Puzzle 166 Solution

Eric Brier

No Institute Given

1 Equivalent condition

The problem is for any even integer n, to find a prime $q(n)$ and an integer $f(n)$ such that:

$$\forall p \text{ prime}, p > q(n), p^n = 1 \bmod f(n)$$

Of course, the number $f(n)$ must be as large as possible. One can replace the condition by the equivalent one:

$$\forall x \in \mathbb{N}, \gcd(x, n) = 1, x^n = 1 \bmod f(n)$$

If this condition is satisfied, the initial condition is obviously satisfied. Suppose now that there exist x with $x^n \neq 1 \bmod f(n)$ and $\gcd(x, f(n)) = 1$. By Dirichlet's Theorem on primes in arithmetic progression, there exist infinitely many primes $p = x \bmod f(n)$. Any of these primes verify:

$$p^n = x^n \neq 1 \bmod f(n)$$

2 How to compute the values ?

To compute $f(n)$, one must first identify the odd primes that can divide $f(n)$. If q divides $f(n)$, then one must have

$$\forall x \in \mathbb{N}, \gcd(x, q) = 1, x^n = 1 \bmod q$$

Since x can take any value except zero modulo q, the integer n must be a multiple of $q-1$. In other words, q is one plus a divisor of n. Then, to compute the highest power of q that can divide $f(n)$, one has to check that:

$$\forall x \in \mathbb{N}, \gcd(x, q) = 1, x^n = 1 \bmod q^\alpha$$

In other terms, the integer n must be a multiple of the order of the group $\mathbb{Z}/q^\alpha\mathbb{Z}$. This order is $(q-1)q^{\alpha-1}$. Concerning the power of two that divides $f(n)$, one can check that it is the power of two that divides n plus two. At the end, $f(n)$ is defined as the product of these prime powers.

3 Examples

Using the techniques described above, one can produce the following results:

$$
\begin{array}{l}
\forall p \text{ prime }, \ p > 3 \ \ , p^2 = 1 \bmod \ 24 \\
\forall p \text{ prime }, \ p > 5 \ \ , p^4 = 1 \bmod \ 240 \\
\forall p \text{ prime }, \ p > 7 \ \ , p^6 = 1 \bmod \ 504 \\
\forall p \text{ prime }, \ p > 5 \ \ , p^8 = 1 \bmod \ 480 \\
\forall p \text{ prime }, p > 11 \, , p^{10} = 1 \bmod \ 264 \\
\forall p \text{ prime }, p > 13 \, , p^{12} = 1 \bmod \ 65520 \\
\forall p \text{ prime }, \ p > 3 \ \ , p^{14} = 1 \bmod \ 24 \\
\forall p \text{ prime }, p > 17 \, , p^{16} = 1 \bmod \ 16320 \\
\forall p \text{ prime }, p > 19 \, , p^{18} = 1 \bmod \ 28728 \\
\forall p \text{ prime }, p > 11 \, , p^{20} = 1 \bmod \ 13200 \\
\forall p \text{ prime }, p > 23 \, , p^{22} = 1 \bmod \ 552 \\
\forall p \text{ prime }, p > 13 \, , p^{24} = 1 \bmod \ 131040 \\
\forall p \text{ prime }, \ p > 3 \ \ , p^{26} = 1 \bmod \ 24 \\
\forall p \text{ prime }, p > 29 \, , p^{28} = 1 \bmod \ 6960 \\
\forall p \text{ prime }, p > 31 \, , p^{30} = 1 \bmod \ 171864 \\
\forall p \text{ prime }, p > 17 \, , p^{32} = 1 \bmod \ 32640 \\
\forall p \text{ prime }, \ p > 3 \ \ , p^{34} = 1 \bmod \ 24 \\
\forall p \text{ prime }, p > 37 \, , p^{36} = 1 \bmod \ 138181680 \\
\forall p \text{ prime }, \ p > 3 \ \ , p^{38} = 1 \bmod \ 24 \\
\forall p \text{ prime }, p > 41 \, , p^{40} = 1 \bmod \ 1082400 \\
\forall p \text{ prime }, p > 43 \, , p^{42} = 1 \bmod \ 151704 \\
\forall p \text{ prime }, p > 23 \, , p^{44} = 1 \bmod \ 5520 \\
\forall p \text{ prime }, p > 47 \, , p^{46} = 1 \bmod \ 1128 \\
\forall p \text{ prime }, p > 17 \, , p^{48} = 1 \bmod \ 4455360 \\
\forall p \text{ prime }, p > 11 \, , p^{50} = 1 \bmod \ 264 \\
\forall p \text{ prime }, p > 53 \, , p^{52} = 1 \bmod \ 12720 \\
\forall p \text{ prime }, p > 19 \, , p^{54} = 1 \bmod \ 86184 \\
\forall p \text{ prime }, p > 29 \, , p^{56} = 1 \bmod \ 13920 \\
\forall p \text{ prime }, p > 59 \, , p^{58} = 1 \bmod \ 1416 \\
\forall p \text{ prime }, p > 61 \, , p^{60} = 1 \bmod \ 6814407600
\end{array}
$$

A funny one:

$$\forall p \text{ prime}, p > 631, p^{630} = 1 \bmod 3539974641006983256$$