

Extensions on the Euler congruence

Joeri Verscheure

1 Introduction

In this short paper I will give a few elementary extensions of the well known *Euler congruence*, also referred to as *Euler's theorem*.

Remark. *To avoid ambiguity, I first give the interpretation of some ambiguous (depends on where you live) symbols used in the text:*

- $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ and
- $\mathbb{N}_0 = \{1, 2, 3, \dots\}$.
- *And to be sure everyone gets it, a vertical bar $|$ means in all cases 'is divisor of' (or 'divides'). The symbol \nmid means 'is no divisor of'.*

Theorem 1.1. *The Euler congruence states that for $n \in \mathbb{N}_0$ and $a \in \mathbb{Z}$ we have*

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

when $\gcd(a, n) = 1$, (or in other words a and n must be coprime).

proof:

Several proofs of this theorem, more or less elementary, can be found in books on elementary number theory. ▲

Of course conversely the congruence does not hold if $\gcd(a, n) \neq 1$, as this is equivalent to a having no inverse modulo n . But we can formulate some easy proved elementary theorems that are in some way generalisations of the Euler congruence in this case.

2 What if $\gcd(a, n)$ is not equal to 1?

Let us begin with the most important theorem (or I find it the most important one). It looks like Euler's theorem, but it is more general.

2 What if $\gcd(a, n)$ is not equal to 1?

Theorem 2.1. Let $n \in \mathbb{N}_0$ and $a \in \mathbb{Z}$. Let d be the number you get by cancellation of all the prime factors in the prime factorisation of n who are no divisor of a . (If everything is cancelled, then you get '1' of course.) In other words $\frac{n}{d}$ is the greatest divisor of n that is relatively prime with a . Then

$$a^{\varphi(n)} \pmod n = d \left(d^{-1} \pmod{\frac{n}{d}} \right),$$

with $d^{-1} \pmod{\frac{n}{d}}$ the inverse of d modulo $\frac{n}{d}$.

proof:

- We have $0 \leq d^{-1} \pmod{\frac{n}{d}} < \frac{n}{d}$, so $0 \leq d(d^{-1} \pmod{\frac{n}{d}}) < n$. Therefore it is sufficient to proof that

$$a^{\varphi(n)} \equiv d(d^{-1} \pmod{\frac{n}{d}}) \pmod n. \quad (1)$$

- To proof (1) it is sufficient to proof the following two statements:

$$d | a^{\varphi(n)} \text{ and} \quad (2)$$

$$a^{\varphi(n)} \equiv 1 \pmod{\frac{n}{d}}, \quad (3)$$

because (2) \Rightarrow take that $k \in \mathbb{Z}$ so that $a^{\varphi(n)} = dk$.

$$\begin{aligned} (3) &\Rightarrow dk \equiv 1 \pmod{\frac{n}{d}} \\ &\Rightarrow k \equiv (d^{-1} \pmod{\frac{n}{d}}) \pmod{\frac{n}{d}} \text{ (because the inverse is unique)} \\ &\Rightarrow dk \equiv d(d^{-1} \pmod{\frac{n}{d}}) \equiv a^{\varphi(n)} \pmod n. \end{aligned}$$

- Proof of (2):

given: $p|d \Rightarrow p|a$

\Rightarrow sufficient to proof: $\varphi(n) \geq$ number of prime factors in the prime factorisation of d

\Rightarrow sufficient to proof: $\varphi(n) \geq$ number of prime factors in the prime factorisation of n .

This is easly argued out from the formula for $\varphi(n)$ in terms of the prime factorisation of n .

- Proof of (3):

From the Euler congruence follows

$$a^{\varphi(\frac{n}{d})} \equiv 1 \pmod{\frac{n}{d}}$$

because $\gcd(a, \frac{n}{d}) = 1$, because it is given that if $p|\frac{n}{d}$, then $p \nmid a$, for each p prime. From this it follows that $a^{\varphi(n)} \equiv 1 \pmod{\frac{n}{d}}$ (argue out that $\varphi(\frac{n}{d}) | \varphi(n)$, because $\frac{n}{d} | n$, from the formula for $\varphi(n)$).

▲

2 What if $\gcd(a, n)$ is not equal to 1?

So as you can see the proof is really simple. You can easily see Euler's theorem as a special case of this theorem. In fact the proof follows directly from splitting up n , remember the Chinese remainder theorem. But I find the theorem beautiful. The proof gives more insight in how it works in general when Euler's theorem doesn't hold immediately.

Remark. Of course to find d you don't have to factorise n , which becomes time-consuming if the number of digits of n grows. You can do it for example by dividing away from n the greatest common divisor with a and from what remains again the greatest common divisor with a and so on until there is nothing left to divide away.

No I will give an immediate consequence, at least in one direction. The other direction is not immediately clear.

Consequence 2.2. Let $n \in \mathbb{N}_0$ en $a, b \in \mathbb{Z}$. Then

$$a^{\varphi(n)} \equiv b^{\varphi(n)} \pmod{n} \iff \forall p \text{ prime, } p|n : (p|a \Leftrightarrow p|b)$$

proof:

Let d_a the 'd that belongs to a and n ' as defined in the previous theorem and d_b de 'd that belongs to b en n '. We must proof both directions.

• \Leftarrow

In this case $d_a = d_b$ by definition; define $d = d_a = d_b$. Then

$$a^{\varphi(n)} \pmod{n} = d \left(d^{-1} \pmod{\frac{n}{d}} \right) = b^{\varphi(n)} \pmod{n}.$$

• \Rightarrow

Proof by contradiction: suppose $\exists p$ prime, $p|n$: $p|a$ and $p \nmid b$, take that p . (This p exists, if necessary after exchanging the role of a and b .) Now apply theorem 2.1:

$$a^{\varphi(n)} \pmod{n} = d_a \left(d_a^{-1} \pmod{\frac{n}{d_a}} \right)$$

|| given

$$b^{\varphi(n)} \pmod{n} = d_b \left(d_b^{-1} \pmod{\frac{n}{d_b}} \right).$$

Then $p|d_a$ and $p \nmid d_b$.

Now $d_b^{-1} \pmod{\frac{n}{d_b}}$ has an inverse modulo $\frac{n}{d_b}$ (namely $d_b \pmod{\frac{n}{d_b}}$).

Therefore $\gcd(d_b^{-1}, \frac{n}{d_b}) = 1$,

but $p|\frac{n}{d_b}$ (because $p|n$ and $p \nmid d_b$) and

$p|d_b^{-1}$ (because $p|d_a(d_a^{-1} \pmod{\frac{n}{d_a}})$, so $p|d_b(d_b^{-1} \pmod{\frac{n}{d_b}})$ and $p \nmid d_b$),

3 Extensions on the reduction of the exponent modulo $\varphi(n)$

which gives us the contradiction. ▲

The next two examples are some remarkable special cases of this consequence.

Example 2.3.

$$a^{\varphi(n)} \equiv \text{ggd}(a, n)^{\varphi(n)} \pmod{n}$$

Anyhow this is easy to prove without this consequence.

Example 2.4.

$$a^{k\varphi(n)} \equiv a^{l\varphi(n)} \pmod{n}, \forall k, l \in \mathbb{N}_0$$

And this gives the link to the next section.

3 Extensions on the reduction of the exponent modulo $\varphi(n)$

Example 2.4 gives us a way to reduce the exponent when calculating a power modulo n . The example says we can always reduce by subtracting a number of times $\varphi(n)$, but it doesn't give a way to reduce below $\varphi(n)$. Now we investigate if we can reduce further below $\varphi(n)$.

Theorem 3.1. *Let $n, l \in \mathbb{N}_0$, $a \in \mathbb{Z}$ en $k \in \mathbb{N}$. Then*

$$a^{l\varphi\left(\frac{n}{\text{ggd}(a^k, n)}\right)+k} \equiv a^k \pmod{n} \quad (1)$$

$$\Leftrightarrow \text{ggd}\left(a, \frac{n}{\text{ggd}(a^k, n)}\right) = 1 \quad (2)$$

$$\Leftrightarrow \exists e \in \mathbb{N}_0 : a^{k+e} \equiv a^k \pmod{n} \quad (3)$$

proof:

(3) \Rightarrow (2) Given: $n|a^k(a^e - 1)$

$$\Rightarrow \frac{n}{\text{ggd}(a^k, n)} | a^e - 1$$

$$\Rightarrow a^e \equiv 1 \pmod{\frac{n}{\text{ggd}(a^k, n)}}$$

$$\Rightarrow a^{e-1} \text{ is the inverse of } a, \text{ modulo } \frac{n}{\text{ggd}(a^k, n)},$$

$$\text{so } \text{ggd}\left(a, \frac{n}{\text{ggd}(a^k, n)}\right) = 1.$$

(2) \Rightarrow (1) From the Euler congruence:

$$a^{\varphi\left(\frac{n}{\text{ggd}(a^k, n)}\right)} \equiv 1 \pmod{\frac{n}{\text{ggd}(a^k, n)}}$$

$$\Rightarrow a^{l\varphi\left(\frac{n}{\text{ggd}(a^k, n)}\right)} \equiv 1 \pmod{\frac{n}{\text{ggd}(a^k, n)}}$$

$$\Rightarrow \frac{n}{\text{ggd}(a^k, n)} | a^{l\varphi\left(\frac{n}{\text{ggd}(a^k, n)}\right)} - 1$$

$$\Rightarrow n | a^k (a^{l\varphi\left(\frac{n}{\text{ggd}(a^k, n)}\right)} - 1).$$

(1) \Rightarrow (3) Take $e = l\varphi\left(\frac{n}{\text{ggd}(a^k, n)}\right)$.



Remark. You may wonder why I put the theorem in this form with the number l . You can take l for example equal to one. But you have an interesting case taking l so that $l\varphi\left(\frac{n}{\text{ggd}(a^k, n)}\right)$ is equal to $\varphi(n)$. This is possible because in general if $m|n$ then $\varphi(m)|\varphi(n)$. Then we have an answer to the question in the beginning of this section. Namely, in this case the first two lines of the theorem gives us precisely in which cases we can reduce further below $\varphi(n)$. It also fits completely with the example 2.4 because $\varphi(n)$ is greater than the number of prime factors in the prime factorisation of d or n . (See the proof of theorem 2.1)

Finally an exercise, which is a bit artificial to be as general applicable as possible.

Exercise 3.2. Let $n, l, l', l'', l''' \in \mathbb{N}_0, a \in \mathbb{Z}$ and $k \in \mathbb{N}$. Then

$$a^{l'\varphi\left(\frac{n}{\text{ggd}(a^k, n)}\right)+k} \equiv a^k \text{ggd}\left(a^{l'''}, \frac{ln}{\text{ggd}(a^k, n)}\right)^{l''\varphi\left(\frac{n}{\text{ggd}(a^k, n)}\right)} \pmod{n}$$

sollution:

We change the exercise to the following question. For wich $b \in \mathbb{Z}$ is

$$a^{l'\varphi\left(\frac{n}{\text{ggd}(a^k, n)}\right)+k} \equiv a^k b^{l''\varphi\left(\frac{n}{\text{ggd}(a^k, n)}\right)} \pmod{n} \quad (4)$$

First we transform the congruence a bit.

$$\begin{aligned} (4) &\Leftrightarrow n|a^k \left(a^{l'\varphi\left(\frac{n}{\text{ggd}(a^k, n)}\right)} - b^{l''\varphi\left(\frac{n}{\text{ggd}(a^k, n)}\right)} \right) \\ &\Leftrightarrow \frac{n}{\text{ggd}(a^k, n)} | a^{l'\varphi\left(\frac{n}{\text{ggd}(a^k, n)}\right)} - b^{l''\varphi\left(\frac{n}{\text{ggd}(a^k, n)}\right)} \\ &\Leftrightarrow a^{l'\varphi\left(\frac{n}{\text{ggd}(a^k, n)}\right)} \equiv b^{l''\varphi\left(\frac{n}{\text{ggd}(a^k, n)}\right)} \pmod{\frac{n}{\text{ggd}(a^k, n)}}. \end{aligned}$$

Because of example 2.4 it is *sufficient* that

$$a^{\varphi\left(\frac{n}{\text{ggd}(a^k, n)}\right)} \equiv b^{\varphi\left(\frac{n}{\text{ggd}(a^k, n)}\right)} \pmod{\frac{n}{\text{ggd}(a^k, n)}}.$$

Because of consequence 2.2 is this equivalent to

$$\forall p \text{ prime, } p \mid \frac{n}{\text{ggd}(a^k, n)} : p|a \Leftrightarrow p|b.$$

And finally we see that $b = \text{ggd}\left(a^{l'''}, \frac{ln}{\text{ggd}(a^k, n)}\right)$ satisfies.

Remark. Again, you may wonder the use of all this numbers l . You can choose them as you want, for example equal to one, and again the l' and l'' outside the φ -function means you can also multiply inside the φ -function (see also the remark for theorem 3.1). You can for example multiply the denominator in the fractions away or you can multiply it partly away, for example you can take k in a^k in the denominators smaller.

4 Conclusions

The first theorem 2.1 gives us a way to calculate $a^{\varphi(n)} \bmod n$ without having to calculate $\varphi(n)$ or in other words without having to factorise n . Although this sounds good, I must admit that I know no applications of this. We also noted a few quite remarkable consequences and special cases.

The last theorem 3.1 together with the example 2.4 gives us a way to reduce the exponent modulo $\varphi(n)$ when we have to calculate a power of a modulo n . Of course this method is not a quick method, because we must know $\varphi(n)$, and there are easy quick methods to calculate powers. But the fact that we can reduce to another lower (simpler) exponent can be important when we don't deal with a specific number a but when we deal with a specific power of a not further defined number a modulo n .