Theorem

Fermat's little theorem

$a \in \mathbb{Z}$、p が素数とする。a と p が互いに素である時、次の式が成り立つ。

$$a^{p-1} \equiv 1 \pmod{p} \tag{1}$$

これを Fermat(フェルマー) の小定理という。

Euler's theorem

$a \in \mathbb{Z}$ とし、$n \in \mathbb{N}$ は a と互いに素であるとする。この時、次の式が成り立つ。

$$a^{\varphi(n)} \equiv 1 \pmod{n} \tag{2}$$

$\varphi(n)$ は Euler(オイラー) 関数で、n 未満の n と互いに素な自然数の個数を表す。これを Euler(オイラー) の定理という。

問題

$999^{\left(999^{\left(999^{\left(999^{999}\right)}\right)}\right)}$ を 11 で割った余りを求めよ。

………………………………………………………………

問題の式を a_0 とし、指数部分を順に a_1, a_2, a_3 を次のように置く。

$$a_0 = 999^{\left(999^{\left(999^{\left(999^{999}\right)}\right)}\right)},\ a_1 = 999^{\left(999^{\left(999^{999}\right)}\right)},\ a_2 = 999^{\left(999^{999}\right)},\ a_3 = 999^{999} \tag{3}$$

999 と 11 は互いに素であるので、フェルマーの小定理より次が成り立つ。

$$999^{11-1} = 999^{10} \equiv 1 \pmod{11} \tag{4}$$

つまり、a_0 の指数部分 a_1 を 10 で割った余り r_1 に置き換えたものと a_0 は合同である。

$$a_0 = 999^{a_1} = 999^{10q_1+r_1} \equiv 999^{r_1} \pmod{11} \tag{5}$$

そこで a_1 を 10 で割った余り r_1 を求める。

$$a_1 = 10q_1 + r_1 \tag{6}$$

$999 = 10^3 - 1 \equiv -1 \pmod{10}$ であるので、2 乗したものが 1 と合同となる。

$$999^2 \equiv (-1)^2 \equiv 1 \pmod{10} \tag{7}$$

つまり、a_1 の指数部分 a_2 を 2 で割った余り r_2 に置き換えたものと a_1 は合同である。

$$a_1 = 999^{a_2} = 999^{2q_2+r_2} \equiv 999^{r_2} \pmod{2} \tag{8}$$

である。

そこで a_2 を 2 で割った余り r_2 を求める。

$$a_2 = 2q_2 + r_2 \tag{9}$$

$999 \equiv 1 \pmod 2$ であるので、a_2 が次のようになる。

$$a_2 = 999^{a_3} \equiv 1^{a_3} \equiv 1 \pmod 2 \tag{10}$$

つまり、式 (9) の余りが 1 になる。

$$a_2 = 2q_2 + 1 \tag{11}$$

これにより a_1 は次のようになる。

$$a_1 = 999^{a_2} = 999^{2q_2+1} = \left(999^2\right)^{q_2} \times 999^1 = 999\left(999^2\right)^{q_2} \tag{12}$$

mod 10 において $999 \equiv 9$ と $999^2 \equiv 1$ であるから上の式は次のようになる。

$$a_1 = 999\left(999^2\right)^{q_2} \equiv 9(1)^{q_2} \equiv 9 \pmod{10} \tag{13}$$

これを用いて式 (6) の r_1 を求める。

$$a_1 = 10q_1 + 9 \tag{14}$$

これより a_0 は次のようになる。

$$a_0 = 999^{a_1} = 999^{10q_1+9} = 999^9\left(999^{10}\right)^{q_1} \tag{15}$$

フェルマーの小定理 (4) より $999^{10} \equiv 1 \pmod{11}$ であるので上の式は次のようになる。

$$a_0 = 999^9\left(999^{10}\right)^{q_1} \equiv 999^9(1)^{q_1} \equiv 999^9 \pmod{11} \tag{16}$$

つまり、a_0 を 11 で割った余りと 999^9 を 11 で割った余りは一致する。

$999 \equiv 9 \equiv -2 \pmod{11}$ であるので、$999^9 \equiv (-2)^9 \equiv -512$ となる。$-512 = 11 \times (-47) + 5$ より $a_0 \equiv 5 \pmod{11}$ となる。

$$999^{\left(999^{\left(999^{\left(999^{999}\right)}\right)}\right)} \equiv 5 \pmod{11} \tag{17}$$

フェルマーの小定理 (4) より $999^{10} \equiv 1 \pmod{11}$ としたが、$999^5 \equiv 1 \pmod{11}$ であるのでこれを用いたほうが少しだけ式が単純になるかもしれない。
