A SHORT JOURNEY WITH PYTHAGORIAN PRIME NUMBERS

by

Hubert Schaetzel

Abstract. — The purpose of this article is a short study of the decomposition of the Pythagorian primes into two squares based on a theorem established by Stan Wagon.

Résumé. — *(Un court voyage parmi les nombres premiers pythagoriens).* Le but de cet article est une courte étude de la décomposition des nombres premiers pythagoriens en deux carrés basée sur un théorème établi par Stan Wagon.

Theorem 1. — *The equation*

$$p = (2\alpha)^2 + \beta^2$$

has a unique solution (α, β), $\alpha > 0$, $\beta > 0$, β *odd,* $p \equiv 1 \mod 4$.
There is no solution to the previous equation if $p \equiv 3 \mod 4$.
Proof. — This is the Fermat's theorem on the sums of two squares. See reference [**1**]. □

Theorem 2. — *Let us consider* $p = (2\alpha)^2 + \beta^2$. *Let us have the successive Euclidean divisions of* p *starting with* $g^{\frac{p-1}{4}} \mod p$ *where* $p \equiv 1 \mod 4$. *Then, not necessarily in that order,* 2α *and* β *are the first divider and remainder such that their squares sum up to* p.
Proof. — This is a result obtained by Stan Wagon [**2**]. □

Not entering the specific of the proof, that the reader can find thanks to the reference, an early hint to this result is to consider the following pairs of

Key words and phrases. — Pythagorian prime numbers, algorithm, enumeration.

equations, which doesn't prove the Stan Wagon result of course, but makes the $g^{\frac{p-1}{4}} \mod p$ ratio emerge.

$$\begin{aligned} p &= (2\alpha)^2 + \beta^2 \\ &\equiv -g^{\frac{p-1}{2}}(2\alpha)^2 + \beta^2 \mod p \\ &\equiv -(g^{\frac{p-1}{4}}2\alpha + \beta)(g^{\frac{p-1}{4}}2\alpha - \beta) \mod p \end{aligned}$$

and

$$\begin{aligned} p &= (2\alpha)^2 + \beta^2 \\ &\equiv (2\alpha)^2 - g^{\frac{p-1}{2}}\beta^2 \mod p \\ &\equiv -(g^{\frac{p-1}{4}}\beta + 2\alpha)(g^{\frac{p-1}{4}}\beta - 2\alpha) \mod p. \end{aligned}$$

Corollary 1. — *Let us have the successive Euclidean divisions of p by $g^{\frac{p-1}{4}} \mod p$. Then, every divider (including $g^{\frac{p-1}{4}} \mod p$) and remainder in the division process are linear combinations of 2α and β.*

Proof. — Starting from the end results of the division process which are 2α and β, the reverse multiplying process provides linear combinations of 2α and β at each step. The final step $p = u_0.2\alpha + v_0.\beta$, $u_0 = 2\alpha$, $v_0 = \beta$, subsequent to the result for $g^{\frac{p-1}{4}} \mod p$, completes the said linear combinations' series. □

So let us have the Euclidean division remainders r_i, with $r_0 = p$ and write the successive equalities

$$r_i = u_i.2\alpha + v_i.\beta.$$

Then numerical experimentation shows that the cross-products

$$cp_i = u_i.v_{i+1} - u_{i+1}.v_i$$

have characteristic properties (which we won't intent to prove here). Ideally, the leading one of these properties is that successive cp_i show alternating 1 and -1 values. This is of course reminiscent of the i^{th} convergent to a continued fraction u_i/v_i (see reference **[3]** theorem 3 and corollary 2) with the likewise formula

$$\frac{u_{i+1}}{v_{i+1}} - \frac{u_i}{v_i} = -\frac{cp_i}{v_i v_{i+1}} = \frac{(-1)^{i+j}}{v_i v_{i+1}}, \quad j = or(0,1).$$

This ideal is not rare as the reader can verify in appendix B and longer series are provided by more and more greater prime numbers. Note that the thereby data is issued for the smallest values of the primitive roots of p. One such ideal example is $p = r_0 = 100000717$:

i	r_i	u_i	v_i	cp_i		i	r_i	u_i	v_i	cp_i
0	100000717	6714	7411	1		8	431858	29	32	1
1	53515428	3593	3966	-1		9	283197	19	21	-1
2	46485289	3121	3445	1		10	148661	10	11	1
3	7030139	472	521	-1		11	134536	9	10	-1
4	4304455	289	319	1		12	14125	1	1	1
5	2725684	183	202	-1		13	7411	0	1	-1
6	1578771	106	117	1		14	6714	1	0	
7	1146913	77	85	-1						

Note that we have often in the above case the pair of relationships

$$u_{i+2} = u_i - u_{i+1}, \quad v_{i+2} = v_i - v_{i+1}.$$

If this pair occurs and if the cross-product cp_i equals $(-1)^{i+j+1}$, it is immediate to prove that $cp_{i+1} = -cp_i = (-1)^{i+j}$ (here case i = 0 for example). The reciprocal is however not true (here case i = 2).
Let us call "almost perfect linear prime for g", a prime such that $cp_i = (-1)^{i+j+1}$ for all i up to the final result and "perfect linear prime for g", a prime such that in addition $u_{i+2} = u_i - u_{i+1}$ at each step. The first kind are quite current, for g the smallest primitive root, as there are still more than 50% of them up to size 1000000. The second kind, on the contrary, gets soon rarer with only 0.2% in the same range. A limited list of this second kind is given is appendix C.
The alternate ± 1 pattern happens in general when 2α and β are of "similar" values. When it is not the case, with a larger difference between these two, the said pattern is partially hidden. It starts usually with the first cross-product requiring a modulo p or $-p$ operation to show the 1 or -1 values like shown underneath.

r_i	u_i	v_i	cp_i	$cp_i \ mod \ m_i$	m_i
100000049	10000	7	40800019993	1	100000049
28570014	1	4080002	-2040001	-1	-10000
14290007	1	2040001	-12250006	-6	-10000
14280007	7	2030001	-2030001	-1	-10000
10000	1	0	1		
7	0	1			

Further cross-products values may be a quite more elaborate composite results. In order to get 1 or -1, one may have to add linear combinations of future values of r_i occurring in the successive divisions. For example, $cp = -12250006 = 1 - 7 - 10000c \equiv 1 - 7 \bmod 10000$ (above) or $cp =$

$1230001 = 1 + 10000c \equiv 1 \bmod 10000$ (underneath).

r_i	u_i	v_i	cp_i	$cp_i \ mod \ m_i$	m_i
100000081	10000	9	98700079946	-1	-100000081
88890072	6	9870008	-32100026	1230001	11110009
11110009	4	1230001	-1230001	-1	-10000
10000	1	0	1		
9	0	1			

As in these cases, a lot of "things" happen in the same time, these examples converge to the $(2\alpha, \beta)$ result faster than the regular continued fractions' type, a systematic $cp_i = (-1)^{i+j+1}$ equality generating the longest path to the end result. The hidden steps go always by odd steps advance so that the alternate ± 1 values shows up at due time and place. Here -6 stands for 1 and 1230001 for 1, both in between -1.

Appendix A provides a computer program to produce quick examples of Euclidean divisions of p by $g^{\frac{p-1}{4}} \mod p$, for g the smallest primitive root of p, and the corresponding successive linear decompositions parametrized by 2α and β. The results for $p \leq 97$ are also provided in the said appendix.

Appendix A. Euclidian divisions program

This appendix enables to get the linear combination's factors (u_i, v_i) of the remainders $t_i = u_i.(2\alpha) + v_i.(\beta)$ starting with the division of $t_0 = p$ by $g^{\frac{p-1}{4}}$ where $p \equiv 1 \ mod \ 4$ and $p = (2\alpha)^2 + \beta^2$.
It suffices to make a copy of the program on the Pari/gp online application (menu Main, GP in your browser).

```
{pmin = 3; /* choose min prime numbers' range */
pmax = 1000; /* choose max prime numbers' range */
s = vector(2); infinite = 1000;
forprime(p = pmin, pmax, g = lift(znprimroot(p)); rep = 1; t = vector(3); hh = 0;
gp4 =1; for(u = 1, (p-1)/4, gp4 = (gp4*g)%p);
if(p%4 == 1,
for(i = 1, p, b = sqrt(p-4*i*i); if(frac(b) == 0, a = i; b = floor(b); break));
a2 = 2*a; s[1] = a2; t[2] = a2; s[2] = b; divi1 = p; divi2 = gp4;
print("p "p); print(divi1" "s);
for(k = 2, infinite,
if(divi2 == b, s[1] = 0; s[2] = 1; t[3] = 0; print(b" "s);
s[1] = 1; s[2] = 0; print(a2" "s);
if(t[3] <> t[1]-t[2], rep = 0);
if(rep == 1, print("perfect linear prime")); break);
if(divi2 == a2, s[1] = 1; s[2] = 0; t[3] = 1; print(a2" "s);
s[1] = 0; s[2] = 1; print(b" "s);
if(t[3] <> t[1]-t[2], rep = 0);
if(rep == 1, print("perfect linear prime")); break);
for(j = 1, floor(divi2/a2), m = (divi2-a2*j)/b;
if(frac(m) == 0, s[1] = j; s[2] = m; t[3] = j; hh = hh+1;
divi3 = divi1-divi2*floor(divi1/divi2);
divi1 = divi2; divi2 = divi3;
if(hh > 1, if(t[3] <> t[1]-t[2], rep = 0));
t[1] = t[2]; t[2] = t[3];
print(divi1" "s); break)))))}
```

Appendix B. Cross-products' sample

A few sampling of the results of the cross-products $cp_i = u_i.v_{i+1} - u_{i+1}.v_i$ of successive couples (u_i, v_i) are given underneath showing mostly alternating 1 and -1 values but also some exceptions.

r_i	u_i	v_i	cp_i	*modulo*
5	2	1	-1	
2	1	0	1	
1	0	1		
13	2	3	1	
8	1	2	-1	
5	1	1	1	
3	0	1	-1	
2	1	0		
17	4	1	35	1+2.17
13	1	9	-9	-1-2.4
4	1	0	1	
1	0	1		
29	2	5	-1	
12	1	2	1	
5	0	1	-1	
2	1	0		
37	6	1	149	1
31	1	25	-25	-1-4.6
6	1	0	1	
1	0	1		
41	4	5	1	
32	3	4	-1	
9	1	1	1	
5	0	1	-1	
4	1	0		
53	2	7	1	
30	1	4	-1	
23	1	3	1	
7	0	1	-1	
2	1	0		
61	6	5	1	
11	1	1	-1	
6	1	0	1	
5	0	1		

r_i	u_i	v_i	cp_i	*modulo*
73	8	3	-1	
27	3	1	1	
19	2	1	-1	
8	1	0	1	
3	0	1		
89	8	5	1	
34	3	2	-1	
21	2	1	1	
13	1	1	-1	
8	1	0	1	
5	0	1		
97	4	9	-1	
22	1	2	1	
9	0	1	-1	
4	1	0		

Appendix C. Perfect linear Pythagorean primes

The numbers of primes numbers, either $1 \mod 4$, "almost perfect linear" or "perfect linear" are given in the underneath table. The data is issued with the choice g being the smallest primitive root of p. The almost perfect linear primes are defined by a systematic cross-product $cp_i = (-1)^{i+j}$, for some fixed value $j = 0$ or 1. The perfect linear primes are defined by $u_{i+2} = u_i - u_{i+1}$, $v_{i+2} = v_i - v_{i+1}$.

$p \leq$	$1 \ mod \ 4$ *type*	p *almost perfect*	p *perfect*
97	11	9	2
997	80	65	5
9949	608	455	15
99989	4783	3183	36
999961	39175	20067	84

The list of the 84 perfect linear prime numbers (for smallest g choice) smaller than $p < 1000000$ is the following:

13, 53, 229, 233, 733, 1093, 1229, 1433, 2089, 2213, 4493, 7573, 8713, 9029, 9413, 10613, 13229, 18229, 21613, 24029, 26573, 27893, 28657, 33493, 41213, 42089, 42853, 45433, 46229, 55229, 59053, 65029, 75629, 82373, 91813, 94253, 120413, 140629, 157181, 162413, 165653, 178933, 182333, 189229, 207029, 214373, 225629, 233293, 237173, 245029, 253013, 257053, 267353, 283117, 284153, 299213, 319289, 368453, 375833, 378229, 388133, 439573, 444893, 494213, 499853, 552053, 570029, 582173, 585289, 588293, 619373, 632029, 677333, 683933, 717413, 727673, 759797, 779693, 815413, 874229, 927373, 935093, 966293, 994073.

Literature and sources

[1] Leonard Eugene Dickson. History of the Theory of Numbers. https://en.wikipedia.org/wiki/Fermat's_theorem_on_sums_of_two_squares.

[2] Stan Wagon (1990). Editor's Corner: The Euclidean Algorithm Strikes Again. American Mathematical Monthly, 97 (2): 125, doi:10.2307/2323912.

[3] https://en.wikipedia.org/wiki/Continued_fraction

[4] https://hubertschaetzel.wixsite.com/website.

September 27, 2022

Hubert Schaetzel, INPG Grenoble • *E-mail :* hubert.schaetzel@wanadoo.fr
Url : https://hubertschaetzel.wixsite.com/website