A formula for generating primes and a possible infinite series of Poulet numbers

Marius Coman
Bucuresti, Romania
email: mariuscoman13@gmail.com

Abstract. An amazingly easy to formulate but rich in consequences property of Fermat pseudoprimes to base 2 (Poulet numbers).

A formula for generating primes

I studied Fermat pseudoprimes for quite a while (I posted on OEIS few series and properties of Carmichael numbers and Poulet numbers) and I always believed that in the structure of pseudoprimes resides a key for obtaining primes. Here I expose such a formula that generates primes and products of few primes.

I first noticed that the first Poulet number, 341, can be written as (2^10 – 1)/3 and after that I found other Poulet numbers that can be written as (2^k – 1)/3: 5461, 1398101, 22369621, 5726623061, 91625968981, respectively for k = 14, 22, 26, 34, 38 (I conjecture that there are infinite Poulet numbers of this form).

I then noticed that the third Poulet number, 645, can be written as (2^4*11^2 – 1)/3 and after that I found other Poulet numbers that can be written as (2^k*q^2 – 1)/3, where q is prime: 2465, 2821, 8321, respectively for q = 43, 23, 79 (I conjecture that there are infinite Poulet numbers of this form too).

From the first 23 Poulet numbers, 19 can be written as (2^k*q – 1)/3, where q is prime or square of prime!

So the formula to generate numbers q that are primes, squares of primes and products of few primes or squares of primes is simply q = (3*P + 1)/2^k, where P is a Poulet number and k is the biggest natural number for that q is an integer.

I list below few values of N = 3*P + 1, for 9 consecutive Poulet numbers with 12 digits taken randomly (I note generically with s the squarefree semiprimes and with r the products of 3 distinct prime factors):

for P = 994738556701 we get N = 2^3*s;
for P = 994738580641 we get N = 2^2*746053935481;
for P = 994750702441 we get N = 2^2*r;
for P = 994767925201 we get N = 2^2*746075943901;
for P = 994788345601 we get N = 2^2*746091259201;
for P = 994818048445 we get N = 2^3*s;
for P = 994830588181 we get N = 2^6*46632683821;
for P = 994853432581 we get N = 2^4*29^2*53^2*281^2;
for P = 994868271001 we get N = 2^2*r.

We obtained, from 9 consecutive values of P, four primes, two semiprimes and two products of 3 distinct primes. It can easily be seen the potential of this formula as a generator of primes. I didn't forget the product of 3 squares; here's something interesting; we got through this formula primes, squarefree products of primes, squares of primes and squares of products of primes, but we didn't find a product to contain primes to a bigger power than two or both primes and squares of primes together, therefore we conjecture that there are no such numbers q, where q = (3*P + 1)/2^k (and P is a Poulet number and k is the biggest n natural for that q is an integer).

We know take the four primes randomly generated, *i.e.* 746053935481, 746075943901, 746091259201 and 46632683821, and we see that they have also the property to generate primes; if we put them in a recurrent formula (Cunningham's chain type), we obtain for M = 3*t + 1 the following values:

for t = 746053935481 we get M = 2^2*559540451611;
for t = 746075943901 we get M = 2^3*1381*202591223;
for t = 746091259201 we get M = 2^2*47*11905711583;
for t = 46632683821 we get M = 2^3*174872256433.

We now take a prime newly generated, 559540451611. We have:

3*559540451611 + 1 = 2*839310677417.

I believe these results are encouraging in the study of recurrent sequences of the type $P_n = (3*P_{n-1} + 1)/2^k$, where k is the biggest natural number for that P_n is an integer and P_0 is a Fermat pseudoprime to base 2.

A possible infinite series of Poulet numbers

We saw above that Poulet numbers 341, 5461, 1398101, 22369621, 5726623061, 91625968981 can be written as (4^k – 1)/3 for k = 5, 7, 11, 13, 17, 19. We did'n obtain a Poulet number for any other value of k from 1 to 19 beside those.

We calculate now (4^k – 1)/3 for k = 23, 29, 31, 37, 41 and we get respectively:

: 23456248059221 = 47*178481*2796203;
: 96076792050570581 = 59*233*1103*2089*3033169;
: 1537228672809129301 = 715827883*2147483647;
: 6296488643826193618261 = 223*1777*25781083*616318177;
: 1611901092819505566274901 = 83*13367*164511353*8831418697.

Unfortunatelly I have just Mr. Richard Pinch’s tables to verify if a number is a Poulet number or not (tables that are just up to 10^12) and there is no such a simple test to verify this as it is the Korselt criterion at Carmichael numbers. But the premises that the numbers we calculated are Poulet numbers are good: they are squarefree products of few primes. I don’t have enough data to conjecture that a number of the form (4^k – 1)/3 is a Poulet number *if and only if* k is prime, k ≥ 5 (which would be a tremendously result, to put prime numbers in a bijection with a subset of Poulet numbers!), but I do make two conjectures:

Conjecture 1: There are infinite many Poulet numbers of the form (4^k – 1)/3, where k is positive integer.

Conjecture 2: Any number of the form (4^k – 1)/3, where k is prime, k ≥ 5, is a Poulet number.

The second conjecture, if true, would be, as I know, the first generic formula for an infinite series of Poulet numbers (of type “for any possible value of this we obtain necessarily that”, cause formulas that generates Poulet numbers, but not only Poulet numbers I submitted myself a few to OEIS). Besides this, the conjecture has yet another major implication: from the first million natural numbers, about 80 thousand are primes and just about 250 are Poulet numbers, which lead to the conclusion that Poulet numbers are far more rare than prime numbers. The conjecture, if true, would show that, in fact, for the first about 7 consecutive prime numbers, we have 7 corresponding Poulet numbers spread in the first about 40 thousand Poulet numbers and, consequently, the set of prime numbers is so just a very mean subset of the set of Poulet numbers!