MATH 115
ÉNONCÉS DES EXERCICES 2

A. ZEYTİN

1. Trouver un entier n pour lequel il existe des entiers k, l et m qui satisfont $\frac{n}{2} = k^2$, $\frac{n}{3} = l^3$ et $\frac{n}{5} = m^5$.
2. Deux nombres premiers p et q est dité nombres premiers jumeaux si $p - q = \pm 2$, e.g. $(3, 5)$ ou $(11, 13)$, etc.
   - Montrer que 5 est le seul premier appartenant à deux ces paires.
   - Montrer que pour chaque paire de nombres premiers jumeaux il existe un entier n tel que $n^2 - 1$ a seulement 4 diviseurs positifs.
3. Soit X l'ensemble de nombres premiers de la forme $4k + 3$ où $k \in \mathbf{N}$.
   - Montrer que X est non-vide
   - Montrer que le produit d'entiers de la forme $4k + 1$ est encore de cette forme. On suppose que X est fini et on lécrit alors comme: $X = \{p_1, p_2, \dots, p_N\}$. Soit $a = p_1 \cdot p_2 \cdot \ldots \cdot p_N - 1$.
   - Montrer que l'entier a admet un diviseur premier de la forme $4k + 3$.
   - Montrer que ceci est impossible et donc X est infini.
4. Si p est premier, montrer que $\sqrt{p}$ ne peut pas être un nombre rationnel.
5. Soient $a, b \in \mathbf{N}$. À l'aide du théorème fondamental de l'arithmetique démontrer que
$$(a, b) \cdot \mathrm{ppcm}(a, b) = a \cdot b$$
6. Soit p un nombre premier.
   - Montrer que $x^2 \equiv 1 (\bmod p)$ si et seulement si $x \equiv \pm 1 (\bmod p)$.
   - Est-ce qu'il est vrai que $x^2 \equiv 1 (\bmod p)$ si et seulement si $x \equiv \pm 1 (\bmod p)$ si p n'est pas premier.
7. Montrer que si p est premier et $a^2 \equiv b^2 (\bmod p)$ alors $p | (a - b)$ ou $p | (a + b)$.
8. Montrer que $19 \nmid (4n^2 + 4)$ pour tout $n \in \mathbf{Z}$.
9. Montrer que $7 | (3^{2n+1} + 2^{n+2})$ pour tout $n \in \mathbf{N}$.
10. Montrer que $71 | 61! + 1$.
11. Montrer que $71 | 63! + 1$.
12. Montrer que si n est composé et $n > 4$ alors $n | (n - 1)!$.
13. Montrer qu'il n'existe pas un polynôme de degré > 1 dont les coefficients sont des entiers qui reprèsente un nombre premier pour chaque entier naturel n.(<u>Indication:</u> Si $f(n) = p$ premier alors $p | f(n + kp) - f(n)$, c'est-à-dire $p | f(n + kp)$ pour tout $k \in \mathbf{N}$.)
14. Étant donné deux entiers a et m avec $m > 0$, montrer que:
   - si $(a, m) = 1$ alors il existe x tel que $ax \equiv 1 (\bmod m)$.
   - si $(a, m) > 1$ alors il n'existe pas un x tel que $ax \equiv 1 (\bmod m)$, c'est-à-dire l'équation $ax \equiv 1 (\bmod m)$ n'a pas une résolution.
15. Trouver tous les résolutions de:
   - $20x \equiv 4 (\bmod 30)$
   - $20x \equiv 30 (\bmod 4)$
   - $353x \equiv 254 (\bmod 400)$
   - $57x \equiv 87 (\bmod 105)$
   - $64x \equiv 83 (\bmod 105)$
   - $589x \equiv 209 (\bmod 817)$
   - $49x \equiv 5000 (\bmod 999)$

16. Combien de résolutions ont l'équations suivantes:
    - $15x \equiv 25(\mod 35)$.
    - $15x \equiv 24(\mod 35)$.
    - $15x \equiv 0(\mod 35)$.
17. Montrer que
    - le reste de la division par 8 du carré de tout nombres impairs est 1.
    - tout nombre pair vérifie:
    $$x^2 \equiv 0(\mod 8) \text{ ou } x^2 \equiv 4(\mod 8).$$
18. Soient a, b, c trois entiers impairs. Déterminer le reste de:
    - $a^2 + b^2 + c^2$ modulo 8, et
    - $2(ab + bc + ca)$ modulo 8.
    - En déduire que ces deux nombres ne sont pas des carrés puisque $ab + bc + ca$ non plus.
19. Il n'existe pas des entiers naturels m et n tels que:
    - $5m^4 = n^4$
    - $405m^4 = n^4$
    - $160m^5 = n^5$
20. On sait que dans $\mathbf{Q}$ si $a^2 = b^2$ alors $a = b$ ou $a = -b$. Donner un exemple de démontrer que si $a^2 \equiv b^2(\mod m^2)$, où a, b et $m > 0$ sont entiers, on ne peut pas déduire que $a \equiv b(\mod m)$ ou $a \equiv -b(\mod m)$.
21. Montrer que:
    - si $p > 2$ est un nombre premier montrer que
    $$1^2 \cdot 3^2 \cdot \ldots \cdot (p-2)^2 \equiv (-1)^{\frac{p+1}{2}}(\mod p), \text{ et}$$
    - si $p > 2$ est un nombre premier montrer que
    $$2^2 \cdot 4^2 \cdot \ldots \cdot (p-1)^2 \equiv (-1)^{\frac{p+1}{2}}(\mod p).$$
    - Déduire que
    $$(p-1)! \equiv 1(\mod p).$$
    - Montrer qu'un entier naturel $n > 1$ est premier si et seulement si $n|(n-1)! + 1$
22. Montrer que si un entier naturel n est composé alors n'est pas une puissance de n.
23. Étant donné un nombre premier p, montrer que $(p-1)! + 1$ est une puissance de p si et seulement si $p = 2, 3$ ou 5.
24. Montrer que l'équation
    - $x^2 + 1 \equiv 0(\mod 7)$ n'a pas de résolution.
    - $x^2 + 1 \equiv 0(\mod 5)$ a exactement 2 résolution.
    - $x^2 - 1 \equiv 0(\mod 8)$ a exactement 4 résolution.
25. Montrer que:
    - $7|n^6 - 1$ si $(n, 7) = 1$.
    - $42|n^7 - 7$ pour tout $n \in \mathbf{Z}$
    - $7|n^{12} - 1$ si $(n, 7) = 1$.
26. Montrer que
    $$\frac{1}{5}n^5 + \frac{1}{3}n^3 + \frac{7}{15}n \in \mathbf{Z}$$
    pour tout $n \in \mathbf{Z}$.
27. Rappel qu'on a définit l'ensemble de nombres rationnels en utilisant une relation binaire R sur l'ensemble $E = \mathbf{Z} \times (\mathbf{Z} \setminus \{0\})$ donné par $(p, q) \sim_R (r, s)$ si et seulement si $ps = qr$. Montrer que $\sim_R$ est une relation d'équivalence sur E. Trouver les classes d'équivalence, notée par $[p, q]$, suivantes:
    - $[0, 115]$
    - $[2, 7]$
    - $[-1, 3]$

28. Soit R une relation d'équivalence sur un ensemble E et soient e, f éléments de E. Montrer que soit $[e] = [f]$, soit $[e] \cap [f] = \emptyset$.

29. Soit E l'ensemble des droites du plan. Pour deux droites $\ell_1, \ell_2 \in E$ on dit que $\ell_1 \sim_R \ell_2$ si et seulement si ℓ_1 est parallèl à ℓ_2. Est-ce qu'il est vrai que ceci est une relation d'équivalence sur E.

30. Soit E l'ensemble des droites du plan. Pour deux droites $\ell_1, \ell_2 \in E$ on dit que $\ell_1 \sim_R \ell_2$ si et seulement si ℓ_1 est perpendiculaire à ℓ_2. Est-ce qu'il est vrai que ceci est une relation d'équivalence sur E.

31. Soit $E = \{0, 1, 2, 3, 4\}$ et soit $A = \{0, 1\}$. Sur l'ensemble de sous-ensembles de E, notée par $\mathcal{P}(E)$, on définit la relation binaire R en posant: pout tout $X, Y \in \mathcal{P}(E)$

$$X \sim_R Y \text{ si et seulement si} A \cap X = A \cap Y.$$

   - Montrer que R est une relation d'équivalence sur $\mathcal{P}(E)$.
   - Expliciter les classes $[\emptyset]$, $[E]$, $[A]$, $[\{2, 3, 4\}]$.
   - Maintenant, soit E un ensemble arbitraire et soit A un sous-ensemble de E. Montrer que la relation R définie par $X \sim_R Y$ si et seulement si $X \cap A = Y \cap A$ est une relation d'équivalence.
   - Expliciter les classes $[\emptyset]$, $[E]$ et $[A]$.
   - Expliciter les classes d'équivalence quand $A = \emptyset$.

32. Soit R la relation binaire défiinie sur $\mathbf{Z}$ par $a \sim_R b$ si et seulement si $3 | (a^2 - b^2)$.
   - Montrer que $\sim_R$ est une relation d'équivalence.
   - Montrer que l'ensemble de classes d'équivalence de R est égal à $\{[0], [1]$.

33. Sur $\mathbf{Z}^\times = \mathbf{Z} \setminus \{0\}$ on définit la relation R par $x \sim_R y$ si et seulement si $x|y$. Justifier que R n'est pas une relation d'équivalence.

34. Montrer que la même relation définit sur $\mathbf{N}$ est une relation d'ordre.