

EULER'S THEOREM

KEITH CONRAD

1. INTRODUCTION

Fermat's little theorem is an important property of integers to a prime modulus.

Theorem 1.1 (Fermat). *For prime p and any $a \in \mathbf{Z}$ such that $a \not\equiv 0 \pmod{p}$,*

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

If we want to extend Fermat's little theorem to a composite modulus, a false generalization would be: if $a \not\equiv 0 \pmod{m}$ then $a^{m-1} \equiv 1 \pmod{m}$. For a counterexample, take $m = 15$ and $a = 2$: $2^{14} \equiv 4 \not\equiv 1 \pmod{15}$.

A correct extension of Fermat's little theorem to non-prime moduli requires a new way of thinking about the hypothesis in Fermat's little theorem. For prime p ,

$$a \not\equiv 0 \pmod{p} \iff (a, p) = 1,$$

but these two conditions are not equivalent when p is replaced with a composite number. It is the relative primality point of view on the right that lets Fermat's little theorem be extended to a general modulus, as Euler discovered.

Theorem 1.2 (Euler). *For $m \geq 2$ in \mathbf{Z}^+ and any $a \in \mathbf{Z}$ such that $(a, m) = 1$,*

$$a^{\varphi(m)} \equiv 1 \pmod{m},$$

where $\varphi(m)$ is the number of invertible integers modulo m .

When $m = p$ is prime, all non-zero integers modulo p are invertible, so $\varphi(p) = p - 1$ and Euler's theorem becomes Fermat's little theorem.

How do we compute $\varphi(m)$? Consider $m = 12$. To count the number of invertible integers modulo 12, write down a set of representatives for integers modulo 12, such as

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12.$$

The numbers here that are invertible modulo 12 are 1, 5, 7, 11, so $\varphi(12) = 4$. Euler's theorem for $m = 12$ says $a^4 \equiv 1 \pmod{12}$ when $(a, 12) = 1$.

Being invertible modulo m is the same as being relatively prime to m (that is, we can solve $ax \equiv 1 \pmod{m}$ for x exactly when $(a, m) = 1$ — use Bezout), so we can describe $\varphi(m)$ concretely as follows:

$$\varphi(m) = \#\{a : 1 \leq a \leq m, (a, m) = 1\}.$$

Here is a small table of values derived from this formula.

m	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$\varphi(m)$	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16

Notice $\varphi(m)$ is even for $m > 2$. We can explain this by observing that when $a \bmod m$ is invertible, so is $-a \bmod m$. Therefore, using the standard representatives modulo m , invertible numbers modulo m come in *pairs* as $\{a, m - a\}$. This really is a pair of different numbers, since if $a = m - a$ then $a = m/2$, so m is even. But $(m/2, m) = m/2$, and this is bigger than 1 when $m > 2$, so $m/2$ is not invertible modulo m . Thus, when $m > 2$, the *invertible* numbers modulo m fall into pairs $\{a, m - a\}$, and that shows $\varphi(m)$ is even.

2. FROM FERMAT TO EULER

Euler's theorem has a proof that is quite similar to the proof of Fermat's little theorem. To stress the similarity, we review the proof of Fermat's little theorem and then we will make a couple of changes in that proof to get Euler's theorem.

Here is the proof of Fermat's little theorem (Theorem 1.1).

Proof. We have a prime p and an arbitrary $a \not\equiv 0 \bmod p$. To show $a^{p-1} \equiv 1 \bmod p$, consider non-zero integers modulo p in the standard range:

$$S = \{1, 2, 3, \dots, p-1\}.$$

We will compare S with the set obtained by multiplying the elements of S by a :

$$aS = \{a, a \cdot 2, a \cdot 3, \dots, a(p-1)\}.$$

The elements of S represent the nonzero numbers modulo p and the elements of aS *also* represent the nonzero numbers modulo p . That is, every nonzero number mod p is congruent to exactly one number in aS . Indeed, for any $b \not\equiv 0 \bmod p$, we can solve the equation $ax \equiv b \bmod p$ for $x \bmod p$ since $a \bmod p$ is invertible, and necessarily $x \not\equiv 0 \bmod p$ (since $b \not\equiv 0 \bmod p$). Choosing x to lie between 1 and $p-1$, so $x \in S$, we see that $b \bmod p$ is represented by an element of aS . Two different elements of aS can't represent the same number mod p since $ax \equiv ay \bmod p \implies x \equiv y \bmod p$ and different elements of S are not congruent mod p .

Since S and aS become the same thing when reduced modulo p , the product of the numbers in each set must be the same modulo p :

$$1 \cdot 2 \cdot 3 \cdots (p-1) \equiv a(a \cdot 2)(a \cdot 3) \cdots (a(p-1)) \bmod p.$$

Pulling the $p-1$ copies of a to the front of the product on the right, we get

$$1 \cdot 2 \cdot 3 \cdots (p-1) \equiv a^{p-1}(1 \cdot 2 \cdot 3 \cdots (p-1)) \bmod p.$$

Now we cancel each of $1, 2, 3, \dots, p-1$ on both sides (since they are all invertible modulo p) and we are left with $1 \equiv a^{p-1} \bmod p$. \square

The proof of Euler's theorem is pretty similar to this, except we replace the condition "non-zero modulo p " with "relatively prime to m ."

Proof. We have a positive integer m and an a such that $(a, m) = 1$. To show $a^{\varphi(m)} \equiv 1 \bmod m$, consider the units modulo m in the standard range:

$$S = \{u_1, u_2, u_3, \dots, u_{\varphi(m)}\},$$

where $1 \leq u_i \leq m-1$, $(u_i, m) = 1$, and the u_i 's are distinct. (If $m = p$ is prime we can use $u_i = i$ for all i , but in general there isn't a simple formula for the i th unit modulo m .)

We will compare S with the set obtained by multiplying the elements of S by a :

$$aS = \{au_1, au_2, au_3, \dots, au_{\varphi(m)}\}.$$

Since $(a, m) = 1$, $a \bmod m$ is a unit and therefore aS consists of units modulo m . We will show that aS represents all the units modulo m . Given any unit $b \bmod m$, the congruence $ax \equiv b \bmod m$ is solvable since $a \bmod m$ is invertible. The solution x is a unit modulo m (why?), and placing x between 1 and $m - 1$ makes ax a member of aS . Thus $b \bmod m$ is represented by an element of aS . If $ax \equiv ay \bmod m$ then $x \equiv y \bmod m$ since $a \bmod m$ is invertible, so the different elements of S remain different mod m after being multiplied by a . Therefore aS is a set of representatives for the units modulo m (no duplicates).

Since the members of S and aS agree modulo m , the product of the numbers in each set must be the same modulo m :

$$u_1 u_2 u_3 \cdots u_{\varphi(m)} \equiv (au_1)(au_2)(au_3) \cdots (au_{\varphi(m)}) \bmod m.$$

Pulling the $\varphi(m)$ copies of a to the front of the product on the right, we get

$$u_1 u_2 u_3 \cdots u_{\varphi(m)} \equiv a^{\varphi(m)} u_1 u_2 u_3 \cdots u_{\varphi(m)} \bmod m.$$

Now we cancel each u_i on both sides (since they are all invertible modulo m) and we are left with $1 \equiv a^{\varphi(m)} \bmod m$. \square

Passing from Fermat's little theorem to Euler's theorem amounted to replacing non-zero numbers modulo a prime p with the invertible numbers (*not* the non-zero numbers) for a general modulus m . There is a common notation for these numbers in elementary number theory courses:¹

$$U_m = \{a \bmod m : (a, m) = 1\}.$$

The notation U_m comes from the fact that invertible numbers mod m are called *units* mod m .

Example 2.1. We have $U_5 = \{1, 2, 3, 4\}$ and $U_{18} = \{1, 5, 7, 11, 13, 17\}$.

When p is prime, $U_p = \{1, 2, 3, \dots, p-1\}$. As a check that you understand this new notation, be sure you understand why $\varphi(m) = \#U_m$.

3. COMPUTING $\varphi(m)$ IN SPECIAL CASES

The function $\varphi(m)$ does not vary in a simple manner from one integer to the next. See the table of values near the end of Section 1. This is typical of functions arising in number theory that are based on divisibility (or lack thereof). The right way to think about $\varphi(m)$ is by thinking about positive integers not in terms of the usual $m \rightarrow m+1$ paradigm, but in terms of the progression

primes \rightarrow prime powers \rightarrow general case.

This progression is how the integers are best arranged from the viewpoint of divisibility: primes are the building blocks for multiplication (rather than 1 being the building block for addition), then come prime powers, and finally we get any positive integer as a product of prime powers. With this in mind, we can get formulas for $\varphi(m)$ directly from its definition in the first two cases of the above progression:

- $\varphi(p) = p - 1$ since there are $p - 1$ integers from 1 to p that are relatively prime to p .
- $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$ for prime p and $k \geq 1$ since among the integers from 1 to p^k , those that are *not* relatively prime to p^k are the multiples of p : $p, 2p, 3p, \dots, p^k$. There are p^{k-1} such numbers, so we subtract this from p^k to compute $\varphi(p^k) = p^k - p^{k-1}$.

¹Many mathematicians write $(\mathbf{Z}/(m))^{\times}$ for U_m .

Make sure you remember this explanation for why $\varphi(p^k) = p^k - p^{k-1}$.

What about $\varphi(m)$ when m is composite? We will treat *one* case here, which is important in elementary cryptography: $m = pq$ is a product of two different primes. If $1 \leq a \leq pq$ and $(a, pq) = 1$, then a is neither a multiple of p nor a multiple of q . The multiples of p in this range are $p, 2p, \dots, qp$ and the multiples of q in this range are $q, 2q, \dots, pq$. There are q numbers in the first case and p numbers in the second case. The two lists only overlap at pq (indeed, a positive integer divisible by p and q is divisible by pq , so can't be less than pq). Therefore, to compute $\varphi(pq)$, we take away from pq the number of terms in both lists without double-counting the common term:

$$\varphi(pq) = pq - p - q + 1 = p(q - 1) - (q - 1) = (p - 1)(q - 1).$$

This is interesting: $\varphi(pq) = \varphi(p)\varphi(q)$ for different primes p and q . (Warning: this formula is false when $p = q$: $\varphi(p^2) = p^2 - p = p(p - 1)$ rather than $(p - 1)^2$.)

With these formulas, we can make Euler's theorem more explicit for certain moduli.

Example 3.1. When p is prime,

$$(a, p^2) = 1 \implies a^{p(p-1)} \equiv 1 \pmod{p^2}.$$

Example 3.2. When p and q are different primes,

$$(a, pq) = 1 \implies a^{(p-1)(q-1)} \equiv 1 \pmod{pq}.$$

This example with modulus pq is crucial for the RSA cryptosystem.

Remark 3.3. Euler's theorem is not the only generalization of Fermat's little theorem to composite moduli. To see another one, write the congruence in Fermat's little theorem as

$$(3.1) \quad a^p \equiv a \pmod{p}.$$

For $a \not\equiv 0 \pmod{p}$, dividing by a shows this is the same as $a^{p-1} \equiv 1 \pmod{p}$, which is the usual form of Fermat's little theorem. The "advantage" of writing it as $a^p \equiv a \pmod{p}$ is that now the congruence holds for all a without exception. There is a congruence generalizing (3.1) to composite moduli that works for all a without exceptions and looks very different from Euler's theorem. Here it is:

$$(3.2) \quad \sum_{k=0}^{m-1} a^{(k,m)} \equiv 0 \pmod{m}$$

for all $a \in \mathbf{Z}$. When $m = p$ is prime, this becomes $a^p + (p - 1)a \equiv 0 \pmod{p}$, which is the same as $a^p - a \equiv 0 \pmod{p}$ since the $pa \pmod{p}$ term is 0 no matter what a is. So we have recovered (3.1) as a special case. When $m = pq$ with distinct primes p and q , (3.2) says

$$a^{pq} + (q - 1)a^p + (p - 1)a^q + (p - 1)(q - 1)a \equiv 0 \pmod{pq}.$$

for all $a \in \mathbf{Z}$. That's quite different from Euler's congruence mod pq in Example 3.2! For yet another generalization of Fermat's little theorem to all moduli, see [1] or [2].

4. APPLICATION: PERIODIC DECIMAL EXPANSIONS

With a calculator we can see that various fractions have periodic decimal expansions, e.g., $3/7 = .428571428571\dots$ has a repeating block of length 6. Which numbers have periodic expansions? And is anything predictable about the period length? To answer these questions, we start by working in reverse. Let's write down a periodic expansion and try to see what kind of number it turns out to be. For simplicity, we focus on *purely periodic*

decimals, meaning those with a repeating block right at the start (like $3/7$ above and unlike $19/55 = .345454545\dots$, which has the initial 3 that is not repeated).

If $x = .\overline{c_1c_2\dots c_d}$ is a purely periodic decimal, where the periodic block we wrote down has length d , each c_i is repeated every d digits as we move through the decimal expansion of x . For instance, c_1 occurs in positions for 10^{-1} , $10^{-(d+1)}$, $10^{-(2d+1)}$, and so on. The digit c_2 occurs in positions 10^{-2} , $10^{-(d+2)}$, $10^{-(2d+2)}$, and so on.² Therefore

$$\begin{aligned} x &= c_1 \sum_{k \geq 0} \frac{1}{10^{dk+1}} + c_2 \sum_{k \geq 0} \frac{1}{10^{dk+2}} + \dots + c_d \sum_{k \geq 0} \frac{1}{10^{dk+d}} \\ &= \left(\frac{c_1}{10} + \frac{c_2}{10^2} + \dots + \frac{c_d}{10^d} \right) \sum_{k \geq 0} \frac{1}{10^{dk}} \\ &= \left(\frac{c_1}{10} + \frac{c_2}{10^2} + \dots + \frac{c_d}{10^d} \right) \frac{1}{1 - 1/10^d}, \end{aligned}$$

where we summed a geometric series in the last step. Writing $1/(1 - 1/10^d)$ as $10^d/(10^d - 1)$ and using 10^d in the numerator to clear out the powers of 10 in the denominators of the other factor, we obtain

$$x = \frac{c_1 10^{d-1} + c_2 10^{d-2} + \dots + c_d}{10^d - 1}.$$

This is a rational number with denominator that is 1 less than a power of 10. The numerator can be any positive integer with at most d decimal digits, so the ratio is a fraction between 0 and 1.

Example 4.1. Let $x = .33333\dots$. The repeating block has length 1, so from the calculations we made,

$$x = \frac{3}{10 - 1} = \frac{3}{9} = \frac{1}{3}.$$

Example 4.2. Let $x = .002870028700287\dots$. The repeating block has length 5 (not 3; include the periodic 0's also), so

$$x = \frac{287}{10^5 - 1} = \frac{287}{99999} = \frac{7}{2439}.$$

In the last step, the greatest common divisor of 287 and 99999 is 41, so the numerator and denominator are divided by 41.

We have shown that any number that has a purely periodic decimal expansion is rational between 0 and 1 and admits an expression as a fraction whose denominator is $10^d - 1$ for some d . Now we want to go the other way: starting with a fraction, say $28/303$, can we decide if its decimal expansion is (purely) periodic or not?

The calculations above, passing from a purely periodic decimal for a number x to its expression as a fraction with denominator $10^d - 1$, can be read forwards and backwards. Reading it in reverse shows that any fraction between 0 and 1 with a denominator of the form $10^d - 1$ has a purely periodic decimal expansion. So the numbers that have purely periodic decimal expansions are precisely the fractions between 0 and 1 with a denominator of the form $10^d - 1$. Of course, a denominator having the form $10^d - 1$ might not be the

²We don't forbid the possibility that some of the c_i 's are equal, *e.g.*, $.11111\dots$ could be considered to have repeating block "1" or repeating block "11."

reduced form denominator, *e.g.*, $7/2439$ from Example 4.2 has to be written as $287/99999$ to get its denominator to be 1 less than a power of 10. So we ask: is there a simple description of the fractions that admit a representation (not necessarily reduced!) with a denominator of the form $10^d - 1$? Since $10^d - 1$ is not divisible by 2 or 5, and the reduced form denominator is a factor of any other denominator for the fraction, if a fraction has a denominator $10^d - 1$ then its reduced form denominator must be relatively prime to 10. It turns out the converse is also true, and the key tool to prove this is Euler's theorem:

Theorem 4.3. *Any reduced form fraction a/b with $(10, b) = 1$ can be written as a fraction with denominator $10^d - 1$ for some $d \geq 1$. Moreover, the period length of the decimal expansion for a/b is the smallest $d \geq 1$ such that $10^d \equiv 1 \pmod{b}$. In particular, $d \leq \varphi(b)$ and the period length is independent of the numerator a .*

Proof. Let the fraction be a/b , where $(10, b) = 1$. By Euler's theorem, $10^{\varphi(b)} \equiv 1 \pmod{b}$. That means $10^{\varphi(b)} - 1$ is a multiple of b , so we can rewrite a/b as a fraction with denominator $10^{\varphi(b)} - 1$.

Let $d \geq 1$ be minimal such that $10^d \equiv 1 \pmod{b}$, so $d \leq \varphi(b)$. Write $10^d - 1 = bn$, so

$$\frac{a}{b} = \frac{an}{bn} = \frac{an}{10^d - 1},$$

Since $a/b < 1$, we have $an < bn = 10^d - 1$. Therefore the base 10 expansion of an requires no more than d digits, so we can write $an = c_1 10^{d-1} + c_2 10^{d-2} + \cdots + c_d$ for some digits c_i . (Some of the top c_i 's may be 0 if an is substantially less than $10^d - 1$.)

Our earlier calculations showed that for any decimal digits c_1, \dots, c_d ,

$$(4.1) \quad \overline{.c_1 c_2 \cdots c_d} = \frac{c_1 10^{d-1} + c_2 10^{d-2} + \cdots + c_d}{10^d - 1},$$

so $a/b = (c_1 10^{d-1} + \cdots + c_d)/(10^d - 1)$ has a periodic decimal expansion of length d .

To show d is the minimal period of the decimal expansion of a/b when d is the smallest positive integer such that $10^d \equiv 1 \pmod{b}$, assume we could write a/b as a decimal expansion with a repeating block of some length ℓ . Then a/b can be written as a fraction with denominator $10^\ell - 1$. Since a/b is the reduced form of the fraction, this means $10^\ell - 1$ is a multiple of b , so $10^\ell \equiv 1 \pmod{b}$. Therefore $\ell \geq d$ (why?), so d is the minimal period length of the decimal expansion of a/b .

Since the least d such that $10^d \equiv 1 \pmod{b}$ has nothing to do with a , we see that the period length of a/b is independent of a (provided the fraction is written in reduced form, *i.e.*, $(a, b) = 1$). \square

Example 4.4. A numerical computation suggests the decimal expansions of $1/7$, $2/7$, $3/7$, $4/7$, $5/7$, and $6/7$ all have period length 6 and the decimal expansions of $1/303$ and $28/303$ both have period length 4. To prove this, check the least d such that $10^d \equiv 1 \pmod{7}$ is 6 and the least d such that $10^d \equiv 1 \pmod{303}$ is 4.

By seeing explicitly how $10^6 - 1$ is a multiple of 7 and $10^4 - 1$ is a multiple of 303, we can even figure out (without a calculator) what the decimal expansions of these fractions are. Since $10^6 - 1 = 7 \cdot 142857$,

$$\frac{3}{7} = \frac{3 \cdot 142857}{7 \cdot 142857} = \frac{428571}{10^6 - 1} = .428571428571 \dots$$

Since $10^4 - 1 = 303 \cdot 33$,

$$\frac{28}{303} = \frac{28 \cdot 33}{303 \cdot 33} = \frac{924}{10^4 - 1} = .092409240924 \dots$$

The whole theory of periodic decimals (*e.g.*, determining which numbers have purely periodic decimal expansions, and how long the periods can be) is explained by Euler's theorem and results related to it. So this is a concrete elementary application of number theory to explain a mystery from elementary school mathematics familiar to all students.

Remark 4.5. The requirement in Theorem 4.3 that a/b lie between 0 and 1 is a red herring. This is best explained by an example. Consider $1543/303$. To find its decimal expansion, first extract the integer part. Since $1543 = 303 \cdot 5 + 28$, we have $1543/303 = 5 + 28/303$. So the decimal part of $1543/303$ is the same as that of $28/303$, and we can apply Theorem 4.3 to $28/303$. Since $28/303 = .092409240924 \dots$, we have $1543/303 = 5.092409240924 \dots$.

In general, check that for any reduced form fraction $a/b > 1$, subtracting its integer part leaves a fraction between 0 and 1 that still has b as its reduced form denominator, so the period of the decimal expansion of a/b is still completely determined by b .

There are further interesting questions worth asking about decimal expansions:

- (1) Which numbers have finite decimal expansions (such as $5/16 = .3125$)?
- (2) Which numbers have periodic decimal expansions with an initial nonrepeating block (such as $7/15 = .466666 \dots$)?
- (3) If we compare all the reduced proper fractions with the same denominator b , they may all have the same expansion as $1/b$ except for a shift, *e.g.*,

$$\begin{aligned} 1/7 &= .\overline{142857}, & 2/7 &= .\overline{285714}, \\ 3/7 &= .\overline{428571}, & 4/7 &= .\overline{571428}, \\ 5/7 &= .\overline{714285} & 6/7 &= .\overline{857142}, \end{aligned}$$

Can you explain when all the reduced fractions with denominator b have this feature?

- (4) For some denominators, more than one digit sequence (up to shifting) occurs, *e.g.*, there are two possibilities when the denominator is 13:

$$\begin{aligned} 1/13 &= .\overline{076923}, & 2/13 &= .\overline{153846}, \\ 3/13 &= .\overline{230769}, & 4/13 &= .\overline{307692}, \\ 5/13 &= .\overline{384615}, & 6/13 &= .\overline{461538}, \\ 7/13 &= .\overline{538461}, & 8/13 &= .\overline{615384}, \\ 9/13 &= .\overline{692307}, & 10/13 &= .\overline{769230}, \\ 11/13 &= .\overline{846153}, & 12/13 &= .\overline{923076}. \end{aligned}$$

Every decimal expansion here is a shift of the expansion for $1/13$ or $2/13$. If we collect numerators of fractions above whose decimal expansions have the same digit sequence, the 12 numerators fall into two sets of size 6: $\{1, 3, 4, 9, 10, 12\}$ and $\{2, 5, 6, 7, 8, 11\}$. Is there some significance to these two sets of numbers? More generally, can you explain how many digit sequences (up to shifting) will occur among all the reduced fractions with a given denominator, and can you predict which fractions will have decimal digits that are shifts of each other?

These kinds of questions were studied in Europe from the 1760s to the 1790s. Mathematicians were interested in understanding decimal expansions for fractions so as to “mechanize

division” to save the labors of astronomers and others who needed to do a lot of numerical computation. (Pocket calculators only became widely available about 200 years later!) Papers by J. H. Lambert, J. Bernoulli, and K. F. Hindenburg during this time contained a mixture of rules and conjectures about periodic decimals. They recognized a connection between period lengths for prime denominators and Fermat’s little theorem, for instance, but they offered little in the way of explanations of their observations. In 1793, the 16-year old Gauss came across these papers and set to work. A few years later he settled nearly all the basic questions in this area through a systematic use of modular arithmetic³ and included his results in the sixth section of the *Disquisitiones Arithmeticae*.

REFERENCES

- [1] L. Levine, “Fermat’s Little Theorem: A Proof by Function Iteration,” *Math. Mag.* **72** (1999), 308–309.
- [2] C. Smyth, “A Coloring Proof of a Generalisation of Fermat’s Little Theorem,” *Amer. Math. Monthly* **93** (1986), 469–471.

³Two fractions a/b and a'/b with denominator b have the same decimal part if and only if $a/b - a'/b$ is an integer, which means $a \equiv a' \pmod{b}$. So the study of decimal expansions might be what led Gauss to discover modular arithmetic in the first place.