Conjectures as to a factor of $2^p \pm 1$

By NEIL Y. WILSON.

More than 300 years ago Mersenne made pronouncements as to the prime or composite nature of $2^p - 1$ for all prime values of p from 1 to 257. His reasons were not disclosed, but the combined efforts of many mathematicians have shown that his statements were substantially correct. Of course when p is composite, two or more factors of $2^p \pm 1$ will often be obvious but, as far as I am aware, only two general theorems relating to a non-obvious factor have been proved. I give these by way of introduction to this article and thereafter proceed to enunciate seven new and original theorems. As I offer no theoretical proofs of the theorems, they must be regarded as conjectures. They are, however, based on extensive computation which has engaged me for a period of three years.

Fermat's Theorem. (Modulus $p + 1$)

$2^p - 1 \equiv 0\ [p + 1]$, provided that p is an even integer and $p + 1$ prime.

Example. 421 is a factor of $2^{420} - 1$.

Euler's Theorem. (Modulus $2p + 1$)

A. $2^p - 1 \equiv 0\ [2p + 1]$, provided that $2p + 1$ is prime and p has the form $4n$ or $4n + 3$.

Example. 73 is a factor of $2^{36} - 1$,
167 ,, ,, $2^{83} - 1$.

B. $2^p + 1 \equiv 0\ [2p + 1]$, provided that $2p + 1$ is prime and p has the form $4n + 1$ or $4n + 2$.

Example. 211 is a factor of $2^{105} + 1$,
4421 ,, ,, $2^{2210} + 1$.

Theorem 1. (Modulus $3p + 1$)

$2^p - 1 \equiv 0\ [3p + 1]$, provided that (1) p is even and $3p + 1$ prime,
(2) $3p+1 = 27\,(2m+1)^2 + 4\,(3n\pm1)^2$
or $3p + 1 = 108m^2 + (6n \pm 1)^2$.

Example. 3271 is a factor of $2^{1090} - 1\ [3271 = 27.11^2 + 4.1^2]$,
11161 ,, ,, $2^{3720} - 1\ [11161 = 108.10^2 + 19^2]$.

Theorem 2. (Modulus $4p + 1$)

A. $2^p - 1 \equiv 0\ [4p + 1]$, provided that

(1) p is even and $4p + 1$ prime,

(2) $4p + 1 = (2m + 1)^2 + 64n^2$.

Example. 2393 is a factor of $2^{598} - 1$ [$2393 = 37^2 + 64.4^2$].

B. $2^p + 1 \equiv 0\ [4p + 1]$, provided that

(1) p is even and $4p + 1$ prime,

(2) $4p + 1 = (2m + 1)^2 + 16\ (2n + 1)^2$.

Example. 2153 is a factor of $2^{538} + 1$ [$2153 = 37^2 + 16.7^2$].

Theorem 3. (Modulus $5p + 1$)

$2^p - 1 \equiv 0\ [5p + 1]$, provided that

(1) p is even and $5p + 1$ prime,

(2) $5p + 1 = 5^{2m+3} + n^2\ [(na)^2 + F_a.5^{m+2}]$

or $5p + 1 = 2^{4m}.5^3 + n^2\ [(na)^2 + F_a.2^{2m}.5^2]$,

where a is any prime of the form $10k \pm 1$ and F_a is any term of the appropriate series: .

Prime.		*Series.*
1	....	89, 34, 13, 5, 2, **1**, 1, 2, 5, 13, 34, ...
11	....	505, 193, 74, 29, 13, **10**, 17, 41, 106, 277, 725, ...
19	....	1018, 389, 149, 58, 25, **17**, 26, 61, 157, 410, 1073, ...
29	....	1489, 569, 218, 85, 37, **26**, 41, 97, 250, 653, 1709, ...
31	....	1261, 482, 185, 73, 34, **29**, 53, 130, 337, 881, 2306, ...
41	....	1973, 754, 289, 113, 50, **37**, 61, 146, 377, 985, 2578 ....

and so on.

In all of these series $T_n = 3T_{n-1} - T_{n-2}$.

Examples. 5821 is a factor of $2^{1164} - 1$ [$5821 = 5^3 + 8^2\ (8^2 + 5^2)$],

54101 ,, $2^{10820} - 1$ [$54101 = 5^5 + 4^2\ (44^2 + 10.5^3)$],

884321 ,, $2^{176864} - 1$ [$884321 = 2^8.5^3 + 19^2\ (19^2 + 5.2^4.5^2)$].

Theorem 4. (Modulus $6p + 1$)

A. $2^p - 1 \equiv 0\ [6p + 1]$, provided that

(1) p is odd and $6p + 1$ prime,

(2) $6p + 1 = 27\ (2m + 1)^2 + 4\ (6n \pm 1)^2$.

Example. 6271 is a factor of $2^{1045} - 1$ [$6271 = 27.15^2 + 4.7^2$].

B. $2^p - 1 \equiv 0\ [6p + 1]$, provided that

(1) p is even and $6p + 1$ prime,

(2) $6p + 1 = 432\ m^2 + (6n \pm 1)^2$.

Example. 3889 is a factor of $2^{648} - 1$ [$3889 = 432.3^2 + 1^2$].

https://doi.org/10.1017/S0950184300003086 Published online by Cambridge University Press

C. $2^p + 1 \equiv 0\ [6p + 1]$, provided that
(1) p is odd and $6p + 1$ prime,
(2) $6p + 1 = 27\ (2m + 1)^2 + 16\ (3n \pm 1)^2$.

Example. 4051 is a factor of $2^{675} + 1$ [$4051 = 27.11^2 + 16.7^2$].

D. $2^p + 1 \equiv 0\ [6p + 1]$, provided that
(1) p is even and $6p + 1$ prime,
(2) $6p + 1 = 108\ (2m + 1)^2 + (6n \pm 1)^2$.

Example. 2749 is a factor of $2^{458} + 1$ [$2749 = 108.5^2 + 7^2$].

Theorem 5. (Modulus $8p + 1$)

A. $2^p - 1 \equiv 0\ [8p + 1]$, provided that
(1) p is odd and $8p + 1$ prime,
(2) $8p + 1 = (2m + 1)^2 + 64\ (2n + 1)^2$.

Example. 3257 is a factor of $2^{407} - 1$ [$3257 = 11^2 + 64.7^2$].

B. $2^p - 1 \equiv 0\ [8p + 1]$, provided that
(1) p is even and $8p + 1$ prime,
(2) $8p + 1 = (2m + 1)^2 + 256n^2$.

Example. 2593 is a factor of $2^{324} - 1$ ($2593 = 17^2 + 256.3^2$].

C. $2^p + 1 \equiv 0\ [8p + 1]$, provided that
(1) p is odd and $8p + 1$ prime,
(2) $8p + 1 = (2m + 1)^2 + 256n^2$.

Example. 2473 is a factor of $2^{309} + 1$ [$2473 = 13^2 + 256.3^2$].

D. $2^p + 1 \equiv 0\ [8p + 1]$, provided that
(1) p is even and $8p + 1$ prime,
(2) $8p + 1 = (2m + 1)^2 + 64\ (2n + 1)^2$.

Example. 3361 is a factor of $2^{420} + 1$ [$3361 = 15^2 + 64.7^2$].

Theorem 6. (Modulus $12p + 1$)

A. $2^p - 1 \equiv 0\ [12p + 1]$, provided that
(1) p is even and $12p + 1$ prime,
(2) $12p + 1 = 432m^2 + (6n \pm 1)^2 = (2x + 1)^2 + 64y^2$.

Example. 18121 is a factor of $2^{1510} - 1$
[$18121 = 432.1^2 + 133^2 = 61^2 + 64.15^2$].

B. $2^p + 1 \equiv 0\ [12p + 1]$, provided that
(1) p is even and $12p + 1$ prime,
(2) $12p + 1 = 432m^2 + (6n \pm 1)^2 = (2x + 1)^2 + 16\,(2y + 1)^2$.

Example. 28057 is a factor of $2^{2338} + 1$
[$28057 = 432.7^2 + 83^2 = 61^2 + 16.39^2$].

https://doi.org/10.1017/S0950184300003086 Published online by Cambridge University Press

Theorem 7. (Modulus $24p + 1$)

A. $2^p - 1 \equiv 0$ $[24p + 1]$ when $24p + 1$ is prime, provided that $24p + 1 = 432m^2 + (6n \pm 1)^2 = (2x + 1)^2 + 64y^2$, where p and y are both even or both odd.

Example. 27409 is a factor of $2^{1142} - 1$

$[27409 = 432.7^2 + 79^2 = 105^2 + 64.16^2]$.

B. $2^p + 1 \equiv 0$ $[24p + 1]$ when $24p + 1$ is prime, provided that $24p + 1 = 432m^2 + (6n \pm 1)^2 = (2x + 1)^2 + 64y^2$, where p is odd and y even or p even and y odd.

Example. 29017 is a factor of $2^{1209} + 1$

$[29017 = 432.8^2 + 37^2 = 91^2 + 64.18^2]$.

My modus operandi in deriving these results was as follows:—

Theorem 1. All prime values of $3p + 1$ from 1 to 1500 were tested and the results were tabulated. Analysis of these results enabled me to infer the formula of the theorem. I found that when $3p + 1$ was not expressible by the formula it was not a factor of $2^p - 1$, whereas when $3p + 1$ was so expressible (33 instances) it was invariably a factor. The last of these instances was $2^{490} - 1 \equiv 0$ $[1471]$ because $1471 = 27{\cdot}1^2 + 38^2$.

Next the formula was applied to all primes of form $3p + 1$ in the range 1500 to 3000, and the results were predicted before being worked out. Without exception the prediction was proved correct.

Thereafter many random examples at much greater ranges were similarly tested, and no departure whatsoever from the formula was found. The same procedure was adopted for each of the other theorems with the initial ranges as indicated.

Theorem 2.	Range for	$4p+1$,	from	1 to 2000, 68	favourable	instances.
Theorem 3.	,,	$5p+1$,	,,	1 to 5000, 32	,,	,,
Theorem 4.	,,	$6p+1$,	,,	1 to 3000, 67	,,	,,
Theorem 5.	,,	$8p+1$,	,,	1 to 2000, 34	,,	,,
Theorem 6.	,,	$12p+1$,	,,	1 to 6000, 29	,,	,,
Theorem 7.	,,	$24p+1$,	,,	1 to 30,000, 46	,,	,,

I am greatly indebted to Professor Aitken for much encouragement and assistance whilst these theorems have been under investigation. For the establishment of the simpler theorems Barlow's Primes (1 to 10^5) proved adequate, but the more complicated ones required the continuous use of Lehmer's Primes (1 to 10^7), which Professor Aitken willingly placed at my disposal.

35 SPOTTISWOODE ROAD,
EDINBURGH 9.