

Quora に投稿されていた次の問題^{*1}を考えます。

5^{400} の答えの下 6 桁を、計算機やソフトを使わずに導き出す方法を教えてください。

この問題は数学的には

$$5^{400} \pmod{10^6} \quad (1)$$

を計算する問題になります。この手の問題はオイラーの公式

$$a^{\varphi(m)} \equiv 1 \pmod{m} \text{ for } \gcd(a, m) = 1 \quad (2)$$

を連想させますが、今回は 5 と 10^6 が互いに素ではないので用いることができません。そこで、 10^6 を 2^6 と 5^6 に分解する、という方針を考えてみます。そのために、次の補題を用意します。

Lemma 1 任意の $n \geq 0$ について、次が成り立つ。

$$5^{2^n} \equiv 1 \pmod{2^{n+2}}. \quad (3)$$

Proof 1 数学的帰納法で示します。 $n = 0$ のときは明らかです。ある n で式 (3) が成り立つとすると、ある自然数 m を用いて、

$$5^{2^n} = 2^{n+2}m + 1 \quad (4)$$

が成り立ちます。このとき、

$$5^{2^{n+1}} = (2^{n+2}m + 1)^2 = 2^{n+3}(2^{n+1}m^2 + m) + 1 \quad (5)$$

なので、

$$5^{2^{n+1}} \equiv 1 \pmod{2^{n+3}} \quad (6)$$

が成り立ちます。よって、 $n + 1$ のときも式 (3) が成り立つことがわかりました。よって、数学的帰納法によって、任意の $n \geq 0$ で式 (3) が成り立つことが示されました。□

この補題で $n = 4$ とすると、

$$5^{16} \equiv 1 \pmod{2^6} \quad (7)$$

となります。 5^{400} とは離れてしましますが、一旦 5^{16} について考えてみましょう。すると、 10^6 のもう一つの片割れ 5^6 については明らかに

$$5^{16} \equiv 0 \pmod{5^6} \quad (8)$$

^{*1} <https://qr.ae/TWRjF2>

が成り立ちます。まとめると、

$$\begin{cases} 5^{16} \equiv 1 \pmod{2^6}, \\ 5^{16} \equiv 0 \pmod{5^6} \end{cases} \quad (9)$$

です。いま、本題は 5^{400} でした。でも、 $400 = 16 \times 25$ なので、

$$\begin{cases} 5^{400} \equiv 1 \pmod{2^6}, \\ 5^{400} \equiv 0 \pmod{5^6} \end{cases} \quad (10)$$

がわかります。ここで、次の定理を思い出しましょう。

Theorem 1 (中国の剰余定理) $\gcd(m, n) = 1$ とする。任意の整数 b, c について、連立合同式

$$x \equiv b \pmod{m}, \quad x \equiv c \pmod{n} \quad (11)$$

は $0 \leq x < mn$ を満たす唯一の解を持つ。

いま、 5^{16} と 5^{400} はともに

$$\begin{cases} x \equiv 1 \pmod{2^6}, \\ x \equiv 0 \pmod{5^6} \end{cases} \quad (12)$$

の解になっていることが式 (9) と式 (10) からわかります。中国の剰余定理によると、式 (12) を満たす解は $0 \leq x < 10^6$ の中に一つしかありません。これより、

$$5^{400} \equiv 5^{16} \pmod{10^6} \quad (13)$$

がわかります。なので、 5^{400} を計算する代わりに 5^{16} を計算すればよいのです。これでだいぶ計算コストが落ちました。あとは根気強く計算すれば*2、

$$5^{400} \equiv 5^{16} \equiv 890625 \pmod{10^6} \quad (14)$$

となり、答えが得られました!

*2 まだまだ楽をしたい人は次のように計算するのも良いかもしれません。 $5^4 = 625$ なので (これくらいは計算して!)、

$$5^{16} = 625^4 \equiv (600 + 25)^4 \equiv 4 \cdot 600 \cdot 25^3 + 25^4 \equiv 5 \cdot 10^5 + 390625 = 890625$$

という風にも解が得られます。