Translation into English of the paper Riesel, Hans (1956). "Några stora primtal". Elementa. 39: 258–260 (in Swedish).[1]

Some large prime numbers

by fil. lic. Hans Riesel, Stockholm

In the June 1955 edition of Elementa, it was described how the author of the present article by means of the electronic computer BESK[2] had been able to determine some large primes[i]. The investigations with BESK have been continued and it turns out that the following numbers of the form $h * 2^e - 1$ are primes:

h	e
5	270, 274
59	12, 16, 72
61	3, 5, 9, 13, 17, 19, 25, 39, 63, 67, 75, 119, 147
65	4, 6, 12, 22, 28, 52, 78, 94
67	5, 9, 21, 45, 65, 77
71	2, 14
73	7, 11, 19, 71, 79, 131
77	2, 4, 14, 26, 58, 60, 64, 100, 122

For $h = 5$ all exponents between 250 and 413 were tested but no other primes than the two in the table was found. For the remaining h-values, the author investigated all $e \leq 150$. Because the computations were not repeated and because a possible malfunctions in the machine with very large probability leads to the number tested being considered composite it is possible that additional primes may exist in the investigated interval.

Following are some questions that one may pose: Does the sequence $N = h * 2^e - 1$ when varying e contain infinitely many primes? Does the sequence contain primes for every h-value? As far as the author is aware, it is not possible at present to determine much concerning the first question. For example, it has not been possible to show that there exists a h-value for which the sequence N contains infinitely many primes. Concerning the second question, we will prove the following theorem:

Theorem: There are infinitely many values of h for which the numbers $N = h * 2^e - 1, e = 0,1,2, \ldots$ are all composite.

The simplest way to prove it is by means of some examples.

[1] Translated by Lars Blomberg, Linghem. N. J. A. Sloane suggested some changes to clarify the translation. It is advisable to check the various numbers against the original article.

[2] BESK (*Binary Electronic Sequence Calculator*) was an early Swedish computer 1953-66. (Translator's note)

If d is the smallest positive integer for which $2^d \equiv 1(mod\ p)$, where p is an odd prime, then we say that 2 belongs to the exponent $d(mod\ p)$. It is clear that this happens for exactly those primes p that are factors of $2^d - 1$ without being factors of any of the numbers $2^s - 1$, where s is a proper positive divisor of d.
Example: $d = 24$ gives $2^{24} - 1 = 3 * 3 * 5 * 7 * 13 * 17 * 241$.
Further we have $2^2 - 1 = 3$, $2^3 - 1 = 7, 2^4 - 1 = 3 * 5, 2^5 - 1 = 3 * 3 * 7$,
$2^8 - 1 = 3 * 5 * 17$ and $2^{12} - 1 = 3 * 3 * 5 * 7 * 13$.
Consequently, 2 belongs to the exponent $24(mod\ 241)$.

Considering now the numbers $N = h * 2^e - 1\ (mod\ p)$, where e is variable, p is an odd prime and $h \neq 0(mod\ p)$ it is clear that these numbers belong to exactly d different residue classes [3] $(mod\ p)$ if d is the exponent to which 2 belongs $(mod\ p)$. These d residue classes are repeated periodically when e varies through all natural numbers. With a suitable choice of h we will be able to achieve that one of these residue classes will be $\equiv 0(mod\ p)$. We can therefore select h so that exactly every d:th number N will be divisible by p; furthermore are we able to determine the smallest exponent $e, 0 \leq e < d$ for which the number $N = h * 2^e - 1$ is $\equiv 0(mod\ p)$. This fact can be used to find h-values for which the number N is composite for every value of e.

The so-called Fermat numbers t_n are defined by the relation $t_n = 2^{2^n} + 1$. Clearly we have $2^{2^n} \equiv -1(mod\ t_n)$. If p is any prime factor of t_n we also have $2^{2^n} \equiv -1(mod\ p)$. $2^d = 2^{2^{n+1}} \equiv 1(mod\ p)$. Since because of the first congruence it is never the case that $2^s \equiv 1\ (mod\ p)$ when s is a proper divisor of d, we see that 2 belongs to the exponent $2^{n+1}\ (mod\ p)$. Furthermore, it is well known that the numbers $2^1 + 1 = 3$, $2^2 + 1 = 5$, $2^4 + 1 = 17$, $2^8 + 1 = 257$ and $2^{16} + 1 = 65\,537$ are prime while $2^{32} + 1 = 642 * 6\,700\,417$ is not[4].

We now calculate as follows:

Case	**We have**	**… for $e =$ …**	**… provided**
$2^2 \equiv 1(mod\ 3)$	$N \equiv 0(mod\ 3)$	$1 + 2k$	$h * 2^1 \equiv 1(mod\ 3)$
$2^4 \equiv 1(mod\ 5)$	$N \equiv 0(mod\ 5)$	$2 + 2^2k$	$h * 2^2 \equiv 1(mod\ 5)$
$2^8 \equiv 1(mod\ 17)$	$N \equiv 0(mod\ 17)$	$2^2 + 2^3k$	$h * 2^4 \equiv 1(mod\ 17)$
$2^{16} \equiv 1(mod\ 257)$	$N \equiv 0(mod\ 257)$	$2^3 + 2^4k$	$h * 2^8 \equiv 1(mod\ 257)$
$2^{32} \equiv 1(mod\ 65537)$	$N \equiv 0(mod\ 65537)$	$2^4 + 2^5k$	$h * 2^{16} \equiv 1(mod\ 65537)$
$2^{64} \equiv 1(mod\ 641)$	$N \equiv 0(mod\ 641)$	$2^5 + 2^6k$	$h * 2^{32} \equiv 1(mod\ 641)$
$2^{64} \equiv 1(mod\ 6700417)$	$N \equiv 0(mod\ 6700417)$	2^6k	$h * 2^{64} \equiv 1(mod\ 6700417)$

[3] Swedish *restklasser* (Translator's note)
[4] It seems that the words *is not* have been left out. (Translator's note)

If we solve the above congruences for h, we obtain an h-value $(mod\ 2^{64}-1)$. For all such values of h, N will contain a known prime factor for the e-values given above. But the way these e-values have been selected means that all natural numbers are included, so we find that: If h satisfies the above congruences, the number N is always divisible by exactly one of the primes *3, 5, 16, 257, 65 537, 641* or *6 700 417*. Solving the congruences is very easy; one observes immediately that the first 6 congruences have the solution $h \equiv -1(mod\ 641(2^{32}-1))$ whereas the seventh congruence can be simplified to $h \equiv 1(mod\ 6700417)$.

These two congruences yield $h \equiv 2\,935\,363\,327\,246\,958\,234\ (mod\ 2^{64}-1)$. Since the smallest positive value of h that satisfies this congruence is larger than the prime factors used, it is clear that all the numbers N are composite for these h-values.

Another example that uses the residue classes $(mod\ 24)$ and one that yields a smaller value of h are the following:

Case	**We have**	**… for $e = …$**	**… provided**
$2^2 \equiv 1(mod\ 3)$	$N \equiv 0(mod\ 3)$	$2k$	$h * 2^0 \equiv 1(mod\ 3)$
$2^4 \equiv 1(mod\ 5)$	$N \equiv 0(mod\ 5)$	$1+4k$	$h * 2^1 \equiv 1(mod\ 5)$
$2^3 \equiv 1(mod\ 7)$	$N \equiv 0(mod\ 7)$	$2+3k$	$h * 2^2 \equiv 1(mod\ 7)$
$2^{12} \equiv 1(mod\ 13)$	$N \equiv 0(mod\ 13)$	$7+12k$	$h * 2^7 \equiv 1(mod\ 13)$
$2^8 \equiv 1(mod\ 17)$	$N \equiv 0(mod\ 17)$	$7+8k$	$h * 2^7 \equiv 1(mod\ 17)$
$2^{24} \equiv 1(mod\ 241)$	$N \equiv 0(mod\ 241)$	$3+24k$	$h * 2^3 \equiv 1(mod\ 241)$

It is easy to verify that the different e-values have been chosen so that all the residue classes $(mod\ 24)$ are represented. Solving the congruences for h one finds $h \equiv 509203(mod\ 5592405)$. Since 509203 is larger than the prime factors 3, 5, 7, 13, 17 and 241, consequently this is another example of h-values for which the numbers $N = h * 2^e - 1$ are all composite.

Obviously, the selection of the e-values in the examples may be made in many different ways, and one can also work with different sets of primes than the ones used here.

[i] H. Riesel, Elementa, 38 (1955), s. 91.
H. Riesel. Arkiv för matematik, 3 (1955), s. 245-253.