## PERRIN PSEUDOPRIMES AND THE SIGMA ORBIT

Given a prime p the P(p) term of the Perrin sequence (3,0,2…) divides p.

For certain composites n = p1v1*p2v2*p3v3.... n can also divide P(n) and n is called a Perrin pseudoprime.

W.W. Adams and D. Shanks, "Strong Primality Tests that are not sufficient", Math. Comp.

39, (1982) introduced primality tests for third order recurrences such as the Perrin recurrence.

They also introduced the concept of "signature" of a sequence which depended on the type of prime.

The correlation of their labeling of primes with types of primes introduced in Chalkboards 2 and 3 (see www.perrin088.org ) is as follows:

S-signature = Type 3 prime

I-signature = Type 2 prime

Q-signature = Type 1 prime

Adams and Shanks also discovered the smallest "unrestricted pseudoprimes" a search which was unsuccessful by Perrin in 1899. A list of these primes (PPP(1)=271441, PPP(2)=904631, PPP(3)=16532714, PPP(4)=24658561,.. can be found in *OEIS A013998*.

Several composites on this list are products of two Type 3 primes,

PPP(6)= 3037*9109
PPP(7)= 4831*9661
(similar type 3 primes are found up to PPP(26).

In Chalkboard 11 (see www.perrin088.org ) it was shown that the total number of unlabeled MISs of the n-cycle is also the number of cyclic combinations of 2 and 3 which add to give n. This number is calculated from the Euler totient transform [ϕ (n/d) or the Euler phi function]

The jth term of the Perrin sequence P and the sigma orbit (Sigorb) is defined

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

where the summation is over all divsors of n and Sigorb(n) is the number of cyclic combinations of 2 and 3 adding to n

If n is a Perrin pseudoprime then this equation can be used to prove that

$$\textbf{P(n) mod n = 0} = \sum_{\frac{d}{n}} P(d) * \emptyset\left(\frac{n}{d}\right) \textbf{ mod n}$$

since Sigorb*n mod(n) = 0

If n is composite, not equal to a pseudoprime then

$$\textbf{(P(n) + } \sum_{\frac{d}{n}} \boldsymbol{P(d)} * \emptyset\left(\frac{n}{d}\right) \textbf{) mod n = 0}$$

where d is not equal to 1 in the summation since $\phi(1) = 1$.

**Example 1**

PPP(1)

Although 521 is a type 1 prime

n= 521*521 and

P(521) mod n = 0

P(521)*$\phi$(521)+ P(521)*$\phi$(521)= 0 mod n

The fact that many type 3 primes have the p3 sequence term P(p3) mod p3=0 makes the above summation true for certain products of two type 3 primes.

$$P(p3_1)*\phi(n/p3_1)+ P(p3_2)*\phi(n/p3_2)= 0 \bmod n$$

**Example 2**

PPP(2) =n= 7*13*9941 = 904631

Primes 7 and 9941 are type 1 and 13 is type 2.

The Euler totient calculator (www.javascripter.net/math ) is used to find $\phi$ (i) where i is a composite and $\phi$(p) = p-1.

1. find all products of two primes:
   9941*13 = 129233
   9941*7 = 69587
   13*7 = 91
   $\phi$(91) =72
   $\phi$(69587) =59640
   $\phi$(129233) =119280
   $\phi$(9941) =9940
   $\phi$(13) =12
   $\phi$(7) =6

2. P(i) is found from Excel x(n+3) = [x(n-1) + x(n)] mod n There are six summations:

   P(129233)*$\phi$(7) + P(69587)*$\phi$(13) +P(91)*$\phi$(9941) +
   P(9941)*$\phi$(91) + P(13)*$\phi$(69587) + P(7)*$\phi$(129233) =

656145*6+49712*12+596460*9940+397640*72
+39*59640+7*119280 = 5965136814
where 5965136814/904631 = 6594 so PPP(2) is a Perrin pseudoprime;
P(904631) = 0 mod 904631

**Example 3:**

PPP(4) =n= 19*271*4789 = 24658561
primes 19 and 4789 are type 1 and 271 is type 3.

1. find all products of two primes:
   4789*271 = 1297819
   4789*19 = 90991
   19*271 = 5149
   ϕ(1297819) =1292760
   ϕ(90991) =86184
   ϕ(5149) =4860
   ϕ(4789) =4788
   ϕ(271) =270
   ϕ(19) =18
2. P(i) is found from Excel x(n+3) = [x(n-1) + x(n)] mod n There are six summations:

P(1297819)*ϕ(19) + P(90991)*ϕ(271) +P(5149)*ϕ(4789) +
P(4789)*ϕ(5149) + P(271)*ϕ(90991) + P(19)*ϕ(1297819) =
8364142*18+6063083*270+19893506*4788+8428640*4860+
1233321*86184+209*1292760 = 244563607998
where 244563607998/24658561 = 9918 so
PPP(4) is a Perrin pseudoprime;
P(24658561) = 0 mod 24658561

The last example is a composite of 3 type 3 primes which is not a Perrin pseudoprime.

n= 59*101*271 = 1614889

1. find all products of two primes:

   101*271 = 27371
   59*101 = 5959 59*271 =
   15989
   ϕ(27371) =27000
   ϕ(15989) =15660
   ϕ(5959) =5800
   ϕ(271) =270
   ϕ(101) =100
   ϕ(59) =58

2. P(i) is found from Excel x(n+3) = [x(n-1) + x(n)] mod n. There are six summations:

P(27371)*ϕ(59) + P(15989)*ϕ(101) +P(5959)*ϕ(271) +
P(271)*ϕ(5959) + P(101)*ϕ(15989) + P(59)*ϕ(27371) =
1581558*58+978790*100+824591*270+317341*5800+
388345*15660+1508866*27000 = 49073691434
where 49073691434 mod 1614889 = 444502 so n is
**not** a Perrin pseudoprime and
P(1614889) = (1614889-444502)= 1170387 mod 1614889

To show this is reasonable, consider the sequence length calculated for the composite n which is the product of the sequence length of 3 type 3 primes: From an earlier Chalkboard:

lcm[(p1-1)*(p2-1)*(p3-1)]=58*100*270 = (2*29)*(2*2*5*5)*(3*3*3*5*2)
lcm($29*2^4*3^3*5^3$) = $29*2^2*3^3*5^2$ = 78300
Subtracting 20 sequence lengths (and 1 step) from 1614889
1614889 -20*78300 -1 = 4889 -1 = 4888
Using Excel I find;

P(4888) = 1170387 mod n = P(1614889) mod 1614889

This above analysis can be used to **predict and confirm** large Perrin pseudoprimes for any combination of primes of type 1, 2, 3 (Q,I,S) signatures

Also, P(n) can be calculated mod n for very large values of n.

***The examples above demonstrate the first time the Euler phi transform has been applied to Perrin pseudoprimes.***

Richard Turk

August 15, 2015