January 31 - February 9, 2023. Limbe (Cameroun)

Number Theory
African Institute for Mathematical Sciences (AIMS)

Michel Waldschmidt, Sorbonne Université

Quizz 1 (15') *February 3, 2023*

Let a and b be two integers ≥ 2.
1. Assume $a^b - 1$ is prime. Prove that $a = 2$ and that b is prime.
2. Assume $a^b + 1$ is prime. Prove that b is a power of 2.
Can you give an example of two integers a and b both ≥ 2 with $a^b + 1$ prime and a is not a power of 2 ?

`Hint.` Recall the identities

$$x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1)$$

and

$$x^{2m+1} + 1 = (x + 1)(x^{2m} - x^{2m-1} + x^{2m-2} - \cdots + x^2 - x + 1).$$

`Comment.`
The prime numbers of the form $2^p - 1$ are called *Mersenne primes.* One knows 51 Mersenne primes.
http://oeis.org/A000043
https://primes.utm.edu/mersenne/index.html
The prime numbers of the form $F_n = 2^{2^n} + 1$ are called *Fermat primes.* One knows 5 Fermat primes :

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537.$$

http://oeis.org/A000215
Largest Know primes : https://primes.utm.edu/primes/

January 31 - February 9, 2023. Limbe (Cameroun)

Number Theory
African Institute for Mathematical Sciences (AIMS)

Michel Waldschmidt, Sorbonne Université

Quizz 1 (15') *February 3, 2023*

Solution

1. Assume $a^b - 1$ is prime. From

$$a^b - 1 = (a-1)(a^{b-1} + a^{b-2} + \cdots + a^2 + a + 1)$$

one deduces that $a-1$ divides $a^b - 1$. Since $b \geq 2$ we have $a - 1 < a^b - 1$, hence $a - 1 = 1$ and $a = 2$.

Let $d > 1$ be a divisor of b. Write $b = dn$ with $n < b$; set $x = 2^d$. From

$$\begin{aligned} 2^b - 1 &= x^n - 1 \\ &= (x-1)(x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1) \\ &= (2^d - 1)(x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1) \end{aligned}$$

we deduce that $2^d - 1$ divides $2^b - 1$. Since $2^d - 1 > 1$, we deduce $2^d - 1 = 2^b - 1$, hence $d = b$. Therefore b has a unique divisor > 1 : this means that b is prime.

2. Let b be an integer with an odd prime divisor $2m + 1 \geq 3$. Write $b = (2m+1)d$ and set $x = a^d$. From

$$\begin{aligned} a^b + 1 &= x^{2m+1} + 1 \\ &= (x+1)(x^{2m} - x^{2m-1} + x^{2m-2} - \cdots + x^2 - x + 1) \\ &= (a^d + 1)(x^{2m} - x^{2m-1} + x^{2m-2} - \cdots + x^2 - x + 1) \end{aligned}$$

we deduce that $a^b + 1$ is divisible by $a^d + 1$. From $d < b$ we deduce $1 < a^d + 1 < a^b + 1$. Hence $a^b + 1$ is not prime.

Examples with a not a power of 2 and $b = 2^n$ for which $a^b + 1$ is prime are

- $37 = 6^2 + 1$ with $a = 6$ and $b = 2$,
- 101 with $a = 10$, $b = 2$,
- $1297 = 6^4 + 1$ with $a = 6$ and $b = 4$.