INTRODUCTION TO A NEW TOOL : THE ANTIORDER

By R. LIFCHITZ [1]

August 2000 (last update : 22 Dec 2000)

1 Definitions :

e is said to be the order of $b \pmod n$ if e is the least positive integer such that $b^e \equiv 1 \pmod n$. Of the same maneer, we can define the number a, which is the least positive integer such that $b^a \equiv -1 \pmod n$. We will call this number a the antiorder of $b \pmod n$.

The antiorder has got many properties, some are in common with the order.

In this article, $\left(\frac{b}{n}\right)$ stands for the Legendre symbol (if n is prime) or for the Jacobi symbol (if n is not necessarily prime). Note that both of them are defined if n is odd.

2 Theorems :

1°) **If** $gcd(b,n) > 1$ **then** a **doesn't exist.**

Proof : Suppose a exists with $gcd(b,n) = d$, we have $n.Q - b^a = 1$ with $d \mid n$ and $d \mid b \Longrightarrow d \mid 1$ (contradiction with $d > 1$).

2°) **If** $gcd(b,n) = 1$ **then** a **doesn't always exist.**

Proof : Just take an example : $b = 2$ and $n = 7$.

If $0 \leq m \leq 6$, $2^m \neq -1 \pmod 7$.

3°) **If** a **exists then** $a < e$**.**

Proof : Suppose $e \leq a$ then $e = a - r$ for a r $(0 \leq r \leq a-1)$, so $b^e = b^{a-r}$, $b^e \equiv b^{a-r} \pmod n$, $b^e.b^r \equiv b^a \pmod n$, and by definition of e and a, $b^r \equiv -1 \pmod n$. But $r \leq a - 1$, so a isn't the antiorder (contradiction).

4°) **If** $b^{a'} \equiv -1$ **(mod** n**) then** a **exists and** $a' = (2k+1).a$**.**

Proof : Suppose a doesn't divide a' : $a' = a.q + r$ with $0 < r < a$. So $b^{a'} \equiv b^{a.q+r} \pmod n \Longrightarrow -1 \equiv (-1)^q.b^r \pmod n$.

If q is even $\Longrightarrow b^r \equiv -1 \pmod n \Longrightarrow$ contradiction because $r < a$.

[1] Student at University of PARIS VI (Jussieu) : **RenaudL@itineris.net**

If q is odd $\Longrightarrow b^r \equiv 1 \pmod{n} \Longrightarrow$ contradiction because $r < a$ and 3°) aren't possible.

$\Longrightarrow a$ divides a' and since $a' = 2k.a$ isn't possible, we have $a' = (2k+1).a$.

5°) **If a exists then $a = \frac{e}{2}$.**

Proof : By 3°) , $a < e$ so $e = a + r$ with $r > 0$. If $e < 2a$ was true, we would have $e = a + r$ with $1 \leq r \leq a - 1$ so $b^e \equiv b^{a+r} \pmod{n} \Longrightarrow b^r \equiv -1 \pmod{n}$, which is a contradiction because a is the antiorder. Then, $2a \leq e$. If $2a < e$ was true, we would have $2a = e - r$ with $0 < r < e$, so $b^{2a} \equiv b^{e-r} \pmod{n}$, $b^r \equiv b^e \pmod{n}$, $b^r \equiv 1 \pmod{n}$ with $r < e$ which is another contradiction (e is the order). It follows that $e = 2a$.

6°) **If a exists and n is prime then $a \mid (n-1)$.**

Proof : Since a exists, $a = \frac{e}{2}$ (by 5°)). n is prime so $e \mid (n-1) \Longrightarrow a \mid (n-1)$.

7°) **If e is odd then a doesn't exist.**

Proof : Equivalent to the contrapositive of 5°) .

8°) **If n is prime and $\left(\frac{b}{n}\right) = -1$ then a exists.**

Proof : If $\left(\frac{b}{n}\right) \neq 0$ then $gcd(b, n) = 1$ so, because n is prime, by Fermat little theorem, $b^{n-1} \equiv 1 \pmod{n}$. But $\left(\frac{b}{n}\right) = -1$, so $b^{\frac{n-1}{2}} \equiv -1 \pmod{n}$. And by 4°) , a exists.

9°) **If e is even and a doesn't exist then n is composite. Moreover, gcd($b^{\frac{e}{2}} + 1$, n), gcd($b^{\frac{e}{2}} - 1$, n) are two non-trivial factors of n.**

Proof : If n was prime, the square root of 1 modulo n could either be 1 or -1. We have $b^e \equiv 1 \pmod{n}$ with $e = 2e'$, so $b^{2e'} \equiv 1 \pmod{n} \Longrightarrow b^{e'} \equiv 1$ or $-1 \pmod{n}$. But $b^{e'} \pmod{n}$ can't be 1 (e wouldn't be the order) and can't be -1 (because a doesn't exist). Then, $b^{e'} \pmod{n}$, which is a square root of 1 $(\text{mod } n)$ is different from 1 and $-1 \Longrightarrow n$ is composite. Moreover, since $b^e \equiv 1 \pmod{n}$ with $e = 2e'$, we have $b^{2e'} - 1 \equiv 0 \pmod{n} \Longrightarrow (b^{e'} - 1).(b^{e'} + 1) \equiv 0 \pmod{n}$. Because n doesn't divide $(b^{e'} + 1)$ nor $(b^{e'} - 1)$, $gcd(b^{e'} + 1, n)$ and $gcd(b^{e'} - 1, n)$ are different from 1 and n : they are non-trivial factors of n.

10°) **If n is prime and e is even then a exists and $a = \frac{e}{2}$.**

Proof : We have $b^e \equiv 1 \pmod{n}$ with $e = 2.e'$, so $b^{e'} \equiv \pm 1 \pmod{n}$ because n is prime (1 and -1 are the only possible values of the square root of 1 $(\text{mod } p)$). But the square root can't be 1 (e wouldn't be the order), so it is $-1 \Longrightarrow b^{e'} \equiv -1 \pmod{n}$. By 4°) , this proves that a exists, so by 5°) , $a = \frac{e}{2}$.

11°) **If $\left(\frac{b}{n}\right) = 1$ and $\left(\frac{-1}{n}\right) = -1$ then a doesn't exists.**

Proof : Suppose a exists. We have $b^a \equiv -1 \pmod{n}$, so we have $\left(\frac{b^a}{n}\right) = \left(\frac{-1}{n}\right) \Longrightarrow \left(\frac{b}{n}\right)^a = \left(\frac{-1}{n}\right) \Longrightarrow 1 = -1$ which is a contradiction. So a doesn't exists.

12°) **Let p^β be the greatest prime power dividing m ($\beta > 0$). If $b^m \equiv -1$ (mod n), and $b^{\frac{m}{p}} \neq -1$ (mod n) then p^β divides a.**

Proof :

By 4°) , $m = (2k+1).a$ with $p \mid m \Longrightarrow p \mid (2k+1)$ or $p \mid a$ because p is prime. Suppose $p \mid (2k+1)$, so we have $b^{\frac{m}{p}} \equiv b^{a \cdot \frac{2k+1}{p}} \equiv (b^a)^{\frac{2k+1}{p}} \equiv (-1)^{\frac{2k+1}{p}} \equiv -1 \pmod{n}$ which is a contradiction with our hypothesis ($b^{\frac{m}{p}} \neq -1 \pmod{n}$). It follows that $p^\beta \mid m$ but p doesn't divide $2k+1$ so $p^\beta \mid a$.

13°) **Let $b = 273$.**

If $M_p = 2^p - 1$ ($p > 3$) is prime then the order of b (mod M_p) is odd.

If $N_p = \frac{2^p+1}{3}$ ($p > 3$) is prime then the order of b (mod N_p) is odd.

Proof :
$\left(\frac{-1}{M_p}\right) = (-1)^{(M_p-1)/2} = (-1)^{2^{p-1}-1} = -1$
and $\left(\frac{273}{M_p}\right) = (-1)^{(273-1).(M_p-1)/4}.\left(\frac{M_p}{273}\right) = (-1)^{68.(M_p-1)}.\left(\frac{M_p}{273}\right) = \left(\frac{M_p}{273}\right)$.

Because $p \equiv 1, 5, 7, 11 \pmod{12}$ and because the order of 2 (mod 273) is 12, $2^p \equiv 2^1, 2^5, 2^7, 2^{11} \equiv 2, 32, 128, 137 \pmod{273}$, so $2^p - 1 \equiv 1, 31, 127, 136 \pmod{273}$. So $\left(\frac{M_p}{273}\right) = \left(\frac{1}{273}\right)$ or $\left(\frac{M_p}{273}\right) = \left(\frac{31}{273}\right)$ or $\left(\frac{M_p}{273}\right) = \left(\frac{127}{273}\right)$ or $\left(\frac{M_p}{273}\right) = \left(\frac{136}{273}\right)$, but $\left(\frac{1}{273}\right) = \left(\frac{31}{273}\right) = \left(\frac{127}{273}\right) = \left(\frac{136}{273}\right) = 1$, so $\left(\frac{273}{M_p}\right) = 1$. By theorem 11°) , a doesn't exist, so, if e was even, M_p would be composite (theorem 9°)), which is a contradiction with our hypothesis (M_p prime). It follows that e is odd.

The proof is very similar for $N_p = \frac{2^p+1}{3}$.

14°) **Let $n-1 = 2^{\beta_0}.p_1^{\beta_1}...p_i^{\beta_i}$ be the prime factorization of $n-1$. If there exist b such that $b^{\frac{n-1}{2}} \equiv -1 \pmod{n}$ and if for each p_i we have $b^{\frac{n-1}{2.p_i}} \neq -1 \pmod{n}$ then n is prime.**

Proof : The first condition implies that a exists (theorem 4°)). The second condition implies by theorem 12°) that $p_1^{\beta_1}$, $p_2^{\beta_2}$, ...,$p_i^{\beta_i}$ divide a but they are relatively prime to each other, so $a = k.p_1^{\beta_1}...p_i^{\beta_i}$. Moreover, the first condition implies that $e = 2^{\beta_0}.k'$ but by theorem 5°) , $e = 2.a$, so $a = 2^{\beta_0-1}.k' \Longrightarrow a = k''.2^{\beta_0-1}.p_1^{\beta_1}...p_i^{\beta_i} = k''.\frac{n-1}{2}$. But $k'' < 2$ by the first condition and 3°) (and because $e \leq n-1$), so $a = \frac{n-1}{2} \Longrightarrow e = n-1$, which proves that n is prime.

Remarks : This test is a little bit faster than the classical Lucas-Brillhart-Selfridge N-1 test because it requires one step less by prime factor (a square and a reduction modulo n).

15°) **If $\left(\frac{b}{n}\right) = -1$ and a doesn't exist then n is composite.**

Proof : Equivalent to the contrapositive of 8°) .

16°) **If $\left(\frac{b}{n}\right) = -1$ then e is even.**

Proof : If $\left(\frac{b}{n}\right) = -1$ then $gcd(b, n) = 1$ so e exists. Let $b^e \equiv 1 \pmod{n}$. This implies $\left(\frac{b^e}{n}\right) = \left(\frac{1}{n}\right)$, $\left(\frac{b}{n}\right)^e = 1$, $(-1)^e = 1$, which implies that e is even.

17°) **If $\left(\frac{b}{n}\right) = -1$, $\left(\frac{-1}{n}\right) = -1$ and a exists then a is odd.**

Proof : $b^a \equiv -1 \pmod{n} \Longrightarrow \left(\frac{b^a}{n}\right) = \left(\frac{-1}{n}\right) \Longrightarrow \left(\frac{b}{n}\right)^a = -1 \Longrightarrow (-1)^a = -1$. It follows that a is odd.

18°) **If n is prime and a doesn't exist then e is odd.**

Proof : Suppose n is prime, a doesn't exist and e is even. There is a contradiction with 10°) , so e is odd.

3 The form of the order and the antiorder

Using the above theorems, sometimes we will be able to know the form of the order or the antiorder. Here are two tables.

• If $\left(\frac{-1}{n}\right) = -1$ then :

	$\left(\frac{b}{n}\right) = -1$	$\left(\frac{b}{n}\right) = 1$
n prime	$e = 4k+2$ $a = 2k+1$	$e = 2k+1$ a doesn't exist
n composite	$e = 2k$ Moreover, if a exists : - $a = 2k'+1$ - $e = 4k'+2$	Nothing about e a doesn't exist

• If $\left(\frac{-1}{n}\right) = 1$ then :

	$\left(\frac{b}{n}\right) = -1$	$\left(\frac{b}{n}\right) = 1$
n prime	$e = 4k$ $a = 2k$	Nothing about e Nothing about a
n composite	$e = 2k$ Moreover, if a exists : - $a = 2k'$ - $e = 4k'$	Nothing about e Nothing about a

4 Primality tests : new ways of research

4.1. Theorem 8°) :
Let $\left(\frac{b}{n}\right) = -1$.
A necessary condition for the primality of n is the existence of a.

4.2. Theorem 13°) (Corollary of the 4.3) :
Let $b = 273$.
A necessary condition for the primality of $M_p = 2^p - 1$ $(p > 3)$ is e odd.
A necessary condition for the primality of $N_p = \frac{2^p+1}{3}$ $(p > 3)$ is e odd.
Remarks : Note that 273 is a very special integer. Indeed, $b = 273$ is the smallest base for which $\left(\frac{b}{M_p}\right) = \left(\frac{b}{N_p}\right) = 1$ for all primes $p > 3$.

If one can know that $e(273, M_p)$ or $e(273, N_p)$ is even, there is no need to test M_p or N_p for primality though no factor is known and no PRP/deterministic test has been made.

4.3. Let $N = 4k+3$ and b such that $\left(\frac{b}{N}\right) = 1$.
A necessary condition for the primality of N is e odd.
Proof : If $N = 4k+3$ then $\left(\frac{-1}{N}\right) = -1$, but $\left(\frac{b}{N}\right) = 1$, so a doesn't exist by 11°) . Then, if e was even, N would be composite by 9°) .