

Exercice 1.

Denote by $M_n = 2^n - 1$ the n th Mersenne number.

1. Prove that if M_n is a prime number then n is prime too.
2. Show that M_{11} is not prime.

Exercice 2.

Déterminer le reste de la division euclidienne de

1. $2^{2^{10}}$ par 7.
2. $3^{2^{189}}$ par 25.

Exercice 3.

1. Soit n un entier impair. Montrer que $n^2 \equiv 1 \pmod{8}$.
2. Soit $p > 3$ un nombre premier. Montrer que $p^2 - 1$ est multiple de 24.

Exercice 4.

Déterminer tous les entiers $n \in \mathbb{N}$ tels que $n + 1$ divise $n^2 + 1$.

Exercice 5.

Montrer que pour tout $n \in \mathbb{N}$, n^2 divise $(n + 1)^n - 1$.

Exercice 6.

Soit p un nombre premier.

1. Montrer que pour tout $k \in \llbracket 1, p - 1 \rrbracket$, $\binom{p}{k}$ est divisible par p .
2. En déduire que pour tout entier $n \in \mathbb{N}$, $n^p - n$ est divisible par p (i.e. $n^p \equiv n \pmod{p}$).

Exercice 7.

Soient $a, b, c \in \mathbb{Z}$ avec $a \wedge b = 1$. Montrer que $a \wedge bc = a \wedge c$.

Exercice 8.

Soient $a, b \in \mathbb{Z}$. On note $d = a \wedge b$ et $m = a \vee b$. Que vaut $(a + b) \wedge m$?

1. Solutions

Solution 1.

1. We prove the contraposition. Let $n = km$ be a natural number which is not prime, $1 < k < n$. Then

$$1 + 2^k + (2^k)^2 + \dots + (2^k)^{m-1} = \frac{2^{km} - 1}{2^k - 1}.$$

This shows that M_n is divided by $2^k - 1$, which is bigger than 1 and smaller than M_n ; thus M_n is not prime.

2. $M_{11} = 2047 = 23 \times 89$.

Solution 2.

1. Le nombre $2^{2^{10}}$ est tellement grand qu'on ne peut pas effectuer cette division sans astuce (ou ordinateur).

On essaie donc d'abord de voir ce qui se passe avec des exposants petits. On a les équivalences suivantes modulo 7 : $2^0 \equiv 1, 2^1 \equiv 2, 2^2 \equiv 2$ et $2^3 \equiv 1$. Donc il y a un cycle de longueur 3 pour les exposants. Ainsi je la division euclidienne de 2^{10} par 3,

$$2^{10} = 3q + r,$$

ce qui permet d'écrire

$$2^{2^{10}} \equiv 2^{3q+r} \equiv (2^3)^q \times 2^r \equiv 2^r \pmod{7}.$$

Il reste alors à déterminer ce reste r . Trois méthodes pour cela :

- Par calcul mental. $2^{10} = 1024 = 341 \times 3 + 1$.
- Les paresseux reconnaissent que 1023 est divisible par 3, donc le reste est 1.

Solution 3.

1. On a $n = 2k + 1$ pour un certain $k \in \mathbb{Z}$. Ainsi $n^2 = (2k + 1)^2 = 4k(k + 1) + 1$. L'un des deux nombres k ou $k + 1$ est un multiple de 2, ce qui entraîne que $4k(k + 1)$ est un multiple de 8, donc $n^2 \equiv 1 \pmod{8}$.

Solution 4.

On écrit $n^2 + 1 = (n - 1)(n + 1) + 2$. Ainsi dès que $n \geq 2$, 2 est le reste de la division euclidienne de $n^2 + 1$ par $n + 1$.

Solution 5.

On utilise la formule du binôme :

$$(n + 1)^n - 1 = \sum_{k=1}^n \binom{n}{k} n^k$$

Solution 6.

1. Soit $k \in \llbracket 1, p - 1 \rrbracket$. On sait que $k \binom{p}{k} = p \binom{p-1}{k-1}$. Donc p divise $k \binom{p}{k}$. Comme p est premier et que $1 \leq k \leq p - 1$, k et p sont premiers entre eux. Par conséquent, p divise $\binom{p}{k}$ en vertu du théorème de Gauss.

2. On démontre le résultat par récurrence sur n .

Initialisation $0^p - 0 = 0$ est clairement divisible par p .

- On écrit $2^{10} \equiv 2^{2 \times 5} \equiv (2^2)^5 \equiv 4^5 \equiv 1^5 \equiv 1 \pmod{3}$.

On obtient alors

$$2^{2^{10}} \equiv 2 \pmod{7}$$

ce qui prouve que reste de la division euclidienne de $2^{2^{10}}$ par 7 est 2.

2. Imitant la méthode ci-dessus nous cherchons une puissance 3^n équivalente à $\pm 1 \pmod{25}$.

$$3^2 \equiv 9, 3^3 \equiv 2, 3^4 \equiv 6, 3^5 \equiv -7, 3^6 \equiv 4,$$

$$3^7 \equiv 12, 3^8 \equiv 11, 3^9 \equiv 8, 3^{10} \equiv -1 \pmod{25}.$$

Comme $2189 = 10 \times 218 + 9$ on trouve

$$3^{2189} \equiv (3^{10})^{218} \times 3^9 \equiv (-1)^{218} \times 8 \equiv 8 \pmod{25}.$$

2. D'après la question précédente on sait déjà que $p^2 \equiv 1 \pmod{8}$. Comme p n'est pas divisible par 3 on a $p \equiv \pm 1 \pmod{3}$, donc $p^2 \equiv 1 \pmod{3}$. Ainsi 8 et 3 divisent $p^2 - 1$, et donc PPCM(8, 3) = 24 divise aussi $p^2 - 1$.

2 étant notoirement non nul, $n + 1$ ne divise pas $n^2 + 1$. 1 est le seul entier n tel que $n + 1$ divise $n^2 + 1$.

Dès que $k \geq 2$, n^2 divise n^k . De plus, $\binom{n}{1} = n$ donc n^2 divise tous les termes de la somme précédente et donc divise $(n + 1)^n - 1$.

Hérédité Supposons que $n^p - n$ soit divisible par n pour un certain $n \in \mathbb{N}$. Alors

$$\begin{aligned} (n+1)^p - (n+1) &= \left(\sum_{k=0}^p \binom{p}{k} n^k \right) - (n+1) \\ &= n^p - n + \sum_{k=1}^{p-1} \binom{p}{k} n^k \end{aligned}$$

Solution 7.

Soit d un diviseur commun à a et bc . Par conséquent d divise bc . Mais d divise a qui est premier avec b . Donc d est premier avec b . Par le théorème de Gauss, d divise donc c . Finalement, d est un diviseur commun à a et c .

Solution 8.

Il existe $a', b' \in \mathbb{Z}$ tels que $a = da'$ et $b = db'$. On a de plus $a' \wedge b' = 1$ et $m = da'b'$. On a donc

$$(a+b) \wedge m = d[(a'+b') \wedge a'b'].$$

Nous allons montrer que $(a'+b') \wedge a'b' = 1$. Supposons par l'absurde qu'il existe un nombre premier p , facteur

Tous les termes de la somme sont divisibles par p d'après la question précédente et $n^p - n$ l'est également d'après l'hypothèse de récurrence. Donc $(n+1)^p - (n+1)$ est aussi divisible par p .

Conclusion Pour tout entier $n \in \mathbb{N}$, $n^p - n$ est divisible par p (i.e. $n^p \equiv n[p]$).

Réciproquement, soit d un diviseur commun à a et c . Il est alors évident que d est aussi un diviseur commun de a et bc .

On conclut donc que $a \wedge bc = a \wedge c$.

commun de $a'b'$ et $a'+b'$. Comme a' et b' sont premiers entre eux, $p|a'b'$ implique soit $p|a'$ soit $p|b'$. Quitte à changer leurs rôles on peut supposer que $p|a'$. Comme d'autre part $p|a'+b'$ on déduit $p|b'$, une contradiction ζ . Ainsi $(a'+b') \wedge a'b' = 1$ et finalement $(a+b) \wedge m = d$.