Arithmétique

Exercice 1 [Divisibilité]. Quelques petits problèmes autour de la divisibilité :

1. Combien d'entiers entre 101 et 1001 sont divisibles par 7
2. Montrer que si p est premier alors $\sqrt{p}$ n'est pas rationnel.
3. Montrer que si $n \in \mathbb{N}$ est un carré dans $\mathbb{Q}$ alors c'est un carré dans $\mathbb{Z}$.

Exercice 2 [Congruences]. Quelques petits problèmes autour des congruences :

1. Soit n un entier naturel. Pour quelles valeurs de n le nombre $n^2 - 3n + 6$ est-il divisible par 5 ?
2. Montrer que $\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15}$ est un entier pour tout $n \in \mathbb{N}$.
3. Montrer que pour tout nombre premier p il existe un entier naturel n tel que $6n^2 + 5n + 1 = 0 \ [\text{mod } p]$.
4. Montrer que $n(n^6 - 1)$ est divisible par 42.
5. Quel est le dernier chiffre de 7^{7^7} ?
6. Déterminer le plus petit multiple de 19 dont l'écriture en base 10 ne comporte que des 1.

Exercice 3 [Critère de divisibilité]. Soit N un entier positif dont la représentation en base 10 est donnée par $N = a_n 10^n + a_{n-1} A 0^{n-1} + \cdots + a_1 10 + a_0$ avec $0 < a_n \leq 9$ et $0 \leq a_i \leq 9$ pour $i \in [0, n-1]$. Montrer que :

1. N divisible par $2 \iff a_0 = 0 \ [\text{mod } 2]$;
2. N divisible par $3 \iff a_n + \cdots + a_0 = 0 \ [\text{mod } 3]$;
3. N divisible par $4 \iff 10a_1 + a_0 = 0 \ [\text{mod } 4]$;
4. N divisible par $5 \iff a_0 = 0 \ [\text{mod } 5]$;
5. N divisible par $6 \iff 4(a_n + \cdots + a_0) = 3a_0 \ [\text{mod } 6]$;
6. N divisible par $7 \iff (100a_2 + 10a_1 + a_0) - (100a_5 + 10a_4 + a_3) + (100a_8 + 10a_7 + a_6) - \cdots = 0 \ [\text{mod } 7]$;
7. N divisible par $8 \iff 100a_2 + 10a_1 + a_0 = 0 \ [\text{mod } 8]$;
8. N divisible par $9 \iff a_n + \cdots + a_0 = 0 \ [\text{mod } 9]$;
9. N divisible par $10 \iff a_0 = 0$;
10. N divisible par $11 \iff a_0 - a_1 + \cdots + (-1)^n a_n = 0 \ [\text{mod } 11]$;

Exercice 4 [Développement décimal périodique et nombre rationnel]. Soient a et b deux entiers **premiers entre eux**.

1. Montrer que le développement décimal de $\frac{a}{b}$ est fini ou ultimement périodique, c'est à dire qu'à partir d'un certain rang le développement décimal est périodique.
2. Montrer que si b et 10 sont premiers entre eux alors la période commence juste après la virgule.
3. Montrer que $\frac{a}{b}$ et $\frac{1}{b}$ ont une période de même longueur.
4. Montrer que si b est premier avec 10 alors la fraction $\frac{1}{b}$ est périodique de période h le plus petit entier h tel que $10^h = 1 \ [\text{mod } b]$.

Exercice 5 [Algorithme d'Euclide].

1. Déterminer le pgcd de 1482 et 1428 de deux façons différentes. On notera d ce pgcd.
2. Trouver deux entiers relatifs u_0 et v_0 tels que $d = 1482u_0 + 1428v_0$.
3. En déduire tous les couples d'entiers relatifs (u, v) tels que $d = 1482u + 1428v$.

Exercice 6 [Fibonacci]. Soit $(F_n)_{n\in\mathbb{N}}$ la suite de Fibonacci ($F_0 = 0$, $F_1 = 1$ et $F_{n+2} = F_{n+1} + F_n$ pour tout $n \in \mathbb{N}$).

1. Montrer que F_m et F_{m+1} sont premiers entre eux.
2. Montrer que $F_{n+m} = F_m F_{m+1} + F_{n-1} F_m$ pour $n > 0$.
3. Soient m et n deux entiers naturels non nuls et soit d leur pgcd . Montrer que
$$\text{pgcd}(F_m, F_n) = F_d.$$

Exercice 7 [Equations diophantiennes].

1. Résoudre dans $\mathbb{Z}$ le système
$$\begin{cases} 4x + y &= 6 \ [\text{mod } 12] \\ x + 4y &= 2 \ [\text{mod } 12] \end{cases}$$
2. Résoudre dans $\mathbb{Z}$ l'équation $10x + 15y = -365$.
3. Montrer que l'équation $x^3 + 3y^3 = 9z^3$ n'a pas de solution entière non triviale.
4. Montrer que l'équation $n^x + n^y = n^z$ admet des solution entière si et seulement si $n = 2$.

Exercice 8 [Nombre de Carmichael]. On appelle nombre de Carmichael tout entier n qui n'est pas premier et tel que $a^n = a \ [\text{mod } n]$ pour tout entier a. Ce sont les nombres qui ne sont pas premier mais qui vérifient le test de Fermat.

1. Montrer que $561 = 3 * 11 * 17$ est un nombre de Carmichael.
2. Montrer qu'un nombre de Carmichael est sans facteur carré.
3. Montrer le théorème de Korselt (1899) : Un entier n est un nombre de Carmichael si et seulement si n est sans facteur carré et pour chaque diviseur premier p de n, le nombre $p - 1$ divise $n - 1$.
4. Montrer qu'un nombre de Carmichael est produit d'au moins trois nombres premiers impairs.

Exercice 9 [Cryptograhpie : le système RSA (Rivest-Shamir-Adelman 1978]). Soient p et q deux nombres premiers distincts. On pose $n = pq$. Soient c et d deux entiers tels que $cd = 1 \ [\text{mod } \varphi(n)]$.

1. Montrer que $t^{cd} = t \ [\text{mod } n]$.
2. Supposons que n et c soient connus de tous (clef publique). Tout le monde peut alors coder un message $t \in \mathbb{Z}$ en appliquant la fonction $t \mapsto t^c \ [\text{mod } n]$. Expliquer comment on décode ce message.
3. Expliquer en quoi ce système de cryptage est particulièrement difficile à attaquer.
4. Peut-on coder tous les messages $t \in \mathbb{Z}$?
5. Est-ce que la contrainte "t premier avec n" est très génante ? (Pour cela calculer la proportion de nombres inférieurs à n et premiers avec n).

Exercice 10 [Répartition des nombres premiers]. On note p_n le $n^{\text{ème}}$ nombre premier et $\pi(x)$ le nombre de nombre premier inférieur à x.

1. Montrer que $p_{n+1} \leq p_1 \dots p_n + 1$ et que $p_{n+1} < 2^{2^n}$ pour $n \geq 1$.
2. Montrer pour x assez grand on a $log_2(log_2(x)) \leq \pi(x) \leq x$.
Remarque : Cet encadrement est très grossier. Le théorème des nombres premiers [Hadamard et de la Valle Poussin, 1896] affirme que
$$\pi(x) \sim \frac{x}{\log(x)}.$$
3. Si $n \geq 4$, montrer qu'au moins un facteur premier de $n! - 1$ est congru à -1 modulo 4. En déduire qu'il existe une infinité de nombres premiers de la forme $4k + 3$.
4. Montrer de même qu'il existe une infinité de nombres premiers de la forme $6k + 5$.
Remarque : Ces exemples se généralise dans le théoème de Dirichlet [1838] : Pour toute paire n et m d'entiers premiers entre eux, il existe infinité de nombres premiers de la forme $n + km$, où k est un entier positif.
5. Montrer qu'il existe des suites d'entiers consécutifs arbitrairement longues telles qu'aucun d'entre eux ne soit la puissance d'un nombre premier.