Mathématiques discrètes. L1 Informatique I23

TD5. Arithmétique I.

Johann Carl Friedrich Gauss (1777 - 1855). Mathématicien, astronome et physicien allemand. Surnommé "le prince des mathématiciens", il est considéré comme un des plus grands mathématiciens de tous les temps. Il caractérisa notamment les polygones réguliers constructibles à la règle et au compas et donna la première démonstration de la loi de réciprocité quadratique.

"Two is the oddest prime" (Anonyme)

Exercice 1. Le Quizz.

1. Le nombre 1 est premier. Vrai ou faux ?
2. Pour montrer qu'un entier est premier, il suffit de montrer qu'il n'est divisible par aucun nombre premier inférieur ou égal à la partie entière de sa racine carrée. Vrai ou faux ?
3. Le nombre 101 est premier. Vrai ou faux ?
4. Il existe une infinité de nombres premiers. Vrai ou faux ?
5. Les entiers $F_n := 2^{2^n}+1$ sont-ils premiers pour $n \in \{0,1,2,3,4\}$? Vous risquerez-vous à faire une conjecture ?

Exercice 2. Une suite de premiers ?

On note p_n le n-ème nombre premier, i.e. $p_1 = 2$, $p_2 = 3$, etc. On définit pour $k \in \mathbf{N}\backslash\{0\}$ l'entier

$$\Pi_k := 1 + \prod_{i=1}^{i=k} p_i.$$

Calculez $\Pi_k \mod p_i$, pour $i \in \{1,\ldots,k\}$. Quelle est la plus petite valeur k telle que Π_k n'est pas un nombre premier ?

Exercice 3. Surjection canonique

Vérifiez que l'application $\varphi : \mathbf{Z} \to \mathbf{Z}/m\mathbf{Z}$ définie par $n \mapsto n \mod m$ est un morphisme d'anneau surjectif. Pour $m \in D := \{2,3,5,7,9,10,11\}$, calculez l'image de $10\mathbf{Z}$ par φ et déduisez des critères de divisibilité d'un entier n pour chacun des entiers de D.

Exercice 4. Crible d'Eratosthène.

On se fixe comme objectif de déterminer tous les nombres premiers inférieurs à une valeur m fixée. Pour cela, on utilise un tableau contenant tous les entiers de 1 à m dans l'ordre croissant et on se propose de cocher tous les entiers qui ne sont pas des nombres premiers de la façon suivante : on coche le nombre 1 initialement et on répète l'opération suivante tant qu'elle est possible : on note p le premier entier du tableau qui suit celui que l'on vient de cocher et qui n'est pas encore coché (2 initialement) et on coche tous ses multiples stricts. Appliquez l'algorithme pour $m = 100$.

Exercice 5. Nombres de Mersenne.

On s'intéresse à la primalité des nombres de la forme $a^m - 1$.

1. En remarquant que 1 est une racine triviale du polynôme $P(X) = X^m - 1$, factoriser ce polynôme. En déduire que si $a^m - 1$ est premier alors $a = 2$.
2. Montrer que si $2^m - 1$ est premier alors m est nécessairement premier. Indication : utilisez la contraposée.
3. Les nombres de la forme
$$M_p = 2^p - 1$$
avec p premier sont appelés nombres de Mersenne. Montrer que M_7 est premier.
4. On dit qu'un nombre (entier) est parfait s'il est égal à la somme de ses diviseurs autres que lui-même. Par exemple, 6 est un nombre parfait car ses diviseurs différents de 6 sont 1, 2 et 3 et on a $6 = 1 + 2 + 3$. Montrez que 28 est un nombre parfait.
5. Montrez que si M_p est un nombre de Mersenne premier alors l'entier
$$\frac{M_p(M_p+1)}{2} = 2^{p-1}(2^p - 1)$$
est un nombre parfait.
6. On s'intéresse à la réciproque de la question 2) : si p est premier alors M_p est-il nécessairement premier ? On pourra utiliser le résultat numérique suivant :
$$3^{2046} \equiv 1013 \pmod{2047}.$$