

$$\begin{array}{ccc} & \vdots & \\ (2^n - 1) & (2^m - 1) & n \quad m \\ & & (n,m) = 1, \\ & & (2^n - 1, 2^m - 1) = 1. \end{array}$$

$$1. \quad n \quad m \quad (n,m) = 1, \quad (1)$$

$$\begin{array}{l} m < n, n \equiv m_i \pmod{m}, m > m_i > 0, \\ m_i = n - mk_i \\ m \quad m_i \\ \quad \ll \quad 1 \gg. \quad . \quad , \quad m \quad m_i \\ \quad \quad \quad p > 1. \\ m = m_o p \end{array} \quad (2)$$

$$\begin{array}{l} m_i = m_{io} p. \\ m_{io} p = n - m_o p k_i \\ m = m_{io} p + m_o p k_i = p(m_{io} + m_o k_i) \end{array} \quad (3)$$

$$\begin{array}{c} n = m_{io} p + m_o p k_i = p(m_{io} + m_o k_i) \\ (3) \quad (4) \quad , \quad n \quad m \quad p > 1. \end{array} \quad (4)$$

$$\begin{array}{c} \ll \quad 1 \gg \quad . \quad , \quad n \quad m \quad m_i \quad k_i, \\ \quad \quad \quad , \\ m > m_i > 0, \quad m_i = n - mk_i. \\ \quad \ll \quad 1 \gg \quad ( \quad \quad \quad \ll \quad 1 \gg ) \quad m > m_i \\ ( \quad m_i \neq 1 ) \quad m_i > m_{i+1}. \quad , \\ \quad \quad \quad , \\ n > m > m_i > m_{i+1} > \dots > m_{i+j} \end{array} \quad (5)$$

$$\begin{array}{c} \vdots \quad . \quad n \quad . \quad ( \quad m_{i+j}) \\ m_{i+j} = 1, \end{array} \quad (5)$$

$$\begin{array}{c} m_{i+b} = m_{i+b-2} - k_{i+b-1} m_{i+b-1}, \\ b \quad (2) \quad j ( \dots m_{i-2} = n, m_{i-1} = m). \\ , \quad (n,m) = 1 \quad (2^n - 1) \quad (2^m - 1) \end{array}$$

$$q > 1.$$

$$\begin{array}{l} (2^n - 1) = A_1 q \\ (2^m - 1) = A_2 q \end{array}$$

$$(2^{mk_i} - 1) = A_3 q \quad \dots \quad (2^{mk_i} - 1) \equiv 0 \pmod{(2^m - 1)}$$

$$A_1 q - A_3 q = q (A_1 - A_3) = (2^n - 1) - (2^{mk_i} - 1) = 2^n - 2^{mk_i} = 2^{mk_i} (2^{n-mk_i} - 1) = 2^{mk_i} (2^m - 1)$$

$$(2^m - 1) \quad (2^{m_{i+1}} - 1) \qquad \qquad \qquad q > 1.$$

$$\begin{array}{lll} (2^{m_{i+j-1}} - 1) & (2^{m_{i+j}} - 1) & q > 1. \\ (2^{m_{i+j}} - 1) = (2^1 - 1) = 1 & & q > 1. \\ (2^n - 1) & (2^m - 1) & q > 1. \\ \ll 1 \gg & . & \end{array}$$

$$\begin{array}{lll} 2. & n \quad m & (n,m)=1, \\ (A^n - 1)/(A - 1) & (A^m - 1)/(A - 1) & , \quad A > 1. \end{array}$$

$$\cdot \qquad \qquad \qquad \ll 1 \gg, \qquad \qquad \qquad \cdot$$

$$\begin{array}{lll} 3. & (A^m - 1)/(A - 1) \equiv 0 \pmod{t} & (A - 1) \equiv 0 \pmod{t^f}, \\ n, & (A^m - 1)/(A - 1) \quad (A^n - 1)/(A - 1) & t, \quad n \quad m \\ , \quad t > 1, \quad f > 0. & \end{array}$$

$$\begin{array}{lll} \ll 3 \gg & \cdot & \ll 2 \gg. \\ \ll 3 \gg, (A^m - 1)/(A - 1) & \ll 2 \gg. & , \qquad , \\ \ll 2 \gg. & & t, \end{array}$$

## THEOREMS OF RELATIVE PRIMES NUMBERS.

Remark: In this work it is spoken only about the natural numbers .

**Theorem 1.** If the numbers  $n$  and  $m$  are relative primes  $(n,m) = 1$ , then the numbers  $(2^n - 1)$  are  $(2^m - 1)$  also relative primes  $(2^n - 1, 2^m - 1) = 1$ .

**Proof.**

Lemma 1. If the numbers  $n$  and  $m$  are relative primes  $(n,m) = 1$ , (1)

where  $m < n$ ,  $n \equiv m_i \pmod{m}$ ,  $m > m_i > 0$ , and

$$m_i = n - mk_i \quad (2)$$

then the numbers  $m$  and  $m_i$  are also relative primes.

Proof of “Lemma 1”. Let’s suppose inversely. Let’s admit that the numbers  $m$  and  $m_i$  have a common divisor  $p > 1$ . Then

$$m = m_0 p \quad (3)$$

and

$$m_i = m_{io} p.$$

Taking into attention of (2) we’ll get

$$m_{io} p = n - m_0 p k_i$$

It means that

$$n = m_{io} p + m_0 p k_i = p(m_{io} + m_0 k_i) \quad (4)$$

Taking into attention of (3) and (4) it is clear that the numbers  $n$  and  $m$  have a common divisor  $p > 1$ . And this goes in contradictory to the condition of (1).

“Lemma 1” is proved.

It’s clear that for any pair of the relative primes  $n$  and  $m$  there are the numbers  $m_i$  and  $k_i$ , where  $m > m_i > 0$ , and  $m_i = n - mk_i$ .

Let’s apply “lemma 1” to the pair of the relative primes (shown in “lemma 1”)  $m > m_i$  (if  $m_i \neq 1$ ) and we’ll get the next pair of the relative primes  $m_i > m_{i+1}$ .

Going on the analogical way we’ll get a line numbers answered to the condition where

$$n > m > m_i > m_{i+1} > \dots > m_{i+j} \quad (5)$$

Consequence: Cause the number  $n$  is terminal and a line of numbers in (5) decreases, it means that applying to the last member of this line (for  $m_{i+j}$ ) it is a condition

$$m_{i+j} = 1,$$

which is concluded as a result of calculations by the formula

$$m_{i+b} = m_{i+b-2} - k_{i+b-1} m_{i+b-1},$$

where  $b$  covers from (-2) to  $j$  (because  $m_{i-2} = n$ ,  $m_{i-1} = m$ ).

Let’s take that if  $(n,m) = 1$  numbers  $(2^n - 1)$  and  $(2^m - 1)$  have the common divisor equaled to  $q > 1$ .

$$(2^n - 1) = A_1 q$$

$$(2^m - 1) = A_2 q$$

So

$$(2^{mk_i} - 1) = A_3 q \text{ because } (2^{mk_i} - 1) \equiv 0 \pmod{(2^m - 1)}$$

Then

$$A_1q - A_3q = q (A_1 - A_3) = (2^n - 1) - (2^{mk_i} - 1) = 2^n - 2^{mk_i} = 2^{mk_i} (2^{n-mk_i} - 1) = 2^{mk_i}(2^{m_i} - 1)$$

So, the numbers  $(2^m - 1)$  and  $(2^{m_i} - 1)$  have the common divisor equaled to  $q > 1$ .

By the analogical way we'll get that the numbers

$(2^{m_i} - 1)$  and  $(2^{m_{i+1}} - 1)$  also have the common divisor equaled to  $q > 1$ . Going on we'll get

$(2^{m_{i+j-1}} - 1)$  and  $(2^{m_{i+j}} - 1)$  have the common divisor equaled to  $q > 1$ . However

$(2^{m_{i+j}} - 1) = (2^1 - 1) = 1$  and can't have the common divisor equaled to  $q > 1$ .

It means that the numbers  $(2^n - 1)$  and  $(2^m - 1)$  can't have the common divisor equaled to  $q > 1$ .

The theorem is proved.

**Theorem 2.** If the numbers  $n$  and  $m$  are relative primes  $(n, m) = 1$ , then the numbers

$(A^n - 1)/(A - 1)$  and  $(A^m - 1)/(A - 1)$  are also relative primes, where  $A > 1$ .

**Proof.**

By the analogical way, like the proof of «theorem 1», it is easy to prove this theorem.

**Theorem 3.** If  $(A^m - 1)/(A - 1) \equiv 0 \pmod{t}$  and  $(A - 1) \equiv 0 \pmod{t^f}$ , then for all the significances of  $n$ , the numbers  $(A^m - 1)/(A - 1)$  and  $(A^n - 1)/(A - 1)$  are not comparable by modal  $t$ , where  $n$  and  $m$  are relative primes,  $t > 1$ ,  $f > 0$ .

**Proof.**

«Theorem 3» is the obvious consequence of «theorem 2». If it is to suppose that the numbers used in «theorem 3»  $(A^m - 1)/(A - 1)$  and  $(A^n - 1)/(A - 1)$  are comparable by modal  $t$ , it contradicts to the condition of «theorem 2».

1.  $(2^n - 1), n, : An + 1, A -$   
 $(2^n - 1) \equiv 0 \pmod{(2^{p-1} - 1)}$ .  
 $(nM!/n^t) = 1, \dots, n \equiv M!/n^t \pmod{M}$ .  
 $p(2^f - 1) \equiv 0 \pmod{p}$ .  
 $(2^f - 1) \equiv 0 \pmod{p}$ .

$\frac{(2^{p-1} - 1)}{(2^f - 1)} \equiv 0 \pmod{p}$ .  
 $\frac{(2^n - 1)}{(2^f - 1)} \equiv 1 \pmod{(n, f)}$ .  
 $p - 1 = Bn, p = Bn + 1$ .  
 $Bn + 1$ .  
 $Bn + 1 = An + 1$ .

2.  $(S^n - 1)/(S - 1), n, : (Tn + 1),$   
 $S = \text{constant}$   
 $d, T -$   
 $(S^n - 1)/(S - 1) \equiv 1 \pmod{(S - 1)}$ .

$(S^n - 1)/(S - 1) \equiv 1 \pmod{(S - 1)}$ .  
 $(S^f - 1)/(S - 1) \equiv 1 \pmod{(S - 1)}$ .  
 $(S^n - 1)/(S - 1) \equiv 1 \pmod{(S - 1)}$ .  
 $(10^3 - 1)/(10 - 1) \equiv 0 \pmod{3}$ .

$n$   
 $(S - 1)$ .

## Theorems of the relative primes

*Remark: In this article it is spoken only about the natural numbers .  $M! - M$  is factorial.*

**Theorem 1.** The prime divisor of the numbers  $(2^n - 1)$ , where  $n$  is simple, has the following aspect:  
 $An + 1$ , where  $A$  – is a natural number.

**Proof.** Let's compare the numbers  $(2^n - 1)$  and  $(2^f - 1)$ , where  $f = M!/n^t$ ,  $M$  – is infinitely large natural number,  $t$  – is infinitely large natural number, where the condition of  $(n, M!/n^t) = 1$ , is satisfied, so the numbers  $n$  and  $M!/n^t$  are relative primes,  $f$  – is a natural number. Because of  $M$  – is infinitely large natural number, for any prime  $p$  (with the exception of some of cases, when  $p - 1 = Bn$ , because  $f$  and  $n$  are relative primes.  $B$  – is a natural number) the following condition is satisfied:

$$(2^f - 1) \equiv 0 \pmod{(2^{p-1} - 1)}.$$

According to the Ferma's Small theorem it is known that

$$(2^{p-1} - 1) \equiv 0 \pmod{p}.$$

So,  $(2^f - 1) \equiv 0 \pmod{p}$ .

We know that (see «Theorems of relative primes numbers» on the site: <http://logman-logman.narod.ru/>) the numbers  $(2^n - 1)$  and  $(2^f - 1)$  are relative primes, because  $(n, f) = 1$ . It means that any prime is a divider of the number  $(2^f - 1)$ , with the exception of some of cases, when  $p - 1 = Bn$  and  $p = Bn + 1$ . So, the prime divisor of the numbers  $(2^n - 1)$  have the following aspect:

$Bn + 1$ .

$Bn + 1 = An + 1$ . The theorem is proved.

**Theorem 2.** The prime divisor of the numbers  $(S^n - 1)/(S - 1)$ , where  $n$  is a prime , have the following aspect:  $(Tn + 1)$ , and for the limit quotation of significances of  $n$  when  $S = \text{constant}$  the numbers  $(S^n - 1)/(S - 1)$  can have the prime divisor  $d$ , where  $T$  – is a natural number,  $d$  – is a number's  $(S - 1)$  divider.

**Proof.** Let's prove «Theorem 2» by the same way like we've done according to the “theorem 1”. Let's compare the numbers  $(S^n - 1)/(S - 1)$  and  $(S^f - 1)/(S - 1)$ , where  $f = M!/n^t$ ,  $M$  – is infinitely large natural number,  $t$  – is infinitely large natural number, where the following condition is satisfied:  $(n, M!/n^t) = 1$ , so the numbers  $n$  and  $M!/n^t$  are relative primes,  $f$  – is a natural number:  
 ) So, we get the analogical result to the “theorem 1”, and the prime divisor of numbers  $(S^n - 1)/(S - 1)$  have the following aspect:  $(Tn + 1)$ . More over,

) Because at the denominator of the number  $(S^f - 1)/(S - 1)$  there is a number  $(S - 1)$ , there are some of cases, when the number  $(S^f - 1)/(S - 1)$  doesn't have any prime divisor  $d$ , which is the prime divisor of the number  $(S - 1)$ . Because of this reason it is possible to suggest that such numbers like  $d$  may turned out to be the prime divisor of numbers  $(S^n - 1)/(S - 1)$ . **There are some of the similar cases. For example:  $(10^3 - 1)/(10 - 1) \equiv 0 \pmod{3}$**

In this way it is obvious that the quantity of significances of  $n$  is limited within quantity of the prime divisor of the number  $(S - 1)$  from above.

The theorem is proved.