Polynomials of the form $P_n^{(a)}(x) = \left(\frac{1}{2}\right) \cdot \left(\left(x - \sqrt{x^2+a}\right)^n + \left(x + \sqrt{x^2+a}\right)^n \right)$ and primality testing

Predrag Terzić

e-mail: `pedja.terzic@hotmail.com`

July 3 , 2019

1 The main result

Theorem 1.1. *Let n be a natural number greater than two . Let r be the smallest odd prime number such that $r \nmid n$ and $n^2 \not\equiv 1 \pmod{r}$. Let $P_n^{(a)}(x) = \left(\frac{1}{2}\right) \cdot \left(\left(x - \sqrt{x^2+a}\right)^n + \left(x + \sqrt{x^2+a}\right)^n \right)$, where a is an integer coprime to n . Then n is a prime number if and only if $P_n^{(a)}(x) \equiv x^n \pmod{x^r - 1, n}$.*

Proof of necessity :
It is true that if n is a prime number, then $P_n^{(a)}(x) \equiv x^n \pmod{x^r - 1, n}$.
We have, by the binomial theorem,

$$P_n^{(a)}(x) = \frac{1}{2}\left(\left(x - \sqrt{x^2+a}\right)^n + \left(x + \sqrt{x^2+a}\right)^n \right)$$

$$= \frac{1}{2}\sum_{i=0}^{n}\binom{n}{i}x^{n-i}\left(\left(-\sqrt{x^2+a}\right)^i + \left(\sqrt{x^2+a}\right)^i \right)$$

$$= \sum_{j=0}^{(n-1)/2}\binom{n}{2j}x^{n-2j}(x^2+a)^j$$

$$= x^n + \sum_{j=1}^{(n-1)/2}\binom{n}{2j}x^{n-2j}(x^2+a)^j$$

Since $\binom{n}{m} \equiv 0 \pmod{n}$ for $1 \leq m \leq n-1$, there exists a polynomial f with integer coefficients such that

$$P_n^{(a)}(x) = x^n + 0 \times (x^r - 1) + nf$$

from which

$$P_n^{(a)}(x) \equiv x^n \pmod{x^r - 1, n}$$

follows. ■

—

Proof of sufficiency :

It is true that if $P_n^{(a)}(x) \equiv x^n \pmod{x^r-1, n}$, then n is a prime number.

Suppose that n is an even number. Then, there exist a polynomial f with integer coefficients and an integer s such that

$$P_n^{(a)}(x) = \sum_{i=0}^{n/2} \binom{n}{2i} x^{n-2i}(x^2+a)^i = x^n + s(x^r - 1) + nf$$

Considering $[x^n]$ where $[x^k]$ denotes the coefficient of x^k in $P_n^{(a)}(x)$, we get

$$\sum_{i=0}^{n/2} \binom{n}{2i} \equiv 1 \pmod{n},$$

i.e.

$$2^{n-1} \equiv 1 \pmod{n}$$

which is impossible.

So, n has to be an odd number.

There exist a polynomial $g = \sum_{i=0}^{n} a_i x^i$ where a_i are integers and an integer t such that

$$P_n^{(a)}(x) = \sum_{j=0}^{(n-1)/2} \binom{n}{2j} x^{n-2j}(x^2+a)^j = x^n + t(x^r-1) + ng$$

Considering $[x^0]$, we have

$$0 = -t + na_0 \implies t = na_0$$

So, we see that there exists a polynomial h with integer coefficients such that

$$P_n^{(a)}(x) = \sum_{j=0}^{(n-1)/2} \binom{n}{2j} x^{n-2j}(x^2+a)^j = x^n + nh \quad (1)$$

It follows that $[x^k] \equiv 0 \pmod{n}$ for all k such that $0 \le k \le n-1$.

Now, (1) can be written as

$$P_n^{(a)}(x) = \sum_{j=0}^{(n-1)/2} \sum_{k=0}^{j} \binom{n}{2j}\binom{j}{k} x^{n-2(j-k)} a^{j-k} = x^n + nh$$

So, we see that

$$[x^3] \equiv 0 \pmod{n}$$

$$\implies \left(\binom{n}{n-3}\binom{(n-3)/2}{0} + \binom{n}{n-1}\binom{(n-1)/2}{1}\right) a^{(n-3)/2} \equiv 0 \pmod{n}$$

$$\implies \binom{n}{n-3} \equiv 0 \pmod{n}$$

since $\gcd(a, n) = 1$.

Also, we have

$$[x^5] \equiv 0 \pmod{n}$$

$$\implies \left(\binom{n}{n-5}\binom{(n-5)/2}{0} + \binom{n}{n-3}\binom{(n-3)/2}{1} + \binom{n}{n-1}\binom{(n-1)/2}{2}\right) a^{(n-5)/2} \equiv 0 \pmod{n}$$

$$\implies \binom{n}{n-5} \equiv 0 \pmod{n}$$

So, we can get (one can prove by induction)

$$[x^3] \equiv [x^5] \equiv [x^7] \equiv \cdots \equiv [x^{n-2}] \equiv 0 \pmod{n}$$

$$\implies \binom{n}{n-3} \equiv \binom{n}{n-5} \equiv \binom{n}{n-7} \equiv \cdots \equiv \binom{n}{2} \equiv 0 \pmod{n}$$

$$\implies \binom{n}{2} \equiv \binom{n}{3} \equiv \binom{n}{4} \cdots \equiv \binom{n}{n-2} \equiv 0 \pmod{n} \quad (2)$$

Suppose here that $n = \prod_{i=1}^{m} p_i^{b_i}$ is a composite number where $p_1 p_2 \cdots p_m$ are primes and b_i are positive integers.

Let $[[N]]$ be the number of prime factor p_i in N.

Then, we have the followings :

+ $[[1!]] = [[2!]] = \cdots = [[(p_i - 1)!]] = 0$

+ $[[p_i!]] = 1$

+ $[[(n-1)!]] = [[(n-2)!]] = \cdots = [[(n-p_i)!]]$

Using these, we see that

$$\binom{n}{1} = \frac{n!}{1!(n-1)!} = n, \binom{n}{2} = \frac{n!}{2!(n-2)!}, \cdots, \binom{n}{p_i - 1} = \frac{n!}{(p_i-1)!(n-(p_i-1))!}$$

are divisible by $p_i^{b_i}$, and that

$$\binom{n}{p_i} = \frac{n!}{p_i!(n-p_i)!}$$

is not divisible by $p_i^{b_i}$.

Therefore, we see that

$$\binom{n}{1} = \frac{n!}{1!(n-1)!} = n, \binom{n}{2} = \frac{n!}{2!(n-2)!}, \cdots, \binom{n}{p_1 - 1} = \frac{n!}{(p_1-1)!(n-(p_1-1))!}$$

are divisible by n, and that

$$\binom{n}{p_1} = \frac{n}{p_1!(n-p_1)!}$$

is not divisible by n, which contradicts (2).

It follows that n is a prime number. ■