Demonstration and method of the 1st primality Test/Sieve by VincS

We are in the domain of natural numbers excluding ***0***. We can say that our test is similar to the Wilson's one but it is more similar to a sieve such as the Eratosthenes one.

As stated by some of the more recent definitions: *"In mathematics, a prime number (for short **prime**) is a natural number greater than 1 that is divisible only by 1 and itself." (from Wikipedia)*

Let x be the number of which we want to test the primality. Let p_i be only prime numbers. Let's define P_k as the multiplication (product of sequence) of all primes less than x also known as the ***primorial*** *(symbol #)* of $(x-1)$ ...

$$P_k = \prod_{i=1}^{k} p_i = (x-1)\# \qquad [1]$$

... such that ...

$$p_k < x \leq p_{k+1} \qquad [2]$$

In practice, the test consists to find out if x is equal to p_{k+1} and so if x is or is NOT the next prime number. All this without, in practice, to know the value of p_{k+1}. Example: Using our test/sieve, and having already concluded that 2,3,5 and 7 are all prime numbers, with the product ... $P_3 = 2 \cdot 3 \cdot 5$ ... we can show that 6 is a composite number and 7 is the prime number next to 5. To know the next composite numbers and find the next prime number we have to use (like a sieve) the product ... $P_4 = 2 \cdot 3 \cdot 5 \cdot 7$.

Let q be the remainder of P_k **divided by** x such as ...

$$P_k \equiv q \pmod{x} \qquad [3]$$

... and we can also write, using the operator **mod**ule, ...

$$q = P_k \bmod x \qquad [4]$$

We can catalog the remainder q in three simple types that will help us determine if we can say immediately that x is composite or it's a prime number or otherwise is necessary to investigate further:

A. *q=0*
B. *q≠0* e *q≠1*
C. *q=1*

A. If *q=0*, x **is composite**!

Demonstration:
if the remainder of P_k/x is equal to *0*, it's also implicitly shown that x is a number composite by the product of some of the primes that build the product P_k, all with exponent equal to 1 (otherwise the denominator would be reduced to 1), and so x is NOT a prime number! x cannot be constituted by only one of the primes forming P_k for the meaning of x and P_k that we stated at the begin of demonstration.

For example:
$x = 6$ ... and so ... $P_3 = 2 \cdot 3 \cdot 5 = 30$ ... and so ...
$q = 30 \ mod \ 6 = 0$ ... and so ... x is composite!

B. If $q \neq 0$ and $q \neq 1$, we can make the initial assumption that x is composite and then, if it is not by exclusion, come to the conclusion proved that x is prime! Let's see how.

Note: let's discard, by this type of remainder, also *q=1* for convenience of demonstration as we will come to demonstrate, for exclusion from the previous cases, that, if *q=1*, then x must be necessarily a prime number.

To check if x is a composite number (obviously in different way how described in A. being precisely that we exclude $q \neq 0$) is sufficient to reiterate the following (let's define j as index of iterations and ω as the maximum number of iterations provided to conclude that x is a prime number), placing at start that $t_{j=0}=q$, ...

$$t_{j+1} = [q \cdot t_j] \bmod x \qquad [5]$$

... till one of this following occurences happens:

1. $t_{j+1}=0$
2. t_{j+1} *is equal to one of the previously calculated* t_j
3. $t_{j+1}=1$
4. $j>\omega$

Note: to speed up the search for primality proof maybe we'll see that we can also reiterate (replacing the [5]), always placing at start $t_{j=0}=q$ ...

$$t_{j+1} = [t_j \cdot t_j] \bmod x \qquad [6]$$

... and maintaining the same final considerations. We will not cover this formula in this context except for some hints.
So, when we will refer to t_{j+1}, we will always speak about that defined in the [5].

1. $t_{j+1}=0$ and so x **is a composite number**!

Demonstration:
in the case that the recurrence will end with $t_{j+1}=0$, to demonstrate that x is a composite number is sufficient to prove that the remainder q in the [5] is a multiple of the primes components of x and so we have to prove that ...

$$q = r \cdot p_c \cdots p_d \cdots p_f \qquad [7]$$

... where $p_c \cdots p_d \cdots p_f$ are the prime numbers components of x while r is an integer of any value that we will not consider at the moment even if it may hide some surprises.

For our demonstration we will take the case of the completest composition of x (which represents all possible types of factorization) in which one of the prime numbers, which we will call p_c, has exponent 1 while mentre $p_d{}^u \cdots p_f{}^z$, let's suppose with $1<u<z$, represent a group of prime numbers that contribute to compose x precisely with exponent greater than 1. This

demonstration is still valid in all subspecies of composition of x as, for example, the absence of the prime with an exponent equal to 1 or the presence of many of them (all represented by da p_c) and/or the presence of only one the primes with exponent greater than 1 (minimum condition necessary for having a remainder ≠ 0 otherwise it falls in the type of remainder described in A.).

And so let's take …

$$x = (p_c \cdot {p_d}^u \cdots {p_f}^z) \qquad [8]$$

To calculate the remainder q let's go throught the fraction …

$$\frac{P_k}{x} = \frac{p_1 \cdots p_c \cdot p_d \cdots p_f \cdots p_k}{p_c \cdot {p_d}^u \cdots {p_f}^z} \qquad [9]$$

… and it's clear that the best reduction to minimum terms that we can do is .....

$$\frac{{P_k}/{(p_c \cdot p_d \cdots p_f)}}{{x}/{(p_c \cdot p_d \cdots p_f)}} = \frac{p_1 \cdots \cdots p_k}{{p_u}^{u-1} \cdots {p_f}^{z-1}} \qquad [10]$$

The result of this division of integers will be surely fractional with remainder ≠ 0. In fact, all the terms in the numerator are coprime with exponent equal to 1, we have reduced to minimum terms and we have defined that at least one of the terms in the denominator has exponent greater than 1.

So we can also write …

$$p_1 \cdots \cdots p_k = G_I \cdot ({p_d}^{u-1} \cdots {p_f}^{z-1}) + G_F \cdot ({p_d}^{u-1} \cdots {p_f}^{z-1}) \qquad [11]$$

… where …
… G_I is the integer part of the division result …
… G_F is the fractional part (0,.....) of the division result …
… while the others are all well known.

Let's define R_R as the "reduced remainder" of the division that so will be equal to …

$$R_R = G_F \cdot (p_d{}^{u-1} \cdots p_f{}^{z-1}) \qquad [12]$$

If the [10] has a fractional result so also the [9] will have a fractional result and so, in the same way, we can write …

$$p_1 \cdots p_c \cdot p_d \cdots p_f \cdots p_k = G_I \cdot (p_c \cdot p_d{}^{u} \cdots p_f{}^{z}) + G_F \ (p_c \cdot p_d{}^{u} \cdots p_f{}^{z}) \qquad [13]$$

… where …
… G_I is, as above, the integer part of the division result …
… G_F is, as above, the fractional part (0,…..) of the division result …
… while the others are all well known.

Let's define R_P as the "full remainder" of the division that so will be equal to … …

$$R_P = G_F \cdot (p_c \cdot p_d{}^{u} \cdots p_f{}^{z}) \qquad [14]$$

If now we divide the [14] by the [12] we will get …

$$\frac{R_P}{R_R} = \frac{G_F \cdot (p_c \cdot p_d{}^{u} \cdots p_f{}^{z})}{G_F \cdot (p_d{}^{u-1} \cdots p_f{}^{z-1})} \qquad [15]$$

… and so …

$$R_P = R_R \cdot p_c \cdot p_d \cdots p_f \qquad [16]$$

Doing the logic parallelism, so that $R_P=q$ and $R_R=r$, the [16] demonstrates that the hypotheses expressed in [7] is true.

It's easy to demonstrate that it is sufficient to reiterate $z-1$ times the [5], using the [7], to obtain $t_{j+1}=0$, thus demonstrating that x is a composite number! In fact, after having reitered $z-1$ times, we obtain (without

resorting to the module but still keeping well in mind the invariance of the module towards the operations of multiplication and, consequently, of exponentiation) ...

$$q^z = (r^z \cdot \ {p_c}^{z-1} \cdot {p_d}^{z-u}) \cdot (\boldsymbol{p_c} \cdot \boldsymbol{p_d}^{\boldsymbol{u}} \cdots \boldsymbol{p_f}^{\boldsymbol{z}}) \qquad [17]$$

... and so ...

$$q^z = (r^z \cdot \ {p_c}^{z-1} \cdot {p_d}^{z-u} \cdots) \cdot \boldsymbol{x} \qquad [18]$$

... and concluding ...

$$\boldsymbol{t_{j+1}} = q^z \ mod \ x = \boldsymbol{0} \qquad [19]$$

It's also easy to prove that if, in the previous from [7] to [18], we replace $\boldsymbol{p_c}$ with the product of two or more primes $\boldsymbol{p_m \cdots p_v}$, the validity of expressions and conclusions do not change.

It's clear the analogy with the Gauss clock having a dial made of $[\boldsymbol{p_c} \cdot \boldsymbol{p_d}^{\boldsymbol{u}} \cdot \boldsymbol{p_f}^{\boldsymbol{z}}]$ hours [equal to x]. In fact, after the reiteration, it's like to start and move the needle lancetta $[\boldsymbol{r^z} \cdot \ \boldsymbol{p_c}^{\boldsymbol{z-1}} \cdot \boldsymbol{p_d}^{\boldsymbol{z-u}} \cdots]$ times throught the hour 0=$\boldsymbol{x}$ (zero equal to $\boldsymbol{x}$) returning always at the end on the hour 0=$\boldsymbol{x}$ (zero equal to $\boldsymbol{x}$). With this demonstration is clear that we can also use also the [6] to perform fewer iterations (in the future we will discuss more deeply this analysis).

Note: we will speak in the future and in a separate analysis about the irreducible part of the remainder ($\boldsymbol{r}$ in the [7]). We will see if it's possible to predict the value and other similar considerations that do not affect the validity of this theorem but can only enrich it.

Summarizing, we can say that we have faced **all** the cases where $\boldsymbol{x}$ can be a composite number. We have also demonstrated the methods that allowed us to be sure of this.
Starting from the calculation of the remainder $\boldsymbol{q}$ in the [4]:

- with A. , where $q=0$, we have shown that x is a composite number made of the product of some of the primes that build even P_k, all with exponent **equal to 1**;
- with B.1. we started with $q \neq 0$ **and** $\neq 1$ and, by reiterating the [5] till to obtain $t_{j+1}=0$, we have shown that x is a composite number consisting of the product of some of the primes that build even P_k, of which some or all with exponent **greater than 1**.

Having used this order, from here onwards, we demonstrate by exclusion the remaining cases in which x is definitely a prime number.

2. t_{j+1} ***is equal to one of the previously calculated*** t_j and then we block the infinite iteration because we have recognized in advance a domain of integrity as will be explained later in B.4.; in which case x **is a prime number!**

3. $t_{j+1}=1$ and then we block the infinite iteration because we have recognized in advance a domain of integrity as will be explained later in B.4.; in which case x **is a prime number!**

Additional demonstration:
if the remainder q is a multiple of some of the primes that build P_k and supposing that x is a composite number, the result of any iteration of [5] cannot be less than any of the primes above. Being the smallest prime equal to 2, we come to conclude that, if $t_{j+1}=1$, then x **is necessarily prime!**

4. $j>\omega$ and, since we have carried out a number of iterations exceeding the foreseeable without reaching any of the previous cases, then x **is a prime number!**

Demonstration:
the proof that x **is a prime number** if iterations last forever is not necessary because you may just take any book of algebra (we quote Wikipedia) to read it.

From … http://en.wikipedia.org/wiki/Integral_domain …“ An integral domain is a commutative ring with identity in which the product of any two nonzero elements is not (never) equal to zero.” ... and following link from ... http://en.wikipedia.org/wiki/Zero-product_property ... " In the branch of mathematics called algebra, the **zero-product property** states that the product of two nonzero elements is (always) nonzero." ... and more ... "If p is a prime number, then the ring of integers modulo p has the zero-product property (in fact, it is a field)."

These quotes are enough to state that, if x **is a prime number**, the cycle of reiteration in the [5] or in the [6] goes on and on without ever coming to $t_{j+1}=0$. But how many iterations do we need before we can say for sure that we have fallen into an integral domain? We assert that it's possible to calculate the maximum number of iterations to be performed (different in the [5] than in the [6]) and it's therefore possible to truncate at a certain point the cycle stating that x is prime. In fact, the worst case scenario that we can foresee is that x is composed solely by an exponentiation z of 2 (3 if we discard the test of x even) and therefore the maximum number of iterations we expect is $\log_2 x$ ($\log_3 x$ if we discard the test of x even). This in the case that we use the [5] but even less in the case of the [6]!

C. If $q=1$, then x **is prime**!

Demonstration:
by exclusion, after that we have proven by A. and B.1. that, if x is a composite number, the remainder q of the division P_k/x is immediately 0 or contains, in its composition, all prime factors of x. Since the smallest prime factor that can occur is 2, it's therefore proven that, if $q=1$, x is NOT a composite number and then x is prime! This case is similar to the additional proof of B.3..

For example:
$x = 11$ … and so … $P_4 = 2 \cdot 3 \cdot 5 \cdot 7 = 210$ … and so …
$q = 210 \ mod \ 11 = 1$ … then x is prime!

In conclusion, the **1st primality test by VincS** shows that it is possible to construct a sieve of consequential prime numbers knowing only that the smallest prime number is *2*.