

Suppose $x^n - 1$ is a prime number, where both x and n are positive integers. For example, if $x = n = 2$ then we get $2^2 - 1 = 3$, which is prime.

Now

$$x^2 - 1 = (x - 1)(x + 1)$$

$$x^3 - 1 = (x - 1)(x^2 + x + 1)$$

$$x^4 - 1 = (x - 1)(x^3 + x^2 + x + 1)$$

and in general

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

So if $2^n - 1$ is prime, we must have either $2^a - 1 = 1$, or else $2^a - 1 = 2^n - 1$. So either $2^a = 2$, which means $a = 1$, or else $2^a = 2^n = 2^{ab}$, which means $b = 1$.

We deduce that if $n = ab$ then either $a = 1$ or else $b = 1$, and that means n is a prime, say $n = p$.

Prime numbers of the form $2^p - 1$, where p is prime, are called *Mersenne* primes. (Marin Mersenne, 1588–1648.) But beware: not every number of the form $2^p - 1$ (with p prime) is itself prime.

Here are the first few values of $2^p - 1$:

$p :$	2	3	5	7	11	13	17	19
$2^p - 1 :$	3	7	31	127	2047	8191	131071	524287

Of these, all are prime except for $2^{11} - 1 = 2047 = 23 \times 89$. After $p = 19$, they are a bit thinner on the ground; by December 2005, just 43 Mersenne primes had been found, the last, corresponding to $p = 30402457$, being a number of 9152052 digits.

Now let's look for primes of the form $x^n + 1$. We have

$$x^3 + 1 = (x + 1)(x^2 - x + 1)$$

$$x^5 + 1 = (x + 1)(x^4 - x^3 + x^2 - x + 1)$$

$$x^7 + 1 = (x + 1)(x^6 - x^5 + x^4 - x^3 + x^2 - x + 1),$$

and in general $x + 1$ is a factor of $x^n + 1$ whenever n is *odd*. Further, unless $x = 0$ or $n = 1$, this factor will not be equal to 1 or $x^n + 1$.

Next, note that $x^6 + 1 = (x^2)^3 + 1$, and this has $x^2 + 1$ as a factor (replacing x by x^2 in the above); and likewise if $n = ab$ with b odd, then $x^n + 1 = (x^a)^b + 1$, and this will have $x^a + 1$ as a factor. So to get a prime of the form $x^n + 1$, we must insist that n has no odd factors, that is, n must be a power of 2.

Clearly we must also take x even (otherwise $x^n + 1$ will be even); in fact, we'll stick to $x = 2$.

Put $F_n = 2^{2^n} + 1$. If F_n is prime, it is called a *Fermat* prime. (Pierre de Fermat, 1601–1665.)

Here are the first few values of F_n :

$n :$	0	1	2	3	4
$F_n :$	3	5	17	257	65537

These are all prime. Fermat conjectured that F_n would always be prime, but Euler proved that F_5 is composite. (Leonhard Euler, 1707–1783.)

Now $F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4294967297$. Here is a version of Euler's argument. First note that $641 = 16 + 625 = 2^4 + 5^4$, and also $640 = 5 \times 128 = 5 \times 2^7$. Then

$$\begin{aligned} F_5 = 2^{32} + 1 &= 2^4 \times 2^{28} + 1 \\ &= (641 - 5^4) \times 2^{28} + 1 \\ &= 641 \times 2^{28} - 5^4 \times 2^{28} + 1 \\ &= 641 \times 2^{28} - (5 \times 2^7)^4 + 1 \\ &= 641 \times 2^{28} - (640^4 - 1). \end{aligned}$$

But $x + 1$ is a factor of $x^4 - 1$ (OK?), so 641 is a factor of $640^4 - 1$, and therefore 641 is a factor of F_5 .

In fact, no further Fermat primes have been found, so Fermat's conjecture was not a very happy one.

The connection with regular polygons is this: a regular n -gon can be constructed with ruler and compasses if n is a power of 2 times a product of distinct Fermat primes. This was first proved by Gauss, who was also the first to construct a regular 17-gon. (Johann Carl Friedrich Gauss, 1777–1855.)

The fact that these are the *only* values of n for which a regular n -gon can be so constructed, was conjectured by Gauss, and proved in 1837 by Pierre Laurent Wantzel (1814–1848).

So a regular n -gon can be constructed for $n = 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34, 40, 48, 51, 60, 64, 68, 80, 85, 96, \dots$

and it *cannot* be constructed for $n = 7, 9, 11, 13, 14, 18, 19, 21, 22, 23, 25, 26, 27, 28, 29, 31, 33, 35, 36, 37, 38, 39, 41, 42, 43, 44, 45, 46, 47, 49, 50, 52, 53, 54, 55, 56, 57, 58, 59, 61, 62, 63, 65, 66, 67, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 81, 82, 83, 84, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 97, 98, 99, 100, \dots$