

Contrôle terminal d'arithmétique et de cryptographie

Mercredi 26 mai 2021

Durée : 2 heures

La consultation de documents est interdite.
L'utilisation d'appareils électroniques est interdite.

Question de cours 1.

Énoncer le théorème de Bézout.

Question de cours 2.

Énoncer le lemme de Gauss.

Question de cours 3.

Montrer que \mathcal{P} est infini.

Indication : considérer (avec précaution) $1 + \prod_{p \in \mathcal{P}} p$.

Exercice 1.

- 1) Soit $k \in \mathbb{N}$. Montrer que $3^{2k} \equiv 2^{2k} \pmod{5}$.
- 2) Soit $m \in \mathbb{N}$. Montrer que $3^{6m} \equiv 2^{6m} \pmod{7}$.
- 3) Soit $n \in \mathbb{N}$. Montrer que $35 \mid 3^{6n} - 2^{6n}$.

Exercice 2.

Soient $a, b \in \mathbb{Z}$. On suppose que a et b sont premiers entre eux.
Soient $c, d \in \mathbb{Z}$. On suppose que c et d sont premiers entre eux.
On suppose que $bd \mid ad + bc$.
Montrer que $b = d$ ou que $b = -d$.

Exercice 3.

Soit $n \in \mathbb{N}^*$.

- 1) Justifier que $n(n+1)$ est pair.
 - 2) On note S_n le quotient de $n(n+1)$ par 2.
- Que valent le quotient et le reste dans la division euclidienne de S_n par n ?

Exercice 4.

On note $S = \left\{ (n, a) \in \mathbb{N}^* \times \mathbb{N} \mid \sum_{k=1}^n k! = a^2 \right\}$. Déterminer S .