Ratio Mathematica Volume 37, 2019, pp. 39-48

Solving some specific tasks by Euler's and Fermat's Little theorem

Viliam Ďuriš*

Abstract

Euler's and Fermat's Little theorems have a great use in number theory. Euler's theorem is currently widely used in computer science and cryptography, as one of the current encryption methods is an exponential cipher based on the knowledge of number theory, including the use of Euler's theorem. Therefore, knowing the theorem well and using it in specific mathematical applications is important. The aim of our paper is to show the validity of Euler's theorem by means of linear congruences and to present several specific tasks which are suitable to be solved using Euler's or Fermat's Little theorems and on which the principle of these theorems can be learned. Some tasks combine various knowledge from the field of number theory, and are specific by the fact that the inclusion of Euler's or Fermat's Little theorems to solve the task is not immediately apparent from their assignment.

Keywords: Euler's theorem, coding, Fermat's Little theorem, linearcongruences, cryptology, primality testing, Matlab

2010 AMS subject classification: 11A07, 14G50†

* Department of Mathematics, Faculty of Natural Sciences Constantine the Philosopher University in Nitra, Tr. A. Hlinku 1, 949 74 Nitra, Slovakia; vduris@ukf.sk.

†Received on December 1st, 2019. Accepted on December 10th, 2019. Published on December 31th, 2019. doi: 10.23755/rm.v37i0.485. ISSN: 1592-7415. eISSN: 2282-8214.

1 Introduction

At present, mathematics provides apparatus for virtually all modern coding systems. The first coding system, with only two symbols - a dot and a comma, was Morse code which was used to send the first coding message by American inventor Samuel F. B. Morse in 1844 using an electric telegraph. Binary code encoding has become a better code for message encryption at a later time, in which each coded word consists of blocks of ones and zeroes, and this encoding is still used today [1]. Significant developments in coding occurred in the 20th century when Euler's theorem was used for coding and the coded text could be broadcasted publicly with the message kept secret. The principle of this coding is that the sender assigns a number to a coded word (e.g. 74) and encodes that word using two additional numbers (e.g. 247 and 5), which may be public in such a way that $74^5 (\mathrm{mod}\, 247) = 120$ is calculated. This will give you a message "120" that will be sent to the recipient. Since numbers 247 and 5 are public keys, anyone can encode the message "74" to "120", but only the actual recipient can decode it correctly. The essence of the key to the cipher lies in the fact that only the recipient knows that number 247 was compiled as the product of primes $p = 13$ and $q = 19$ and using Euler's theorem searches for the value x for which the congruence is $5x \equiv 1(\mathrm{mod}\, [(p-1)(q-1)])$. The recipient can easily get the result $x = 173$. Using this figure, the remainder by dividing 120^{173} by number 247 is found, thereby obtaining the original coded word 74 which can already be assigned to the message [2]. In practice, with this type of coding, the product of two very large primes is used, where the decomposition of the thus obtained number is very difficult, virtually impossible for someone who does not know the product of which two primes have been executed. Despite the fact that the principle of this coding was discovered and started to be used practically in the 20th century, it is actually derived from Euler's knowledge from the 18th century.

Most of the results in mathematics in the 18th century stemmed from efforts to solve various separate problems discovered in the 17th century. In this period, the theory of numbers remained more or less in the background, and the only mathematician who dealt with the issues of number theory after 1730 to a greater extent was Euler. In 1736, he proved Fermat's Little theorem which claims that for any natural number a and prime p, $a^{p-1} \equiv 1(\mathrm{mod}\, p)$. Later in 1760, after the introduction of Euler's totient function $\varphi(n)$ he demonstrated the validity of congruence $a^{\varphi(m)} \equiv 1(\mathrm{mod}\, m)$ which is a generalization of Fermat's Little theorem. Euler also dealt with many other Fermat's claims. He also achieved several accomplishments related to the decomposition of certain expressions with the powers of natural numbers and to perfect and friendly numbers. He was also interested in the problem of integer roots of Pell's equation, about which he published several articles, and presented his own

method of solution. Euler has introduced a number of concepts into number theory, such as the quadratic residue and the quadratic nonresidue in the law of quadratic reciprocity and his work and accomplishments, despite the lack of exact evidence in several areas, were generally accepted by respected mathematicians of the 18th and 19th centuries (e.g. Gauss or Legendre) [3]. We would like to mention there's also another principle of coding using Fibonacci numbers and can be seen in [4].

2 Euler's theorem, Fermat's Little theorem

Let us consider two natural numbers *a, m* where $(a, m) = 1$. Euler's theorem [5] then states that $m|a^{\varphi(m)} - 1$, or that congruence $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$ applies. The symbol $\varphi(n)$ denotes the number of natural numbers smaller than *n* and relatively prime to *n* and is called *Euler's totient function* [6].

To show the validity of Euler's theorem, we will use the basic properties of congruences and residue classes. Let's write all relatively prime numbers to m less than m. These are $x_1, x_2, \cdots, x_{\varphi(m)}$. Let us further consider the sequence $ax_1, ax_2, \cdots, ax_{\varphi(m)}$ and indirectly show that all its members are relatively prime to m. If $\exists i: (ax_i, m) = d > 1$, then $d|ax_i \wedge d|m$. Then $(d, a) = 1$, because $(a, m) = 1 \wedge d|m$. In that $d|x_i$ and numbers m, x_i are commensurable which is a controversy.

Furthermore, let us indirectly show that numbers $ax_1, ax_2, \cdots, ax_{\varphi(m)}$ are non-congruent modulo m. $\exists i, j: ax_i \equiv ax_j (\mathrm{mod}\, m)$. Then $m|ax_i - ax_j = a(x_i - x_j) \wedge (a, m) = 1$, of which $m|x_i - x_j$ and then $x_i \equiv x_j (\mathrm{mod}\, m)$, which is a controversy, because x_i are differently lower from each other than m, and therefore cannot give the same remainder after division by m.

Before completing the evidence, we recall, that based on the basic properties of congruences, [7] we know that integers a and b belong to the same class R_i modulo m just when $a \equiv b \ (\mathrm{mod}\, m)$. If we first express the numbers $a, b \in R_i$ in the form $a = m \cdot q + i, b = m \cdot p + i$, then $a - b = m(q - p)$, which means $m|a - b$, and thus $a \equiv b (\mathrm{mod}\, m)$. On the other hand, let us assume that $a \equiv b \ (\mathrm{mod}\, m)$ and $a = mq + i, b = mp + j \ (0 \leq i, j < m)$. For example, it is supposed that $i > j$. Since $a \equiv b \ (\mathrm{mod}\, m)$, $m|a - b$. But then $m \nmid (a - b) = [m(q - p) + (i - j)]$, of which $m \nmid (i - j)$. This would be a controversy though, because $0 < i - j < m$. Similarly, a controversy arises even with the assumption $i < j$. Therefore $i = j$ must hold, hence the numbers a and b belong to the same residual class modulo m with $a \equiv b \ (\mathrm{mod}\, m)$.

As the class representative does not matter, we can write $ax_1 \cdot ax_2 \cdot \cdots \cdot ax_{\varphi(m)} \equiv x_1 \cdot x_2 \cdot \cdots \cdot x_{\varphi(m)} (\mathrm{mod}\, m)$. Then $m|ax_1 \cdot ax_2 \cdot \cdots \cdot ax_{\varphi(m)} - x_1 \cdot$

$x_2 \cdot \cdots \cdot x_{\varphi(m)} = \left(a^{\varphi(m)} - 1\right) x_1 \cdot x_2 \cdot \cdots \cdot x_{\varphi(m)}$. Since $\left(m, x_1 \cdot x_2 \cdot \cdots \cdot x_{\varphi(m)}\right) = 1$, then $m | a^{\varphi(m)} - 1$.

If m is a prime number and $p \nmid a$, then $\varphi^{(m)} = m - 1$ and we get *Fermat's Little theorem* $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$ directly from Euler's theorem. A variation of Fermat's Little theorem can be used to test primality [8]. If there exists $a \in \{2, \cdots, n-1\}$, $n > 3$, where $a^{n-1} \not\equiv 1 (\mathrm{mod}\, n)$, then *n* is a composite number and we call it *Fermat's witness for the compositeness of number n* [9].

Fermat's primality test can be suitably algorithmically presented in a selected computational environment (e.g. Matlab). The algorithm consists of two steps:

a) we randomly select number *a* for which $1 < a < n$
b) it is tested whether congruence $a^{n-1} \equiv 1 (\mathrm{mod}\, n)$ is satisfied

If congruence $a^{n-1} \equiv 1 (\mathrm{mod}\, n)$ is satisfied, the number n may or may not be a prime number. If congruence is not satisfied, the number n is not a prime and number a is the Fermat's witness for the compositeness of n.

Fermat's primality test works well for numbers that are not products of prime numbers different from each other. It can be demonstrated that if we test the number n, which is not the product of different prime numbers, hence there is such a prime p where $p^2 | n$, then with a probability of at least 75% we can choose between numbers $2, \cdots, n-1$ such a number which will be the Fermat's witness for the compositeness of n [9].

First, in Matlab, we create a function that helps us test congruence $a^{n-1} \equiv 1 (\mathrm{mod}\, n)$ generally for two given numbers a and n. The function will calculate the value $a^{n-1} \bmod n$ which we will compare with 1 within the residue classes.

```
function res = test_congruence(a, n)

expn = n - 1;
res = 1;

while expn ~= 0
  if rem(expn, 2) == 1
    res = rem(res * a, n);
  end
  expn = floor(expn / 2);
  a = rem(a^2, n);
end
```

The second function randomly generates $a \in \{2, \cdots, n-1\}$ and we look for the Fermat's witness for the compositeness of n.

```
function test_fermat(n, cnt)

fo = false;
ii = 1;
while (ii <= cnt) && (~fo)
  a = 1 + unique(ceil((n - 2) * rand(1, 1)));
  tc = test_congruence(a, n);
  if(tc ~= 1)
    fermat_witness = a;
    fo = true;
  else
    ii = ii + 1;
  end
end

if fo
  disp(['Number ' num2str(n) ' is a composite
        number.']);
  disp(['Number ' num2str(fermat_witness) ' is a
        Witness for the compositeness of '
        num2str(n) '.']);
else
  disp(['Number ' num2str(n) ' can be a prime or a
        composite number.']);
end
```

The created test function is activated through the command line for any number n.

```
>> test_fermat(223, 1)
Number 223 can be a prime or a composite number.

>> test_fermat(273, 1)
Number 273 is a composite number.
Number 220 is a Witness for the compositeness of
273.
```

3 Euler's, Fermat's Little theorem applications

In this section, we have selected and compiled a number of specific tasks [10], [11] that guide on how to solve certain types of tasks using Euler's or Fermat's

Little theorem. We remark that for a natural number n greater than 1 in canonical decomposition $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ it holds that

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_k}\right) \text{ [6]}$$

Example 3.1. First, we demonstrate that if we divide number 17^{24} by number 39, the remainder 1 is obtained.

Solution. It is determined that $a = 17,\ m = 39.\ (39,17) = 1$ and Euler's theorem can be applied. Let us calculate $\varphi(m) = \varphi(39) = 39\left(1-\frac{1}{3}\right)\left(1-\frac{1}{13}\right) = 24$. Then according to Euler's theorem $39|17^{24}-1$, thus $\exists k \in \mathbb{Z}: 17^{24}-1 = 39k$. Then we can write $17^{24} = 39k+1$, and 1 is obtained as a remainder.

Example 3.2. It is demonstrated that p and $8p^2+1$ are simultaneously prime just when $p = 3$.

Solution. 1. First, $p = 3$. Then $8p^2+1 = 8\cdot 9+1 = 73$, which is a prime.
2. Now let p and $8p^2+1$ be prime numbers simultaneously. $8p^2+1$ is adjusted as $8p^2+1 = 8p^2-8+9 = 8(p^2-1)+9$. Let p be a prime number other than 3. Then $(p,3) = 1$ a $3|p^{\varphi(3)}-1 = p^2-1$. Since $3|p^2-1$, then $8(p^2-1) \wedge 3|9$, then $3|8(p^2-1)+9 = 8p^2+1$ and $8p^2+1$ would not be a prime number, which is a controversy, thus $p = 3$.

Example 3.3. We show if a is not divisible by 5, then only one number from a^2-1, a^2+1 is divisible by 5.

Solution. If a is a multiple of 5, according to Euler's theorem a^4-1 is a multiple of 5. Then only one of numbers a^2-1 and a^2+1 is a multiple of 5. They both concurrently cannot be, otherwise their difference would also be divisible by number 5, which is not, since $(a^2+1)-(a^2-1) = 2$.

Example 3.4. We find all primes p for which $5^{p^2}+1 \equiv 0(mod\ p^2)$.

Solution. The prime number $p = 5$ does not satisfy the task and at the same time $(p,5) = 1$. Then according to Euler's theorem $5^{p-1} \equiv 1 \pmod p$. By exponentiation to $p+1$ we get $5^{p^2-1} \equiv 1 \pmod p$, of which $5^{p^2} \equiv 5 \pmod p$.
Next, the task assignment states that $5^{p^2}+1 \equiv 0 \pmod{p^2}$, that implies $5^{p^2} \equiv -1 \pmod{p^2}$ and also $5^{p^2} \equiv -1 \pmod p$. Then congruences $5^{p^2} \equiv$

$5 \pmod p$ and $5^{p^2} \equiv -1 \pmod p$ hold that $5 \equiv -1 \pmod p$. Then $p|6$. In that $p = 2$ or $p = 3$. For $p = 2$ it holds that $5^4 + 1 \equiv 1^4 + 1 = 2 \not\equiv 0 \pmod 4$. For $p = 3$ it holds that $5^9 + 1 = 5^6 \cdot 5^3 + 1 \equiv 5^3 + 1 = 126 \equiv 0 \pmod 9$. Then, the only prime number satisfying the task is $p = 3$.

Example 3.5. For the odd number $m > 1$ we find the remainder after division of $2^{\varphi(m)-1}$ by number m.

Solution. Euler's theorem implies that $2^{\varphi(m)} \equiv 1 \equiv 1 + m = 2 \cdot \frac{1+m}{2} = 2r \pmod m$ where r is a natural number $0 \leq r < m$.
The basic properties of congruences [7] determine that if $a \equiv b \pmod m$ and d is an integer with properties $d|a,\ d|b,\ (d,m) = 1$, then $\frac{a}{d} \equiv \frac{b}{d} \pmod m$. Indeed $a = a_1 d$, $b = b_1 d$ and according to assumption $m|(a - b)$, it holds that $m|d(a_1 - b_1)$. Since $(d,m) = 1$, it holds that $m|(a_1 - b_1)$. Then $a_1 \equiv b_1 \pmod m$, thus $\frac{a}{d} \equiv \frac{b}{d} \pmod m$.
Then, however, we can divide both sides of the congruence $2^{\varphi(m)} \equiv 2r \pmod m$ by their common divisor, number 2, which is relatively prime to the modulo. Then $2^{\varphi(m)-1} \equiv r \pmod m$, and thus the remainder sought is $r = \frac{1+m}{2}$.

Example 3.6. We find the last two digits of number 137^{42}.

Solution. The task leads to the search for the remainder when dividing number 137^{42} by number 100. Since $(137{,}100) = 1$, according to Euler's theorem it holds that $137^{\varphi(100)} - 1$ is a multiply of 100 $(100|137^{\varphi(100)} - 1)$. Next $\varphi(100) = 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 40$. Then $137^{40} - 1$ is a multiply of 100.
Therefore $137^{42} = 137^2 137^{40} - 137^2 + 137^2 = 137^2(137^{40} - 1) + +137^2 = 137^2(137^{40} - 1) + (100 + 37)^2 = 100k + (100 + 37)^2$.
Next, we use the formula $(a + b)^2 = a^2 + 2ab + b^2$. Then $137^{42} = 100k + 100l + 37^2 = 100n + 1369 = 100n + 1300 + 69 = 100m + 69$. Thus, the remainder sought is 69.

Example 3.7. We find the last 2 digits of number $a = 137^{47}$.

Solution. The last 2 digits of number *a* are again obtained as the remainder after dividing the number a by 100. $(100{,}137) = 1$ and Euler's theorem can be applied. Then $100|137^{\varphi(100)} - 1$, thus $100|137^{40} - 1$. Then $137^{40} - 1$ is a multiply of 100 and $137^{40} = 100k + 1$.

Let us calculate $137^{47} = 137^{40} \cdot 137^7 = (100k + 1) \cdot 137^7 = 100k \cdot 137^7 + 137^7$ Number $100k \cdot 137^7$ cannot specify last 2 digits (ending with 2 zeroes), and so just number 137^7 has the last 2 digits of the given number a. Next, the binomial theorem is applied.
$137^7 = (130 + 7)^7 = \binom{7}{0}130^7 + \binom{7}{1}130^6 \cdot 7 + \cdots + \binom{7}{6}130 \cdot 7^6 + \binom{7}{7}7^7$. In this summation only the members $\binom{7}{6}130 \cdot 7^6$ a $\binom{7}{7}7^7$ decide the last two digits (other contribute zeroes in last two digits).
Their summation is calculated as $\binom{7}{6}130 \cdot 7^6 + \binom{7}{7}7^7 = 130 \cdot 7^7 + 7^7 = 131 \cdot 7^7 = 107884133$. Overall, we get the last 2 digits of the number $a = 137^{47}$ which are 33.

Example 3.8. We find the remainder when dividing $(85^{70} + 19^{32})^{16}$ by number 21.

Solution. According to the binomial theorem $85^{70} = (84 + 1)^{70} = \binom{70}{0}84^{70} + +\binom{70}{1}84^{69} \cdot 1 + \cdots + \binom{70}{69}84 \cdot 1^{69} + \binom{70}{70}1^{70}$. We see that number 21 can be removed from every member except the last one. Then $85^{70} = (84 + 1)^{70} = 21n + 1$.
Because $\varphi(21) = 12$, $19^{12} - 1$ is a multiply of 21 (applying Euler's theorem), then $19^{32} = 19^8(19^{24} - 1) + 19^8 = 21m + 19^8$. Therefore $(85^{70} + 19^{32})^{16} = (21n + 1 + 21m + 19^8)^{16} = (21k + 1 + (21 - 2)^8)^{16} = (21q + 1 + 2^8)^{16} = (21r + 5)^{16} = 21t + 5^{16} = 21t + 5^4(5^{12} - 1) + 5^4 = 21t + 21r + 625 = 21u + 16$. The remainder sought is 16.

Example 3.9. We demonstrate if $x^p + y^p = z^p$ where p is a prime number, then $x + y - z$ is a multiply of p.

Solution. According to Fermat's Little theorem, if p is a prime and $p \nmid x$, then $x^{p-1} \equiv 1 (\mathrm{mod}\, p)$, that means $p|x^{p-1} - 1$ and thus $p|x(x^{p-1} - 1) = x^p - x$. Similarly, $p|y^p - y$, $p|z^p - z$. Therefore we can write $x^p = pt_1 + x$, $y^p = pt_2 + y$ a $z^p = pt_3 + z$. If we substitute in the equation $x^p + y^p = z^p$, we get $p(t_3 - t_1 - t_2) = x + y - z$ after adjustment, thus $x + y - z$ is a multiply of p.

These examples are the basis for understanding the principle of working with large numbers using congruences through Euler's and Fermat's Little theorem. Congruences are a modern and irreplaceable security tool for protecting data by a public key. It is important to realize that the public key uses such large numbers for which there is no effective method of decomposing to primes even in today's modern computer age. That is why Euler's theorem plays its role in encryption even today, when encryption uses keys of up to 256 bits in length

and deciphering the word while trying out all the options would probably take more years than the age of the universe is.

4 Conclusion

The paper points out some specific applications suitable for presenting and understanding the basic principle of Euler's and Fermat's Little theorems which are currently used in cryptography. Leonhard Paul Euler was such a great mathematician that many of the principles he had known almost 300 years ago were actually used by contemporary society. Euler, nicknamed as a "magician" in his time, had a great influence not only on number theory, but also on mathematical analysis or graph theory. He introduced many mathematical symbols such as the letter sigma Σ to denote the sum, or introduced numbers such as e and i, whereas e is probably the most important number of the whole mathematics [12] and occurs in various areas. When Mathematical Intelligencer in 2004 asked readers to vote for "the most beautiful theorem of mathematics", Euler's Identity $e^{i\pi} + 1 = 0$ won by a large margin [13]. It is a formula that connects the five most important symbols of mathematics. Several mathematicians have marked this equation as so mystical that it can only be reproduced and its consequences continually explored. In addition to Euler's theorem itself and its evidence by means of linear congruences, we also wanted to highlight the work and the "size" of Leonhard Euler and his key contribution to number theory.

References

[1] Bose R. (2008). *Information Theory, Coding and Cryptography*. New Delhi, India: McGraw-Hill Publishing Company Limited, ISBN: 9780070669017.

[2] Crilly T. (2007). *50 Mathematical Ideas You Really Need to Know*. London: Quercus Publishing Plc, ISBN: 9781847240088.

[3] Čižmár J. (2017). *Dejiny matematiky – od najstarších čias po súčasnosť*. Bratislava, Slovak Republic: PERFECT, ISBN: 9788080468293.

[4] Ďuriš V. et al. (2019). *Fibonacci Numbers and Selected Practical Applications in the Matlab Computing Environment*. In: Acta Mathematica Nitriensia, ISSN 2453-6083, Vol. 5, No. 1, p. 14-22, DOI 10.17846/AMN.2019.5.1.14-22.

[5] Koshy T. (2001). *Elementary Number Theory with Applications*. USA: Academic Press, 1st ed., ISBN: 9780124211711.

[6] Znám Š. (1975). *Teória čísel*. Bratislava, Slovak Republic: SPN.

[7] Jones G. A., Jones J. M. (1998). *Elementary Number Theory*. London: Springer, London, ISBN: 9783540761976.

[8] Riesel H. (1994). *Prime numbers and computer methods for factorisation*. 2nd ed., Progress in Mathematics 126, Birkhauser.

[9] Pommersheim J. E., Marks T. K., Flapan E. L. (2010). *Number theory*. USA: Wiley, 753 p., ISBN 978-0-470-42413-1.

[10] Davydov U. S., Znám Š. (1972). *Teória čísel – základné pojmy a zbierka úloh*. Bratislava, Slovak Republic: SPN.

[11] Apfelbeck A. (1968). *Kongruence*. Prague, Czech Republic: Mladá fronta.

[12] Clifford A. P. (2011). *The Math Book: From Pythagoras to the 57th Dimension, 250 Milestones in the History of Mathematics*. New York, NY: Sterling Publishing, ISBN: 9781402757969.

[13] Jackson T. (2017). *Mathematics: An Illustrated History of Numbers (Ponderables: 100 Breakthroughs that Changed History) Revised and Updated Edition*. New York, NY: Shelter Harbor Press, ISBN: 9781627950954.