from the book : « Integer Numbers - Aritmetica »
Author: Vincenzo Vitale ; e-mail: vincenzovitale@integernumbers.org

google translation from the Italian language

The set ϕ

published on the web: 31-03-2016

Let's go back to the speech that previously led us to Euler's theorem and deepen the analysis of the set ϕ_q of the integer numbers greater than zero, less than the odd number q and coprime with q, in order to demonstrate the theorem that i indicated with the symbol 'V-V'.
For a better understanding of what is asserted here, it is appropriate that the reader starts from the relations:
"From Wilson to Fermat" and «Euler's Theorem"
We want to show that there is a single thread between the three most famous theorems of 'Number Theory':
Wilson's theorem; Fermat's little theorem; Euler's theorem

Theorem V-V

They are: q any odd integer ; ϕ_q the set of numbers greater than zero, less than q and coprime with q ; $\phi(q)$ how many are the elements of ϕ_q ; $\phi_q!$ is the product of all the elements of ϕ_q: $\phi_q! = 1 \cdot c_2 \cdot c_3 \cdot \ldots \cdot c_{\phi(q)}$

- If q is composed of two or more prime factors, or is a power of two or more prime factors,

$$\phi_q! \equiv 1 \pmod{q}$$

$$a^{\phi(q)/2} \equiv \phi_q! \equiv 1 \pmod{q} \ , \ a \in \phi_q$$

- If q is prime number, or the power of one prime number only:

$$\phi_q! \equiv -1 \pmod{q}$$

$$a^{\phi(q)/2} \equiv \phi_q! \equiv -1 \pmod{q} \ , \ a \in \phi_q \quad \text{quadratic non-residue}$$

$$-a^{\phi(q)/2} \equiv \phi_q! \quad ; \quad a^{\phi(q)/2} \equiv 1 \pmod{q} \ , \ a \in \phi_q \quad \text{quadratic residue}$$

* We show that:

- If q is odd multiple, necessarily must be valid the congruence relation: $\phi_q! \equiv 1 \pmod{q}$

To this end, we review the previous report on Euler's theorem and we begin again the discussion to the point where it was proposed to calculate the value of the product of all elements of ϕ_q.
This time we will face the question in a more specific and we will solve it.

When a = 1, the set ϕ_q is an abelian group with respect to multiplication operation, for which, if none of the elements $c \in \phi_q$ were to have himself as inverse, the calculation would be immediate: $\phi_q! = c_1 \cdot c_2 \cdot c_3 \cdot \ldots \cdot c_{\phi(q)} \equiv 1 \pmod{q}$
But the calculation of $\phi_q!$ we can properly run only after having verified whether there are elements in pairs with themselves , that is, such that: $c \cdot c \equiv 1 \pmod{q}$.

If we assume that this element $c \in \phi_q$ exists, we will have equality: $c^2 = t \cdot q + 1$, namely: $(c-1) \cdot (c+1) = t \cdot q$
So, to ensure that this supposition is true, we must determine whether there is any element $c \in \phi_q$ with these requirements: the product of his earlier for his next one must be a multiple of q.
The equality $(c-1) \cdot (c+1) = t \cdot q$ is always true for c = 1 and c = q-1.
These two values of c determine the equalities: $0 \cdot 2 = 0$; $(q-2) \cdot q = m \cdot q$.
For these two elements, always present in ϕ_q , whatever odd q, are valid these congruences :

$$1^2 \equiv 1 \pmod{q} \ ; \ (q-1)^2 \equiv 1 \pmod{q} \ ; \ 1 \cdot (q-1) \equiv -1 \pmod{q}$$

Because of the latter congruence, if in the set ϕ_q there were only these two items paired with themselves, as they are after all the prime numbers, the calculation would be: $\phi_q! \equiv -1 \pmod{q}$
But to draw the right conclusions we have to go looking for other possible elements of ϕ_q paired with themselves, such as to render valid the equality $(c-1) \cdot (c+1) = t \cdot q$ also for $c \neq 1$ and for $c \neq (q-1)$.

To this end, we wonder if there is:
- Some element $c \in \phi_q$ $(c \neq 1)$ such that $(c-1) \notin \phi_q$, that is, such that (c-1) has among its prime factors some divisor of q.
- Some element $c' \in \phi_q$ $(c' \neq q-1)$ such that $(c'+1) \notin \phi_q$, that is, such that (c'+1) has among its prime factors some divisor of q.

The set ϕ_q is not a group with respect to the subtraction and even with respect to addition, because these operations are not internal binary operation on a set ϕ_q .
In fact, assuming that ϕ_q is closed with respect to the subtraction, we consider two of its elements: $c_1 = 1$ and $c_{\phi(q)} = q-1$ and calculate their difference d1. Having supposed ϕ_q closed, we will have to admit that d1 belongs to ϕ_q.
Then we calculate the difference d2 = d1 - 1. Even d_2 belong to ϕ_q .
We proceed with the next differences to the last difference $d_o = 1$: (q-1)-1 = q-2 ; (q-2)-1 = q-3 ; (q-3)-1 = q-4 . . .
By doing so we will have to admit ϕ_q coincides with a full set of remains module q.
Because this occurs only when q is prime, we fall into contradiction with the hypothesis that q instead be composed.
Then, necessarily, if q is composite number, there exists some element $c \in \phi_q$ $(c \neq 1)$, such that $(c-1) \notin \phi_q$.
With similar reasoning, considering this time the addition operation and the two elements 1 and 2 of ϕ_q , we come to the conclusion that there is some element $c' \in \phi$ $(c' \neq q-1)$, such that $(c'+1) \notin \phi_q$.

Returning to examine the equality $(c-1) \cdot (c+1) = t \cdot q$, we can now be certain that there is some divisor of q of the form:
$0 < (c-1) < q$, $c \in \phi_q$, $c \neq 1$ and some divisor of q of the form: $0 < (c'+1) < q$, $c' \in \phi$, $c' \neq q-1$
But we have to answer a few more questions.

- When $[(c-1), q] \neq 1$, it is possible that (c-1) contains all the prime divisors of q?
The answer is no, because $0 < (c-1) < q$, $(c \neq 1)$.
- When $[(c'+ 1), q] \neq 1$, it is possible that (c'+1) contains all the prime divisors of q?
Also in this event the answer is negative, because $0 < (c'+1) < q$, $c' \neq q-1$

Thus, the "double" element of ϕ_q exists only when c=c' . This implies that, in equality $(c-1)\cdot(c+1) = t \cdot q$, (c-1) and (c+1) have the dividers of q at the same time: some prime factors of q in (c-1) and all other prime factors of q necessarily in (c+1).

We are looking for all the numbers c "double" of ϕ_q $(c \neq 1 , q-1)$, relative to the base **a**=1, provided that it exists someone.
We observe first that in the expression $(c-1)\cdot(c+1)=t\cdot q$, assumed as reference for our research, if we put c-1=k and c+1=j , wi have: j=k+2 , for which the numbers (c-1) and (c+1) of our research must be coprime.
In fact, if $d \mid k$ it follows that $d \nmid (k+2)$, $(d \neq 2$, because we consider odd q).
After that, we proceed as follows.

* Break it down into its prime factors the odd composite number q: $q = g \cdot j \cdot \ldots \cdot k$

We group these prime factors, no one belonging to ϕ_q , into two disjoint sets: $A=\{g , j , \ldots , h\}$; $B= \{e , f , \ldots , k\}$
Let be: $\mathbf{w} = g \cdot j \cdot \ldots \cdot h$ and $\mathbf{y} = e \cdot f \cdot \ldots \cdot k$

w and **y** are coprime, and neither of them belongs to ϕ_q , while their product is: $\mathbf{w}\cdot\mathbf{y}= q$

If $\mathbf{w} < \mathbf{y}$, we consider the set ϕ_y of numbers greater than zero, less than **y** and coprime with **y** .

(If $\mathbf{w} > \mathbf{y}$, we reverse **w** with **y** and consider the set ϕ_w of numbers greater than zero, less than **w** and coprime with **w) .**

Among the elements of ϕ_y there are definitely: 1 and y-1, all powers of 2 smaller than **y** and the corresponding $y-2^n$, **w** and **y-w**.

As we had occasion to ensure, choice in ϕ_y the base **a** = 2, exists and is unique another element s of ϕ_y , such that $s\cdot\mathbf{w} \equiv 2 \pmod{y}$, that is: $s\mathbf{w}-2 = m\mathbf{y}$, for which : $s\mathbf{w}-1 = m\mathbf{y}+1$; $(s, y)=1$, because $s \in \phi_y$; $(m , w)=1$, otherwise their common divisor would even divisor of 2, contradicting the hypothesis that q is odd.

Having engaged in **w** and **y** all of q prime factors, we found a "double" element of ϕ_q , it is $s\mathbf{w}-1$
In fact, this number has criteria for the hunt:

- (Sw-1) is an element of ϕ_q , because it is greater than 0, smaller than q , coprime to q.
From the equality $q=\mathbf{w}\cdot\mathbf{y}$, given that $s<\mathbf{y}$, it follows that $(s\mathbf{w}-1) < q$; $s\mathbf{w}-1>0$, because $s>0$ e $\mathbf{w}>1$.
From the equality $s\mathbf{w}-1 = m\mathbf{y}+1$, if (sw-1) had h prime divisor of q, since h is, by hypothesis, a prime factor or of **w** or of **y**, h would be even divisor of 1. Which is absurd.
- $(s\mathbf{w}-1)+1 = s\mathbf{w}$; $(s\mathbf{w}-1)-1 = s\mathbf{w}-2=m\mathbf{y}$, then: $[(s\mathbf{w}-1)+1]\cdot[s\mathbf{w}-1)-1] = s\mathbf{w}\cdot m\mathbf{y} = nq$, because in **w** and in **y** are all prime divisors of q, some in **w** and all other in **y**. (We have shown above that s and m are coprime to q)
- Because $[(s\mathbf{w}-1)+1]\cdot[s\mathbf{w}-1)-1] = (s\mathbf{w}-1)^2 - 1 = nq$, it follows that: $(s\mathbf{w}-1)^2 \equiv 1 \pmod{q}$.

So that $s\mathbf{w}-1$ is a square root of 1 in ϕ_q , then is a double element of ϕ_q .
This double element was found in correspondence to a specific choice of prime factors of q.
Let now w' is the product of another grouping of prime factors of q and y' the product of the remaining prime factors of q.
Proceeding in the same way as we described above, we find another double element: s'w' - 1.
But it is possible that (s'w' - 1) is the same item found before?
If sw-1=s'w'-1 , you will have the equality: sw=s'w' . Let d be a divisor of w' , but not a divisor of w.
Replacing s'w' to sw in the equality $s\mathbf{w}= m\mathbf{y}+2$, you will have: $s'w' = m\mathbf{y}+2$
The divisor d of w' , if does not divide **w**, it must, by hypothesis, divide **y**, so you come to the absurd that d also divides 2, which instead is coprime with the odd number q.
So the double element (s'w'-1) relative to w' can not be equal to the element double (sw-1) relative to w.

In the light of this last observation, since **w** is the product of any grouping of prime factors of q, we come to the conclusion that the "double" elements of ϕ_q are as many as the ways to select into two disjoint sets the prime factors of q.
The calculation of all the combinations is summarized by the formula:

n	m
1	2
2	4
3	8
4	16
n	2^n

$m = 2^n$ (n is the amount of the prime divisors of q ; m is the quantity of the double elements of ϕ_q)

Now we can calculate the exact value of $\phi_q!$

In fact, as we have already established, the elements of ϕ_q can be associated:

- some in pairs of inverse elements, that is, such that $c_1 \cdot c_2 \equiv 1 \pmod{q}$;
- all the others, those who have themselves as inverses, in pairs of the form (c ; q-c) , such that $c \cdot (q - c) \equiv -1 \pmod{q}$:

$$\phi_q! = (c_1 \cdot c_j) \cdot (c_2 \cdot c_t) \cdot \ldots \cdot [c_h \cdot (q - c_h)] \cdot \ldots \cdot [c_k \cdot (q - c_k)]$$

As can be seen from the formula, when the prime divisors of q are two or more than two (n > 1), the pairs (c ; q-c) are even in number, for which the value of $\phi_q!$ it is given by the congruence:

$$\phi_q! \equiv 1 \pmod{q} \text{ , whatever the number odd composite q}$$

Only when the exponent is n = 1, that is, when q is prime, it forms a single pair (c ; q-c) and this event determines the value: $\phi_q! \equiv -1 \pmod{q}$ found in Wilson's theorem: $(p-1)! \equiv -1 \pmod{p}$, p prime.

For the calculation of the formula $m = 2^n$, click «Combination ϕ»

***

Once established the value of $\phi_q!$, we concentrate on any one base **a** of the set ϕ_q .

* We show that for each base **a** are valid he congruences:

$$\mathbf{a}^{\phi(q)/2} \equiv \phi_q! \equiv 1 \pmod{q} \text{ , } \mathbf{a} \in \phi_q$$

In the report on Euler's theorem we have already shown that, given an odd number q, and taken from the ϕ_q whatever element **a**, which we call base, all the elements **c** of ϕ_q can be coupled, uniquely, in the congruence:
$c' \cdot c'' \equiv \mathbf{a} \pmod{q}$

But, to be able to calculate the value of $\mathbf{a}^{\phi(q)/2}$, it must also determine if there are pairs formed by the same element, and, if there are, you need to count how many are these couples.

If you choose the base **a** non-quadratic residue, the calculation is quickly made, because the square root of **a** in ϕ_q does not exist, for which the pairs of congruences $c' \cdot c'' \equiv \mathbf{a} \pmod{q}$ are formed all by two distinct elements $c' \neq c''$) :

$$\mathbf{a}^{\phi(q)/2} \equiv \phi_q! \equiv 1 \pmod{q} \text{ , } \mathbf{a} \in \phi_q \text{ non-quadratic residue}$$

There remains the problem of calculating the value of $\mathbf{a}^{\phi(q)/2}$ when you choose the base **a** quadratic residue $(a \neq 1)$.

The quadratic residues, by their very definition, have at least one square root in ϕ_q , for which there is always some element v "double" of ϕ_q concerning the selection of the base **a**, that is, such that: $v^2=tq+\mathbf{a}$; $v^2\equiv\mathbf{a} \pmod q$

But, if v is a square root of **a** in ϕ_q , also (q - v) it is. In fact: $(q-v)^2\equiv\mathbf{a} \pmod q$

We can therefore assert: whatever the odd number q, for each quadratic residue **a** , there are always at least two square roots in ϕ_q : v and v-c, and their product is: $v\cdot(q-v)\equiv-\mathbf{a} \pmod q$

If the double elements were only two, the calculation of ϕ_q! it would be once again well determined, but some practical examples give us a glimpse that the roots of the quadratic residue **a** can be more than two in ϕ_q

It's time to examine well ϕ_q, in order to find the general law that allows us to determine how many and what are the square roots of each quadratic residue.

If, in addition to v, is there any other root c of **a**, we have the congruences:

$v^2\equiv\mathbf{a} \pmod q$; $c^2\equiv\mathbf{a} \pmod q$ and then: $c^2\equiv v^2 \pmod q$

From this last congruence we get the :

$$(c-v)(c+v)=tq \qquad <*>$$

We analyze carefully this equality in order to derive all the square roots of **a** in ϕ_q , and then all the "double" elements of ϕ_q , relative to **a**.

For c = v and for c = q-v, the expression <*> is always true, because the respective equalities are: $0\cdot2v=0$; $(q-2v)\cdot q=tq$

It is important to note that for each of these two values the prime factors of q are or all in (c-v) or all in (c + v).

So, for any quadratic residue **a**, the two solutions of <*> found are always elements "double" of ϕ_q :

$v^2\equiv\mathbf{a} \pmod q$; $(q-v)^2\equiv\mathbf{a} \pmod q$; $v\cdot(q-v)=vq-v^2\equiv-\mathbf{a} \pmod q$

We are looking for all the other possible square roots of **a** in ϕ_q based on the following considerations.

In order that the equality <*> is valid for $c\neq v$ and for $c\neq q-v$ there must be another value $c\in\phi_q$ such that:

- the difference (c-v) and the sum (c+v) are not elements of ϕ_q : $(c-v)\notin\phi_q$; $(c+v)\notin\phi_q$
- in (c-v) there are only some prime divisors of q and, simultaneously, in (c+v) there are all the other prime divisors of q
- the distance between (c-v) and (c+v) is 2v: (c+v)-(c-v)=2v

* Given the odd composite number q , we choose in the ϕ_q the quadratic residue $\mathbf{a}\equiv v^2 \pmod q$, $v\in\phi_q$

If $2v>q$, we will choose, as the square root of a, v' = q-v , so that it is definitely $2v'<q$.

Break it down into its prime factors the odd composite number q: $q=g\cdot j\cdot\ldots\cdot k$

We group these prime factors, no one belonging to ϕ_q , into two disjoint sets:

$$\mathbf{A}=\{g\ ,\ j\ ,\ \ldots\ ,\ h\}\ \ ;\ \ \mathbf{B}=\{e\ ,\ f\ ,\ \ldots\ ,\ k\}$$

Let be: $\mathbf{w}=g\cdot j\cdot\ldots\cdot h$ and $\mathbf{y}=e\cdot f\cdot\ldots\cdot k$ (**w** and **y** are coprime and neither of them belongs to ϕ_q , while $\mathbf{w}\cdot\mathbf{y}=q$)

If $\mathbf{w}<\mathbf{y}$, we consider the set ϕ_y of numbers greater than zero, less than y, and coprime with **y**.

(If $\mathbf{w}>\mathbf{y}$, we reverse **w** with **y** and consider the set ϕ_w of numbers greater than zero, less than **w** and coprime with **w**).

If $2v>y$, we increase the value of **y**, raising to the power one or more of its prime factors: $\mathbf{y}=e^n\cdot f\cdot\ldots\cdot k$ in such a way that it becomes: $2v<y$ In this case, $\mathbf{w}\cdot\mathbf{y}=d\cdot q$.

The elements: 1, 2, v, 2v certainly belong to ϕ_y , because they are also elements of ϕ_q and are smaller than **y**; while **w** and **y-w** are elements of ϕ_y because coprime with y and $0<\mathbf{w}<\mathbf{y}$.

As we have had occasion to see, the set ϕ_y is such that, fixed the element $2v\in\phi_y$ as a base, exists, and is unique, another element s of the same ϕ_y which determines the congruence: $s\cdot\mathbf{w}\equiv2v \pmod{\mathbf{y}}$, that is: $s\mathbf{w}-2v=t\mathbf{y}$.

It is important to note that:

- s has no prime divisor of **y**, because $s\in\phi_y$;
- t has no prime divisor of **w**, otherwise v could not be coprime to q. (It follows from: $s\mathbf{w}-2v=t\mathbf{y}$) .

Our attention should be paid to the number $(s\mathbf{w}-v)=(t\mathbf{y}+v)$ obtained from the equality $s\mathbf{w}-2v=t\mathbf{y}$.

Let's examine it:

* $(s\mathbf{w}-v)$ is greater than zero and may belong to ϕ_q (happens when $sw-v<q$) , but, in any case, is coprime to q.

In fact, taking into account that $(s\mathbf{w}-v)=(t\mathbf{y}+v)$, if $(s\mathbf{w}-v)$ had a prime divisor g of q , g should: or divide both **w** and v , or divide both y and v. But v, by assumption, has not divisors of q, then, necessarily: $[(s\mathbf{w}-v)\ ,\ q]=1$

* $(s\mathbf{w}-v)-v=s\mathbf{w}-2v=t\mathbf{y}$; $(s\mathbf{w}-v)+v=s\mathbf{w}$.

* $(s\mathbf{w}-v)-v\equiv b-v \pmod q$; $(s\mathbf{w}-v)+v\equiv b+v \pmod q$

The number b of these congruences is a "double" element of ϕ_q , because it has the requirements:

- $b\in\phi_q$ In fact, remembering that $(s\mathbf{w}-v)>0$ and $[(s\mathbf{w}-v)\ ,\ q]=1$, we have:
  - $0<b<q$, because b is the minimum positive remainder of division of (sw-v) by q: $(sw-v)=kq+b$, $k\geq0$;
  - $(b\ ,\ q)=1$, b is coprime to q, because even (sw-v) and q are coprime.
- (b-v) contains all prime factors of q that are contained in **y**, and none of those contained in **w**.

  In fact, from the congruence $(s\mathbf{w}-v)-v\equiv b-v \pmod q$, being $s\mathbf{w}-2v=t\mathbf{y}$, it follows that $t\mathbf{y}=fq+(b-v)$, $f\geq0$ for which:
  - if d is a divisor of **y**, d must be well divisor of (b-v), because it also divides q. Then: $d\mid\mathbf{y}\Rightarrow d\mid(b-v)$
  - if we suppose instead that a divider g of **w** divides (b-v), since it also divides q, g should also divide **y** , contradicting the hypothesis made and we already ruled on that g can not divide t. Then: $g\mid\mathbf{w}\Rightarrow g\nmid(b-v)$.
- (b+v) contains all prime factors of q that are contained in **w** and none of those contained in **y**.

  In fact, from the congruence $(s\mathbf{w}-v)+v\equiv b+v \pmod q$, it follows that $s\mathbf{w}=jq+(b+v)$, $j\geq0$ for which:
  - if f is a divisor of **w**, f must be well divisor of (b+v), because it also divides q. So: $f\mid\mathbf{w}\Rightarrow f\mid(b+v)$
  - if we suppose instead that a divider h of **y** divides (b+v), since it also divides q, h should divide as well **w**, in contradict the assumptions made, and we already ruled on that h can divide s. Then: $h\mid\mathbf{y}\Rightarrow h\nmid(b+v)$.
- $(b-v)\cdot(b+v)=mq$, because in (b-v) and in (b+v) there are all the prime divisors of q, some in (b-v) and all the others in (b+v)
- The distance between (b-v) and (b + v) is 2v.

Therefore the element b of ϕ_q is a square root of the quadratic residue **a** in ϕ_q :

$(b-v)\cdot(b+v)=b^2-v^2\ \Rightarrow\ b^2\equiv a \pmod q$

We wish to know if the w' number, obtained by a different choice of q prime factors, we do find a root b' of the quadratic residue **a**, different from b.

Comparing the congruences: $b\equiv(s\mathbf{w}-v) \pmod q$; $b'\equiv(s'w'-v) \pmod q$, taking into account that q and v remain constant.

If b=b' it follows that: $s'w'-v\equiv sw-v \pmod q$ and then: $s'w'-sw=tq$

If d is a prime factor of w' , but not of w, the latter equality is valid only if d divides s, because d also divides q.

But s is the element of ϕ_y that we used above: sw=ty+2v

From this we see that, assuming that d divides s, we should also admit that d divides $2v\in\phi_q$.

In fact, if d is not a factor of **w**, by definition it is instead a factor of **y**.

Given the contradiction in which they would face, we are sure that the new root b' of **a** is different from the previous one: $b'\neq b$

It easily infers that the proof does not change, whether among the factors of q there are powers of prime numbers: each power of a prime number should be considered a single unit of factorization and treated as a single prime.

If $q=g^a \cdot j^b \cdot \ldots \cdot k^m$ the powers of the prime factors must be distributed into two disjoint sets:

$$\mathbf{A} = \{g^a, j^b, \ldots, h^n\} \;\; ; \;\; \mathbf{B} = \{e^d, f^g, \ldots, k^m\}$$

$$\mathbf{W} = g^a \cdot j^b \cdot \ldots \cdot h^n \;\; ; \;\; \mathbf{Y} = e^d \cdot f^g \cdot \ldots \cdot k^m$$

The procedures to find the "double" elements of ϕ_q are the same as those described before.

Having found a method to derive the square roots of a quadratic residue in ϕ_q and taking into account the comments made before, since **W** is the product of any grouping of powers of prime factors of q and **Y** the corresponding product of the remaining powers, we arrive at conclusion that the "double" elements of ϕ_q are as many as the ways to select into two disjoint sets a quantity of objects equal to the quantity of the prime factors present in the factorization of q.

The calculation of all possible combinations of n objects, is synthesized by the formula:

$$m = 2^n$$

In our case: n is the amount of the prime divisors of q, m is the quantity of the double elements of ϕ_q .

Now we can calculate the exact value of $\phi_q!$

As we already know, fixed whatever quadratic residue $\mathbf{a} \in \phi_q$ as the base, all of ϕ_q elements can be associated, some in pairs of inverse elements with respect to **a**, that is, such that the product of each of them is $c_1 \cdot c_2 \equiv \mathbf{a} \pmod{q}$, and the others, those who have themselves as **a**-symmetrical, in pairs of the form $(c\,;\,q-c)$, that is, such that the product of each of these is $c \cdot (q-c) \equiv -\mathbf{a} \pmod{q}$:

$$\phi_q! = (c_1 \cdot c_j) \cdot (c_2 \cdot c_t) \cdot \ldots \cdot [c_h \cdot (q - c_h)] \cdot \ldots \cdot [c_k \cdot (q - c_k)] \equiv a \cdot a \cdot \ldots \cdot (-a) \cdot \ldots \cdot (-a) \pmod{q}$$

As can be seen from the formula $m=2^n$, when the prime divisors of q are two or more than two, the pairs $(c\,;q-c)$ of "double" elements of ϕ_q are even in number, and more precisely: $m/2 = 2^{n-1}$ (n is the amount of the prime divisors of q).

For which:

$$[c_h \cdot (q - c_h)] \cdot \ldots \cdot [c_k \cdot (q - c_k)] \equiv (-a)^{2^{n-1}} \equiv a^{2^{n-1}} \pmod{q} \;, \; (n \geq 2 \text{ , because q is composite})$$

Consequently, the value of $\phi_q!$, relative to each base **a**, is given by the congruences:

$$\phi_q! \equiv \mathbf{a}^{\phi(q)/2} \equiv 1 \pmod{q} \;\; , \;\; \mathbf{a} \in \phi_q \;\; \text{quadratic residue , q odd composite}$$

As we have seen before, this same congruence is true even when choosing **a**=1 and also applies when choosing **a** non quadratic residue, to which, whatever $\mathbf{a} \in \phi_q$, we have:

$$\mathbf{a}^{\phi(q)/2} \equiv \mathbf{1} \pmod{q} \;\; , \;\; \mathbf{a} \in \phi_q \;\; , \;\; q \text{ odd composite}$$

Only if in formula $m=2^n$ arises n = 1, which happens when q is prime number, it will form a single pair $(c\,;q-c)$ to which corresponds the congruence $c \cdot (q-c) \equiv -\mathbf{a} \pmod{q}$.

This event determines the congruences, already found in my report that i entitled « From Wilson to Fermat » :

$$\mathbf{a}^{\phi(q)/2} \equiv -\phi_q! \equiv \mathbf{1} \pmod{q} \;, \; \mathbf{a} \in \phi_q \;\; \text{quadratic residue, other than 1, and q prime}$$

$$\mathbf{a}^{\phi(q)/2} \equiv \phi_q! \equiv \mathbf{-1} \pmod{q} \;, \; \mathbf{a} \in \phi_q \;\; \text{no quadratic residue and q prime}$$

For the calculation of the formula $m=2^n$, click "Combination ϕ"

How many quadratic residues are in the set ϕ_q

An immediate consequence of the theorem v-v is this:
given the composite number q, the quantity $\mathbf{r(\phi_q)}$ of quadratic residues of ϕ_q is:

$$\mathbf{r(\phi_q) = \phi(q)/2^n} \;\; , \;\; \text{n is the amount of the prime factors of q}$$

This is because each quadratic residue has 2^n square roots in ϕ_q .

For example, the amount of quadratic residues of the composite numbers 91, 105, 1155, 539, 1547 are:

$r(\phi_{91})=72/4=18$; $r(\phi_{105})=48/8=6$; $r(\phi_{1155})=480/16=30$; $r(\phi_{539})=420/4=105$; $r(\phi_{1547})=1152/8=144$