Encore quelques exercices pour les colles de cette semaine (C1)

Exercice 1.
Résoudre l'équation $x^2 + 6x - 13 \equiv 0\,[21]$ sans tester les 21 cas possibles.

Exercice 2. Soit $N \in \mathbb{N}$. Montrer que $(N+1)$ divise $\binom{2N}{N}$.

Exercice 3. Soit $p \in \mathbb{P}$. Montrer que pour tout $k \in [[0, p-1]]$, $\binom{p-1}{k} \equiv (-1)^k\,[p]$.

Exercice 4. Déterminer *le nombre* de solutions de l'équation $x^2 = \bar{1}$, dans $\mathbb{Z}/n\mathbb{Z}$:
a) pour $n = 89$, b) pour $n = 49$, c) pour $n = 300$.

Exercice 5 (Thm. de Wilson)**.** a) Soit p un nombre premier, montrer que $(p-1)! \equiv -1\,[p]$.
Indication – Regrouper chaque élément de $\{1, \ldots, p-1\}$ avec son inverse dans $\mathbb{Z}/p\mathbb{Z}$.
b) Réciproquement, montrer que si $n \geq 2$ vérifie $(n-1)! \equiv -1\,[n]$ alors n est premier.
Indication – Montrer que $\mathbb{Z}/n\mathbb{Z}$ est un corps.
c) Plus précisement, si n n'est pas premier, déterminer la classe de $(n-1)!$ modulo n.
(On distinguera le cas exceptionnel $n = 4$).

Exercice 6 (Quand (-1) est un carré modulo p : utilise Wilson)**.** a) On a dit en cours, à propos des équations du second degré dans $\mathbb{Z}/p\mathbb{Z}$, à quel point il était important de savoir si un nombre est ou n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$. On examine ici le cas de $-\bar{1}$.
Le résultat est : *Soit $p \in \mathbb{N}$ un nombre premier $p \geq 3$, $-\bar{1}$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si, et seulement si, $p \equiv 1\,[4]$.*
(i) Condition nécessaire : montrer que si $-\bar{1}$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$ alors $(-\bar{1})^{\frac{(p-1)}{2}} = \bar{1}$, et conclure.
(ii) Montrer que la condition $p \equiv 1\,[4]$ est suffisante grâce au théorème de Wilson ci-dessus, en regroupant les facteurs...
b) Déduire de cette caractérisation une preuve du fait qu'il y a une infinité de nombres premiers congrus à 1 mod. 4.

Solution 1 Je ne l'ai pas rédigé car nous l'avons fait en classe !

$$\boxed{\text{Essentielle : la relation } \binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}.}$$

Solution 2 La relation encadrée appliquée à $n-1 = 2N$ et $k-1 = N$, donne que
$\binom{2n+1}{n+1} = \dfrac{2n+1}{n+1}\binom{2n}{n}$ et donc que $(n+1)\binom{2n+1}{n+1} = (2n+1)\binom{2n}{n}$.
Donc $(n+1)$ divise $(2n+1)\binom{2n}{n}$.
Or $(n+1) \wedge (2n+1) = 1$ comme le prouve la relation de Bézout $(2n+1) - 2(n+1) = 1$.
Donc $(n+1)$ divise $\binom{2n}{n}$. □

Remarque culturelle : Les nombres $c_n = \dfrac{1}{n+1}\binom{2n}{n}$ sont appelés *nombre de Catalan*. Ils interviennent dans le calcul du nombre de parenthésages possibles pour calculer $x_1 \ldots . x_n$ pour une lci non associative.
On peut aussi les exprimer comme différence de deux binomiaux : $c_n = \binom{2n+1}{n} - 2\binom{2n}{n-1}$.

Solution 3 *L'idée est la formule du triangle de Pascal.*
Soit $p \in \mathbb{P}$. Notons $H(k)$ la propriété : $\binom{p-1}{k} \equiv (-1)^k\,[p]$.
Montrons par récurrence finie que $H(k)$ est vraie pour tout $k \in [[0, p-1]]$.
• Initialisation : pour $k = 0$, $\binom{p-1}{0} = 1 \equiv 1\,[p]$.
• H.R., on suppose que $H(k)$ est vraie pour un $k \in [[0, p-2]]$.
Montrons que $H(k+1)$ est vraie. Par la formule du triangle de Pascal, $\binom{p}{k+1} = \binom{p-1}{k+1} + \binom{p-1}{k}$.
Or comme $k+1 \in [[1, p-1]]$, on sait que $\binom{p}{k+1} \equiv 0\,[p]$.
Donc $\binom{p-1}{k+1} \equiv -\binom{p-1}{k}\,[p]$.
Or par H.R. $\binom{p-1}{k} \equiv (-1)^k\,[p]$, donc $\binom{p-1}{k+1} \equiv -(-1)^k\,[p]$ d'où $H(k+1)$.
La récurrence est établie. □

Solution 4 Fait en classe.

Solution 5 a) Soit $p \in \mathbb{P}$. Si $p = 2$, $(p-1) = 1$ et $(p-1)! \equiv 1\,[2] \equiv -1\,[2]$ donc le résultat est vrai.
On suppose désormais que $p \in \mathbb{P}_{\geq 3}$.
On considère la classe de $(p-1)!$ dans $\mathbb{Z}/p\mathbb{Z}$: $\overline{(p-1)!} = \prod_{k=1}^{p-1} \overline{k}$ $(*)$.
Dans ce produit, les $p-1$ facteurs sont distincts. L'énoncé invite à regrouper chaque facteur avec son inverse, mais il faut prendre garde aux facteurs qui sont leur propre inverse. Quels sont les éléments de $\mathbb{Z}/p\mathbb{Z}$ qui sont leur propre inverse ? Ceci est réglé par la remarque suivante.

Remarque : $\forall\, x \in \mathbb{Z}/p\mathbb{Z}^*,\ x = x^{-1} \Leftrightarrow \begin{cases} x = \overline{1} \quad \text{ou} \\ x = -\overline{1}. \end{cases}$

Preuve de la remarque : $x = x^{-1} \Leftrightarrow x^2 = \overline{1} \Leftrightarrow x^2 - \overline{1} = 0 \Leftrightarrow (x-\overline{1})(x+\overline{1}) = \overline{0} \Leftrightarrow \begin{cases} x - \overline{1} = \overline{0}, \quad \text{ou} \\ x + \overline{1} = \overline{0} \end{cases}$

La dernière équivalence est vraie par intégrité de $\mathbb{Z}/p\mathbb{Z}$. On conclut bien que $x = x^{-1}$ ssi $x = \overline{1}$ ou $x = -\overline{1}$. □
Application de la remarque : Dans $(*)$, en isolant le premier facteur $\overline{k} = \overline{1}$ et le dernier $\overline{p-1} = -\overline{1}$, on peut réécrire la formule $(*)$ sous la forme :

$$\overline{(p-1)!} = -\prod_{k=2}^{p-2} \overline{k} \quad (**)$$

Dans le produit $\prod_{k=2}^{p-2} \overline{k}$ (qui a $p-3$ facteurs, ce qui est heureusement un nombre pair), on peut regrouper les facteurs par couples, $(\overline{i}.(\overline{i})^{-1})$ en commençant par $\overline{i} = \overline{2}$, puis à chaque fois en prenant le premier facteur qui n'a pas déjà été pris et son symétrique.
On déduit alors de $(**)$ que $\overline{(p-1)!} = -\overline{1}$ dans $\mathbb{Z}/p\mathbb{Z}$, ce qui est le résultat demandé.

b) On suppose cette fois réciproquement que $n \geq 2$ et$(n-1)! \equiv -1\,[n]$.
Dans $\mathbb{Z}/n\mathbb{Z}$, on en déduit que $\prod_{k=1}^{p-1} \overline{k} = -\overline{1}$ et donc comme au a) en simplifiant les deux termes extrêmes que $\prod_{k=2}^{p-2} \overline{k} = \overline{1}$.

Mais cette égalité signifie que pour tout $k \in [\![2, p-2]\!]$,

$$\overline{k}.\left(\prod_{i\neq k, i\in[\![2,p-2]\!]} \overline{i}\right) = \overline{1}.$$

Avec cette égalité, on voit donc que pour tout $k \in [\![2, p-2]\!]$, $\overline{k}$ admet un inverse pour la multiplication dans $\mathbb{Z}/p\mathbb{Z}$.

Comme $\overline{1}$ et $\overline{p-1}$ ont aussi un inverse (eux-même), on conclut que tous les éléments de $\mathbb{Z}/p\mathbb{Z}\setminus\{\overline{0}\}$ ont un inverse pour la multiplication donc que $\mathbb{Z}/n\mathbb{Z}$ est un corps, donc que n est premier.

c) On suppose n non premier, $n \geq 2$, donc en fait $n \geq 4$.

Expérimentation au brouillon :

• Puisque l'énoncé demande de distinguer le cas $n = 4$, remarquons tout de suite que pour $n = 4$, $(n-1)! = 3! = 6 \equiv 2\ [4]$.

• Ensuite si l'on teste les exemples suivants, pour $n = 6, 8, 9$, on trouve $(n-1)! \equiv 0\ [n]$.

En fait ce qui se passe pour $n = 6$, $5! = 1 \times 2 \times 3 \times 4 \times 5$, et dans ce produit, il y a 2×3 qui fait 6.

Pour $n = 8$, c'est pareil avec $1 \times 2 \times 3 \times 4 \times \cdots \times 7$, on a le produit 2×4 qui fait 8.

Pour $n = 9$, c'est un peu plus subtil $1 \times 2 \times 3 \times \cdots \times 6 \times 7 \times 8$, et là c'est avec 3×6 qu'on aura en particulier 3×3 qui divisera notre $(9-1)!$.

Généralisons au propre pour le cas général :

Comme n n'est pas premier et $n \neq 1$, il s'écrit $n = a \times b$ avec $1 < a < n$ et $1 < b < n$.

Premier cas : on peut avoir une telle écriture avec $a \neq b$. Supposons alors SRdG $a < b$.

Alors $(n-1)! = 1 \times \cdots \times a \times \cdots \times b \times \cdots \times (n-1)$ donc $(n-1)!$ est divisible par $a \times b = n$.

Donc $(n-1)! \equiv 0\ [n]$.

Deuxième cas : on ne peut pas écrire n comme un produit de deux facteurs *distincts*. Mais cela signifie alors que $n = p^2$ avec $p \in \mathbb{P}$.

Le cas $n = 4$ est celui obtenu pour $p = 2$, et il est spécifique.

Mais ensuite si $p \geq 3$, on remarque que $2p < p^2$, donc pour $n = p^2$, $(n-1)! = 1 \times \cdots \times p \times \cdots \times (2p) \times \cdots \times (p-1)$ donc $(n-1)!$ est divise par $2p^2$ en particulier par p^2 donc $(n-1)! \equiv 0\ [n]$.

Conclusion : pour tout $n \in \mathbb{N}^*$ non premier, différent de 4, $(n-1)! \equiv 0\ [n]$.

Solution 6 a) (i) supposons qu'il existe un $m \in \mathbb{N}$ tel que $m^2 \equiv -1\ [p]$.

Comme p est premier, on sait par petit théorème de Fermat que $m^{p-1} \equiv 1\ [p]$.

Comme p est impair, $(p-1)/2$ est un entier, et on peut considérer $(-1)^{(p-1)/2} = (m^2)^{(p-1)/2} = m^{p-1} \equiv 1\ [p] \quad (*)$.

Or $(-1)^k \equiv 1\ [p]$ ssi k est pair. Donc ici avec $(*)$, on sait $(p-1)/2$ est pair, et on conclut bien que $p \equiv 1\ [4]$.

(ii) On suppose maintenant que $p \equiv 1\ [4]$ donc que $(p-1)/2 = r$ est un entier pair.

Le théorème de Wilson nous dit que, dans $\mathbb{Z}/p\mathbb{Z}$, $\prod_{k=1}^{p-1} \overline{k} = -\overline{1} \quad (*)$

Dans le produit du membre de gauche de $(*)$, on peut regrouper chaque facteur $\overline{k}$ pour $k \in [\![1, (p-1)/2]\!]$ avec son opposé $-\overline{k} = \overline{n-k} = \overline{i}$ où $i \in [\![p-(p-1)/2, p-1]\!] = [\![(p+1)/2, p-1]\!]$.

Alors $(*)$ devient $\prod_{k=1}^{(p-1)/2} \overline{k}(-\overline{k}) = -\overline{1}$ ce qui donne encore :

$$(-1)^{(p-1)/2} \prod_{k=1}^{(p-1)/2} \overline{k}^2 = -\overline{1}.$$

Comme on a dit que $(p-1)/2$ est pair, $(-1)^{(p-1)/2} = 1$ et en voyant le produit du carré comme le carré du produit, on obtient enfin :

$$\left(\prod_{k=1}^{(p-1)/2} \overline{k}\right)^2 = -\overline{1},$$

ce qui non seulement montre que $-\overline{1}$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$ mais donne une expression de ses racines carrées. □

b) Par l'absurde, supposons qu'il y ait un nombre fini de nombres premiers congrus à 1 modulo 4, qu'on note $\pi_1, \ldots, \pi_r$.

On considère $A = (\pi_1 \dots \pi_r)^2 + 1$.

Alors pour tout $i = 1, \dots, r$, $A \wedge \pi_i = 1$ (relation de Bézout évidente entre A et chaque π_i).

Mais on sait que A admet au moins un diviseur premier p. Or $(\pi_1 \dots \pi_r)^2 + 1 \equiv 0\ [A]$ autrement dit $-1 \equiv (\pi_1 \dots \pi_r)^2\ [A]$.

En particulier $(-1) \equiv (\pi_1 \dots \pi_r)^2\ [p]$. Donc (-1) est un carré modulo p donc $p \equiv 1\ [4]$.

Donc A admet un diviseur premier congru à -1 modulo 4, qui n'est pas l'un des π_i, *contradiction.*