1 Fermat's little theorem

1.0.1 Remainders

When dividing with the prime number p you will get p-1 possible remainders:

$$1, 2, 3, ..., p-1$$

What about the products:

$$1 \cdot a, 2 \cdot a, 3 \cdot a, ..., (p-1) \cdot a$$

Where a do not have a divisor in common with p greater than 1.
When we divide these products with p, we will get remainders from the list above. But will we get all - only in another order? Well when 2 or more products have the same remainders, we will miss one or more remainders in the list.
But we can prove this to be wrong, prove that all the products have different remainders
Let us imagine, we have 2 products: $m \cdot a$ and $n \cdot a$, which we have found to have the same remainders: r.

$$m < n <= (p-1)$$

$$m \cdot a = s \cdot p + r$$

$$n \cdot a = t \cdot p + r$$

We subtract the left sides and the right sides of the 2 products and get:

$$(n-m) \cdot a = (t-s) \cdot p$$

As a cannot be divided with p, the prime number p must be a factor in $(n-m)$: $u \cdot p$ (u being a natural number).
In the same way on the right side: a cannot be a factor in the prime number p but must be a factor in $(t-s)$: $v \cdot a$ (v being a natural number). We get

$$u \cdot p \cdot a = v \cdot a \cdot p$$

and

$$u = v$$

$$(n-m) = u \cdot p$$

$$n = u \cdot p + m$$

But n was supposed to be smaller than p.
We have a contradiction.
We conclude all our $(p-1)$ products have different remainders.
Now we multiplies all these $(p-1)$ products:

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

After dividing all these products with p we gets this product of remainders though not in this order

$$1 \cdot 2 \cdot 3 \cdots (p-1)$$

but the order of the factors in a product does not alter the result.

Remembering that $b \cdot c$ has the same remainder after being divided with p as the remainders of b and c multiplied and then divided with p
We can write

$$1 \cdot a \cdot 2 \cdot a \cdot 3 \cdot a \cdots (p-1) \cdot a = a^{p-1} \cdot 1 \cdot 2 \cdot 3 \cdots (p-1)$$

$a^{p-1} \cdot 1 \cdot (2 \cdot 3 \cdots (p-1))$ and $1 \cdot (2 \cdot 3 \cdots (p-1))$
has the same remainder after being divided with p

$a^{p-1} \cdot 1$ **has the remainder** 1 **after being divided with the prime number** p.
Which was to be demonstrated.

2 Euler's theorem

Could we pull this trick off again with other numbers than prime numbers. Yes Euler showed, that to every natural number, prime or not: n, there will always be a natural number depending on n: $\varphi(n)$, so that $a^{\varphi(n)}$ has the remainder 1 after being divided with n, a being a natural number and having no common factor (divisor) with n.

Again we start with this list of remainders after dividing with n:

$$1, 2, 3, ..., (n-1)$$

But now, if n is not a prime number, we must remove some of them. If p and q are prime factors in n, we must remove not only p and q but all the

numbers in the list: say $3 \cdot p$, which are products of them and smaller than or equal to $(n-1)$
The number of permitted remainders is $(n-1)$ when n is a prime number p, but otherwise it is smaller often much smaller than $(n-1)$
We shall call the number of permitted remainders: $\varphi(n)$.

Again we shall multiply all the permitted remainders with a, and gets $\varphi(n)$ not $(n-1)$ products and ask, if we divide these products with n, shall we get the same permitted remainders though not in the same order?
We do have 2 problems hier:

1. Do not-permitted remainders appear in our new list of remainders after dividing our products: $a \cdot r$, (r being a permitted remainder)?

2. Do any (though permitted) remainder appear more than one time?

Let's say, after factoring n we have found the prime factor p and as explained above, remainders with such factors are removed from the list of the permitted remainders, and we must not choose an a with a common divisor with n greater than 1.
Either our a is in our list of permitted remainders, and is no product of p, or it is greater than n and can be written as a sum of a natural number and a fraction of n, which cannot be reduced, because they have no common divisor greater than 1.
a is greater than n gives only permitted remainders, otherwise we have a contradiction

$$\frac{a}{n} = s + \frac{t \cdot p}{n}$$

s and t being natural numbers

$$a = s \cdot n + t \cdot p$$

But p is a prime factor in n.
n can be written as a product $u \cdot p$, where u is a natural number.

$$a = s \cdot u \cdot p + t \cdot p$$

$$a = p \cdot (s \cdot u + t]$$

which contradicts, that a do not have divisors: (p) greater than 1 in common with n.
We can conlude, that

$$a = s \cdot n + r$$

s being a natural number or zero, and r being a permitted remainder.
What about the products $a \cdot r$?
Well

$$a \cdot r = s \cdot n \cdot r + r_1 \cdot r$$

r and r_1 being 2 different or identical permitted remainders. We divide the last product $r \cdot r_1$ with n and get $\frac{r \cdot r_1}{n}$

$$\frac{r \cdot r_1}{n} = t + \frac{r_2}{n}$$

Where t is a natural number or zero. We mutiply the equation with n and get

$$r \cdot r_1 = t \cdot n + r_2$$

Is r_2 a permitted remainder?
Yes, because if not, it has a divisor p in commen with n ($n = p \cdot u$ and $r_2 = p \cdot v$, u and v being natural numbers), and we can write:

$$r \cdot r_1 = t \cdot u \cdot p + v \cdot p$$

$$r \cdot r_1 = p \cdot (t \cdot u + v)$$

But this is a contradiction, because r and r_1 are permitted remainders. They have no devisors (p) in common with n. We can conclude r_2 is a permitted remainder

$$a \cdot r = s \cdot n \cdot r + r_1 \cdot r$$

and

$$r \cdot r_1 = t \cdot n + r_2$$

implies

$$a \cdot r = s \cdot n \cdot r + t \cdot n + r_2$$

or

$$a \cdot r = n \cdot (s \cdot r + t) + r_2$$

So at last $a \cdot r$ has a permitted remainder after being divided with n.
Which was to be demonstrated.

Then we must address the second problem:

2. Do any (though permitted) remainder appear more than one time?
When dividing with the number p (a prime number), you will get $(p - 1)$ remainders:

$$1, 2, 3, ..., (p - 1)$$

When dividing with a number n (not being a prime number), you will get fewer than $(n-1]$ remainders, because we do not want those with a common divisor with n greater than 1.
You will only get $\varphi(n)$.
We could write this list so:

$$1, b, c, ..., (n-1)$$

b, c and so on being permitted remainders.
What about the products: We have seen that the remainders after dividing the $\varphi(n)$ products with n:

$$1 \cdot a, b \cdot a, c \cdot a, ..., (n-1) \cdot a$$

are all permitted remainders.

But will we get all - only in another order?
Well, if 2 or more products have the same remainders, we will miss one or more remainders in the list.
But we can prove this to be wrong, prove that all the products have different remainders.
Let us imagine, we have 2 products: $k \cdot a$ and $l \cdot a$, which we have found to have the same remainders: r (k, l, s and t being natural numbers).

$$k < l <= (n-1)$$

$$k \cdot a = s \cdot n + r$$

$$l \cdot a = t \cdot n + r$$

We subtract the left sides and the right sides of the 2 products and get:

$$(l-k) \cdot a = (t-s) \cdot n$$

As a cannot be divided with n, the number n must be a factor in $(l-k)$: $u \cdot n$ (u being a natural number).
In the same way on the right side: a cannot be a factor in the number n but must be a factor in $(t-s)$: $v \cdot a$ (v being a natural number). We get

$$u \cdot n \cdot a = v \cdot a \cdot n$$

and

$$u = v$$

$$(l-k) = u \cdot n$$

$$l = u \cdot n + k$$

But l was supposed to be smaller than $(n-1)$.
We have a contradiction.
We conclude all our permitted products have different remainders.
Now we multiply all these $\varphi(n)$ products:

$$1 \cdot a \cdot b \cdot a \cdot c \cdot a \cdots (n-1) \cdot a$$

After dividing all these products with n we gets this product of remainders though not in this order

$$1 \cdot b \cdot c \cdots (n-1)$$

but the order of the factors in a product does not alter the result.

Remembering that $b \cdot c$ has the same remainder after being divided with n as the remainders of b and c multiplied and then divided with n
We can write

$$1 \cdot a \cdot b \cdot a \cdot c \cdot a \cdots (n-1) \cdot a = a^{\varphi(n)} \cdot 1 \cdot b \cdot c \cdots (n-1)$$

$a^{\varphi(n)} \cdot 1 \cdot (b \cdot c \cdots (n-1))$ and $1 \cdot (b \cdot c \cdots (n-1))$
has the same remainder after being divided with n

$a^{\varphi(n)} \cdot 1$ **has the remainder** 1 **after being divided with the number** n.

Which was to be demonstrated.

2.1 n is the product of the 2 prime number p and q

We can easily calculate $\varphi(n)$, when $n = p \cdot q$, p and q being prime numbers.
We get $n - 1 = p \cdot q - 1$ remainders, when we divide with n.
We discard products of p:
$1 \cdot p, 2 \cdot p, 3 \cdot p, \cdots, (q-1) \cdot p$ that will make $q-1$ remainders to be excluded from the list.
and products of q: $1 \cdot q, 2 \cdot q, 3 \cdot q, \cdots, (p-1) \cdot q$ that will make $p-1$ remainders to be excluded from the list.
We end up with
$\varphi(n) = (p \cdot q - 1) - (q-1) - (p-1) = (p-1) \cdot (q-1)$
remainders.