Université de Tours
Licence de Mathématiques

Session 1 — 6 Novembre 2024

EP 2 : Arithmétique

L'épreuve dure 2h. Les exercices sont indépendants mais les questions dans chaque exercices sont interdépendantes. La notation tiendra compte de la clarté de la rédaction. Toute affirmation doit être justifiée.

Exercice 1 (Vrai ou Faux)

1. 3 ne divise jamais n^2+1.
2. 8 divise $(2n+1)^2-1$.
3. Si $d|a+b$ et $d|a-b$ alors $d|a$ et $d|b$
4. Pour tout a,b $pgcd(5a+2b,2a+b)=pgcd(a,b)$
5. Si $xy=z^2$ alors x et y sont des carrés $(\exists x',y,': x=x'^2, y=y'^2)$
6. Soit p_n le nième nombre premier. $1+p_1\cdot p_2\cdots p_n$ est divisible par un nombre premier $p>p_n$.
7. $31^{362}\equiv 21 \mod 37$.

Exercice 2

1 Soit $a\in\mathbb{Z}^*$. Démontrer par récurrence que

$$a^n-1=(a-1)(a^{n-1}+a^{n-2}+\ldots+a+1)\ \forall n\in\mathbb{N}^* \tag{1}$$

2 En déduire que si a^n-1 est premier alors $a=2$.
3 En utilisant l'équation (1) Montrer que si m divise n alors a^m-1 divise a^n-1
4 En déduire que si 2^n-1 est premier alors n est premier.
5 Vérifier que 2^p-1 sont premiers pour $p=2,3,5,7$.
6 Montrer que pour p,q premiers distincts $(2^p-1,2^q-1)=1$.
7 Le 21 octobre 2024, un nouveau record pour le plus grand nombre premier connu a été atteint : le nombre $p=2^{136279841}-1$ est premier. Ce nombre s'écrit avec plus de 41 millions de chiffres. On va chercher à calculer son dernier chiffre.

(a) Montrer par récurrence que pour tout $n\in\mathbb{N}^*$, $2^{4n}\equiv 6 \mod 10$.
(b) En déduire les restes modulo 10 de 2^k pour tout $k\in\mathbb{N}^*$.
(c) Calculer p modulo 10 puis conclure.

Exercice 3

On rappelle l'algorithme d'Euclide. Pour calculer (a,b), on pose comme conditions initiales $r_0:=a, r_1=b$ et on itère N fois la division Euclidienne

$$r_{i-1}=q_ir_i+r_{i+1},\ 0<r_{i+1}<r_i \quad i=1,\ldots,N-1$$

jusqu'à $r_{N-1}=q_Nr_N+0$, ce qui donne: $(a,b)=r_N$ et une suite de restes strictement décroissante.
1. Utiliser l'algorithme d'Euclide pour calculer $d=pgcd(119,187)$.
2.En déduire les solutions entières de l'équation

$$187x+119y=d \tag{2}$$

Seules 4 divisions euclidiennes sont nécessaires pour trouver d.
Majorons le nombre d'itérations dans le cas général en fonction de la taille de a.
4 L'objectif de cette question est de montrer que $r_2<\frac{r_0}{2}$.

(a) Montrer que si $r_1<\frac{r_0}{2}$ alors $r_2<\frac{r_0}{2}$.
(b) Supposons que $r_1\geq\frac{r_0}{2}$; montrer alors que $q_1=1$ où q_1 est le quotient de la division Euclidienne $r_0=q_1r_1+r_2$. Puis en déduire que $r_2<\frac{r_0}{2}$.

5 On montre de même que $r_j<\frac{r_{j-2}}{2}$ pour tout $j=2,\ldots,N-2$. En déduire que $1\leq r_N<\frac{r_{N-2k}}{2^k}$ pour tout entier k tel que $N-2k\geq 0$.
6 En conclure que le nombre d'itérations $N<1+\frac{2\ln a}{\ln 2}$.
7 Majorer le nombre d'itérations N sachant que a est formé d'une centaine de chiffres (on peu utiliser $\ln(10)<2.3, \ln(2)>.6$).