# ON THE ROOTS OF DIOPHANTINE EQUATIONS

$\mathrm{mod}(X^n + Y^n, P) = 0$

SEPPO MUSTONEN

Abstract. This is a report of numerical and graphical experiments about the roots of Diophantine equations of the form $\mathrm{mod}(X^n + Y^n, P) = 0$.
Example: `https://www.survo.fi/demos/index.html#ex130`

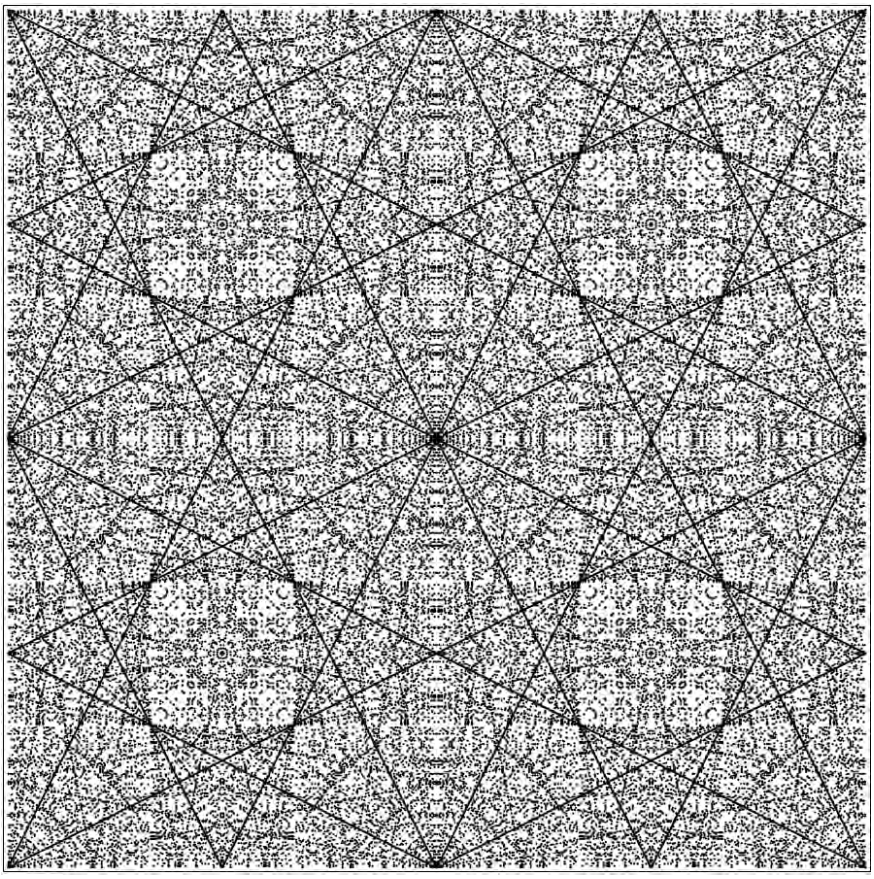


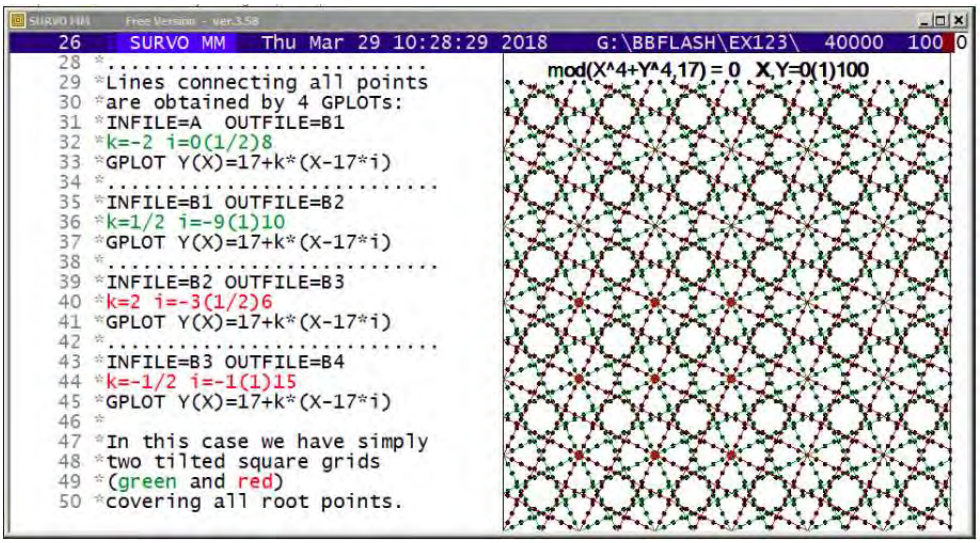
FIGURE 1. Roots for $n = 32, P = 641, \quad 0 \leq X, Y \leq 2 \times 641$

*Date*: 21 August 2018.

I have been developing the Survo software for statistical data analysis and graphics since 1960'ies. Especially during the last decades I have tested the functions of Survo by numerical and graphical examples related to purely mathematical subjects [1] - [7].
The first paper [1] related to roots of the Pythagorean equation $X^2+Y^2=Z^2$ led me to make plots of the roots of Diophantine equations $X^a+Y^b=cZ$ for various combinations of randomly selected positive integers $a,b,c$ as shown in the Survo demo `https://www.survo.fi/demos/index.html#ex121`

This simple experiment revealed some interesting cases and let me study the topic more specifically.

When computing numerical values of $\mathrm{mod}(X^a+Y^b,c)$ modular exponentiation [8] is used in the Survo module `DIOPH` which I created for numerical solving of Diophantine equations of this kind.
According to my first experiments, nontrivial roots for Diophantine equations $X^4+Y^4=cZ$ are obtained for primes of the form $c=8n+1$ and their multiples. In the demo `https://www.survo.fi/demos/index.html#ex122`
the roots are calculated and plotted for these $c$ values until 433.




The first target was the case $X^4+Y^4=17Z$ or $\mathrm{mod}(X^4+Y4,17)=0$ documented as `https://www.survo.fi/demos/index.html#ex123`
and it showed that the roots $(X,Y)$ are located in the integer points of lines

$$Y=17+k(X-17i),\quad k=-2,-1/2,1/2,2,\quad i\in\mathbb{Z}$$

and thus forming two slanted grids of squares so that all solutions can be covered by straight lines with 4 different slopes. In the comments of this demo more examples of cases $\mathrm{mod}(X^4+Y^4,P)=0$ where $P$ is a prime of the form $P=8n+1$ are shown.
In them all solutions $(X,Y)$ can be covered by straight lines with 4 different slopes

of the form $p/q, -q/p, -p/q, q/p$ where $p$ and $q$ are small integers.

According to my experiments, 'interesting' symmetric configurations of roots $(X, Y)$ for Diophantine equations $\mathrm{mod}(X^n + Y^n, c) = 0$ are obtained when

$$n = 2^m k \quad \text{and} \quad c = 2^{m+1} i + 1 \quad \text{is a prime,} \quad k, m, i = 1, 2, \ldots$$

as shown in `https://www.survo.fi/demos/index.html#ex124`
There the roots are plotted for $X, Y = 0, 1, 2, \ldots, 2c$. Then a common feature in all these graphs is that the square determined by points $(0, 0)$ and $(2c, 2c)$ is divided into four subsquares of size $c$ having identical configuration of points. In any of them, say in the square $(0, c)$ the points are symmetric to both diagonals since when $\mathrm{mod}(X^n + Y^n, c) = 0$ also $\mathrm{mod}(Y^n + X^n, c) = 0$ and $\mathrm{mod}((c - X)^n + (c - Y)^n, c) = 0$ when $n$ is even. Then, for example, the configuration of points in the triangle with vertices $(0, 0), (0, c/2), (c/2, c/2)$ determines the entire graph by rotations and translations.
Due to these symmetric properties, a unique symmetric pattern (B) locates around the middle point $(c, c)$ and symmetric patterns of another kind (A) are located around middle points of the four corner squares. This basic structure covers the entire $XY$ space.

The graphs created in the previous demos related to roots $(X, Y)$ of Diophantine equations $\mathrm{mod}(X^n + Y^n, c) = 0$ have a lot of symmetrical (kaleidoscopic) features. Using the case $\mathrm{mod}(X^{32} + Y^{32}, 641) = 0$ as an example it is shown in the demo
`https://www.survo.fi/demos/index.html#ex125`
how the graph of of roots $(X, Y)$ for $X, Y = 0, 1, \ldots, 2 \times 641 = 1282$ can be generated from a small triangular part of it by using that part or its transpose as a 'building block' 32 times. A graph of this case is displayed also on the cover page of this paper.

When finding solutions $(X, Y)$ for Diophantine equations $\mathrm{mod}\ (X^n + Y^n, P) = 0$ where $n$ is even, $(P, P)$ is always one solution. If $(P + p, P + q)$ is another solution, it is easy to see that $(P + 2p, P + 2q), (P + 3p, p + 3q), \ldots$ are also solutions and the points of solutions $(P + kp, P + kq), k = 0, 1, 2, \ldots$ are on the same straight line in the $XY$ plane.
The most visible clusterings appear for small $p, q$ values giving series of solutions where the distance between consecutive points is the square root of $p^2 + q^2$. Suitable $p, q$ values are found by applying the `DIOPH` operation of Survo for values $0 \le X, Y \le M$ where $M$ can be considerably smaller than $P$. Then the list of solutions $(X, Y)$ is reduced by cancelling cases where $\gcd(X, Y) > 1$ and $X > Y$. Thereafter by sorting the list in ascending order of $X^2 + Y^2$ the 'best' $p, q$ combinations and related sets of straight lines are found.
The entire set of these lines for given $p, q$ values is
$Y = P \pm p/q(X - i/pP)$,
$Y = P \pm q/p(X - i/qP), \quad i = \cdots - 2, -1, 0, 1, 2, \ldots$

For finding linear clusterings numerically a sucro `/DIOPH` was created.

```
------------------------------------------------------------------
*TUTSAVE DIOPH
/
/ def Wm=W1 Wm2=W2 Wprime=W3 Wn=W4
/
*{R}
*SCRATCH {act}{home}
*DIOPH {write Wm},{write Wm2},{write Wprime},{write Wn},CUR+4{act}
*{R}
*FILE COPY DIOPH1 TO NEW DIOPH{R}
*DATA DIOPH1{R}
*p q{R}
/  The results of DIOPH are saved{R}
/  in a Survo data file DIOPH as variables p,q.{R}
*{u3}{act}
*SCRATCH {act}{home}
*VAR G:2=gcd(p,q) TO DIOPH{act}{R}
*VAR C1:1=if(p>q)then(0)else(1) TO DIOPH{act}{R}
*VAR C2:1=if(G>1)then(0)else(1) TO DIOPH{act}{R}
*VAR C3:1=C1*C2 TO DIOPH{act}{R}
*FILE COPY DIOPH TO NEW DIOPH2 / IND=C3,1{act}{R}
*VAR R:2=sqrt(p*p+q*q) TO DIOPH2{act}{R}
*FILE SORT DIOPH2 BY R TO DIOPH3{act}{R}
*FILE LOAD DIOPH3 / IND=ORDER,2,20 VARS=p,q,R{act}
*{end}
------------------------------------------------------------------
```

When applied to the current case $\mathrm{mod}(X^{32} + Y^{32}, 641) = 0$ `/DIOPH` gives the following result:

```
------------------------------------------------------------------
/DIOPH 32,32,641,100
DIOPH 32,32,641,100,CUR+4                          / n_comb=533
  The results of DIOPH are saved
  in a Survo data file DIOPH as variables p,q.
VAR G:2=gcd(p,q) TO DIOPH
VAR C1:1=if(p>q)then(0)else(1) TO DIOPH
VAR C2:1=if(G>1)then(0)else(1) TO DIOPH
VAR C3:1=C1*C2 TO DIOPH
FILE COPY DIOPH TO NEW DIOPH2 / IND=C3,1
VAR R:2=sqrt(p*p+q*q) TO DIOPH2
FILE SORT DIOPH2 BY R TO DIOPH3
FILE LOAD DIOPH3 / IND=ORDER,2,20 VARS=p,q,R
DATA DIOPH3*,A,B,C
   p   q      R
   1   2      2
   1   5      5
   4   5      6
   1   8      8
   9  13     15
```

```
 5  16     16
 1  20     20
 2  25     25
 8  25     26
17  27     31
 1  32     32
21  31     37
13  36     38
19  33     38
23  33     40
25  32     40
 3  41     41
12  41     42
29  31     42
```

---

Formulas for all the points of solution $(X, Y)$ are obtained as follows.
The essential $p, q$ combinations are found by using the `DIOPH` command of Survo.
For each combination the roots $(X, Y)$ are located equidistantly on lines

$$Y = P + p/q(X - i/pP), \quad i = \cdots -2, -1, 0, 1, 2, \ldots \tag{1}$$

The equations (1) can be written in the form

$$pX - qY = (i - q)P, \quad i = \cdots -2, -1, 0, 1, 2, \ldots \tag{2}$$

Then the Diophantine equation

$$pX - qY = 1, \tag{3}$$

is solved by the extended Euclidean algorithm giving roots $(X_0, Y_0)$ and we get a basic solution

$$X_1 = (i - q)PX_0, \quad Y_1 = (i - q)PY_0. \tag{4}$$

Then the general solution will be

$$X = iPX_0 + qt, \quad Y = iPY_0 + pt, \quad i, t = \cdots -2, -1, 0, 1, 2, \ldots \tag{5}$$

This derivation of the solution in the case $(p, q)$ is not needed in cases $(q, p), (p, -q), (-q, p)$ since when $(X, Y)$ is a solution for (5) also $(Y, X), (P - X, P - Y), (P - Y, P - X)$ are solutions.

In general, the graph of the roots $(X, Y)$ of the Diophantine equation

$$\mathrm{mod}(X^n + Y^n, P) = 0$$

can always be covered by square grids so that all integer points of grids are roots.
In the case $n = 2^m$ at most $2^{m-1}$ square grids are needed and the $p, q$ pairs for defining these grids are the first $2^{m-2}$ pairs given by the sucro `/DIOPH`.
For other $n$ values the number of square grids is smaller.

The graphs related to roots $(X, Y)$ of Diophantine equations $\mathrm{mod}(X^n + Y^n, P) = 0$ have a lot of symmetrical properties.

It is easy to see that if $(X, Y)$ is a root in the area $0 \le X, Y \le P$, also $(Y, X), (X, P-Y), (P-Y, X), (P-X, Y), (Y, P-X), (P-X, P-Y), (P-Y, P-X)$

are roots in the same area. At the same time also $(kX, kY), k = 0, 1, 2, \ldots$ as well their 7 counterparts $(kY, kX), (kX, P - kY), \ldots$ are roots. The 'minimal solutions' $(X, Y)$ with smallest gaps $\sqrt{X^2 + Y^2}$ provide the optimal starting points $(X, Y)$ for finding all roots in the area $0 \leq X, Y \leq P$ ($P$ square).

In the demo `https://www.survo.fi/demos/index.html#ex126`
it is shown how all roots in the case $n = 32, P = 641$ in the area $0 \leq X, Y \leq 641$ are found by the sucro `/DIOPH` and by an extended version of of `DIOPH2` module of Survo by starting from 'minimal solutions' and using the symmetrical and multiplicity features just described.

The roots $(X, Y)$ located in the $P$ square and related to a minimal solution $(p, q)$ are equidistantly on parallel lines

$$X = iPX_0 + qt, Y = iPY_0 + pt, \quad i = -q, -q + 1, \ldots, p - 1, p \tag{6}$$

where $X_0$ and $Y_0$ are obtained from the Diophantine equation $pX_0 + qY_0 = 1$. The line for a given value of $i$ encounters the line connecting the diagonal of the $P$ square with end points $(0, P)$ and $(P, 0)$ in the point determined by $t = P(1 - i(X_0+Y_0))/(p+q)$. When $t$ is rounded to the closest integer $t_0$, the point of solution $X_1 = iPX_0 + qt_0, Y_1 = iPY_0 + pt_0$ is located in the $P$ square (or in its corner for $i = -q$ and $i = p$). Then it is easy to determine all points of solution in the $P$ square related to to minimal solution $p, q$ by using (6) and by the basic properties given above.

In the demo `https://www.survo.fi/demos/index.html#ex127`
a general procedure is presented for determining how many minimal solutions are needed in each case. The $p, q$ values will be processed in the order given by `/DIOPH` until in the set of solutions $(X, Y)$ the next pair $(p, q)$ already appears among those solutions.

Thus the top values in the list of $p, q$ values from `/DIOPH` should give minimal solutions. This view is supported e.g. by the fact that a small distance $\sqrt{p^2 + q^2}$ between consecutive roots implies thicker covering of roots than a big distance. Thus this principle guarantees an economic approach for finding all roots.

The following 'snapshot' of the demo `ex127` tells how the sucro `/D_SOLVE` works in the case $n = 64, P = 641$:

```
-----------------------------------------------------------------------
 1 *
 2 *  Automatic solution of Diophantine equations mod(X^n+Y^n,P)=0
 3 *
 4 *I have created a new sucro /D_SOLVE for finding the numbers p,q
 5 *and associated straight lines covering all solution points (X,Y)
 6 *of the Diophantinec equation mod(X^n+Y^n,P)=0.
 7 *It is sufficient to study the area 0<=X,Y<=P.
 8 *All roots in this area are determined by using /DIOPH and listed.
 9 *At first a reasonable number of basic solutions (smallest roots X,Y)
10 *are computed and sorted in increasing order according to X^2+Y^2.
11 *Then by starting from the first p,q pair the points of solution related
12 *to solution (p,q)=(X,Y) according to the symmetry and multiplicity
13 *relations described in the previous demo are 'removed' from the list.
14 *This process is continued until all points in the list have been
15 *removed and this procedure gives the number of essential p,q pairs.
```

```
*It is possible (typically for the last pairs) that some p,q pairs
*do not remove any points. Such pairs are eliminated.
*
*For example, in the case n=64, P=641 the number of p,q pairs is 16,
*but 17 pairs has to be processed since the last two pairs are
*(11,24),(16,21) and 11^2+24^2=16^2+21^2=697 (equal distances).
*(11,24) removes no points from the list, but (16,21) empties the list.
*
*/D_SOLVE 64,64,641,100,20 / Basic solutions <100, 20 p,q pairs to test
*
*Solving Diophantine equation mod(X^64+Y64,641)=0
*
*DIOPH 64,64,641,100,CUR+4                          / n_comb=995
*VAR G:2=gcd(p,q) TO DIOPH
*VAR C1:1=if(p>q)then(0)else(1) TO DIOPH
*VAR C2:1=if(G>1)then(0)else(1) TO DIOPH
*VAR C3:1=C1*C2 TO DIOPH
*FILE COPY DIOPH TO NEW DIOPH2 / IND=C3,1
*VAR R=sqrt(p*p+q*q) TO DIOPH2
*FILE SORT DIOPH2 BY R TO DIOPH3
*FILE LOAD DIOPH3 / IND=ORDER,2,21 VARS=p,q,R
*
*MAT SAVE AS PQ
*MAT PQ_X0Y0=ZER(20,5)
*MAT PQ_X0Y0(1,1)=PQ
*
*Solving 20 Euclidean equations p*X0-q*Y0=1
*MAT_PQ_X0Y0(20,1) 20
*MAT_PQ_X0Y0(20,2) 21
*EUCLID 20,21
*-1 1 1
*
*MAT PQ_X0Y0(20,1)=21
*MAT PQ_X0Y0(20,2)=20
*MAT PQ_X0Y0(20,4)=1
*MAT PQ_X0Y0(20,5)=1
*
*MAT NAME PQ_X0Y0 AS p_q_X0_Y0_values_for_n=64_P=641
*Matrix PQ_X0Y0 of p,q,X0,Y0 values created!
*Computing roots:
*
*SLOPES=PQ_X0Y0 POINTS=A64_641.TXT
*DIOPH3 64,64,641,641,CUR+1                         / n_comb=0
*
*Number of slopes needed is 16 .
*
*DIOPH has saved the validities of p,q combinations in a text file
*#VALID.TXT. These values (0 or 1) shall appear as a column 'valid'
```

```
 64 *in the table of results.
 65 *
 66 *Values of p,q,R,X0,Y0,valid for these 16 slopes are:
 67 *(Rejected p,q combinations indicated by 0's in the last column)
 68 *///           p      q      R     X0     Y0  valid
 69 *  1           3     11     11      4      1      1
 70 *  2           6     11     13      2      1      1
 71 *  3          12     11     16      1      1      1
 72 *  4          15     11     19      3      4      1
 73 *  5           1     21     21      1      0      1
 74 *  6          19      9     21      1      2      1
 75 *  7          21      2     21      1     10      1
 76 *  8          21      4     21      1      5      1
 77 *  9          21      5     22      1      4      1
 78 * 10          22      3     22      1      7      1
 79 * 11           8     21     22      8      3      1
 80 * 12          13     19     23      3      2      1
 81 * 13          21     10     23      1      2      1
 82 * 14          23      9     25      2      5      1
 83 * 15          19     18     26      1      1      1
 84 * 16          11     24     26     11      5      0 / eliminated p,q pair
 85 * 17          16     21     26      4      3      1
 86 *
 87 *Number of slopes needed is 16 .
 88 *
 89 *# of points 0<=X,Y<=641 is 40964.
 90 *Density of points is round(40964/641^2,4)=0.0997
 91 *
 92 *................................
 93 *Plotting the graph for 0<=X,Y<=2*641:
 94 *
 95 *4*40964+300 164156
 96 *REDIM 164156,120 / More rows in the edit field!
 97 *WSTYLE=0 HEADER=  XLABEL= YLABEL= XDIV=0,1,0 YDIV=0,895,30 FRAME=3
 98 *WSIZE=895,925  WHOME=872,0  POINT=6,3 MODE=2000,2000 TEXTS=T
 99 *
100 *T=[SwissB(70)],mod(X^64+Y^64;641)_=_0___X;Y=0(1)1282,100,1925
101 *DIOPH 64,64,641,1282,CUR+4                        / n_comb=163849
102 *GPLOT K,X,Y / SCALE=0,1282 POINT=0,3
103 *DATA K
104 *X Y
105 *0 0
106 *0 641
107 *0 1282
108 *1 21
109 *1 29
110 *. ....
```

---

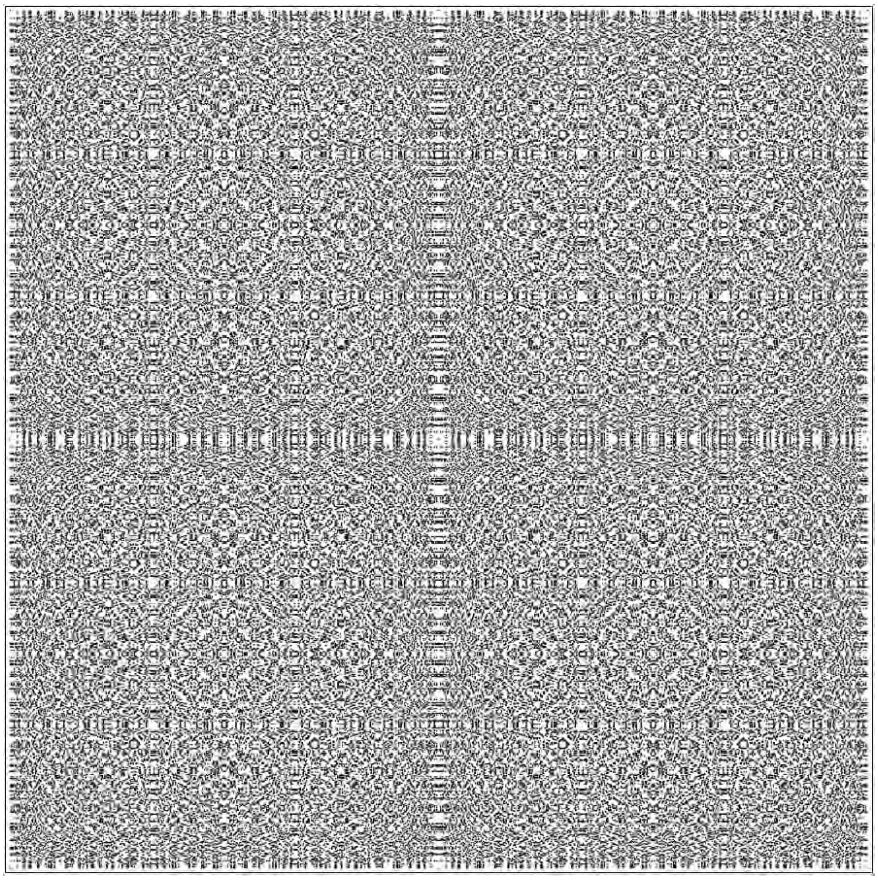


FIGURE 2. Roots for $n = 64, P = 641, \quad 0 \le X, Y \le 2 \times 641$

By using this technique I have solved over 100 cases with various $n$ and $P$ values. The results of these experiments support the following conjecture about the number of $p, q$ pairs needed:
Assume that $P$ is a prime number. The trivial roots $(X, Y)$ of $\mathrm{mod}(X^n+Y^n, P) = 0$ are $(iP, jP), \quad i, j = \ldots, -2, -1, 1, 2, \ldots$.
Let the $P-1$ be divisible by $2^k$ but not by $2^{k+1}$. Then non-trivial roots can appear only when $n < 2^k$. For any even $n < 2^k$ giving also nontrivial roots, the number of $p, q$ combinations needed for straight lines to cover the roots $(X, Y)$ in the $XY$ plane is

$$N(n, P) = \lceil \gcd(n, P-1)/4 \rceil. \tag{7}$$

Example: $N(64, 641) = 16$
The above $N(n, P)$ formula holds in all cases I have tested and they are listed in `https://www.survo.fi/demos/ex127_pq.txt`
(# of roots and slopes in 120 cases and lists of some interesting $p, q$ values).

In some cases as for $n = 64, P = 641$ all 'optimal' $p, q$ combinations do not appear in the order determined by $\sqrt{p^2 + q^2}$. Tables of $p, q$ combinations of such

cases are also given at the end of this list.
Covering the points of solution by orthogonal grids with various slopes may happen in multiple ways depending on the order of $p, q$ combinations suggested. So far the order has been determined by the gap $\sqrt{p^2+q^2}$ between consecutive points on a particular straight lines determined by $p/q$.
Replacing $\sqrt{p^2+q^2}$ by $(p^4+q^4)^{1/4}$ or $\min(p,q)$ may lead to different optimal selections. However, in all cases the number of essential combinations is the same. Also when $n$ is odd, the lines determining the locations of the the roots of $\mathrm{mod}(X^n+Y^n,P)=0$ can be obtained by the principles described in this demo.
The number of different slopes of straight lines needed to cover all the roots is according to my latest experiments is simply $\#\mathrm{slopes}(n,P)=\gcd(n,P-1)$ when $P$ is a prime number and this is valid also for even $n$ values.
This is equivalent with the previous formula (7) of $N(n,P)$ giving the number of $p,q$ combinations for any even $n$, because then each $p,q$ combination corresponds to 4 different slopes. For odd values of $n$ the first slope is always $-1$ since all $(X,X)$'s are roots. Also in this case when $(X,Y)$ is a root then $(Y,X)$ is a root.

The demonstration `https://www.survo.fi/demos/index.html#ex128` shows plotting of five examples in the order the `DIOPH3` program module finds the roots in a slow speed so that the user can see the final graph emerging through symmetric steps. This takes place by using a specification `POINTS2=1` in the sucro command `/D_SOLVE` which saves the roots in a text file `POINTS.TXT` and activates thereafter the `DIOPH3` operation to display the graph in 'slow motion'.

The graphs can be enhanced by using colors so that points related to directions specified by the same $p,q$ numbers have the same color. This is shown in demos
`https://www.survo.fi/demos/index.html#ex129` ,
`https://www.survo.fi/demos/index.html#ex130` ,
and especially in their YouTube versions.

## References


[1] S.Mustonen, *Pythagorean triples: visualization and characterization*, (2005)
`https://www.survo.fi/papers/pythagorean3.pdf`
[2] S.Mustonen, *Statistical accuracy of geometric constructions*, (2008)
`https://www.survo.fi/papers/GeomAccuracy.pdf`
[3] S.Mustonen, *On lines and their intersection points in a rectangular grid of points*, (2009)
`https://www.survo.fi/papers/PointsInGrid.pdf`
[4] S.Mustonen, *On lines through a given number of points in a rectangular grid of points*, (2010)
`https://www.survo.fi/papers/LinesInGrid2.pdf`
[5] S.Mustonen, *'Simple constructions' of regular n-sided polygons at any given accuracy*, (2013)
`https://www.survo.fi/papers/Polygons2013.pdf`
[6] S.Mustonen, *Lengths of edges and diagonals and sums of them in regular polygons as roots of algebraic equations*, (2013)
`https://www.survo.fi/papers/Roots2013.pdf`
[7] S.Mustonen, *On the roots of an algebraic equation related to regular polygons*, (2017)
`https://www.survo.fi/papers/Roots2017.pdf`
[8] *Modular exponentiation*, `https://en.wikipedia.org/wiki/Modular_exponentiation`



Department of Mathematics and Statistics, University of Helsinki
*E-mail address*: `seppo.mustonen@survo.fi`