Properties of Mersenne and Fermat numbers

Tony Reix (Tony.Reix@laposte.net)
2004, 30th of September

1 Mersenne numbers: $M_q = 2^q - 1, q\ prime$

When $M_q = 2^q - 1$ is prime, it is said to be a Mersenne prime.

$$M_q = 2^q - 1 \text{ is prime } \Longrightarrow q \text{ is prime .}$$

1.1 M_q = Sum of binomial coefficients

$$M_q = \sum_{i=0}^{q} \binom{q}{i} - 1$$

1.2 $\sum \{d; d \mid N\} = 2^n \Longleftrightarrow N = \prod M_{q_i}$

The sum of the divisors of $N(> 1)$ is a power of 2 if and only if N is the product of distinct Mersenne primes.

1.3 Perfect numbers

A positive integer N is called a perfect number if it is equal to the sum of all of its positive divisors, excluding N itself.

P is an even perfect number if and only if it has the form $2^{n-1}(2^n - 1)$ and $2^n - 1$ is prime.

1.4 Form of divisors

$$a \mid M_q \Longrightarrow \begin{cases} a \equiv 1 \pmod{2q} \\ a \equiv \pm 1 \pmod 8 \end{cases}$$

$$\begin{cases} M_q \equiv 1 \pmod{6q} & , q \geq 5 \\ M_q \equiv -1 \pmod 8 & , q \geq 3 \end{cases}$$

1.5 Other properties

Let $q = 3 \pmod 4$ be a prime.
$2q + 1$ is also a prime if and only if $2q + 1$ divides M_q .

1.6 Fermat factorisation

$$M_q = (8x)^2 - (3qy)^2 = (1 + Sq)^2 - (Dq)^2$$

1.7 $M_q = (2x)^2 + 3(3y)^2$

M_q is a prime if and only if there exists only one pair (x, y) such that: $M_q = (2x)^2 + 3(3y)^2$, $q \geq 5$.

The primes p such that: $p = x^2 + 3y^2$ are all of the form: $1 \pmod 6$.

1.8 Proving primality: Lucas-Lehmer Test (LLT)

q being a prime > 2 , the Mersenne number $M_q = 2^q - 1$ is a prime if and only if it divides S_{n-2} where $S_{n+1} = S_n^2 - 2$, and $S_0 = 4$.

1.9 Ramanujan's Square Equation

The equation: $2^q - 1 = 6 + x^2$ has only 3 solutions with q prime: 3, 5, and 7 (and 2 solutions with q composite).

2 Fermat numbers: $F_n = 2^{2^n} + 1, n = 0, 1, 2, ...$

2.1

3 Binomial coefficients

3.1 Binomials modulo a prime

A property about Binomial coefficients, found by Edouard Lucas.
Let p be a prime, and define:

$$a = \prod_{i=0}^{\alpha} a_i p^i \qquad b = \prod_{i=0}^{\beta} b_i p^i \qquad 0 \leq a_i < p \ \ , \ \ 0 \leq b_i < p$$

We have:

$$\binom{a}{b} \equiv \prod_{i=0}^{\min(\alpha,\beta)} \binom{a_i}{b_i} \pmod p$$

3.2 Other properties

p being a prime, we have:

$$\binom{p-1}{0 \leq i < p} \equiv (-1)^i \pmod p$$

$$\binom{p}{0 < i < p} = 0$$