1 Exercices

Exercice 1.1 Montrer qu'il existe une infinité de nombres premiers de la forme $4n-1$ (on pourra considérer $4p_1...p_n-1$)

Exercice 1.2 Montrer que pour tout entier naturel p non nul, il existe p entiers **consécutifs** $N_1,..,N_p$ tous non premiers. (on les cherchera divisible respectivement par 2, 3, ...)

Exercice 1.3 Soit p un nombre premier.

1. Montrer que $\forall k \in \{1,..,p-1\} \quad p \mid C_p^k$
2. Montrer que $\forall n \geqslant 0$ $p \mid n^p - n$ puis que $p \mid n^{p-1}-1$

Exercice 1.4 Soit p un nombre premier.
Soit $k \in [\![1,p-1]\!]$. On note r_k le reste de la division euclidienne de $\dfrac{(p-1)!}{k}$ par p.

1. Justifier rapidement que $\dfrac{(p-1)!}{k}$ est un entier
2. Montrer que $k \mapsto r_k$ est une bijection de $[\![1,p-1]\!]$ sur lui-même.
   En déduire que $\sum_{k=1}^{p-1} r_k = \sum_{k=1}^{p-1} k$.
3. Soit N l'entier naturel tel que $\sum_{k=1}^{p-1} \dfrac{1}{k} = \dfrac{N}{(p-1)!}$.
   Montrer que p divise N.

Exercice 1.5 Soit n un entier naturel.

1. Montrer que 2^n-1 premier $\Rightarrow n$ est premier
2. Montrer que $\text{pgcd}(2^a-1,2^b-1) = 2^{\text{pgcd}(a,b)}-1$

2 Indications

Indication pour l'exercice 1.1 : Procéder par l'absurde en supposant qu'il n'y en ait qu'un nombre fini $p_1, .., p_n$, introduire le nombre $4p_1...p_n - 1$ qui admet au moins un diviseur premier. Ce diviseur ne peut être 2 ni l'un des p_i donc c'est un diviseur de la forme $4n + 1$ et tous les diviseurs de $4p_1...p_n - 1$ sont nécessairement de cette forme. En déduire une contradiction

Indication pour l'exercice 1.2 : Considérer $N! + k$ lorsque $k = 0, 1, .., N$

Indication pour l'exercice 1.3 :

1. Ecrire $k!C_p^k$ sous la forme d'un produit d'entier et montrer que p divise de produit (C_k^p est un entier !!)
2. Par récurrence sur n, pour l'hérédité, utiliser le binôme à $(n + 1)^p$.
   Pour la dernière assertion, factoriser $n^p - n$

Indication pour l'exercice 1.4 :

1. Expliciter la factorielle.
2. Justifier que $r_k \in [\![1, p - 1]\!]$ (sinon r_k est divisible .... par donc $(p - 1)!$ aussi !! Justifier qu'il suffit de montrer l'injectivité.
   Soit $1 \leqslant k < k' \leqslant p - 1$. Si $r_k = r_{k'}$, en notant q_k et $q_{k'}$ les quotients des divisions euclidiennes correspondantes, montrer que $(k' - k)r_k$ est divisible par p.
   Pour l'égalité, r_k décrit ..... donc la somme $\sum_k r_k$ est en fait la somme .... dont seuls les termes sont permutés.
3. Multiplier l'égalité par $(p - 1)!$ et conclure.

Indication pour l'exercice 1.5 :

1. Utiliser une factorisation classique de $x^{ab} - 1$ par $x^a - 1$ (si vous ne la connaissez pas, effectuer à la main la division euclidienne (des polynômes) de $x^{ab} - 1$ par $x^a - 1$). En déduire que $x^{ab} - 1$ n'est pas premier si $a > 1$ et $b > 1$
2. On suppose $b > a$. Effectuer la division de $2^a - 1$ par $2^b - 1$ de la même façon que la division des polynômes ($a = x$!!). Faire apparaitre la forme du quotient et du reste et prouver le résultat en explicitant le quotient partiel et le reste partiel à la $k^{\text{ème}}$ étape et en prouvant alors que l'étape $(k + 1)^{\text{ème}}$ est de la même forme. On remarquera que le plus grand entier k tel que $b - ak$ soit positif est simplement le quotient de la division euclidienne de b par a. On obtiendra alors comme reste $a^r - 1$ et comme quotient $2^{b-a} + 2^{b-2a} + \cdots + 2^r + 1$, où r est le reste de la division euclidienne de b par a.
   On constate alors que $\text{pgcd}(2^b - 1, 2^a - 1) = \text{pgcd}(2^a - 1, 2^r - 1)$ et que $\text{pgcd}(b, a) = \text{pgcd}(a, r)$. En itérant le processus, la méthode d'Euclide montre que le processus s'achève en un nombre fini d'étape et que le dernier " r " non nul est le $\text{pgcd}(b, a)$, ce qui se transpose sur $2^b - 1, ...$

3 Corrections

Correction de l'exercice 1.1 : Indisponible actuellement (mais cela va venir)

Correction de l'exercice 1.2 : Indisponible actuellement (mais cela va venir)

Correction de l'exercice 1.3 : Indisponible actuellement (mais cela va venir)

Correction de l'exercice 1.4 : Indisponible actuellement (mais cela va venir)

Correction de l'exercice 1.5 : Indisponible actuellement (mais cela va venir)