Chapitre 6: Arithmétique et Dénombrement

Groupe de Kholle Paris-Saclay

March 28, 2021

Exercice 1 *Montrer que pour* $(a_1, \cdots, a_n) \in \mathbb{Z}^n$,
$\prod_{1 \leq i < j \leq n} (j-i) \mid \prod_{1 \leq i < j \leq n} (a_j - a_i)$

Solution. On note $\binom{X}{k} = \frac{X(X-1)\cdots(X-k+1)}{k!}$.
$\Delta(X_1, \cdots, X_n) \widehat{=} (\binom{X_i}{j})_{1 \leq i,j \leq n}$
$|\Delta(X_1, \cdots, X_n)| = \frac{1}{0!1!\cdots(n-1)!} V(X_1, \cdots, X_n)$ où $V(X_1, \cdots, X_n)$ est le déterminant de Vandermonde.
Or pour $X_1, \cdots, X_n$ entier, $\binom{X_i}{j} \in \mathbb{Z}$ donc $|\Delta(X_1, \cdots, X_n)| \in \mathbb{Z}$ et donc $0!1! \cdots (n-1)! \mid \prod_{1 \leq i < j \leq n} (a_j - a_i)$ ie $\prod_{1 \leq i < j \leq n} (j-i) \mid \prod_{1 \leq i < j \leq n} (a_j - a_i)$

Exercice 2 *Soit p premier. Déterminer les solutions de* $a^n + pb^n = p^2 c^n$

Solution. On suppose une telle solution non triviale et $|a| + |b| + |c|$ minimal. $a^n = p^2 c^n - pb^n$ donc $p | a^n$ donc $p | a$. On note alors $a = a'p$
$p^n a'^n = pb^n = p^2 c^n$ donc $p | b$ et on note alors $b = b'p$.
$p^n a'^n + p^{n+1} b'^n = p^2 c^n$ et donc $p | c$ et on note alors $c = c'p$
Après simplification, (a', b', c') est aussi solution ce qui contredit la minimalité de $|a| + |b| + |c|$ exclu.
Il n'y a donc pas de solution non triviale #.

Exercice 3 (Formule de Legendre) *Montrer que* $v_p(n!) = \sum_{i \geq 1} \lfloor \frac{n}{p^i} \rfloor$

Solution. Il s'agit ici d'effectuer une resommation astucieuse.
On remarque d'abord que $v_p(ab) = v_p(a) + v_p(b)$
$\bullet v_p(n!) = \sum_{k=0}^{n} v_p(k) = \sum_{k=1}^{n} \sum_{1 \leq i \leq v_p(k)} 1 = \sum_{i=1}^{+\infty} \sum_{\substack{k \leq n \\ i \leq v_p(k)}} 1 = \sum_{i=1}^{+\infty} \lfloor \frac{n}{p^i} \rfloor$ #

Exercice 4 *Montrer que* $\frac{(2n)!(2m)!}{n!m!(m+n)!} \in \mathbb{N}$ *pour* $n, m \in \mathbb{N}$

Solution. Par la formule de Legendre cela est équivalent à montrer que $\lfloor \frac{2n}{p^r} \rfloor + \lfloor \frac{2m}{p^r} \rfloor \geq \lfloor \frac{m}{p^r} \rfloor \lfloor \frac{n}{p^r} \rfloor \lfloor \frac{m+n}{p^r} \rfloor$ pour tout p premier et r entier naturel.
Par un changement de variable clair, une condition suffisante est que $\lfloor 2x \rfloor + \lfloor 2y \rfloor \geq \lfloor x \rfloor + \lfloor y \rfloor + \lfloor x + y \rfloor$, ce qui est facilement vérifiable #

Exercice 5 *Soit* p *premier et* $k \in [|1, p-1|]$*, montrer que* $p | \binom{p}{k}$

Solution. Trivial.

Exercice 6 *Soit* p *premier. Montrer que* $\forall n \in \mathbb{N}, \forall i \in [|1, p^n|], v_p(\binom{p^n}{i}) + v_p(i) = n$

Solution. Pour $i = p^n$ c'est clair.
Soit $i \in [|1, p^n|]$, $(i+1)\binom{p^n}{i+1} = (p^n - 1)\binom{p^n}{i}$ donc $v_p(i+1) + v_p(\binom{p^n}{i+1}) = v_p(p^n - 1) + v_p(\binom{p^n}{i})$
Or $v_p(p^n - i) = v_p(i)$, ainsi pour $i = p^n - 1$ on trouve bien n et la relation est indépendante de i ie conclusion.

Exercice 7 *Déterminer* $\gcd(2^n - 1, 2^m - 1)$

Solution. On note $n = qm + r$. Ainsi $2^n - 1 = 2^{qm}2^r - 1 = 2^{qm}(2^r - 1) + 2^{qm} - 1 = 2^{qm}(2^m - 1) + (2^n - 1)(\cdots)$ et de même, $2^n - 1 = (2^m - 1)(\cdots) + 2^r - 1$
De faite, un diviseur commun de $2^m - 1$ et $2^n - 1$ est un diviseur de $2^m - 1$ et $2^r - 1$.
Donc $\gcd(2^n - 1, 2^m - 1) = 2^{\gcd(n,m)} - 1$ par l'algorithme d'Euclide.

Exercice 8 *Caractériser le groupe* $\mathbb{Z}_n^\times$

Solution. On montre premièrement que $i \in \mathbb{Z}_n^\times \iff (i,n) = 1$ à l'aide de l'identité de Bézout.
Il en découle que $|\mathbb{Z}_n^\times| = \varphi(n)$ et que $\forall i \in \mathbb{Z}_n^\times, i^{\varphi(n)} = 1$

Exercice 9 (Théorème de Wilson) *Montrer l'équivalence :*
$p \in \mathcal{P} \iff (p-1)! = -1[p]$

Solution. On note $p \in \mathcal{P}$. $\#\ker(x \mapsto x^2) = 2$ donc seul 1 et $p-1$ sont leurs propre inverses. Ainsi on peut regrouper les autres termes par paires $x \cdot x^{-1}$ et donc $(p-1)! \equiv 1 \cdot (p-1) \equiv -1[p]$
Supposons $n = ab$, $a, b \geq 2$ alors si $a \neq b$, $(n-1)! \equiv 1 \cdots a \cdots b \cdots (n-1) \equiv 0[n]$
Si $a = b \geq 3$, $(n-1)! \equiv 1 \cdots a \cdots 2a \cdots (n-1)! \equiv 0[n]$ et si $n = 4$, $3! \equiv 2 \not\equiv -1[4]$
Remarque : Pour le sens direct, dans $\mathbb{Z}_p[X]$ avec p premier, $X^{p-1} - 1 = \prod_{i=1}^{p-1}(X - i)$ permet de conclure.

Exercice 10 (Inversibles de Z_{p^k}) *Soit $p \geq 3$ premier, $k \geq 1$. Montrer qu'il existe au moins un élément d'ordre $p-1$ dans $\mathbb{Z}_p^k$*

Solution. On procède par récurrence sur k. Pour $k = 1$ c'est clair.
Soit $k \geq 1$, on suppose qu'il existe u d'ordre $p-1$ dans $\mathbb{Z}_{p^k}$, alors il existe $a \in \mathbb{Z}$ tq $u^{p-1} \equiv 1 + ap^k$. On note alors $v = u + bp^n$ avec b à choisir.
$v^{p-1} = u^{p-1} + (p-1)u^{p-2}bp^n + \text{multiples de } (p^n)^2$
$= 1 + p^n(a + (p-1)u^{p-2}b)$, on prend alors b tel que $a + (p-1)u^{p-2}b = 0[p]$ et donc $u^{p-1} = 1[p^{n+1}]$ et donc $\text{ord}_{Z_{p^{n+1}}^\times}(v) \mid p-1$, or $p-1 | \text{ord}_{Z_{p^{n+1}}^\times}(v)$ d'où égalité et hérédité, ce qui conclue la récurrence.

Remarque : On peut conclure en prenant g générateur de $\mathbb{Z}_p$, $q = \text{ord}_{Z_{p^n}^\times}(g)$ donc $g^q = 1[p^n]$, donc $g^p = 1[p]$ et donc $p-1|q$. On note alors $q = k(p-1)$ et finalement g^k est d'ordre $p-1$ dans $\mathbb{Z}_{p^n}$

Exercice 11 (Cyclicité de $\mathbb{Z}_p^\times$) *Soit p premier. Montrez que $\mathbb{Z}_p^\times$ est cyclique.*

Solution. Notons $F = \{\text{ord}(x) | x \in \mathbb{Z}_p^\times\}$. Soit a, b d'ordres n, m respectivement. On note $d = \gcd(m, n)$.
Ainsi $m = dm', n = dn'$ et donc $\gcd(m, n') = 1$ et $mn' = m \vee n$
$\text{ord}(a) = m$, $\text{ord}(b^d) = n'$ donc ab^d d'ordre mn'.
Finalement, F est stable par ppcm.
On note $\lambda = \min\{k \in \mathbb{Z} | \forall x \in \mathbb{Z}_p^\times, x^k = 1\}$. $X^\lambda - 1$ possède $p-1$ racines donc $\lambda \geq p-1$ et $p-1$ conviens donc $\lambda = p-1$.
Par suite, $\lambda =$ppcm des éléments du groupe, donc il existe un élément de tel ordre, et donc le groupe est cyclique.

Remarque : Il est possible de montrer ce résultat, en montrant que $\varphi(p-1) > 0$ à l'aide de l'identité d'Euler, et conclure avec la structure de corps.

Exercice 12 (Les points visibles de $\mathbb{Z}^2$) *On dit qu'un point de $\mathbb{Z}^2$ est visibles ssi le segment entre $(0,0)$ et le point ne passe par aucun autre point entier. Montrer qu'il existe des rectangles arbitrairement grand de points non visibles.*

Solution. L'équation de droite passant par (a, b) et $(0, 0)$ est $ya - xb = 0$.
On va montrer que :

(a, b) visible $\iff$ l'équation $\lambda(a, b) \in \mathbb{Z}^2$ avec $0 < \lambda < 1$ est impossible.

Si $a \wedge b = d > 1$, alors $0 < \frac{1}{d} < 1$ et $\frac{1}{d}(a, b) \in \mathbb{Z}^2$ donc (a, b) non visible
Si $a \wedge b = 1$ et s'il existe $0 < \lambda < 1$ tq $\lambda(a, b) = (\alpha, \beta) \in \mathbb{Z}^2$ alors nécessairement $\lambda = \frac{u}{v} \in \mathbb{Q}$ et :
$$\begin{cases} \lambda a &= \alpha \\ \lambda b &= \beta \end{cases} \iff \begin{cases} ua &= v\alpha \\ ub &= v\beta \end{cases} \text{ donc } \begin{cases} v|a \\ v|b \end{cases} \text{ et donc } a \wedge b \neq 1 \text{ absurde}$$
donc (a, b) visible.

Notons maintenant $n \in \mathbb{N}$ et (p_k) la suite croissante des nombres premiers, posons $A = (p_{j+n(i-1)})_{1 \leq i,j \leq n}$.
Notons encore m_i le produit de la ligne i, M_j le produit de la colonne j.
D'après le théorème des restes chinois, il existe $a, b \in \mathbb{Z}$ tel que :
$$\begin{cases} a &= -1[m_1] \\ a &= -2[m_2] \\ \vdots & \\ a &= -n[m_n] \end{cases} \text{ et } \begin{cases} b &= -1[M_1] \\ b &= -2[M_2] \\ \vdots & \\ b &= -n[M_n] \end{cases}$$
En effet les m_i sont 2 à 2 premiers entre eux, et on peut supposer spdg $a, b > 0$

Ainsi pour tout $i,j \leq n, \begin{cases} a+i & = 0[m_i] \\ b+j & = 0[M_j] \end{cases}$ et $p_{j+n(i-1)} | m_i, M_j$ impliquant $a+i \wedge a+j \neq 1$ donc $(a+i, b+j)$ non visibles, et donc le rectangle $((a+i, b+j))_{i,j \leq n}$ est non visible.