Lecture Notes for International Mathematical Olympiad

EULER'S THEOREM

1. Statement and proof

The following Euler's theorem is usually viewed as a generalization of Fermat's little theorem.

Theorem 1 (Euler's theorem). *Let $m \in \mathbb{N}^*$ and $a \in \mathbb{Z}$ such that $(a, m) = 1$. Then*

$$a^{\varphi(m)} \equiv 1 \bmod m.$$

Here $\varphi(m)$ is the Euler totient function of m.

Proof. Suppose $\{a_1 \bmod m, \ldots, a_{\varphi(m)} \bmod m\}$ is a reduced residue system, i.e. $a_1, \ldots, a_{\varphi(m)}$ givens all elements that are coprime to m after modulo m. Since $(a, m) = 1$, we see $\{aa_1, \ldots, aa_{\varphi(m)}\}$ is a reduced residue system of m as well. Then

$$(aa1) \cdots (aa_{\varphi(m)}) \equiv a_1 \cdots a_{\varphi(m)} \bmod m.$$

Then $a^{\varphi(m)} a_1 \cdots a_{\varphi(m)} \equiv a_1 \cdots a_{\varphi(m)} \bmod m$ with $(a_1 \cdots a_{\varphi(m)}, m) = 1$. Hence

$$a^{\varphi(m)} \equiv 1 \bmod m.$$

In particular, when $m = p$ is prime, we have $\varphi(p) = p - 1$, and then $a^{p-1} \equiv 1 \bmod p$. □

2. Primary applications

Problem 2. *Compute the last three digits of* $2016^{2017^{2018}}$.

Solution. Denote $A = 2016^{2017^{2018}}$. It suffices to find $A \bmod 8$ and $A \bmod 125$. It is clear that $8 \mid A$. Also,

$$A \equiv 16^{2017^{2018}} \bmod 125, \quad (16, 125) = 1.$$

Then

$$\varphi(125) = 125 \times \frac{4}{5} = 100, \quad 16^{\varphi(125)} = 16^{100} \equiv 1 \bmod 125.$$

This suggests us to find $2017^{2018} \bmod 100$. We have $2017^{2018} \equiv 17^{2018} \bmod 100$, and $(17, 100) = 1$ with $\varphi(100) = 40$. Hence

$$17^{40} \equiv 1 \bmod 100 \implies 17^{2018} \equiv (17^{40})^{50} \times 17^{18} \equiv 17^{18} \bmod 100.$$

For this, note that $17^{18} \equiv 1^{18} = 1 \bmod 4$, and

$$(17, 25) = 1 \implies 17^{\varphi(25)} = 17^{20} \equiv 1 \bmod 25.$$

Then

$$17^{18} \equiv \frac{17^{20}}{17^2} \equiv \frac{1}{289} \equiv \frac{1}{14} = \frac{2}{28} \equiv \frac{2}{3} = \frac{16}{24} \equiv \frac{16}{-1} = -16 \equiv 9 \bmod 25.$$

It follows that $17^{18} \equiv 9, 59 \bmod 100$, and hence $17^{2018} \equiv 9 \bmod 10$. Denote $17^{2018} = 100k+9$ for some $k \in \mathbb{Z}$. Then

$$A \equiv 16^{100k+9} \equiv (16^{100})^k \times 16^9 \equiv 16^9 \equiv (16^2)^4 \times 16 \equiv 6^4 \times 16 \equiv 736 \equiv 111 \bmod 125.$$

Date: August 30, 2022.

Therefore, $A \bmod 1000 \in \{111, 236, 486, 736, 986\}$. As $8 \mid A$, we conclude that

$$A \bmod 1000 = 736.$$

□

Problem 3. *Determine the last two digits of* $S = f(17) + f(18) + f(19) + f(20)$, *where*

$$f(x) = x^{x^{x^x}}.$$

Solution. Firstly, we have

$$f(17) = 1^{17^{17^{17}}} \equiv 1 \bmod 4, \quad f(19) \equiv (-1)^{19^{19^{19}}} \equiv -1 \bmod 4, \quad f(18) \equiv f(20) \equiv 0 \bmod 4.$$

Then $S \equiv 1 + 0 + (-1) + 0 \equiv 0 \bmod 4$. On the other hand,

$$f(20) \equiv 0 \bmod 25, \quad f(18) \equiv (-7)^{18^{18^{18}}} \equiv (-7)^{4k} \equiv 1 \bmod 25$$

for some $k \in \mathbb{Z}$, as $7^4 = 2401 \equiv 1 \bmod 25$. Also, since $(17, 25) = 1$,

$$\varphi(25) = 20 \implies 17^{20} \equiv 1 \bmod 25.$$

To determine $f(17) = 17^{17^{17^{17}}} \bmod 25$, we are to find $y = 17^{17^{17}} \bmod 20$. But $y \equiv 1 \bmod 4$ and

$$y \equiv 2^{17^{17}} \equiv 2^{4k+1} \equiv (2^4)^k \times 2 \equiv 2 \bmod 5.$$

Then $y = 20p + 17$ for $p \in \mathbb{Z}$. So

$$f(17) \equiv 17^{20p+17} \equiv 17^{17} \equiv 17^{20} \times 17^{-3} \equiv 17^{-3} \bmod 25.$$

We have $3 \times 17 \equiv 51 \equiv 1 \bmod 25$. Thus,

$$17^{17} \equiv \frac{1}{3^{-3}} \equiv 27 \equiv 2 \bmod 25 \implies f(17) \equiv 2 \bmod 25.$$

It remains to compute $f(19)$, which is given by $z = 19^{19^{19}} \bmod 20$. We obtain

$$z = (-1)^{19^{19}} \equiv -1 \bmod 20 \implies z = 20h - 1,\ h \in \mathbb{Z}.$$

Therefore,

$$f(19) = 19^{20h-1} \equiv (19^{20})^h \times \frac{1}{19} \equiv \frac{1}{19} = \frac{4}{19 \times 4} \equiv 4 \bmod 25.$$

To conclude, we have

$$S \equiv 0 + 1 + 2 + 4 \equiv 7 \bmod 25 \implies S \equiv 32 \bmod 100.$$

□

Problem 4. *Prove that for any* $a \geqslant 2$ *and* $n \geqslant 1$, *we have*

$$n \mid \varphi(a^n - 1).$$

Proof. We introduce a fact that for $a, b, m, n \in \mathbb{N}^*$ with $ab \neq 1$ and $(a, b) = 1$,

$$(a^m - b^m) \mid (a^n - b^n) \iff m \mid n.$$

Since $(a, a^n - 1) = (a, -1) = 1$, by Euler's theorem,

$$a^{\varphi(a^n-1)} \equiv 1 \bmod (a^n - 1).$$

This is equivalent to $a^n - 1 \mid a^{\varphi(a^n-1)} - 1$. By the fact, we get $n \mid \varphi(a^n - 1)$. □

Exercise 5. Prove that for any even number $n > 0$,

$$n^2 - 1 \mid 2^{n!} - 1.$$

(Hint: apply Euler's theorem to $n+1$ and $n-1$ together with 2, respectively; also note that $\varphi(n \pm 1) \leqslant n$, and therefore $\varphi(n \pm 1) \mid n!$.)

Problem 6. *Prove that there is some positive integer n divides infinitely many terms in the series* $1, 11, 111, \ldots$.

Proof. It suffices to prove that there are infinitely many $k \in \mathbb{N}$ such that n divides $(10^k - 1)/9$. This is implied by $9n \mid (10^k - 1)$. But by Euler's theorem, if $(n, 10) = 1$, then

$$10^{\varphi(9n)} \equiv 1 \bmod 9n.$$

So we can take $k_m = m\varphi(9n)$ for some fixed m. Then n divides a_{k_m}. □

3. Two difficult problems

Problem 7. *Show that for any* $n \in \mathbb{N}^*$ *and* $a \in \mathbb{Z}$, *we have*

$$\sum_{d \mid n} \varphi(d) a^{\frac{n}{d}} \equiv 0 \bmod n.$$

Proof. For convenience we denote $x_n(a) = \sum_{d \mid n} \varphi(d) a^{n/d}$. Let $P(n)$ be the proposition that $n \mid x_n(a)$ for all $a \in \mathbb{Z}$. We are to prove that if $(m, n) = 1$, then $P(mn)$ holds if both $P(m)$ and $P(n)$ are valid. That is, assuming $P(m), P(n)$, we have

$$mn \mid x_{mn}(a) = \sum_{d \mid mn} \varphi(d) a^{mn/d}.$$

To prove this, by symmetry of m and n, it suffices to prove that $m \mid x_{mn}(a)$. Note that $(m, n) = 1$ and φ is a multiplicative function, so

$$\begin{aligned} x_{mn}(a) &= \sum_{d \mid mn} \varphi(d) a^{mn/d} \\ &= \sum_{e \mid m, f \mid n} \varphi(e)\varphi(f) a^{(m/e)\cdot(n/f)} \\ &= \sum_{f \mid n} \varphi(f) \sum_{e \mid m} \varphi(e) (a^{n/f})^{m/e} \\ &= \sum_{f \mid n} \varphi(f) x_m(a^{n/f}). \end{aligned}$$

Since $p(m)$ is hold by the hypothesis, we see $m \mid x_m(a^{n/f})$, and $m \mid x_{mn}(a)$. This proves the first assertion.

Now we apply the induction. Write $n = p_1^{a_1} \cdots p_k^{a_k}$ into arithmetic factorization into distinct primes $p_1, \ldots, p_k$. By Chinese remainder theorem, it suffices to prove that

$$\sum_{d \mid n} \varphi(d) a^{n/d} \equiv 0 \bmod p_i^{a_i}, \quad i = 1, \ldots, k.$$

Since $p_1^{a_1}, \cdots, p_k^{a_k}$ are mutually coprime, if we assumed

$$p_i^{a_i} \mid \sum_{d \mid p_i^{a_i}} \varphi(d) a^{p_i^{a_i}/d} = x_{p_i^{a_i}}(a), \quad i = 1, \ldots, k,$$

then the first assertion would render that

$$n = p_1^{a_1} \cdots p_k^{a_k} \mid \sum_{d \mid n} \varphi(d) a^{n/d}.$$

Therefore, we are remained to show $p^n \mid x_{p^n}(a)$ for each prime p and $a \in \mathbb{Z}$. This is given as follows:

$$\begin{aligned} x_{p^n}(a) &= \sum_{d \mid p^n} \varphi(d) a^{p^n/d} = \sum_{k=0}^{n} \varphi(p^k) a^{p^{n-k}} = \sum_{k=0}^{n} (p-1) p^{k-1} a^{p^{n-k}} \\ &= a^{p^n} - a^{p^{n-1}} + p(a^{p^{n-1}} + (p-1) a^{p^{n-2}} + \cdots + p^{n-2}(p-1)a \\ &= a^{p^n} - a^{p^{n-1}} + p x_{p^{n-1}}(a). \end{aligned}$$

This suggests us to induct on n. When $n = 1$,

$$x_p(a) = a^p + (p-1)a = a^p + pa - a \equiv a^p - a \equiv 0 \bmod p$$

by Fermat's little theorem. Suppose $p^{n-1} \mid x_{p^{n-1}}(a)$. Our goal is to show

$$x_{p^n}(a) \equiv a^{p^n} - a^{p^{n-1}} \equiv 0 \bmod p^n.$$

If $p \mid a$ this is clear. Suppose $p \nmid a$ and then by Euler's theorem,

$$a^{\varphi(p^n)} = a^{(p-1)p^{n-1}} = a^{p^n - p^{n-1}} \equiv 1 \bmod p^n.$$

This implies $a^{p^n} - a^{p^{n-1}} \equiv 0 \bmod p^n$ by multiplying $a^{p^{n-1}}$ on both sides. So we finally accomplish the proof. □

Exercise 8. Using the argument that is similar to the proof of Problem 7, show that for any positive integer n as well as any $a \in \mathbb{Z}$,

$$n \mid \sum_{i=1}^{n} a^{\gcd(i,n)}.$$

Problem 9. *Let $n > 1$ be an odd integer. Let $a_1, a_2, \ldots, a_{\varphi(n)}$ be all positive integers among $1, 2, \ldots, n$ that are relatively prime to n. Prove that*

$$\left| \prod_{k=1}^{\varphi(n)} \cos \frac{a_k \pi}{n} \right| = \frac{1}{2^{\varphi(n)}}.$$

Proof. Denote that

$$A = \left| \prod_{k=1}^{\varphi(n)} \cos \frac{a_k \pi}{n} \right|, \quad B = \left| \prod_{k=1}^{\varphi(n)} \sin \frac{a_k \pi}{n} \right|.$$

Then we compute directly for

$$2^{\varphi(n)} AB = \left| \prod_{k=1}^{\varphi(n)} 2 \sin \frac{a_k \pi}{n} \cos \frac{a_k \pi}{n} \right| = \left| \prod_{k=1}^{\varphi(n)} \sin \frac{2 a_k \pi}{n} \right|.$$

Since $2 \nmid n$, and $\{a_1, \ldots, a_{\varphi(n)}\}$ is a reduced residue system modulo n, so also is $\{2a_1, \ldots, 2a_{\varphi(n)}\}$. It follows that

$$\left|\prod_{k=1}^{\varphi(n)} \sin \frac{2a_k\pi}{n}\right| = \left|\prod_{k=1}^{\varphi(n)} \sin \frac{a_k\pi}{n}\right| = B.$$

To check the identity above, note that

$$\frac{a_k\pi}{n} = m\pi + \frac{r}{n}\pi \implies \left|\sin \frac{a_k\pi}{n}\right| = \left|\sin \frac{r\pi}{n}\right|.$$

This completes the proof that $2^{\varphi(n)}A = 1$. □

School of Mathematical Sciences, Peking University, 100871, Beijing, China
Email address: daiwenhan@pku.edu.cn