Soit $p > 3$ un nombre premier. Montrer que le numérateur de la fraction (réduite)

$$\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{p-1}$$

est divisible par p^2. Par exemple, pour $p=5$,

$$\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}=\frac{25}{12},$$

et le numérateur est concrètement divisible par 5^2.

On se propose dans cet article [1] de démontrer cet énoncé. [2] Pour commencer et afin d'avoir une meilleure implication dans la recherche d'une solution, la première chose à faire est de calculer à la main davantage d'exemples. Explicitons le cas $p=5$, la somme des inverses donne

$$\begin{aligned}\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\frac{1}{4} &= \frac{2\cdot3\cdot4}{1\cdot2\cdot3\cdot4}+\frac{1\cdot3\cdot4}{1\cdot2\cdot3\cdot4}+\frac{1\cdot2\cdot4}{1\cdot2\cdot3\cdot4}+\frac{1\cdot2\cdot3}{1\cdot2\cdot3\cdot4}\\ &=\frac{24}{24}+\frac{12}{24}+\frac{8}{24}+\frac{6}{24}\\ &=\frac{12}{12}+\frac{6}{12}+\frac{4}{12}+\frac{3}{12}\\ &=\frac{25}{12}.\end{aligned}$$

Notez qu'on aurait pu mettre nos fractions sous le même dénominateur réduit 12, qui est le plus petit commun multiple des dénominateurs des 4 fractions à gauche de l'égalité. Multiplier tous les dénominateurs s'avère plus utile dans le cas général. Je vous invite à prendre davantage d'exemples à la main. Si vous souhaitez aller plus loin, vous pouvez utiliser le programme Python suivant

```python
def add_frac(frac1, frac2):
    num = frac1[0]*frac2[1] + frac1[1]*frac2[0]
    den = frac1[1]*frac2[1]
    return [num, den]

def somme(p):
    s = [1, 1]
    for i in range(1, p - 1):
        s = add_frac(s, [1, i+1])
    return s
```

Revenons à nos moutons. Dans cette question, nous devons prouver une propriété du numérateur d'une fraction simplifiée, pas chose évidente en général. Ainsi, ce numérateur doit être transformé sous une forme plus intelligible, à savoir une expression algébrique, afin de pouvoir mieux le manipuler. Par ailleurs, cet énoncé ne nécessite pas seulement la divisibilité

1. Cet article est une traduction d'une résolution proposée par Terence Tao dans son livre, Solving Mathematical Problems, A Personal Perspective. 2006, Oxford University Press, USA.
2. Ce problème est tiré du livre *The USSR Olympiad Problem Book*, écrit par SHKLARSKY, CHENTZOV et YAGLOM

par un nombre premier mais plutôt la divisibilité par le carré d'un nombre premier, ce qui est en général bien plus difficile à prouver. Ainsi on souhaite réduire ce problème à la simple divisibilité par un nombre premier, dans le but d'en faire un problème plus abordable.
En inspectant davantage cette question, nous devons donc garder en tête les deux objectifs suivants :

1. Exprimer le numérateur sous une forme littérale, facilement manipulable.

2. Réduire la p^2—divisibilité à une forme plus simple, probablement une p—divisibilité.

Commençons par traiter le premier point. D'abord, nous pouvons obtenir une expression du numérateur assez facilement, mais pas nécessairement le numérateur réduit. En mettant au même dénominateur on obtient

$$\frac{[2\cdot 3\cdots(p-1)]+[1\cdot 3\cdots(p-1)]+\cdots+[1\cdot 2\cdot 3\cdots(p-2)]}{(p-1)!}.$$

Supposons maintenant qu'on arrive à montrer que ce numérateur est divisible par p^2. En quoi cela nous aide-t-il à montrer que le numérateur réduit est lui aussi divisible par p^2 ? En fait, combien vaut le numérateur réduit ? Il s'agit bien sûr du numérateur original simplifié avec des facteurs du dénominateur. Cette simplification détruit-elle la p^2—divisibilité ? Oui, si un multiple de p est détruit. Dans notre cas, cela ne peut pas arriver puisque le dénominateur est premier avec p. [3] Ahh ! Cela signifie donc qu'il suffit de montrer que le numérateur initial (et peu esthétique) est divisible par p^2. Autrement dit, nous devons montrer que

$$[2\cdot 3\cdots(p-1)]+[1\cdot 3\cdots(p-1)]+\cdots+[1\cdot 2\cdot 3\cdots(p-2)]\equiv 0 \pmod{p^2}.$$

Pour l'instant, nous sommes devant une impasse ! L'expression obtenue n'est pas très simple et on ne voit pas pourquoi elle serait divisible par p^2. À ce stade donc, nous devons la simplifier davantage. En effet, nous pouvons l'écrire sous une forme plus compacte, à savoir

$$\frac{(p-1)!}{1}+\frac{(p-1)!}{2}+\frac{(p-1)!}{3}+\cdots+\frac{(p-1)!}{p-1}\equiv 0 \pmod{p^2}.$$

Cette écriture, somme des $(p-1)!/i$, est tout à fait légitime puisque la division par i est permissible modulo p^2. [4] En factorisant on obtient

$$(p-1)!\left[\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{p-1}\right]\equiv 0 \pmod{p^2}.$$

Rappelez vous qu'on travaille en arithmétique modulaire, donc un nombre comme $1/2$ est équivalent à un entier. Par exemple, modulo 5

$$\frac{1}{2}\equiv 3 \pmod 5,$$

puisque $2\cdot 3\equiv 6\equiv 1 \pmod 5$. [5] Regardons donc ce qu'on a obtenu : une expression de la forme

$$(\text{facteur})\times(\text{facteur})\equiv 0 \pmod{p^2}.$$

3. p est premier et $(p-1)!$ est le produit d'entiers strictement plus petits que p.
4. i et p^2 sont premiers entre eux, ce qui implique que i est inversible modulo p^2.
5. Attention, on ne peut pas inverser tout le monde modulo un entier naturel quelconque.

Dans le monde des réels, une telle égalité permet de d'affirmer que l'un des facteurs est nul. Ce n'est pas toujours le cas en arithmétique modulaire, donc la prudence s'impose. Fort heureusement, le premier facteur, $(p-1)!$ est premier avec p^2 (puisque $(p-1)!$ et p sont premiers entre eux), ce qui implique qu'on peut simplifier par $(p-1)!$. Ainsi, notre énoncé est équivalent à montrer que

$$\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{p-1}\equiv 0 \pmod{p^2}.$$

Oh ! N'est-ce pas notre question de départ ? Pas vraiment, puisqu'ici on considère toute la fraction, pas seulement son numérateur. Le paragraphe précédent est donc indispensable pour arriver à cette conclusion, mais c'est loin d'être fini. Comment peut-on prouver cette dernière ? Un exemple peut nous aider à comprendre : pour $p=5$, on obtient

$$\begin{aligned}\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\frac{1}{4} &\equiv 1+13+17+19 \pmod{25}\\ &\equiv 50 \pmod{25}\\ &\equiv 0 \pmod{25},\end{aligned}$$

comme souhaité. Mais pourquoi cela fonctionne-t-il ? Les nombres 1, 13, 17 et 19 semblent aléatoires, mais de façon magique, leur somme tombe pile multiple de 5^2. Peut-être qu'un autre essai sera plus instructif. Pour $p=7$, on obtient

$$\begin{aligned}\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\frac{1}{6} &\equiv 1+25+33+37+10+41 \pmod{49}\\ &\equiv 147 \pmod{49}\\ &\equiv 0 \pmod{49}.\end{aligned}$$

Pour ceux souhaitant faire davantage d'expérimentations, l'algorithme suivant, qui n'est autre que l'algorithme d'Euclide étendu, permet d'avoir les inverses modulaires en un claquement de doigts.

```
def euc_ext(a,mod):
    x = 1 ; xx = 0
    y = 0 ; yy = 1
    while mod != 0:
        q = a // mod
        a, mod = mod, (a % mod)
        xx, x = x - q*xx , xx
        yy, y = y - q*yy , yy
    return x
```

Revenons à notre dernier exemple. Là encore, rien n'est bien clair et il n'est pas évident pourquoi la somme donne un multiple de 7^2. Je vous rappelle alors que notre deuxième objectif était de réduire la p^2—divisibilité à la p—divisibilité. Si notre résultat est vrai pour p^2 alors il l'est aussi pour p. Essayons donc d'abord de montrer que

$$\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{p-1}\equiv 0 \pmod{p}. \tag{1}$$

Coup de chance, ce problème est bien plus facile à manipuler que le premier. Par exemple, pour $p=5$, on a

$$\begin{aligned}\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\frac{1}{4} &\equiv 1+3+2+4 \pmod{5}\\ &\equiv 0 \pmod{5}.\end{aligned}$$

Pour $p=7$, on a

$$\begin{aligned}\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\frac{1}{6} &\equiv 1+4+5+2+3+6 \pmod 7\\ &\equiv 1+2+3+4+5+6 \pmod 7\\ &\equiv 0 \pmod 7.\end{aligned}$$

Le schéma est clair ici, les inverses $1/1, 1/2, \ldots, 1/(p-1)$ semblent parcourir tous les nombres $1, 2, \ldots, (p-1) \pmod p$. Prenons un dernier exemple pour s'en convaincre. Pour $p=11$, on obtient

$$\begin{aligned}\frac{1}{1}+\frac{1}{2}+\cdots+\frac{1}{11} &\equiv 1+6+4+3+9+2+8+7+5+10 \pmod{11}\\ &\equiv 1+2+3+4+5+6+7+8+9+10 \pmod{11}\\ &\equiv 0 \pmod{11}.\end{aligned}$$

La preuve générale est assez directe. Modulo p, une heure non nulle admet un inverse et cet inverse est unique. Il s'ensuit que deux heures non nulles et distinctes admettent deux inverses distincts. Ainsi, les inverses parcourent tous les nombres non nuls modulo p. Leur somme vaut

$$1+2+3+\cdots+(p-1)=\frac{(p-1)p}{2},$$

qui est bien un entier car $p-1$ est pair. Le résultat tombe ainsi comme la pomme de Newton puisque la somme est clairement multiple de p.

Il existe une autre méthode permettant d'arriver à la même conclusion en un rien de temps ! Ceux qui ont un peu d'expérience avec l'arithmétique modulaire savent que modulo p, nous pouvons remplacer $p-1$ par -1, $p-2$ par -2 et ainsi de suite. On obtient ainsi

$$\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{p-1}\equiv\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{-3}+\frac{1}{-2}+\frac{1}{-1} \pmod p.$$

En réordonnant, on voit facilement que le tout donne $0 \pmod p$. Notez qu'il n'y a pas de terme au milieu de cette somme car p est impair, et donc aucun terme ne reste isolé. Peut-on alors faire la même chose $\pmod{p^2}$? Modulo p, nous avons regroupé $1/1$ et $1/(p-1)$, $1/2$ et $1/(p-2)$ et ainsi de suite. Si on fait la même chose modulo p^2, on obtient

$$\begin{aligned}\frac{1}{1}+\frac{1}{2}+\cdots+\frac{1}{p-1} &= \left(\frac{1}{1}+\frac{1}{p-1}\right)+\left(\frac{1}{2}+\frac{1}{p-2}\right)+\cdots+\left(\frac{1}{(p-1)/2}+\frac{1}{(p+1)/2}\right)\\ &= \frac{p}{1\cdot(p-1)}+\frac{p}{2\cdot(p-2)}+\cdots+\frac{p}{(p-1)/2\cdot(p+1)/2}\\ &= p\left[\frac{1}{1\cdot(p-1)}+\frac{1}{2\cdot(p-2)}+\cdots+\frac{1}{(p-1)/2\cdot(p+1)/2}\right].\end{aligned}$$

Cette expression, d'apparence compliquée, nous permet de gagner un facteur p, important pour la suite. En effet, au lieu de prouver

$$(\text{expression})\equiv 0 \pmod{p^2},$$

nous devons maintenant prouver la congruence

$$(p\times\text{expression})\equiv 0 \pmod{p^2},$$

ce qui est équivalent à prouver que

$$(\text{expression}) \equiv 0 \pmod{p}.$$

En d'autres termes, nous avons réduit une question de p^2—divisibilité à une question de p—divisibilité. Bingo, notre deuxième objectif est atteint ! Nous gagnons énormément au change, puisque modulo p, beaucoup de termes se simplifient, contrairement à $\pmod{p^2}$. En effet, nous devons montrer que

$$\frac{1}{1\cdot(p-1)} + \frac{1}{2\cdot(p-2)} + \cdots + \frac{1}{(p-1)/2\cdot(p+1)/2} \equiv 0 \pmod{p}.$$

Mais modulo p, $p-1$ est équivalent à -1, $p-2$ est équivalent à -2 et ainsi de suite. Notre expression devient donc

$$\frac{1}{-1^2} + \frac{1}{-2^2} + \cdots + \frac{1}{-((p-1)/2)^2} \equiv 0 \pmod{p},$$

ou de façon équivalente

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{((p-1)/2)^2} \equiv 0 \pmod{p}.$$

Cette dernière congruence n'est pas si mal, sauf qu'elle se termine par un terme un peu obscur, à savoir $1/((p-1)/2)^2$, alors qu'on a l'habitude de trouver des termes plus naturels comme $1/(p-1)^2$. Nous pouvons remédier à cela en prenant le double de la somme et en utilisant la propriété $(-a)^2 = a^2$. Ainsi, [6]

$$\begin{aligned}
&\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{((p-1)/2)^2} \\
&\quad\equiv \frac{1}{2}\Bigg[\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{((p-1)/2)^2} \\
&\qquad + \frac{1}{(-1)^2} + \frac{1}{(-2)^2} + \frac{1}{(-3)^2} + \cdots + \frac{1}{(-(p-1)/2)^2}\Bigg] \pmod{p} \\
&\quad\equiv \frac{1}{2}\Bigg[\frac{1}{1^2} + \cdots + \frac{1}{(p-1)^2}\Bigg] \pmod{p}
\end{aligned}$$

Ainsi prouver que $1/1^2 + \cdots + 1/((p-1)/2)^2$ vaut $0 \pmod{p}$ est équivalent à montrer que $1/1^2 + \cdots + 1/(p-1)^2$ le vaut aussi. Cette dernière expression sera notre préférée de par sa forme symétrique. Il nous reste donc à montrer que

$$\frac{1}{1^2} + \frac{1}{2^2} + \cdots + \frac{1}{(p-1)^2} \equiv 0 \pmod{p}. \tag{2}$$

Cette congruence est bien plus facile à prouver que notre question initiale contenant des numérateurs et de la divisibilité par p^2, qui est en général, plus difficile à prouver. Rassurez-vous donc, nous ne sommes pas en train de tournez en rond, mais plutôt en spirale, nous atteindrons ainsi la solution tant attendue sous peu !

6. N'oubliez pas que $-1 \equiv p-1 \pmod{p}, -2 \equiv p-2 \pmod{p} \cdots$ et $-(p-1)/2 \equiv p-(p-1)/2 \equiv (p+1)/2 \pmod{p}$.

Notre objectif maintenant est de prouver la congruence (2). Je vous rappelle qu'on a déjà résolu la (1), qui est une version plus simple de notre question, avec deux méthodes. La première consiste à réordonner les inverses et la deuxième à exploiter l'antisymétrie en éliminant deux à deux les opposés. Peut-on alors utiliser ces mêmes méthodes pour prouver (2) ? Malheureusement, à cause de la présence des carrés, l'antisymétrie ne peut plus fonctionner ici, mais heureusement que l'on peut utiliser le réordonnement des inverses. Prenons, là encore, l'exemple de $p = 5$ pour mieux comprendre ce qui se passe.

$$\begin{aligned}\frac{1}{1^2}+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2} &\equiv \left(\frac{1}{1}\right)^2+\left(\frac{1}{2}\right)^2+\left(\frac{1}{3}\right)^2+\left(\frac{1}{4}\right)^2 \pmod 5\\ &\equiv 1^2+3^2+2^2+4^2 \pmod 5\\ &\equiv 1^2+2^2+3^2+4^2 \pmod 5\\ &\equiv 0 \pmod 5.\end{aligned}$$

Le constat est sans appel, modulo p, les nombres $1/1^2, 1/2^2, \ldots, 1/(p-1)^2$ sont une permutation des nombres $1^2, 2^2, 3^2, \ldots, (p-1)^2$. En d'autres termes,

$$\frac{1}{1^2}+\frac{1}{2^2}+\frac{1}{3^2}+\cdots+\frac{1}{(p-1)^2} \equiv 1^2+2^2+3^2+\cdots+(p-1)^2 \pmod p.$$

Voilà, c'est quasiment plié. En utilisant l'identité classique

$$1^2+2^2+\cdots+n^2 = \frac{n(n+1)(2n+1)}{6},$$

on obtient

$$1^2+2^2+\cdots+(p-1)^2 = \frac{(p-1)p(2p-1)}{6}.$$

Notre problème se réduit donc à montrer que

$$\frac{(p-1)p(2p-1)}{6} \equiv 0 \pmod p,$$

ce qui est trivial puisque $(p-1)(2p-1)/6$ est un entier quand p est un nombre premier > 3. [7]

Source : Terence Tao, Solving Mathematical Problems, A Personal Perspective. 2006, Oxford University Press, USA.

7. Regardez $(p-1)(2p-1)$ modulo 2 puis modulo 3.

