Primes, Pseudoprimes and Binary Sequences

In Chapter 13 it was shown that the sigma orbit (sigOrb) was defined from the Perrin sequence P(n) and the Euler totient ϕ(n) function.

[1] $$\text{SigOrb}(n) = \left(\frac{1}{n}\right) * \sum_{\frac{d}{n}} P(d) * \emptyset\left(\frac{n}{d}\right)$$

where $\frac{d}{n}$ represent all the divisors of n. If this equation is multiplied by n and P(n) is subtracted then the result is zero for prime numbers and Perrin pseudoprimes:

[2] $$n*\text{SigOrb}(n) - P(n) = 0$$

if and only if n is a prime or pseudoprime.

When the first 56 values of [2] are calculated and converted to a binary mod 2, a period 14 binary sequence is found. The pattern [0,0,0,0,0,1,0,0,0,1,0,1,0,1] repeats for all integers mod 14 as can be seen in Table 1 of Chapter 13b.[OEIS A127687] The conclusion from this pattern is that primes can only be found at 1, 3, 5, 7, 9, 11 and 13 mod 14, which is true, as these are odd numbers. It also proves that Perrin pseudoprimes cannot be found at 6, 10, 12 and 0 mod 14 since [2] is required to be zero by the definition of a pseudoprime. Of the first 33 Perrin unrestricted and restricted pseudoprimes, none are found at 6, 8, 10, 12 or 0 mod 14. Some examples were shown in Chapter 13.

This chapter explores the question; *Is the Period 14 binary sequence unique to the Perrin sequence?* Does this binary sequence represent the location of primes and sequence pseudoprimes for other integer sequences? We have demonstrated previously that any irreducible polynomial of the form G(x) = $x^3 + a_2x^2 + a_1x + a_0$, generates an integer sequence.

Define with subscripts (a_2, a_1, a_0) the sigma orbit and integer sequence associated with G(x).

[3] $$\text{SigOrb}(n)_{(a2,\,a1,\,a0)} = \left(\frac{1}{n}\right) * \sum_{\frac{d}{n}} P(d)_{(a2,a1,a0)} * \emptyset\left(\frac{n}{d}\right)$$

A binary sequence is generated from [3],

[4] $$[\, n*\text{SigOrb}(n)_{(a2,\,a1,\,a0)} - P(n)_{(a2,\,a1,\,a0)}] \bmod 2$$

The binary sequence for the Perrin sequence is then represented as,

[5] $$[n*\text{SigOrb}(n)_{(0,-1,-1)} - P(n)_{(0,-1,-1)}] \bmod 2$$

We start by looking at a few examples of equation [4] for other G(x) and sequences; their discriminant and their corresponding binary sequence.

[5a,b,c,d,e,f,g]	$[n*\text{SigOrb}(n)_{(0,-1,-1)} - P(n)_{(0,-1,-1)}] \bmod 2$	(-23)	[0,0,0,0,0,1,0,0,0,1,0,1,0,1]
	$[n*\text{SigOrb}(n)_{(-1,0,-1)} - P(n)_{(-1,0,-1)}] \bmod 2$	(-31)	[0,1,0,1,0,0,0,1,0,0,0,0,0,1]
	$[n*\text{SigOrb}(n)_{(-2,0,-1)} - P(n)_{(-2,0,-1)}] \bmod 2$	(-59)	[0,0,0,0,0,1]
	$[n*\text{SigOrb}(n)_{(-2,-2,-1)} - P(n)_{(-2,-2,-1)}] \bmod 2$	(-83)	[0,0,0,0,0,1]
	$[n*\text{SigOrb}(n)_{(-5,1,-2)} - P(n)_{(-5,,1,-2)}] \bmod 2$	(-907)	[0,1,0,1,0,0]

$[n*SigOrb(n)_{(0,-2,-2)} - P(n)_{(0,-2,-2)}] \bmod 2$ (-76) [0,0,0,0,0,0,0, …….

$[n*SigOrb(n)_{(-1,-1,-1)} - P(n)_{(-1,-1,-1)}] \bmod 2$ (-44) [0,1,0,1,0,1]

These examples show at least 6 distinct patterns; 2 patterns of period 14, 2 patterns of period 6, 1 pattern of period 2, and an infinite pattern of zeros. There appears no connection of the class 3 cubic polynomials (first 4 examples) to the pattern type. It is interesting that the first two examples are mirror images of each other for positive integers between 1 and 14. When the pattern is calculated for discriminants (-23)and (-31) to include negative integers the complete pattern from integers -14 to 14 show this mirror structure: [1,0,1,0,1,0,0,0,1,0,0,0,0,0,1,0,0,0,0,0,1,0,0,0,1,0,1,0,1] and [1,0,0,0,0,0,1,0,0,0,1,0,1,0,1,0,1,0,1,0,0,0,1,0,0,0,0,0,1]. The mod 2 values for negative sequences with $a_0>|1|$ cannot be calculated since these negative sequences are rational numbers. (See my Chalkboard #8).

It can be shown that equation [2] is valid for all primes if modified as;

[6] $$n*SigOrb(n)_{(a2,a1,a0)} - P(n)_{(a2,a1,a0)} - a_2*(n-1) = 0$$

where a_2 is the x^2 coefficient of the general cubic polynomial G(x). It is still to be proven if [6] is valid for pseudoprimes for polynomials with $a_2> 0$. For the Perrin sequence $a_2 = 0$ and both odd and even valued unrestricted Perrin pseudoprimes do not contribute to the term $a_2*(n-1)$. Equation [6] is valid for all prime numbers and independent of the sequence used for calculation. The classification of primes into Type 1,2, and 3 (Adam and Shank's Q, I, and S) differs from sequence to sequence. Classification is based on the period length of the prime, p mod p. For example, 23 and 59 are type S for the Perrin sequence, $P(n)_{(0,-1,-1)}$, and there are only 3, S primes (599, 883, 991) common to both $P(n)_{(0,-1,-1)}$ and $P(n)_{(-1,-1,-1)}$ and only 2, S primes (47,617) common to both $P(n)_{(-1,0,-1)}$ and $P(n)_{(-1,-1,-1)}$.[see reference [1]]. Although [6] indicates which number is prime it cannot detect whether a prime is S, Q or I. The best method is to show whether a prime is S type is to find if { $P(p-1)_{(a2,a1,a0)}$, $P(p)_{(a2,a1,a0)}$, $P(p+1)_{(a2,a1,a0)}$} mod p has a signature {3, $P(1)_{(a2,a1,a0)}$, $P(2)_{(a2,a1,a0)}$} indicating a return to the beginning of the sequence.

What determines the patterns in [5a] through [5g]? It can be shown that the magnitude of the discriminant is not responsible since cubic polynomials of the same discriminant can have different patterns. The answer appears to be the relative values of the triad (a_2, a_1, a_0). The rules are:

1. [0,0,0,0,0,1,0,0,0,1,0,1,0,1] if a_0 is odd, a_2 is even and $a_1 = a_2/2$ is odd.
2. [0,1,0,1,0,0,0,1,0,0,0,0,0,1] if a_0 is odd, a_2 is odd and a_1 is even.
3. [0,0,0,0,0,1] if a_0 is odd, a_2 even, a_1 is even or $a_1 = a_2/2$ is even.
4. [0,1,0,1,0,0] if a_0 even and a_1 and a_2 are odd.
5. [0,0,0,0,0,0,0, ……. If a_0 is even and a_2 is even and $a_1 = a_2/2$ is odd.
6. [0,1,0,1,0,1] if a_0 is even, a_2 is odd and a_1 is even.

Examples of rules for each pattern: G(x) (Discriminant)

1. $x^3 - 2x^2 + x + 1$ (-31), $x^3 - 6x^2 - 3x - 1$ (-783)
2. $x^3 - 7x^2 + 6x - 3$ (-1191), $x^3 + x^2 + 2x - 1$ (-87)
3. $x^3 - 4x^2 + 2x - 1$ (-107), $x^3 + 2x^2 + 3$ (-147)

4. $x^3 - 3x^2 - 3x + 2$ (621), $x^3 - x^2 + 5x + 4$ (-1251)
5. $x^3 - 6x^2 - 3x - 2$ (-2052), $x^3 + 2x^2 - x - 4$ (-152)
6. $x^3 - 3x^2 - 2x - 2$ (-472), $x^3 - x^2 - 2$ (-116)

***Mathematica* code for the binary sequence**

Given a general polynomial $G(x) = x^3 - a_2x^2 - a_1x - a_0$, and the first integers of the corresponding integer sequence {A0, A1, A2} the binary sequence for G(x) is generated using *Mathematica*. The following example assumes $(a_2, a_1, a_0) = (1, 0, 1)$ and (A0, A1, A2) = (3, 1, 1);

```
Mod[With[{kmax=14}, Table[N[m*Sum[((RecurrenceTable[{a[n+3] ==a0*a[n]+a1*a[n+1] +a2*a[n+2], a[0] ==A0,a[1] ==A1,a[2] ==A2},a,
        {n, m/i, m/i}]) * EulerPhi[i]), {i, Divisors[m]}] * (1/m)-RecurrenceTable[{a[n+3] ==a0*a[n] +a1*a[n+1] +a2*a[n+2], a[0] ==A0,a[1] ==A1,a[2] ==A2},a,
      {n,m,m}],4],{m,1,kmax}]],2]
```

{{0}, {1.000}, {0.*10^{-4}}, {1.000}, {0.*10^{-4}}, {0.*10^{-4}}, {0.*10^{-4}}, {1.00}, {0.*10^{-3}}, {0.*10^{-3}}, {0.*10^{-3}}, {0.*10^{-3}}, {0.*10^{-3}},{1.00}}

1. W. Adams and D. Shanks, *Strong Primality Tests that are not Sufficient, Mathematics of Computation*, **39** (159), July 1982, pp 255-300.

Richard Turk

September 2, 2017