Générateurs multiplicatifs modulo p

Florent Noisette

March 17, 2018

Le but de cette séance est de démontrer le résultat suivant: "le groupe multiplicatif $\mathbb{Z}/p\mathbb{Z}^*$ est cyclique". Pour cela, on a besoin d'un certain nombre de résultats classiques d'arithmétiques. Ces résultats, bien qu'élémentaires, n'en sont pas moins importants. Cette feuille contient des exercices d'applications pour se familiarisé avec eux.

1 Congruence et applications

Exercice 1. Montrer qu'il existe une infinité de nombres premiers congrus à 3 modulo 4

Exercice 2. Soit $a, b \in \mathbb{N}$, montrer que $a+b+1 | a^3+b^3-3ab+1$

Exercice 3. Soit p un nombre premier et w, n des entiers.
On suppose que $w^n = 2^p + 3^p$.
Montrer que $n = 1$

Exercice 4. Soit n, m des entiers, on suppose que $\sqrt{7} > \frac{n}{m}$
Montrer que: $\sqrt{7} \geq \frac{n}{m} + \frac{1}{mn}$

2 Bezout,Gauss, théorème chinois

Exercice 5. Calculer $pgcd(a^n - 1, a^m - 1)$, pour $a, m, n \in \mathbb{N}^*$

Exercice 6. Soit $X \in \mathbb{R}$, on suppose que $x^7, x^{12} \in \mathbb{Q}$.
Montrer que $x \in \mathbb{Q}$

Exercice 7. *Wilson*. Soit p premier, montrer que $(p-1)! = -1[p]$

Exercice 8. Montrer que pour tout $n \in \mathbb{N}^*$, il existe n entiers consécutifs qui ont un facteur carré.

Exercice 9. Montrer que pour tout $n \in \mathbb{N}^*$, il existe n entiers consécutifs qui ont au moins 2018 diviseurs.

3 Petit Fermat, Ordre modulo p premier

Exercice 10. Existe t il $m \in \mathbb{N}^*$ qui soit premier avec $2^n + 3^n + 6^n - 1$ pour tout entier n

Exercice 11. Trouver les n tq: $9 | 7^n + n^3$

Exercice 12. Montrer qu'il existe une infinité de nombres premiers congrus à 1 modulo 4

Exercice 13. Soit p un nombre premier qui divise $F_n = 2^{2^n} + 1$, montrer que $p = 1[2^{n+1}]$ (bonus: $p = 1[2^{n+2}]$)

Exercice 14. Soit p, q deux nombres premiers, on suppose $q | 2^p - 3^p$, montrer que $p | q - 1$

Exercice 15. *Euler*. Montrer que a est un résidu quadratique modulo p ssi $a^{\frac{p-1}{2}} = 1[p]$