Le plus grand nombre premier

Question

Le plus grand nombre premier connu à ce jour est $2^{57\,885\,161}-1$. Quels sont ses deux derniers chiffres ?

(On peut résoudre cette question sans ordinateur.)

Réponse

Il s'agit donc de calculer $p = 2^{57\,885\,161} - 1$ modulo 100.

Puisque $100 = 2^2 \times 5^2 = 4 \times 25$, le théorème chinois invite a calculer ce nombre modulo 4 et 25, pour en déduire sa valeur modulo 100.

Tout d'abord, modulo 4, l'énorme puissance de 2 se réduit évidemment à 0. On a donc

$$p \equiv -1 \pmod 4.$$

Ensuite, il faut examiner le comportement des puissances de 2 modulo 25. Pour cela, on peut par exemple remarquer que $2^{10} = 1024 \equiv 24 \equiv -1 \pmod{25}$. En élevant au carré, on a donc $2^{20} \equiv 1 \pmod{25}$. (C'est également une conséquence du théorème d'Euler sur les congruences).

Par ailleurs, il est visible que $57\,885\,161 \equiv 1 \pmod{20}$. On peut donc trouver $r \in \mathbb{N}$ (qu'il serait facile mais inutile de calculer) tel que $57\,885\,161 = 20r + 1$. On peut alors calculer la réduction de p modulo 25 :

$$p = 2^{20r+1} - 1 = 2 \times (2^{20})^r - 1 \equiv 2 \times 1^r - 1 \equiv 1 \pmod{25}.$$

Ainsi, $p \equiv -1 \pmod 4$ et $p \equiv 1 \pmod{25}$. Le théorème chinois assure que cela détermine la réduction de p modulo 100. Ici, c'est assez facile à vérifier à la main : si un nombre est congru à 1 modulo 25, il est congru à 1, 26, 51 ou 76 modulo 100. De toutes ces possibilités, seule la troisième est congrue à -1 modulo 8.

On en déduit donc

$$p \equiv 51 \pmod{100}$$

et les deux derniers chiffres du plus grand nombre premier connu à ce jour sont 5 et 1.