DIOPHANTINE EQUATIONS $X^n + Y^n \equiv 0 \pmod{P}$
ADDITIONAL RESULTS AND GRAPHICAL PRESENTATIONS

SEPPO MUSTONEN

ABSTRACT. This is the second report of numerical and graphical experiments about the roots of Diophantine equations of the form $X^n + Y^n \equiv 0 \pmod{P}$.

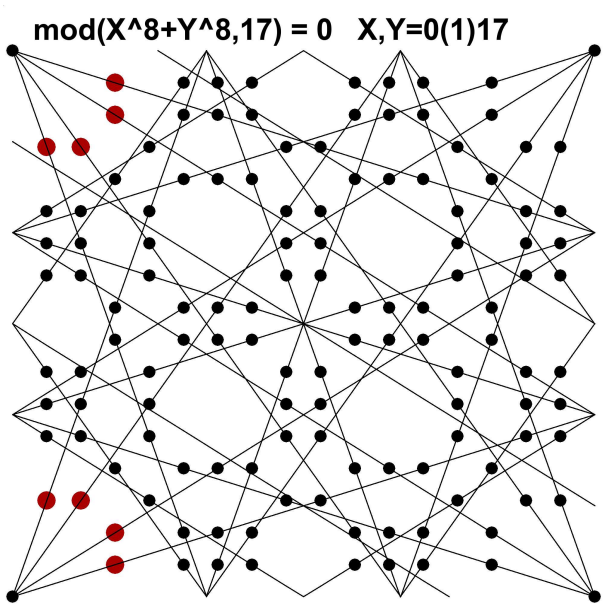

FIGURE 1. Roots for $n = 8, P = 17, \quad 0 \leq X, Y \leq 17$
$\gcd(P-1, n) = 8$

Larger 8 points defining the slopes in the graph are the basic roots defining all other roots as 'multiples'.

Common features in this and three following graphs are:
1. Number of directions of straight lines covering all roots is $\gcd(P-1, n)$.
2. Number of nontrivial roots in each direction is $P-1$ in the area $0 < X, Y < P$.
3. Each of nontrivial roots are covered by only one of these straight lines. Then the number of nontrivial roots in the area $0 < X, Y < P$ is $(P-1)\gcd(P-1, n)$.

My general conjecture is that those three statemets are valid for all Diophantine equations $X^n + Y^n \equiv 0 \pmod{P}$ where P is a prime number.

Date: 5 November2022.

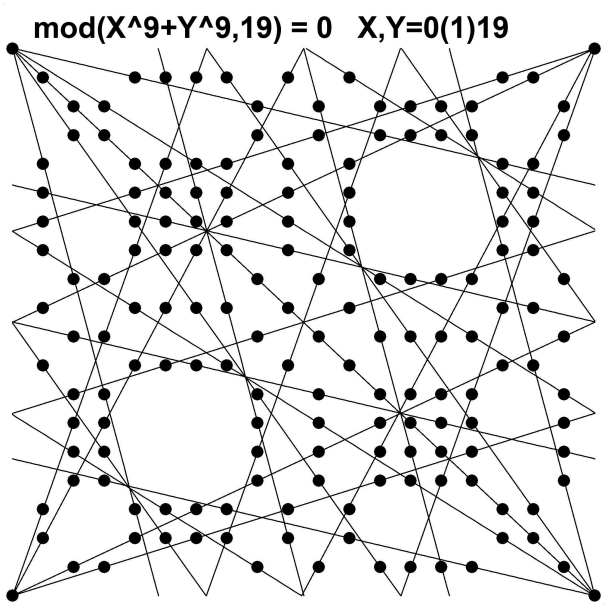

FIGURE 2. Roots for $n = 9, P = 19, \quad 0 \leq X, Y \leq 19$
$\gcd(P-1, n) = 9$

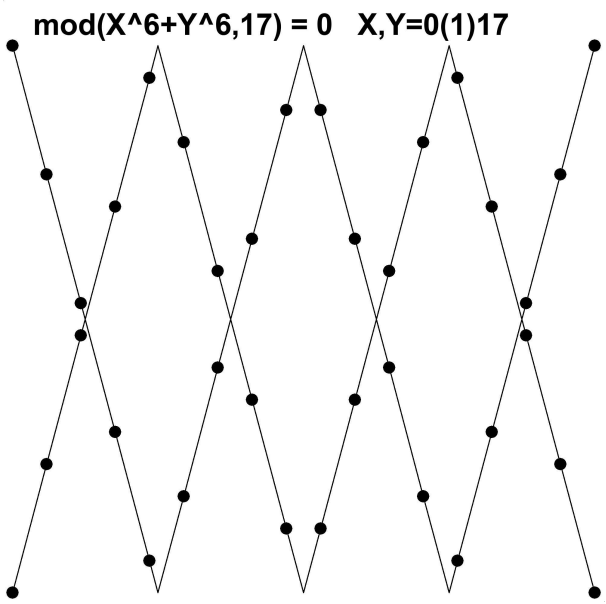

FIGURE 3. Roots for $n = 6, P = 17, \quad 0 \leq X, Y \leq 17$
$\gcd(P-1, n) = 2$

Many properties of the roots are based on the observation that the configuration of the roots is similar in all $P \times P$ squares.

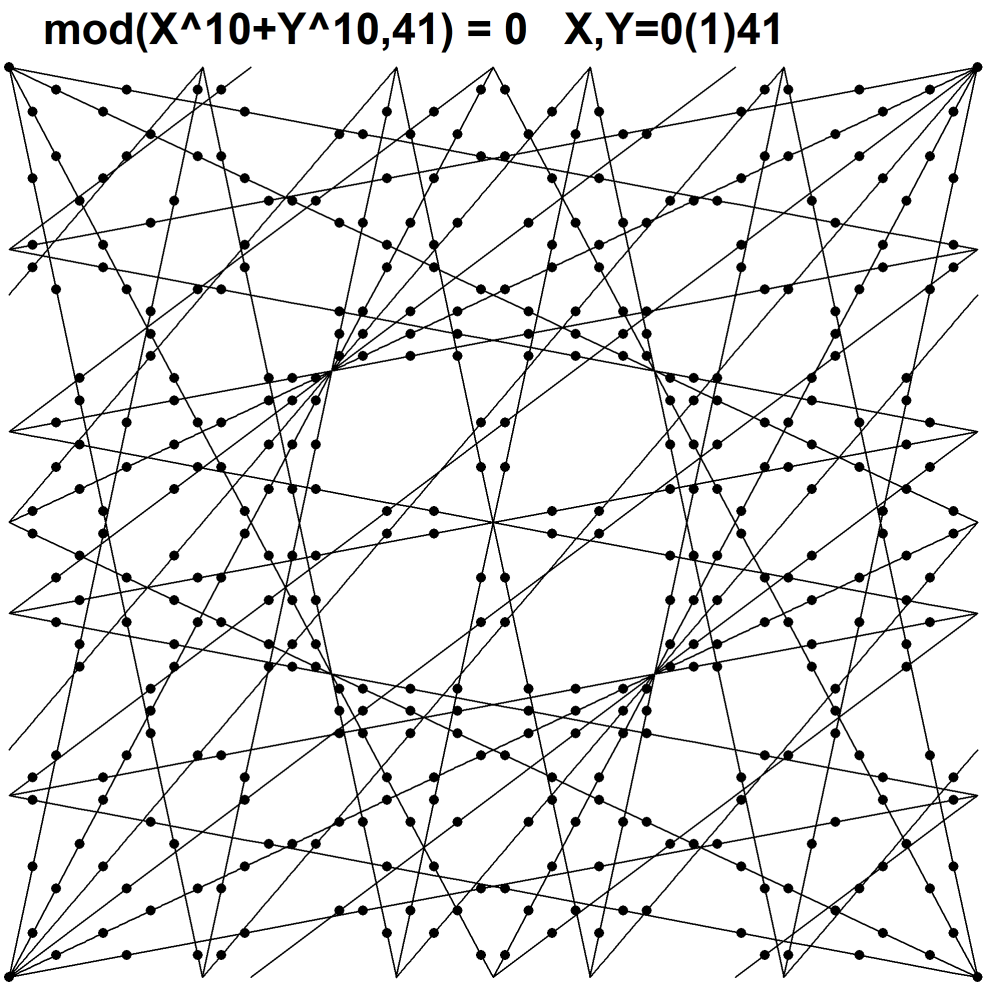

FIGURE 4. Roots for $n = 10, P = 41, \quad 0 \le X, Y \le 41$
$\gcd(P-1, n) = 10$

In this graph there are 6 ascending and 4 descending directions of straight lines covering all the roots. Each internal root is covered by only one line. The essential basic roots are (1,2), (1,5) with 4 variants $(p,q), (-p,q), (q,p), (-q,p)$ and (4,5) with only two variants $(p,q), (q,p)$.

By using different colors for different directions, enlarging the size of points in the graph, and by selecing a background color, various 'artistic' graphs may be generated.

The graphs become more interesting by drawing them for $0 \le X, Y \le 4 \times P$. Then an interesting cluster of points appears in the center of the graph.

Three sets of 12 solutions of Diophantine equations $mod(X^n + Y^n, P) = 0$ are available by starting from

`https://www.survo.fi/demos/index.html#ex141`

The essential information about solutions of these equations is obtained by studying solutions in the square $0 \leq X, Y \leq P$ since the same configuration of roots appears in all squares with (iP, jP) as the left lower point. Thus any root (x, y) outside the square $0 \leq X, Y \leq P$ has a corresponding root $\mod (x, P), \mod (y, P)$ in this original square.

As one can see in the preceding examples, the entire solution depends on minimal solutions close to $(0, 0)$. Let (p, q) be such a solution like (1,3) in Fig.1. The numbers p, q have no common factors. Then all points $(ip, iq), i = 0, 1, 2, \ldots$ are solutions. When P is a prime, we get $P + 1$ solutions and the last solution is (Pp, Pq) which corresponds to $(0, 0)$ in the original square. Then roots above $y = P$ can be replaced by $\mod (y, P)$ values.

Then, for example, in the Fig.1 we have three ascending lines going through roots related to (1,3) with $P + 1 = 18$ roots or $P - 1 = 16$ nontrivial roots. Since $(P, q) = 1$, the y coordinates of these roots are numbers $1, 2, \ldots P-1$ in some order. If some integer in this sequence would appear two times, the point (Pp, Pq) would not be reached. Therefore on each level of y the same number of roots will appear and this common number is 8 in the case of Fig.1 which is equal to $\gcd(P, n - 1)$.

On the lowest level $y = 1$ the number of roots should then be number of roots of a Diophantine equation
$X^n + 1 \equiv 0 \pmod{P}$
for $X = 1, 2, \ldots, n - 1$
and this number should be $\gcd(P, n - 1)$.

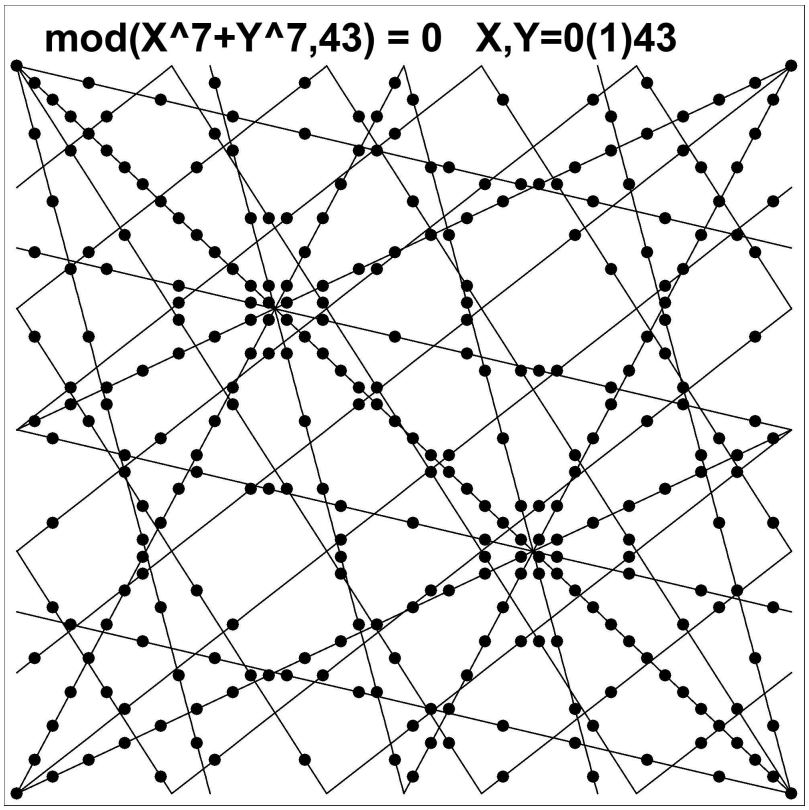

FIGURE 5. Roots for $n = 7, P = 43, \quad 0 \leq X, Y \leq 43$
$\gcd(P-1, n) = 7$

In this graph on the roots of $X^7 + Y^7 \equiv 0 \pmod{43}$ there are $\gcd(P, n-1) = 7$ basic roots (p, q)
(1,-1) (1,2) (2,1) (4,-1) (1,-4) (6,5) (3,-5).
In this case it is difficult to predict these values formally. They are detected just by studying the graph or by listing all roots (X, Y) with $\gcd(X, Y) = 1$ close to $(0, 0)$ or $(0, P)$.
As a consequence there are $P - 1 = 42$ roots in each direction.
Each of the inner roots is covered by only one straight line.

It is rather simple to find all roots in the area $0 \leq X, Y \leq P$ since this can be done fastly by using residual arithmetic.

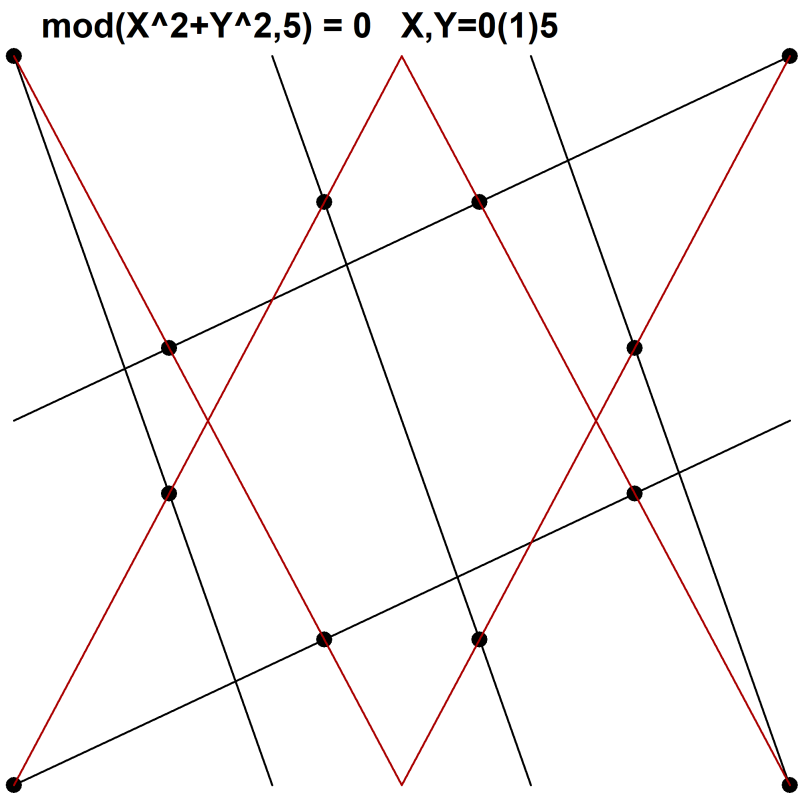

FIGURE 6. Roots for $n = 2, P = 5, \quad 0 \leq X, Y \leq 5$
$\gcd(P-1, n) = 2$

The covering of roots by straight lines is not always unique.
In the above case the roots can be covered optimally in two ways by black and red straight lines.
The black covering is based on minimal roots (2,1) and (1,-3).
The red covering is based on minimal roots (1,2) and 1,-2).

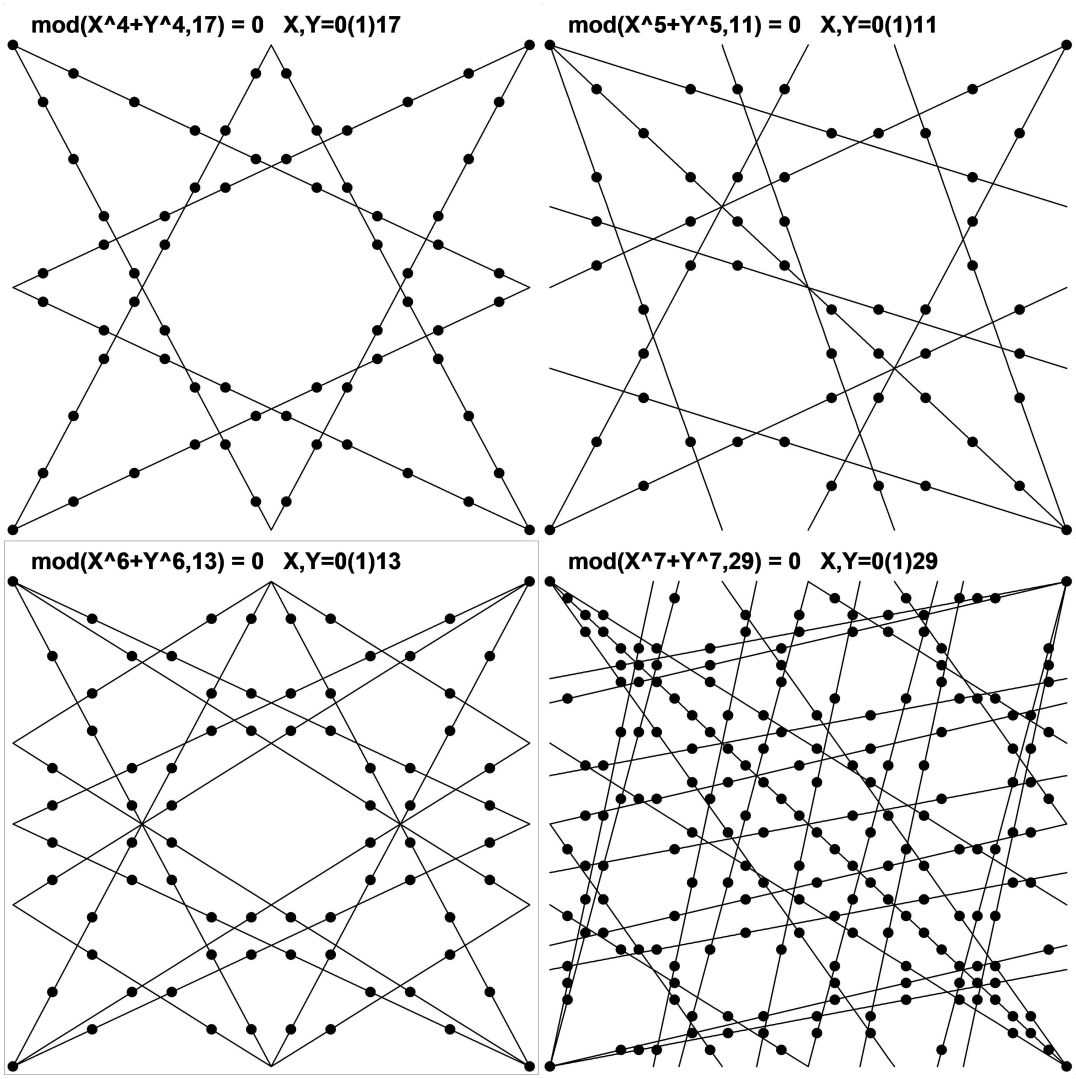

FIGURE 7. Roots for four Diophantine equations

Minimal roots in these four cases are:
$n = 4, P = 17$: (1,2) (1,-2) (2,1) (2,-1)
$n = 5, P = 11$: (1,-1) (2,1) (1,2) (1,-3) (3,-1)
$n = 6, P = 13$: (1,2) (2,1) (1,-2) (2,-1) (3,2) (3,-2)
$n = 6, P = 29$: (1,-1) (4,1) (1,4) (5,1) (1,5) (2,-3) (3,-2)

```
------------------------------------------------------------------
10*
11*/DI_CHECK 6,13
12*   Number of roots in mod(X^n+Y^n,P)=0
13*
14*/DISOLVE2 6,6,13,30
15*DISOLVE 6,6,13,2
16*
17*  n   p   q   points
18*  1   1   2     52   =4*12+4
19*  2   2   3     24   =2*12
20*
21*npq=2 n_total=76 P=13
22*FILE SAVE POINTS.TXT TO NEW POINTS / Activate!
23*FILE DEL POINTS.TXT                / Activate!
24*FILE SHOW POINTS
25*Checking results by activating:
26*DIOPHF 6,6,13,13
27*n=76
28*
------------------------------------------------------------------
```

When n is an even integer, the roots can be detected by the Survo commands as shown in the graph above. For $p = 1, q = 2$ all four combinations are possible, but for $p = 2, q = 3$ only two combinations (3,2),(3,-2) are needed as shown in the graph on the previous page.

More features of these equations are given in following YouTube demos created since 2018.

Plotting solutions of Diophantine equations $X^a + Y^b = cZ$
https://www.survo.fi/demos/index.html#ex121
Patterns of roots in Diophantine equations $X^4 + Y^4 = cZ$
https://www.survo.fi/demos/index.html#ex122
Grids of roots in Diophantine equations $X^4 + Y^4 = 17 * Z$
https://www.survo.fi/demos/index.html#ex123
Patterns of roots in Diophantine equations $X^n + Y^n = cZ$
https://www.survo.fi/demos/index.html#ex124
Solutions (X, Y) of $X^n + Y^n = cZ$ from minimal setup
https://www.survo.fi/demos/index.html#ex125
Symmetries of roots in Diophantine equations $X^n + Y^n = cZ$
https://www.survo.fi/demos/index.html#ex126
Automatic solution of Diophantine equations $mod(X^n + Y^n, P) = 0$
https://www.survo.fi/demos/index.html#ex127
Stepwise display: Roots of Diophantine equation $mod(X^n + Y^n, P) = 0$
https://www.survo.fi/demos/index.html#ex128
Colored textures by roots of Diophantine equations $mod(X^n + Y^n, P) = 0$
https://www.survo.fi/demos/index.html#ex129
Colored textures 2 by roots of Diophantine equations $mod(X^n + Y^n, P) = 0$
https://www.survo.fi/demos/index.html#ex130
Extended plots of roots in nonlinear Diophantine equations $X^n + Y^n = cZ$
https://www.survo.fi/demos/index.html#ex135
More extended plots of roots in nonlinear Diophantine equations $X^n + Y^n = cZ$
https://www.survo.fi/demos/index.html#ex136
Roots of Diophantine equations $mod(X^4 + Y^2, P) = 0$
https://www.survo.fi/demos/index.html#ex138
Roots of $mod(X^n + Y^n, P) = 0$ by simple arithmetics
https://www.survo.fi/demos/index.html#ex139
Roots of $mod(X^n + Y^n, P) = 0$ by simple arithmetics 2
https://www.survo.fi/demos/index.html#ex140
Roots of $mod(X^n + Y^n, P) = 0$ by simple arithmetics 3
https://www.survo.fi/demos/index.html#ex141
Roots of $mod(X^n + Y^n, P) = 0$ in colors
https://www.survo.fi/demos/index.html#ex142
Number of slopes for lines covering roots of $mod(X^n + Y^n, P) = 0$
https://www.survo.fi/demos/index.html#ex143
Roots of $mod(X^n + Y^n, P) = 0$ for odd integers n (1/2)
https://www.survo.fi/demos/index.html#ex144
Roots of $mod(X^n + Y^n, P) = 0$ for odd integers n (2/2)
https://www.survo.fi/demos/index.html#ex145

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