prod p_i$ qui vaut $\pm 1 \mod 4$. Alors l'un au moins de, disons, $N + 2, N + 4$ égale $-1 \mod 3$. Appelons le M. Il est immédiat que M a au moins un facteur premier p qui vaut $-1 \mod 4$, et que par construction $p \neq p_i$.

Dans le second cas, on remarque que cette stratégie ne marche pas : si on construit un $M = 1 \mod 4$, ça n'implique pas qu'il a un facteur premier qui vaut aussi $1 \mod 4$. En revanche, il est facile de voir que si -1 est un carré mod p, alors $p = 1 \mod 4$ (en fait la réciproque est vraie aussi). Donc on pose $M = N^2 + 1$ et p un divisuer premier de M. Par construction $-1 = N^2 \mod p$.

Exercice 3 Soit n un nombre de Carmichael (nécessiarement impair), p un de se diviseurs premiers, r l'exposant de p dans n. Puisque $p \neq 2$, le groupe des inversibles de $\mathbb{Z}/p^r\mathbb{Z}$ est cyclique. On choisit grâce au lemme chinois (par construction p^r et n/p^r sont premiers entre eux) un entier a tel que (la classe de) a engendre ce groupe cyclique, et tel que a est inversible $\mod n/p^r$. Par Carmichael-itude n, donc p^r, divise $a^{n-1} - 1$, donc l'ordre multiplicatif de $a \mod p^r$, càd $p^{r-1}(p-1)$ puisque c'est un générateur, divise $n - 1$. Donc $r = 1$, et $p - 1$ divise $n - 1$.

Réciproquement, si n est un produit de premiers $p_1, \ldots, p_k$ distincts, et si $p_i - 1$ divise $n - 1$, alors pour tout a premier avec n (docn en particulier avec chacun des p_i) on a $a^{p_i - 1} = 1 \mod p_i$ par le petit thm de Fermat, et puisque $p_i - 1$ divise $n - 1$ on a aussi $a^{n-1} = 1 \mod p_i$. Par le lemme chinois, on a donc $a^{n-1} = 1 \mod n$.

Exercice 4 On applique le Lemme chinois pour décomposer chacun de $\mathbb{Z}/k\mathbb{Z}$ en produit direct de $\mathbb{Z}/p_i^{r_i}\mathbb{Z}$ avec p_i premier. Puisque le lemme chinois donne un iso d'anneau, ça donne une décomposition du groupe des inversibles. Ensuite il suffit de compter.

Exercice 5 Itou. Remarquons juste que l'équation $x^m = a$ n'a soit pas de solutions, soit en a le même nombre que l'équation $x^m = 1$, et que part le lemme chinois on a $x^m = a \mod N$, ssi c'est vrai modulo chacun des facteurs $p_i^{r_i}$ de N.