Arithmétique

1 Pour commencer

Exercice 1 (*)
En utilisant l'algorithme d'Euclide, déterminer les PGCD des nombres suivants :

1) 3465 et 1764.
2) 4310 et 1755

Exercice 2 (*)

1) Décomposer en facteurs premiers 588.
2) Décomposer en facteurs premiers 525.

Exercice 3 (*)

1) Donner le reste de la division euclidienne de 5^{2001} par 6.
2) Donner le reste de la division euclidienne de $3^{80} + 50^{90}$ par 17.
3) Montrer que 7 divise $3245^{495} - 1$.
4) Calculer le reste de 91^{94} modulo 3 et modulo 4.
   En déduire le reste modulo 12.

Exercice 4 (*)
Résoudre l'équation d'inconnues $(x, y) \in \mathbf{Z}^2 : 7x - 12y = 3$.

Exercice 5 (*)
Démontrer le lemme de Gauss avec les valuation p-adiques.
Exercice formel : pour établir le théorème de décomposition et donc les valuations $p-$adiques, on a besoin du lemme de Gauss...

Exercice 6 (*)
Démontrer, en utilisant les valuations p-adiques que $a|b$ et $a'|b$ avec $a \wedge a' = 1$, implique que $aa'|b$.

Exercice 7 ((*))**

1) Trouver deux entiers $(a, b) \in \mathbf{Z}^2$ tels que $a \wedge b = 12$ et $a \vee b = 60$.
2) Donner une condition nécessaire et suffisante sur d et m entiers naturels non nuls pour que le système d'équations $a \wedge b = d$ et $a \vee b = m$ d'inconnues a et b admette au moins une solution.
3) Déterminer en fonction de d et m dans $\mathbf{N}^*$, le nombre de solutions du système $a \wedge b = d$ et $a \vee b = m$.

Exercice 8 (*)
Résoudre $\begin{cases} n \equiv 27\ [11] \\ n \equiv 4\ [7] \end{cases}$.

Exercice 9 (*)

1) *Passage aux sous-familles.*
   (a) Montrer que si $(a_1, \cdots a_n) \in \mathbf{Z}^n$ forme une famille d'entiers premiers entre eux deux à deux, alors, pour toute sous famille, les entiers sont encore premiers deux à deux entre eux.
   (b) Montrer par contre, que s'ils sont premiers entre eux dans leur ensemble, alors il peut exister des sous-familles où les entiers ne sont pas premiers entre eux dans leur ensemble.
2) Réfléchir aux énoncés correspondants pour des familles *complétées.*

Exercice 10 (**)
Montrer que pour tout $n \in \mathbf{N}$, $n^5 - 5n^3 + 4n$ est divisible par 120.

2 Entraînement

Exercice 11 (*)
Résoudre pour $n \in \mathbf{N},\ 3 \times 4^n \equiv -2\ [11]$.

Exercice 12 (*)
Montrer que $a^2|b^2 \Rightarrow a|b$.

Exercice 13 (*)
Soit $a \in \mathbf{Z}$. Montrer que $a^2 \not\equiv 3\ [4]$.

Exercice 14 (*)
Montrer que pour tout entier naturel n, $2^{4n+1} + 3^{4n+1} \equiv 0\ [5]$.

Exercice 15 (**)
Rédoudre dans $\mathbf{Z}^2,\ x^2 - 7y^2 = 3$.

Exercice 16 (**)

1) Justifier la règle : « un nombre est divisible par 3 si, et seulement si la somme de ses chiffres est également divisible par 3 ».
2) Montrer que la même règle s'applique avec 9.
3) Une telle règle s'applique-t-elle avec 7 ?

Exercice 17 (**)
Soit $a = \prod_{k=1}^{n} p_k^{\alpha_k}$ avec les p_k des nombres premiers deux à deux distincts
et $\forall k \in [\![1,\, n]\!],\ \alpha_k \in \mathbf{N}^*$.
Déterminer le nombre de diviseurs entiers naturels de a.

Exercice 18 (**)
Soit $(a, n) \in \mathbf{N}^* \times \mathbf{N}^*$ tel que $n \geqslant 2$. Notons $d = a \wedge n$.
Montrer que ad divise $(a+1)^n - 1$.

Exercice 19 (**) (Nombres de Mersenne $M_n = 2^n - 1$)
Soit $n \geqslant 2$.

1) Montrer que si $2^n - 1$ est premier, alors n est premier.
   Remarque : La réciproque est fausse, $2^{11} - 1 = 23 \times 89$.
2) Plus généralement, soit $a \geqslant 2$.
   Montrer que si $a^n - 1$ est premier impair, alors $a = 2$ et n est premier.

Exercice 20 (**) (Nombres de Fermat)
Pour $n \in \mathbf{N}$, on définit $F_n = 2^{2^n} + 1$ le n-ième nombre de Fermat.

1) Soit $n \in \mathbf{N}^*$, montrer que $F_n - 2 = \prod_{k=0}^{n-1} F_k$.
2) Montrer que deux nombres de Fermat distincts, sont premiers entre eux.

Exercice 21 (**)
Soit $s \in \mathbf{N}^*,$ on note $n_s = \sum_{k=0}^{s-1} 10^k = 11 \cdots 1$.

1) On suppose que n_s est premier, montrer alors que s est premier.
2) Montrer que la réciproque est fausse.

Exercice 22 (***)
On considère la suite de Fibonacci définie par :

$$u_0 = 0,\ u_1 = 1 \quad \text{et} \quad \forall n \in \mathbf{N},\ u_{n+2} = u_{n+1} + u_n.$$

1) Montrer que : $\forall n \in \mathbf{N}^*,\ u_{n+1}u_{n-1} - u_n^2 = (-1)^n$.
2) En déduire que : $\forall n \in \mathbf{N},\ u_n \wedge u_{n+1} = 1$.
3) Montrer que : $\forall n \in \mathbf{N}, \forall m \in \mathbf{N}^*,\ u_{n+m} = u_m u_{n+1} + u_{m-1} u_n$.
4) Montrer que pour tout $(m,\, n) \in (\mathbf{N}^*)^2,\ u_m \wedge u_n = u_{m \wedge n}$.
   Utiliser l'algorithme d'Euclide.

3 Approfondissement

Exercice 23 (***)
Montrer qu'il existe une infinité de nombres premiers congrus à 3 modulo 4.

Exercice 24 (***)
Déterminer 2000 nombres non premiers consécutifs.

Exercice 25 (***)
On considère l'équation

$$(E)\ :\qquad X^2+Y^2=Z^2 \quad \text{dans} \quad \mathbf{N}^3.$$

1) On suppose que Y et Z sont de même parité et que X,Y,Z sont premiers entre eux deux à deux.
Montrer que les solutions (quitte à échanger X et Y) sont nécessairement les nombres de la forme :

$$X=2ab,\quad Y=a^2-b^2,\quad Z=a^2+b^2 \quad \text{avec } a\wedge b=1.$$

2) Résoudre (E).

4 Exercices CCINP

Exercice 26 (CCINP 86)

1) Soit $(a,b,p)\in\mathbf{Z}^3$. Prouver que : si $p\wedge a=1$ et $p\wedge b=1$, alors $p\wedge(ab)=1$.

2) Soit p un nombre premier.

   (a) Prouver que $\forall k\in[\![1,p-1]\!]$, p divise $\binom{p}{k}k!$
   puis en déduire que p divise $\binom{p}{k}$.

   (b) Prouver que: $\forall n\in\mathbf{N},\ n^p\equiv n \mod p$.
   Indication: procéder par récurrence.

   (c) En déduire, pour tout entier naturel n, que : p ne divise pas $n \iff n^{p-1}\equiv 1 \mod p$.

Exercice 27 (CCINP 94)

1) Énoncer le théorème de Bézout dans $\mathbf{Z}$.

2) Soit a et b deux entiers naturels premiers entre eux.
Soit $c\in\mathbf{Z}$. Prouver que: $(a|c \text{ et } b|c)\iff ab|c$.

3) On considère le système (S): $\begin{cases} x \equiv 6 & [17] \\ x\equiv 4 & [15]\end{cases}$ dans lequel l'inconnue x appartient à $\mathbf{Z}$.

   (a) Déterminer une solution particulière x_0 de (S) dans $\mathbf{Z}$.

   (b) *Déduire des questions précédentes* la résolution dans $\mathbf{Z}$ du système (S).

Exercice 28 (CCINP 94 - version 2025)

1) En raisonnant par l'absurde, montrer que la système (S): $\begin{cases} x \equiv 5 & [6] \\ x\equiv 4 & [8]\end{cases}$ n'a pas de solution x appartenant à $\mathbf{Z}$.

2) (a) Énoncer le théorème de Bézout dans $\mathbf{Z}$.

   (b) Soit a et b deux entiers naturels premiers entre eux.
   Soit $c\in\mathbf{N}$. Prouver que: $(a|c \text{ et } b|c)\iff ab|c$.

3) On considère le système (S): $\begin{cases} x \equiv 6 & [17] \\ x\equiv 5 & [16] \\ x\equiv 4 & [15]\end{cases}$ dans lequel l'inconnue x appartient à $\mathbf{Z}$.

   (a) Déterminer une solution particulière x_0 de (S) dans $\mathbf{Z}$.

   (b) *Déduire des questions précédentes* la résolution dans $\mathbf{Z}$ du système (S).
   On exprimera les solutions en fonction de la solution particulière x_0.