Definition. A set $\{r_1, r_2, \ldots, r_s\}$ of integers is called a *reduced residue system modulo* m if the r_i are relatively prime to m and pairwise incongruent modulo m, and if for each integer n relatively prime to m we have $n \equiv r_i \pmod{m}$ for some i, $1 \leq i \leq s$.

Definition. Let m be a natural number. $\phi(m)$ is defined to be the number of all $j \geq 1$ such that $j \leq m$ and $\gcd(j, m) = 1$.

ϕ is called the Euler phi function, also known as the *totient function*.

Lemma 1. *If distinct integers $r_1, r_2, \ldots, r_s$ form a reduced residue system mod m, then $s = \phi(m)$.*

Proof. The r_i are in 1–1 correspondence with the $\phi(m)$ positive numbers $\leq m$ coprime with m. □

Definition. A function f defined on the set of all positive integers is *multiplicative* if $f(mn) = f(m)f(n)$ whenever $\gcd(m, n) = 1$.

Proposition 2. *The Euler function ϕ is multiplicative.*

Proof. (Sketch.) If $\gcd(m, n) = 1$ and if x and y assume all values in a reduced system modulo m and n, respectively, then $nx + my$ assumes all values in a reduced residue system modulo mn. □

Corollary 3. *For any $m \geq 2$ we have $\phi(m) = m \prod(1 - 1/p)$ where the product is taken over all prime divisors of m.*

Proof. Observe that $\phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha(1 - 1/p)$ for any prime p. Use multiplicativity. □

Exercise 1. Calculate $\phi(3708)$.

Theorem 4 (L. Euler)**.** *If $m \geq 2$ and $\gcd(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod{m}$.*

Proof. Let $S = \{r_1, r_2, \ldots, r_{\phi(m)}\}$ be a reduced residue system mod m. Observe that aS is also a reduced residue system mod m, since for each r_i there exists a unique r_j such that $ar_i \equiv r_j \pmod{m}$. Therefore, $ar_1 ar_2 \ldots ar_{\phi(m)} \equiv r_1 r_2 \ldots r_{\phi(m)} \pmod{m}$, and hence $a^{\phi(m)} \equiv 1 \pmod{m}$. □

Note: All the results on the Euler phi function have a natural place in the setting of finite cyclic groups. We note the following facts for a finite cyclic group $G = \langle g \rangle$ of order n:

(1) G has $\phi(n)$ generators [they are the elements g^i with $\gcd(i, n) = 1$].
(2) A finite cyclic group of order n has a unique subgroup of order d for each divisor d of n; there are no other subgroups and they are all cyclic [this implies for example that $\sum_{d|n} \phi(d) = n$].
(3) If m, n are relatively prime and $G_1 = \langle g_1 \rangle, G_2 = \langle g_2 \rangle$ are cyclic groups of orders m, n respectively, then $G_1 \times G_2$ is a cyclic group of order mn. [This implies the multiplicativity of the Euler function.]
(4) If we denote by $\mathbb{Z}_n^*$ the set $\{i : 1 \leq i \leq n-1, \gcd(i, n) = 1\}$, then $\mathbb{Z}_n^*$ is a group (of order $\phi(n)$) under multiplication modulo n. Euler's Theorem above is an immediate consequence.

Exercise 2. Establish these connections in detail.

The following theorems can all be obtained from a good look (or rather: *two* good looks) at the factorial $(p-1)!$.

Theorem 5 (Fermat's Little Theorem)**.** *If p is a prime and $\gcd(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$.*

Proof. Note that a is congruent to one of the factors in $(p-1)! = 1 \cdot 2 \cdots (p-1)$, and that the products $a, 2a, \ldots, (p-1)a$ are congruent mod p to $1, 2, \ldots, p-1$ (in *some* order). Then

$$(p-1)! \equiv a \cdot 2a \cdots (p-1)a = a^{p-1}(p-1)! \pmod{p}.$$

Since $\gcd((p-1)!, p) = 1$, we can cancel the factorial term, and obtain $a^{p-1} \equiv 1 \pmod{p}$. (Wilson's theorem below gives the inverse of $(p-1)!$ explicitly, it is -1.) □

Exercise 3. Find a small integer which is congruent to 45^{90} modulo 17.

Exercise 4. Let p be a prime. Give an alternative proof of Fermat's Little Theorem as follows:

(1) Show that almost all binomial coefficients $\binom{p}{k}$ are divisible by p.
(2) Show that $(1 + \cdots + 1)^p \equiv (1 + \cdots + 1) \pmod{p}$ (induction).

Theorem 6 (Wilson's Theorem)**.** *If p is a prime then $(p-1)! \equiv -1 \pmod{p}$.*

Proof. Each factor in the product $(p-1)!$ has an inverse mod p. So we pair each factor with its inverse, replacing the product by 1. The only problem arises when there are factors which are their own inverses. $x = \bar{x}$ means $x^2 \equiv 1 \pmod{p}$ or $(x+1)(x-1) \equiv 0 \pmod{p}$, and thus the only such factors are 1 and -1. It follows that $(p-1)! \equiv -1 \pmod{p}$. □

Theorem 7 (Euler's Criterion)**.** *Let p be an odd prime, and $a \not\equiv 0 \pmod{p}$. Then a is a square modulo p (i.e. the congruence $x^2 \equiv a \pmod{p}$ has a solution) if and only if $a^{(p-1)/2} \equiv 1 \pmod{p}$.*

Proof. For each factor a in the product $(p-1)!$ we can find another factor $\tilde{x}$ such that $x\tilde{x} \equiv a \pmod{p}$. Now pair the factors of $(p-1)!$ in this way as $x, \tilde{x}$, so the product of each such pair equals a. Problems arise if a is a square, say $a = (\pm z)^2$.

Case 1: If $a = z^2$ we can pair up only $p-3$ of the factors in $(p-1)!$:

$$(p-1)! = a \cdot a \cdots \cdot a \cdot z \cdot (-z) \equiv a^{(p-3)/2} a \cdot (-1) \pmod{p}.$$

Using Wilson's theorem we now have $a^{(p-1)/2} \equiv 1 \pmod{p}$.

Case 2: If a is not a square, then all the $p-1$ factors in $(p-1)!$ can be paired up, and we obtain $a^{(p-1)/2} \equiv -1 \pmod{p}$, using Wilson's theorem as before. □

Note that one can 'strengthen' this theorem to say that an integer n is a prime if and only if n divides $(n-1)! + 1$. (But this is not useful for primality testing!)

Exercise 5. Give an alternative proof of Euler's Criterion, using the fact that if p is a prime, then $\mathbb{Z}_p^*$ is a cyclic group.

Corollary 8. *Let p be an odd prime. The congruence $x^2 \equiv -1 \pmod{p}$ has a solution if and only if $p \equiv 1 \pmod{4}$.*

Proof. Apply Euler's criterion: -1 is a square modulo p if and only if $(-1)^{(p-1)/2} \equiv 1 \pmod{p}$. This means that -1 is a square modulo p if and only if $(p-1)/2$ is even, i.e. if and only if $p \equiv 1 \pmod{4}$. □

GAP Commands:

`PrimeResidues(20)` will return a list of all integers from 1 to 19 which are relatively prime to 20 (and which have therefore an inverse modulo 20). The total number of such integers is called $\phi(20)$, and can be obtained in GAP with the command `Phi(20)`.