Nombres premiers et congruences

Proposition 1. *Décomposition en facteurs premiers.*
Soient n un entier naturel supréieur ou égal à 2 et $p_1 < p_2 < ... < p_i < ...$ la suite de tous les nombres premiers ($p_1 = 2$, $p_2 = 3$,...). Alors il existe une unique d'entiers naturels $(\alpha_i)_{i\geq 0}$ telle que $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_i^{\alpha_i}$....

Exercice 1. Soit $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_i^{\alpha_i} ...$ et $m = p_1^{\beta_1} p_2^{\beta_2} ... p_i^{\beta_i}$.... Trouver une formule pour $\mathrm{pgcd}(n, m)$ et une formule pour $\mathrm{ppcm}(n, m)$.

Nombres premiers

Exercice 2. Décomposer en facteurs premiers les nombres : 315, 312, 1225, 529. A l'aide de décompositions en facteurs premiers, calculer :
1. pgcd(45,12) et ppcm(45,12)
2. pgcd(91,28) et ppcm(91,28)
3. pgcd(3150,5880) et ppcm(3150,5880)

Exercice 3. Déterminer le nombre de diviseurs de 5880.

Exercice 4. Factoriser en produits de nombres premiers les nombres suivants :
1. 713
2. 1591
3. 9991
4. 28891
5. 1041541
6. Est-ce facile ?

Exercice 5. Soit p un nombre premier. Déterminer le nombre de diviseurs de p^n.

Exercice 6. Soit n un entier natuel suprérieur ou égal à 2. On suppose que la décomposition de n en facteurs premiers est $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$. Déterminer le nombre de diviseurs de n.

Exercice 7. Prouver par l'absurde qu'il existe une infinité de nombre premiers.

Exercice 8. Soit p un nombre premier. Prouver que $\sqrt{p} \notin \mathbb{Q}$.

Congruences

Exercice 9. Déterminer les congruences :
1. modulo 5 de 12, 45, 87, 104
2. modulo 7 de 14, 85, 24, 46
3. modulo 8 de 12, 204, 36, 48

Exercice 10. Montrer que $10^6 \equiv 1[7]$

Exercice 11. Trouver, en fonction de n, le plus petit entier naturel auquel est congru :
1. $2n^2$ modulo 5
2. $3n - 5$ modulo 7
3. $n^2 - 2n + 3$ modulo 4

Exercice 12. Prouver que pour tout $n \in \mathbb{N}$:
1. $5n^3 + n$ est divisible par 6
2. $n^7 - n$ est divisible par 7
3. $3^{2n+1} + 2^{n+2}$ est divisible par 7

Exercice 13. Déterminer les restes de la division euclidienne de :
1. 12^{15}, 10^7, 78^{15}, 13^{12} par 11
2. 91234^{2016} par 7
3. 2^{55} par 7
4. 5^{789} par 12

Exercice 14. On note $\mathbb{Z}/5\mathbb{Z}$ l'ensemble des restes de la division euclidienne par 5.
1. Déterminer les éléments de $\mathbb{Z}/5\mathbb{Z}$.
2. Donner la table d'additionde $\mathbb{Z}/5\mathbb{Z}$.
3. Donner la table de multiplication de $\mathbb{Z}/5\mathbb{Z}$.

Exercice 15. On note $\mathbb{Z}/4\mathbb{Z}$ l'ensemble des restes de la division euclidienne par 4.
1. Déterminer les éléments de $\mathbb{Z}/4\mathbb{Z}$.
2. Donner les tables d'addition et de multiplication de $\mathbb{Z}/4\mathbb{Z}$.
3. Tous les éléments ont-ils un inverse pour la loi $\times$?

Exercice 16. Soient a et n deux entiers naturels. Démontrer que :
1. $\exists b \in \mathbb{N} : ab \equiv 1[n] \Leftrightarrow \ \text{pgcd}(a, n) = 1$
2. Quel nom donner à b ?
3. Donner une méthode pour trouver b.

Exercice 17. Résoudre (dans $\mathbb{N}$) :
1. $4x \equiv 1[11]$
2. $4x \equiv 2[5]$
3. $2x \equiv 8[10]$

Exercice 18. a et b sont deux entiers relatifs et n est un entier naturel non nul. Prouver que $a \equiv b[n] \Rightarrow a^n \equiv b^n[n^2]$.

Théorème 1. *Petit théorème de Fermat.*
Soit p un nombre premier et $n \in \mathbb{Z}$. Alors :

$$n^p \equiv n[p]$$

De plus, si n ne divise pas p, alors :

$$n^{p-1} \equiv 1[p]$$

Exercice 19. Soit p un nombre permier. Démontrer que pour tout $n \in \mathbb{N}$, $3^{n+p} - 3^{n+1}$ est divisible par p.

Exercice 20. Soit $n \in \mathbb{N}$. Prouver que 7 divise $3^{6n} - 1$:
1. en utilisant les congruences
2. en utilisant le petit théorème de Fermat

Exercice 21. Soit a un entier naturel non nul. Prouver que $a^{13} - a$ est divisible par 26.

Exercice 22. Soit $a = 4$.
1. Déterminer a^{-1} modulo 15.
2. Calculer a^{-2}, a^{-3}, a^{-4},...

Exercice 23. Vers le chiffrement RSA.
Soient p et q deux nombres premiers distincts. On pose $n = pq$. Soient $m < n$ et k deux entiers naturels.

1. On suppose que p ne divise pas m. Prouver que $m^{1+k(p-1)(q-1)} \equiv m[p]$.
2. La formule est-elle valable si p divise m ?
3. Prouver que $m^{1+k(p-1)(q-1)} \equiv m[n]$.