

The Mathematical Super Element

In this book “The Mathematical Super Element” I make the case for a new definition and tabulate many examples

For those interested in [my] Mathematical discovery process see Chapter 30

If you are only interested in primes then Chapters 28,29, 32 and 37 will be of most interest

(c) Gary Wright 2026

Chapter 1 - Defining a Sturdy element

The set of elements modulo 35 is a set

Working modulo 35 does not give you a group because we can find zero divisors and those are not invertible.

Multiples of 5 and 7 are zero divisors because they are divisors of 35.

There is no inverse for the elements 5,7,10,14,15,20,21,25,28,30 in that set

Listing the elements not on that list gives us a subset consisting of 24 elements as follows
 $\{ 1,2,3,4,6,8,9,11,12,13,16,17,18,19,22,23,24,26,27,29,31,32,33,34 \}$

Does the zero divisor 5 generate a group?

Powering of 5 just gives us a series of non-invertible results $\{ 5,25,20,30,10,15 \}$

Our generated results do not include the identity element 1 or similar and as we noted there are no inverses.

Does the element 6 generate a group?

We obtain a cyclic group having 2 elements $\{ 6, 1 \}$

Does the zero divisor 7 generate a group?

Successive powering of 7 just gives us a series of non-invertible results $\{ 7,14,28,21 \}$

Our generated results do not include the identity element 1 or similar and as we noted there are no inverses.

Does the element 3 generate a multiplicative group?

We obtain a cyclic group having 12 elements $\{ 3,9,27,11,33,29,17,16,13,4,12,1 \}$

Does the element 11 generate a multiplicative group?

We obtain a cyclic group having 3 elements $\{ 11,16,1 \}$

See the next page for sturdy element.

Next we attempt to define what a sturdy element is

- (i) A sturdy element requires context [a set in which it's properties are special]
- (ii) A sturdy element always generates a group [or stronger] from that enclosing context.
- (iii) A sturdy element generates a multiplicative group whose order is $\leq \frac{(n-1)}{2}$
- (iv a) A sturdy element shares the context set with an element that generates a maximal group (n-1) elements (depending on the value of our source variable [t])
- (iv b) A sturdy element shares the context set with an element that generates a near maximal group (n-1-zero divisors based adjustment) elements (depending on the value of our source variable [t])

For the set $1+(-1+2^t) \times (2^{t+1})$ the element $-1+2^t$ is a sturdy element

For the set $1+(-1+2^t) \times (2^{t+1})$ the element $392+t$ is not a sturdy element

Setting $t=5$ we obtain 397 for $392+t$

Working modulo 1985 we obtain the following from successive powering of 397
{ 397, 794, 1588, 1191, 397, ... }

That subset cannot be a group as it contains a zero divisor in 397

That series of elements is not a group so our element $392+t$ fails property (ii) and is therefore not a sturdy element.

For the set $1+(1+2^t) \times (2^{t+1})$ the element $1+2^t$ is a sturdy element

For the set $1+(1+2^t) \times (2^{t+1})$ the element $105+t$ is not a sturdy element

Setting $t=4$ we obtain 109 for $105+t$

Working modulo 545 we obtain the following from successive powering of 109
{ 109, 436, 109 }

That subset cannot be a group as it contains a zero divisor in 109

That series of elements is not a group so our element $105+t$ fails property (ii) and is therefore not a sturdy element.

For the set $1+(-1+3^t)\times(3^{t+1})$ the element $-1+3^t$ is a sturdy element

For the set $1+(-1+3^t)\times(3^{t+1})$ the element $38+t$ is not a sturdy element

Setting $t=5$ we obtain 43 for $38+t$

Working modulo 2107 we obtain the following from successive powering of 43

{ 43, 1849, 1548, 1247, 946, 645, 344, 43, ... }

That subset cannot be a group as it contains a zero divisor in 43

That series of elements is not a group so our element $38+t$ fails property (ii) and is therefore not a sturdy element.

For the set $1+(1+3^t)\times(3^{t+1})$ the element $1+3^t$ is a sturdy element

For the set $1+(1+3^t)\times(3^{t+1})$ the element $25406+t$ is not a sturdy element

Setting $t=5$ we obtain 25411 for $25406+t$

Working modulo 177877 we obtain the following from successive powering of 25411

{ 25411 }

That subset cannot be a group as it contains a zero divisor in 25411

That series of elements is not a group so our element $25406+t$ fails property (ii) and is therefore not a sturdy element.

Examples of a proposed notation for sturdy element are given next.

$\langle\langle -1+2^t \rangle\rangle$ for set $1+(-1+2^t)\times(2^{t+1})$ for $t=4,5$

$\langle\langle 1+2^t \rangle\rangle$ for set $1+(1+2^t)\times(2^{t+1})$ for $t=4,5$

$\langle\langle -1+3^t \rangle\rangle$ for set $1+(-1+3^t)\times(3^{t+1})$ for $t=4,5$

$\langle\langle 1+3^t \rangle\rangle$ for set $1+(1+3^t)\times(3^{t+1})$ for $t=4,5$

Chapter 2 – Element $-1+2^t$ and set $1+(-1+2^t) \times (2^{t+1})$

Consider the Proth space $1+(-1+2^t) \times (2^{t+1})$

We will be using generating element $-1+2^t$

The [sub]groups generated by $-1+2^t$ have low order [a lot lower than $n-1$]

A related Conjecture is given next.

Conjecture: Order of $-1+2^t \pmod P$ when P is prime and P of the form $1+(-1+2^t) \times (2^{t+1})$ divides $Lcm(2+4 \times t - (t+1), 2+4 \times t)$

Tabulating the elements of groups generated by $-1+2^t$ next.

Using the prefix TNw to avoid clashing with existing letter conventions for groups.
Prefer G or S? Replace them in your local copy.

For 3 from $t=2$ the elements **TNw20** are {3,9,2,6,18,4,12,11,8,-1,22,**16**,23,19,7,**21**,13,14,17,1}

When $t=3$ we have $P=1+7 \times 16$ and the set of elements modulo P is a multiplicative group.

Our generator $-1+2^t$ is 7 and the subset it generates has 14 elements.

The elements in **TNw14** are {7,49,4,28,83,**16**,-1,106,64,**109**,85,30,97,1}

For 3 from $t=2$ the 20 elements in **TNw20** are
{ 3,9,2,6,18,4,12,11,8,24,22,**16**,23,19,7,21,13,14,17,1 }
which when put in numeric order are
1,2,3,4,6,7,8,9,11,12,13,14,16,17,18,19,21,22,23,24
Elements that do not appear are 5,10,15,20

For 7 from $t=3$ the 14 elements in **TNw14** are as shown next
{7,49,4,28,83,**16**,-1,106,64,**109**,85,30,97,1}

If W14 is really a group then we need inverses so let us document those next.

- Inverse of 7 is 97 mod P
- Inverse of 49 is 30 mod P
- Inverse of 4 is 85 mod P
- Inverse of 28 is 109 mod P
- Inverse of 83 is 64 mod P
- Inverse of 16 is 106 mod P

For 15 from $t=4$ the 36 elements in **TNw36** are as shown next
{ 15,225,8,120,357,64,479,451,31,465,241,248,353,4,60,419,32,-1,
466,256,473,361,124,417,2,30,450,**16**,240,233,128,**477**,421,62,449,1 }

For 31 from $t=5$ the 11 elements in **TNw11** are

{ 31,961,16,496,1481,256,**1981**,1861,126,1921,1 }

For 63 from $t=6$ the 52 elements in **TNw52** are as shown next

{ 63, 3969, 32, 2016, 6033, 1024, 8057, 7561, 508, 7809,2,126,7938,
64,4032,4001,2048,8049,7057,1016,7553,4,252,7811,128,-**1**,
8002,4096,8033,6049,2032,7041,8,504,7557,256,8063,7939,127,
8001,4033,4064,6017,**16**,1008,7049,512,**8061**,7813,254,7937,1 }

The fifth to last element is always -4

The fourth element can be obtained as $2016 \equiv \text{Mod}(-4,8065)^{-1}$ alternatively

The eighth element can be obtained as $7561 \equiv \text{Mod}(16,8065)^{-1}$ alternatively

For 127 from $t=7$ the 30 elements in **TNw30** are as shown next

{ 127,16129,64,8128,24353,4096,32497,30481,2040,31489,
4,508,32003,256,-**1**,32386,16384,32449,24385,8160,
28417,**16**,2032,30473,1024,**32509**,32005,510,32257,1 }

The fourth element can be obtained as $8128 \equiv \text{Mod}(-4,32513)^{-1}$ alternatively

The eighth element can be obtained as $30481 \equiv \text{Mod}(16,32513)^{-1}$ alternatively

For 255 from $t=8$ the 68 elements in **TNw68** are as shown next

{ 255,65025,128,32640,97857,16384,130529,122401,8176,126465
8,2040,128517,1024,130559,130051,511,130305,65281,65408
97793,64,16320,114209,8192,130545,126481,4088,128513,4
1020,129539,512,-**1**,130306,65536,130433,97921,32704,114177,
32,8160,122385,4096,130553,128521,2044,129537,2,510,
130050,256,65280,65153,32768,130497,114241,16352,122369,**16**
4080,126473,2048,**130557**,129541,1022,130049,1 }

The fourth element can be obtained as $32640 \equiv \text{Mod}(-4,130561)^{-1}$ alternatively

The eighth element can be obtained as $122401 \equiv \text{Mod}(16,130561)^{-1}$ alternatively

Conjecture: The number of elements in the group generated by $-1+2^t$ working modulo P where P is $1+(-1+2^t) \times (2^{t+1})$ must be a multiple of $1+2 \times t$

For 511 from $t=9$ the 19 elements in **TNw19** are as shown next

{ 511,261121,256,130816,392321,65536,523201,490561,32736,506881
16,8176,515081,4096,**523261**,521221,2046,522241,1 }

For 1023 from $t=10$ the 84 elements in **TNw84** are as shown next

{ 1023,1046529,512,523776,1571073,262144,2094977,1964161,131008,2029569,
32,32736,2062353,16384,2095097,2086921,8188,2091009,2,2046,
2093058,1024,1047552,1047041,524288,2094849,1833217,262016,1964033,64,
65472,2029601,32768,2095089,2078737,16376,2086913,4,4092,2091011,
2048,-**1**,2094082,1048576,2094593,1571329,524032,1832961,128,130944,

1964097,65536,2095073,2062369,32752,2078721,8,8184,2086917,4096
 2095103,2093059,2047,2094081,1047553,1048064,1570817,256,261888,1833089,
 131072,2095041,2029633,65504,2062337,**16**,16368,2078729,8192,**2095101**,
 2091013,4094,2093057,1 }

The fourth element can be obtained as $523776 \equiv \text{Mod}(-4, 2095105)^{-1}$ alternatively

The eighth element can be obtained as $1964161 \equiv \text{Mod}(16, 2095105)^{-1}$ alternatively

For 2047 from $t=11$ the 46 elements in **TNw46** are as shown next

{ 2047,4190209,1024,2096128,6287873,1048576,8384257,7860481,524160,8122369,
 64,131008,8253473,65536,8384497,8351761,32760,8368129,4,8188,
 8376323,4096,-**1**,8382466,4194304,8383489,6288385,2096640,7335937,256,
 524032,7860353,262144,8384449,8253505,131040,8318977,**16**,32752,8351753,
 16384,**8384509**,8376325,8190,8380417,1 }

The fourth element can be obtained as $2096128 \equiv \text{Mod}(-4, 8384513)^{-1}$ alternatively

The eighth element can be obtained as $7860481 \equiv \text{Mod}(16, 8384513)^{-1}$ alternatively

For 4095 from $t=12$ the 100 elements in **TNw100** are not tabulated here

For 8191 from $t=13$ the 27 elements in **TNw27** are not tabulated here

For 16383 from $t=14$ the 116 elements in **TNw116** are not tabulated here

For 32767 from $t=15$ the 62 elements in **TNw62** are not tabulated here

For 65535 from $t=16$ the 132 elements in **TNw132** are not tabulated here

For 131071 from $t=17$ the 35 elements in **TNw35** are not tabulated here

For 262143 from $t=18$ the 148 elements in **TNw148** are not tabulated here

For 524287 from $t=19$ the 78 elements in **TNw78** are not tabulated here

For 1048575 from $t=20$ the 164 elements in **TNw164** are not tabulated here

For 2097151 from $t=21$ the 43 elements in **TNw43** are not tabulated here

For 4194303 from $t=22$ the 180 elements in **TNw180** are not tabulated here

For 8388607 from t=23 the 94 elements in **TNw94** are shown next

```
{ 8388607, 70368727400449, 4194304, 35184367894528, 105553101586433,
17592186044416, 140737470529537, 131941379604481, 8796092497920, 136339425067009,
262144, 2199022993408, 138538448453633, 1099511627776, 140737471512577,
140187715829761, 549755781120, 140462593671169, 16384, 137438937088,
140600032632833, 68719476736, 140737471574017, 140703111843841, 34359736320,

140720291708929, 1024, 8589933568, 140728881644033, 4294967296,
140737471577857, 140735324094721, 2147483520, 140736397836289, 64,
536870848, 140736934707233, 268435456, 140737471578097, 140737337360401,
134217720, 140737404469249, 4, 33554428, 140737438023683,
16777216, -1, 140737463189506, 70368744177664, 140737467383809,

105553103683585, 35184369991680, 123145285533697, 1048576, 8796091973632,
131941379080193, 4398046511104, 140737471315969, 138538448584705, 2199023124480,
139637959950337, 65536, 549755748352, 140187715796993, 274877906944,
140737471561729, 140600032641025, 137438945280, 140668752101377, 4096,
34359734272, 140703111841793, 17179869184, 140737471577089, 140728881644545,

8589934080, 140733176610817, 256, 2147483392, 140735324094593,
1073741824, 140737471578049, 140736934707265, 536870880, 140737203142657,
16, 134217712, 140737337360393, 67108864, 140737471578109,
140737438023685, 33554430, 140737454800897, 1 }
```

Every eighth element after 16 from the end of the subgroup is a power of 2

In order we would write them as follows

$$2^4, 2^8, 2^{12}, 2^{16}, 2^{20}, 2^{24}, 2^{28}, 2^{32}, 2^{36}, 2^{40}, 2^{44}$$

Writing them longhand we might say

eight from last is 2^8

sixteenth from last is 2^{16}

...

eighty-eighth from last is 2^{44}

If our subgroup was big enough then 2^{48} would be ninety-sixth from last, but we have not got that many elements!

In calculation terms we can jump to any portion of our subgroup and be at most 7 elements away from the element we require.

This can be a tremendous labour saver as instead of repeated powering to obtain an element of the subgroup, we can jump near our required element and then conduct a much smaller number of repeated powering to gain our result.

For 16777215 from t=24 the 196 elements in **TNw196** not tabulated here

However we have confirmed that 96 from last at power 100 is the value 2^{48} and 2^{24} is equivalent to $-1 + 2^t$ to the 148th power

For 33554431 from t=25 the 51 elements in **TNw51** are as shown next

{ 33554431,1125899839733761,16777216,562949936644096,
1688849801543681,281474976710656,2251799742382081,2111062262415361,
140737486258176,2181431002398721,1048576,35184371040256,
2216615375011841,17592186044416,2251799746314241,2243003653816321,
8796092891136,2247401700065281,65536,2199023190016,
2249600723353601,1099511627776,2251799746560001,2251249990778881,
549755805696,2251524868669441,4096,137438949376,
2251662307624961,68719476736,2251799746575361,2251765386839041,
34359737856,2251782566707201,256,8589934336,
2251791156641921,4294967296,2251799746576321,2251797599092801,
2147483616,2251798672834561,**16**,536870896,
2251799209705481,268435456,**2251799746576381**,2251799612358661,
134217726,2251799679467521,1 }

The expectation from powers $2^4, 2^8, 2^{12}, 2^{16}, 2^{20}, 2^{24}$ tell us that the third element should be 2^{24}

The third element is indeed 2^{24}

Using sturdy element notation we might say the results tabulated in this document are

$\langle\langle -1+2^t \rangle\rangle$ for set $1+(-1+2^t) \times (2^{t+1})$ for t=2,3,4,5,6,7,8,9,10,11,23,25

Chapter 3 – Sturdy element $1+2^t$ in set $1+(1+2^t)\times(2^{t+1})$

Consider the Proth space $1+(1+2^t)\times(2^{t+1})$

We will be using generating element $1+2^t$

The [sub]groups generated by $1+2^t$ have low order [a lot lower than $n-1$]

A related Conjecture is given next.

Conjecture: Order of $1+2^t \pmod P$ when P is prime and P of the form $1+(1+2^t)\times(2^{t+1})$ divides $Lcm(2+4\times t-(t+1), 2+4\times t)$

Tabulating the elements of groups generated by $1+2^t$ next.

Using the prefix TPy to avoid clashing with existing letter conventions for groups.
Prefer G or S? Replace them in your local copy.

For 5 from $t=2$ the 20 elements in **TPy20** are as shown next

{ 5,25,2,10,9,4,20,18,8,40,36,16,39,31,32,37,21,23,33,1 }

which when put in numeric order are

1,2,4,5,8,9,10,16,18,20,21,23,25,31,32,33,36,37,39,40

Elements that do not appear are as shown next

3,6,7,11,12,13,14,15,17,19,22,24,26,27,28,29,30,34,35,38

When $t=3$ we have $P=1+9\times 16$ and the set of elements modulo P is a multiplicative group.

Our generator $1+2^t$ is 9 and the subset it generates has 14 elements.

The elements in **TPy14** are { 9,81,4,36,34,16,144,136,64,141,109,111,129,1 }

If **TPy14** is really a group then we need inverses so let us document those next.

- Inverse of 9 is 129 mod P
- Inverse of 81 is 111 mod P
- Inverse of 4 is 109 mod P
- Inverse of 36 is 141 mod P
- Inverse of 34 is 64 mod P
- Inverse of 16 is 136 mod P

For 17 from $t=4$ the 36 elements in **TPy36** are as shown next

{ 17,289,8,136,132,64,543,511,512,529,273,281,417,4,68,66,32,-1,528,256,537,409,413,481,2,34,33,16,272,264,128,541,477,479,513,1 }

For 33 from $t=5$ the 11 elements in **TPy11** are as shown next

{ 33,1089,16,528,520,256,2109,1981,1983,2049,1 }

For 65 from $t=6$ the 52 elements in **TPy52** are as shown next

{ 65,4225,32,**2080**,2064,1024,8313,7801,7805,8065,
2,**130**,129,64,4160,4128,2048,8305,7281,**7289**,
7809,4,260,258,128,8320,8256,**4096**,8289,6241,
6257,7297,8,520,516,**256**,8319,8191,8192,8257,
4161,4193,6273,**16**,1040,1032,512,**8317**,8061,8063,
8193,1 }

The fifth to last element is always -4

Every eighth element after 16 from the end of the subgroup is a power of 2.

In order we would write them as follows

$$2^4, 2^8, 2^{12}, 2^{16}, 2^{20}, 2^{24}, 2^{28}, 2^{32}, 2^{36}, 2^{40}$$

Writing them longhand we might say

eight from last is 16

sixteenth from last is 2^8

twentyfourth from last is 2^{12}

...

eightieth from last is 2^{40}

In calculation terms we can jump to any portion of our group and be at most 7 elements away from the element we require.

This can be a tremendous labour saver as instead of repeated powering to obtain an element of the subgroup, we can jump near our required element and then conduct a much smaller number of repeated powering to gain our result.

For 129 from $t=7$ the 30 elements in **TPy30** are as shown next.

{ 129, 16641, 64, 8256, 8224, **4096**, 33009, 30961, 30969, 32001,
4, 516, 514, **256**, **-1**, 32896, 16384, 32961, 24769, 24801,
28929, **16**, 2064, 2056, 1024, **33021**, 32509, 32511, 32769, 1 }

The fourth element can be obtained as $8256 \equiv \text{Mod}(-4, 33025)^{-1}$ alternatively

The eighth element can be obtained as $30961 \equiv \text{Mod}(16, 33025)^{-1}$ alternatively

For 257 from $t=8$ the 68 elements in **TPy68** are as shown next.

{ 257, 66049, 128, **32896**, 32832, 16384, 131553, 123361, 123377, 127489,
8, **2056**, 2052, 1024, 131583, 131071, 131072, 131329, 65793, **65921**,
98817, 64, 16448, 16416, 8192, 131569, 127473, **127481**, 129537, 4
1028, 1026, 512, **-1**, 131328, **65536**, 131457, 98689, 98753, 115201,
32, 8224, 8208, **4096**, 131577, 129529, 129533, 130561, 2, 514
513, **256**, 65792, 65664, 32768, 131521, 115137, 115169, 123393, **16**,
4112, 4104, 2048, **131581**, 130557, 130559, 131073, 1 }

Conjecture: The number of elements in the group generated by $1+2^t$ working modulo P where P is $1+(1+2^t)(2^{t+1})$ must be a multiple of $1+2 \times t$

For 513 from $t=9$ the 19 elements in **TPy19** are as shown next

{ 513, 263169, 256, 131328, 131200, 65536, 525249, 492481, 492513, 408929, 16, 8208, 8200, 4096, 525309, 523261, 523263, 524289, 1 }

For 1025 from $t=10$ the 84 elements in **TPy84** are not tabulated here

For 2049 from $t=11$ the 46 elements in **TPy46** are not tabulated here

For 4097 from $t=12$ the 100 elements in **TPy100** are not tabulated here

For 8193 from $t=13$ the 27 elements in **TPy27** are not tabulated here

For 16385 from $t=14$ the 116 elements in **TPy116** are not tabulated here

For 32769 from $t=15$ the 62 elements in **TPy62** are not tabulated here

For 65537 from $t=16$ the 132 elements in **TPy132** are not tabulated here

For 131073 from $t=17$ the 35 elements in **TPy35** are not tabulated here

For 262145 from $t=18$ the 148 elements in **TPy148** are not tabulated here

For 524289 from $t=19$ the 78 elements in **TPy78** are not tabulated here

For 1048577 from $t=20$ the 164 elements in **TPy164** are not tabulated here

Using sturdy element notation we might say the results tabulated in this document are

$\langle\langle 1+2^t \rangle\rangle$ for set $1+(1+2^t)\times(2^{t+1})$ for $t=2,3,4,5,6,7,8,9$

Chapter 4 – Element $-1+3^t$ and set $1+(-1+3^t)\times(3^{t+1})$

Consider the Proth space $1+(-1+3^t)\times(3^{t+1})$

We will be using generating element $-1+3^t$

The [sub]groups generated by $-1+3^t$ have low order [a lot lower than $n-1$]

Tabulating the elements of groups generated by $-1+3^t$ next.

Using the prefix **Ent** to avoid clashing with existing letter conventions for groups.
Prefer G or S? Replace them in your local copy.

For 8 from $t=2$ elements **Ent5** are { 8, 64, 78, 190, 1 }

For 26 from $t=3$ the elements in **Ent42** are as shown next.

{ 26, 676, 720, 1864, 3, 78, 2028, 53, 1378, 9
234, 1870, 159, 2027, 27, 702, 1396, 477, 1867, 81
2106, 2081, 1431, 1387, 243, 2104, 2029, 79, 2054, 729
2098, 1873, 237, 1948, 80, 2080, 1405, 711, 1630, 240
2026, 1 }

When $t=4$ we have $P=1+80\times 243$ and the set of elements modulo P is a multiplicative group.

Our generator $-1+3^t$ is 80 and the subset it generates has 27 elements.

The elements in **Ent27** are as shown next

{ 80, 6400, 6534, 17254, 9, 720, 18718, 483, 19199, 81,
6480, 12934, 4347, 17263, 729, 19438, 19201, 241, 19280, 6561,
19414, 17281, 2169, 17992, 726, 19198, 1 }

If **Ent27** is really a group then we need inverses so let us document those next.

- Inverse of 80 is 19198 mod P
- Inverse of 6400 is 726 mod P
- Inverse of 6534 is 17992 mod P
- Inverse of 17254 is 2169 mod P
- Inverse of 9 is 17281 mod P
- Inverse of 720 is 19414 mod P
- Inverse of 18718 is 6561 mod P
- Inverse of 483 is 19280 mod P
- Inverse of 19199 is 241 mod P
- Inverse of 81 is 19201 mod P
- Inverse of 6480 is 19438 mod P
- Inverse of 12934 is 729 mod P
- Inverse of 4347 is 17263 mod P

For 242 from $t=5$ the 22 elements in **Ent22** are as shown next

{ 242, 58564, 58968, 156736, 27, 6534, 169876, 4365, 174235, 729, 176418, 176177, 117855, 117451, 19683, **176392**, 169885, 6543, 172054, 2184, 175690, 1 }

The seventh to last element is always -27

The thirteenth to last element is always 729 alternatively written as 3^6

For 728 from $t=6$ the 39 elements in **Ent39** are as shown next

{ 728, 529984, **531198**, 1414990, 81, 58968, 1533142, 39339, 1572463, 6561, 1592134, 1589953, 2185, 1590680, **531441**, 1591894, 1415233, 176985, 1474120, 59022, 1572454, 9, 6552, 1585582, 4371, 1589951, **729**, 530712, 1061182, 354051, 1415071, 59049, 1592110, 1572481, 19665, 1579024, 6558, 1589950, 1 }

Every twelfth element after 3^6 from the end of the subgroup is a power of 3.

In order we would write them as follows

$3^6, 3^{12}, 3^{18}, 3^{24}, 3^{30}, 3^{36}, 3^{42}, 3^{48}, 3^{54}, 3^{60}$

Writing them longhand we might say

thirteenth from last is 3^6
 twentyfifth from last is 3^{12}
 ...
 fortyninth from last is 3^{24}
 ...

In calculation terms we can jump to any portion of our group and be at most 11 elements away from the element we require.

This can be a tremendous labour saver as instead of repeated powering to obtain an element of the subgroup, we can jump near our required element and then conduct a much smaller number of repeated powering to gain our result.

For 2186 from $t=7$ the 90 elements in **Ent90** are as shown next.

{ 2186, 4778596, 4782240, 12748024, 243, **531198**, 13811068, 354213, 14165227, 59049, 14342338, 14322673, 19677, 14329228, 6560, 14340160, 9561565, **4781511**, 11154430, 1594080, 13810906, 81, 177066, 14165254, 118071, 14283307, 19683, 14342344, 14335789, **6559**, 14337974, 4782969, 14341618, 12748753, 1593837, 13279708, 531360, 14165200, 27, 59022, 14283316, **39357**, 14322667, 6561, **-1**, 14340161, 9563751, 9560107, 1594323, 14342104, 13811149, 531279, 13988134, **177120**, 14283298, 9, 19674, 14322670, 13119, 14335787, 2187, 4780782, 9560836, 3187917, 12748267, **531441**, 14342266, 14165281, 177093, 14224276, 59040, 14322664, 3, 6558, 14335788, 4373, 9559378, **729**, 1593594, 12748510, 1062639, 13810987, 177147, **14342320**, 14283325, 59031, 14302990, 19680, 14335786, 1 }

The sixth element can be obtained as $531198 == \text{Mod}(-27, 14342347)^{-1}$ alternatively

The twelfth element can be obtained as $14322673 == \text{Mod}(729, 14342347)^{-1}$ alternatively

For 6560 from $t=8$ the 68 elements in **Ent17** are as shown next.

{ 6560, 43033600, 43044534, 114771574, 729, 4782240, 124337998,
3188403, 127526239, 531441, 129120454, 128943361, 177129, 129002392,
59046, 129100798, 1 }

Conjecture: The number of elements in the group generated by $-1+3^t$ working modulo P where P is $1+(-1+3^t) \times (3^{t+1})$ must be a multiple of $1+2 \times t$

For 19682 from $t=9$ the 114 elements in **Ent114** are not tabulated here

For 59048 from $t=10$ the 63 elements in **Ent63** are not tabulated here

For 177146 from $t=11$ the 46 elements in **Ent46** are not tabulated here

For 531440 from $t=12$ the 75 elements in **Ent75** are not tabulated here

For 1594322 from $t=13$ the 162 elements in **Ent162** are not tabulated here

For 4782968 from $t=14$ the 29 elements in **Ent29** are not tabulated here

For 14348906 from $t=15$ the 186 elements in **Ent186** are not tabulated here

For 43046720 from $t=16$ the 99 elements in **Ent99** are not tabulated here

For 129140162 from $t=17$ the 70 elements in **Ent70** are not tabulated here

For 387420488 from $t=18$ the 111 elements in **Ent111** are not tabulated here

For 1162261466 from $t=19$ the 234 elements in **Ent234** are not tabulated here

For 3486784400 from $t=20$ the 41 elements in **Ent41** are not tabulated here

Using sturdy element notation we might say the results tabulated in this document are

$\langle\langle -1+3^t \rangle\rangle$ for set $1+(-1+3^t) \times (3^{t+1})$ for $t=2,3,4,5,6,7,8$

Chapter 5 – Element $1+3^t$ and set $1+(1+3^t)\times(3^{t+1})$

Consider the Proth space $1+(1+3^t)\times(3^{t+1})$

We will be using generating element $1+3^t$

The [sub]groups generated by $1+3^t$ have low order [a lot lower than $n-1$]

Tabulating the elements of groups generated by $1+3^t$ next.

Using the prefix EPu to avoid clashing with existing letter conventions for groups.
Prefer G or S? Replace them in your local copy.

When $t=2$ we have $P=1+10\times 27$ and the set of elements modulo P is a multiplicative group.

Our generator $1+3^t$ is 10 and the subset it generates has 5 elements.

The elements in **EPu5** are { 10, 100, 187, 244, 1 }

If **EPu5** is really a group then we need inverses so let us document those next.

- Inverse of 10 is 244 mod P
- Inverse of 100 is 187 mod P

For 28 from $t=3$ the elements in **EPu42** are as shown next.

{ 28, 784, 1531, 2026, 3, **84**, 83, 55, 1540, 9,
252, 249, 165, 82, 27, 756, 747, **495**, 246, 81,
-1, 2241, 1485, 738, 243, 2266, 2185, 2186, 2214, **729**,
2260, 2017, 2020, 2104, 2187, **2242**, 1513, 1522, 1774, 2023,
2188, 1 }

The seventh to last element is always -27

The thirteenth to last element is always 729 alternatively written as 3^6

Every twelfth element after 3^6 from the end of the subgroup is a power of 3.

In order we would write them as follows

$3^6, 3^{12}, 3^{18}, 3^{24}, 3^{30}, 3^{36}, 3^{42}, 3^{48}, 3^{54}, 3^{60}$

Writing them longhand we might say

thirteenth from last is 3^6

twentyfifth from last is 3^{12}

...

fortyninth from last is 3^{24}

...

In calculation terms we can jump to any portion of our group and be at most 11 elements away from the element we require.

This can be a tremendous labour saver as instead of repeated powering to obtain an element of the subgroup, we can jump near our required element and then conduct a much smaller number of repeated powering to gain our result.

For 82 from $t=4$ the 27 elements in **EPu27** are shown next.

{ 82, 6274, **13339**, 17740, 9, 738, 735, 489, 244, 81,
6642, 6615, 4401, 2196, **729**, 19924, 19681, 19682, 19764, 6561,
19900, 17713, 17722, 18460, 19195, 19684, 1 }

For 244 from $t=5$ the 22 elements in **EPu22** are not tabulated here

For 730 from $t=6$ the 39 elements in **EPu39** are not tabulated here

For 2188 from $t=7$ the 90 elements in **EPu90** are not tabulated here

For 6562 from $t=8$ the 17 elements in **EPu17** are not tabulated here

For 19684 from $t=9$ the 114 elements in **EPu114** are not tabulated here

For 59050 from $t=10$ the 63 elements in **EPu63** are not tabulated here

For 177148 from $t=11$ the 46 elements in **EPu46** are not tabulated here

For 531442 from $t=12$ the 75 elements in **EPu75** are not tabulated here

For 1594324 from $t=13$ the 162 elements in **EPu162** are not tabulated here

For 4782970 from $t=14$ the 29 elements in **EPu29** are not tabulated here

For 14348908 from $t=15$ the 186 elements in **EPu186** are not tabulated here

For 43046722 from $t=16$ the 99 elements in **EPu99** are not tabulated here

For 129140164 from $t=17$ the 70 elements in **EPu70** are not tabulated here

For 387420490 from $t=18$ the 111 elements in **EPu111** are not tabulated here

For 1162261468 from $t=19$ the 234 elements in **EPu234** are not tabulated here

For 3486784402 from $t=20$ the 41 elements in **EPu41** are not tabulated here

Using sturdy element notation we might say the results tabulated in this document are

$$\langle\langle 1+3^t \rangle\rangle \text{ for set } 1+(1+3^t) \times (3^{t+1}) \text{ for } t=2,3,4$$

Chapter 6 – What single word?

In this chapter we present the problem of navigating to an individual group

If you are lucky, your [multiplicative] group is readily labelled.

But what if it is not.

But you know the order.

So surely it is a case of a simple lookup?

Not so.

What you have is a bit like a road system for which the named groups are the Motorways and A roads, and the isomorphisms are the B roads.

“What is the minimum number of isomorphisms you can use to get from Z20 to the group $\{5, 25, 2, 10, 9, 4, 20, 18, 8, 40, 36, 16, 39, 31, 32, 37, 21, 23, 33, 1\}$?”

Pretend you are a taxi driver in a UK city and the client is asking you to get them to the group.

A typical reaction to this sort of question on a forum might be to throw up an order 20 paper that has been published.

This is the taxi driver throwing an A-Z at the client!

The client has posed a problem.

Is the system of navigation sufficient and easy?

Certainly the Motorways and A roads are established and easy to get to via name.

But the B roads are [isomorphism] links between and are not very accessible/transparent.

If they were, then you would be able to quickly say the group equivalent to something like..

Go to named group

Navigate the [how to describe?] isomorphism to other named group

...

Navigate the [how to describe?] isomorphism to other named group

You have arrived at your destination group

The above may not be easy to extract even from the author of the order 20 paper themselves.

One solution is to expand the network of Motorways and A roads further, but the problem here is (I) Neatness and simplicity – some would argue more A roads breaks this (II) Naming – are there obvious non-clashing names for groups to be added to A roads list?

It is easier to be added to the main named groups if you have a well understood lattice / matrix representation already or if you are a real world shape like a rectangular or prism like structure.

But what about if the group has not yet had the matrix / lattice representation yet or if the real world shape seems unreal or are difficult to visualise?

Perhaps there are barriers to getting things added to a top level naming system.

Perhaps if we find a solution to the navigation woes described, the unnamed groups will be [obviously] attached to the main system or the need for any new name established.

Should we name isomorphisms as a concatenation of the two group names?

This and other questions about navigation systems are not resolved here.

Is your request for directions resolved by the equivalent of “Asking the highways agency for a new A road”

If so who are the highways agency? A quorum of Mathematicians perhaps?

How do you ask?

Perhaps we can ask a similar navigation question online and see if we get any A-Z's thrown at us.

In the meantime here is a way of navigating that is new and could potentially solve this problem for 16 bunches of groups we have documented.

$\langle\langle 1+2^t \rangle\rangle$ for set $1+(1+2^t)\times(2^{t+1})$ for $t=2 = \{ 5,25,2,10,9,4,20,18,8,40,$
 $36,16,39,31,32,37,21,23,33,1 \}$ is **TPy20**

$\langle\langle 1+2^t \rangle\rangle$ for set $1+(1+2^t)\times(2^{t+1})$ for $t=3 = \{ 9,81,4,36,34,16,144,$
 $136,64,141,109,111,129,1 \}$ is **TPy14**

$\langle\langle 1+2^t \rangle\rangle$ for set $1+(1+2^t)\times(2^{t+1})$ for $t=5 = \{ 33,1089,16,528,520,256,$
 $2109,1981,1983,2049,1 \}$ is **TPy11**

$\langle\langle 2 \rangle\rangle$ for set $1+(-1+2^t)\times(2^{t+1})$ for $t=5 = \{ 2,4,8,16,7,14,3,6,12,-1,$
 $23,21,17,9,18,11,22,19,13,1 \}$ is **TNx20**

So if you do not like saying TPy20 instead just refer to $\{ 5,25, 2, \dots, 23, 33, 1 \}$ with the following notation:

$\langle\langle 1+2^t \rangle\rangle$ for set $1+(1+2^t)\times(2^{t+1})$ for $t=2$

Chapter 7 – Sturdy element 2 and set $1+(-1+2^t)\times(2^{t+1})$

Consider the Proth space $1+(-1+2^t)\times(2^{t+1})$

We will be using generating element 2

The [sub]groups generated by 2 have low order [a lot lower than $n-1$]

Tabulating the elements of groups generated by 2 next.

Using the prefix **TNx** to avoid clashing with existing letter conventions for groups.
Prefer G or S? Replace them in your local copy.

From $t=2$ the elements in **TNx20** are { 2, 4, 8, 16, 7, 14, 3, 6, 12, -1, 23, 21, 17, 9, 18, 11, 22, 19, 13, 1 }

Conjecture: Order of 2 mod N when N of the form $1+(-1+2^t)\times(2^{t+1})$ is $4\times(1+2\times t)$

When $t=3$ we have $P=1+7\times 16$ and the set of elements modulo P is a multiplicative group.

The subgroup generated by 2 has 28 elements

The elements in **TNx28** are as shown next

{ 2, 4, 8, 16, 32, 64, 15, 30, 60, 7, 14, 28, 56, -1, 111, 109, 105, 97, 81, 49, 98, 83, 53, 106, 99, 85, 57, 1 }

If **TNx28** is really a group then we need inverses so let us document those next.

- Inverse of 2 is 57 mod P
- Inverse of 4 is 85 mod P
- Inverse of 8 is 99 mod P
- Inverse of 16 is 106 mod P
- Inverse of 32 is 53 mod P
- Inverse of 15 is 98 mod P
- Inverse of 30 is 49 mod P
- Inverse of 60 is 81 mod P
- Inverse of 7 is 97 mod P
- Inverse of 14 is 105 mod P
- Inverse of 28 is 109 mod P
- Inverse of 56 is 111 mod P

We could alternatively write the group **TNx28** as follows:

{ 2, 4, 8, 16, 32, 64, 15, 30, 60, 7, 14, 28, 56, -1, -2, -4, -8, -16, -32, -64, $-(2^7)$, $-(2^8)$, $-(2^9)$, $-(2^{10})$, $-(2^{11})$, $-(2^{12})$, $-(2^{13})$, 1 }

From $t=4$ the 36 elements in **TNx36** are as shown next

{ 2, 4, 8, 16, 32, 64, 128, 256, 31, 62, 124, 248, 15, 30, 60, 120, 240, -1, 479, 477, 473, 465, 449, 417, 353, 225, 450,

419, 357, 233, 466, 451, 421, 361, 241, 1 }

From $t=5$ the 44 elements in **TNx44** are as shown next

{ 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024,
63, 126, 252, 504, 1008, 31, 62, 124, 248, 496,
992, **-1**, 1983, 1981, 1977, 1969, 1953, 1921, 1857, 1729
1473, 961, 1922, 1859, 1733, 1481, 977, 1954, 1923, 1861,
1737, 1489, 993, 1 }

From $t=6$ the 52 elements in **TNx52** are as shown next.

{ 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024,
2048, 4096, 127, 254, 508, 1016, 2032, 4064, 63, 126,
252, 504, 1008, 2016, 4032, **-1**, 8063, 8061, 8057, 8049,
8033, 8001, 7937, 7809, 7553, 7041, 6017, 3969, 7938, 7811,
7557, 7049, 6033, 4011, 8002, 7939, 7813, 7561, 7057, 6049,
4033, 1 }

From $t=7$ the 60 elements in **TNx60** are as shown next.

{ 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024,
2048, 4096, 8192, 16384, 255, 510, 1020, 2040, 4080, 8160,
16320, 127, 254, 508, 1016, 2032, 4064, 8128, 16256, **-1**,
32511, 32509, 32505, 32497, 32481, 32449, 32385, 32257, 32001, 31489,
30465, 28417, 24321, 16129, 32258, 32003, 31493, 30473, 28433, 24353,
16193, 32386, 32259, 32005, 31497, 30481, 28449, 24385, 16257, 1 }

From $t=8$ the 68 elements in **TNx68** are as shown next.

{ 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024,
2048, 4096, 8192, 16384, 32768, 65536, 511, 1022, 2044, 4088,
8176, 16352, 32704, 65408, 255, 510, 1020, 2040, 4080, 8160,
16320, 32640, 65280, **-1**, 130559, 130557, 130553, 130545, 130529, 130497,
130433, 130305, 130049, 129537, 128513, 126465, 122369, 114177, 97793, 65025
130050, 129539, 128517, 126473, 122385, 114209, 97857, 65153, 130306, 130051,
129541, 128521, 126481, 122401, 114241, 97921, 65281, 1 }

From $t=9$ the 76 elements in **TNx76** are not tabulated here

For $t=10$ the 84 elements in **TNx84** are not tabulated here

For $t=11$ the 92 elements in **TNx92** are not tabulated here

For $t=12$ the 100 elements in **TNx100** are not tabulated here

For $t=13$ the 108 elements in **TNx108** are not tabulated here

For $t=14$ the 116 elements in **TNx116** are not tabulated here

For $t=15$ the 124 elements in **TNx124** are not tabulated here

For $t=16$ the 132 elements in **TNx132** are not tabulated here

For $t=17$ the 140 elements in **TNx140** are not tabulated here

For $t=18$ the 148 elements in **TNx148** are not tabulated here

For $t=19$ the 156 elements in **TNx156** are not tabulated here

For $t=20$ the 164 elements in **TNx164** are not tabulated here

Using sturdy element notation we might say the results tabulated in this document are

$\langle\langle 2 \rangle\rangle$ for set $1 + (-1 + 2^t) \times (2^{t+1})$ for $t=2,3,4,5,6,7,8$

Chapter 8 – Sturdy element 2 and set $1+(1+2^t)\times(2^{t+1})$

Consider the Proth space $1+(1+2^t)\times(2^{t+1})$

We will be using generating element 2

The [sub]groups generated by 2 have low order [a lot lower than $n-1$]

Tabulating the elements of groups generated by 2 next.

Using the prefix TPv to avoid clashing with existing letter conventions for groups.
Prefer G or S? Replace them in your local copy.

When $t=2$ we have $P=1+5\times 8$ and the set of elements modulo P is a multiplicative group.

The subgroup generated by 2 has 20 elements

The elements in **TPv20** are as shown next

{ 2, 4, 8, 16, 32, 23, 5, 10, 20, -1
39, 37, 33, 25, 9, 18, 36, 31, 21, 1 }

If **TPv20** is really a group then we need inverses so let us document those next.

- Inverse of 2 is 21 mod P
- Inverse of 4 is 31 mod P
- Inverse of 8 is 36 mod P
- Inverse of 16 is 18 mod P
- Inverse of 32 is 9 mod P
- Inverse of 23 is 25 mod P
- Inverse of 5 is 33 mod P
- Inverse of 10 is 37 mod P
- Inverse of 20 is 39 mod P

Conjecture: Order of 2 mod N when N of the form $1+(1+2^t)\times(2^{t+1})$ is $4\times(1+2\times t)$

From $t=3$ the 28 elements in **TPv28** are as shown next

{ 2, 4, 8, 16, 32, 64, 128, 111, 77, 9,
18, 36, 72, -1, 143, 141, 137, 129, 113, 81,
17, 34, 68, 136, 127, 109, 73, 1 }

We could alternatively write the group **TPv28** as follows:

{ 2, 4, 8, 16, 32, 64, 128, 2^8 , 2^9 , 2^{10} , 2^{11} , 2^{12} , 2^{13} , -1,
-2, -4, -8, -16, -32, -64, $-(2^7)$, $-(2^8)$, $-(2^9)$, $-(2^{10})$, $-(2^{11})$, $-(2^{12})$, $-(2^{13})$, 1 }

From $t=4$ the 36 elements in **TPv36** are as shown next

{ 2, 4, 8, 16, 32, 64, 128, 256, 512, 479,
413, 281, 17, 34, 68, 136, 272, -1, 543, 541,
537, 529, 513, 481, 417, 289, 33, 66, 132, 264,
528, 511, 477, 409, 273, 1 }

From t=5 the 44 elements in **TPv44** are as shown next

{ 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024,
2048, 1983, 1853, 1593, 1073, 33, 66, 132, 264, 528,
1056, -1, 2111, 2109, 2105, 2097, 2081, 2049, 1985, 1857,
1601, 1089, 65, 130, 260, 520, 1040, 2080, 2047, 1981,
1849, 1585, 1057, 1 }

From t=6 the 52 elements in **TPv52** are as shown next.

{ 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024,
2048, 4096, 8192, 8063, 7805, 7289, 6257, 4193, 65, 130,
260, 520, 1040, 2080, 4160, -1, 8319, 8317, 8313, 8305,
8289, 8257, 8193, 8065, 7809, 7297, 6273, 4225, 129, 258,
516, 1032, 2064, 4128, 8256, 8191, 8061, 7801, 7281, 6241,
4161, 1 }

From t=7 the 60 elements in **TPv60** are as shown next.

{ 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024,
2048, 4096, 8192, 16384, 32768, 32511, 31997, 30969, 28913, 24801,
16577, 129, 258, 516, 1032, 2064, 4128, 8256, 16512, -1,
33023, 33021, 33017, 33009, 32993, 32961, 32897, 32769, 32513, 32001,
30977, 28929, 24833, 16641, 257, 514, 1028, 2056, 4112, 8224,
16448, 32896, 32767, 32509, 31993, 30961, 28897, 24769, 16513, 1 }

From t=8 the 68 elements in **TPv68** are as shown next.

{ 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024,
2048, 4096, 8192, 16384, 32768, 65536, 131072, 130559, 129533, 127481,
123377, 115169, 98753, 65921, 257, 514, 1028, 2056, 4112, 8224,
16448, 32896, 65792, -1, 131583, 131581, 131577, 131569, 131553, 131521,
131457, 131329, 131073, 130561, 129537, 127489, 123393, 115201, 98817, 66049,
513, 1026, 2052, 4104, 8208, 16416, 32832, 65664, 131328, 131071,
130557, 129529, 127473, 123361, 115137, 98689, 65793, 1 }

From t=9 the 76 elements in **TPv76** are not tabulated here

For t=10 the 84 elements in **TPv84** are not tabulated here

For t=11 the 92 elements in **TPv92** are not tabulated here

For t=12 the 100 elements in **TPv100** are not tabulated here

For t=13 the 108 elements in **TPv108** are not tabulated here

For t=14 the 116 elements in **TPv116** are not tabulated here

For t=15 the 124 elements in **TPv124** are not tabulated here

For t=16 the 132 elements in **TPv132** are not tabulated here

For t=17 the 140 elements in **TPv140** are not tabulated here

For t=18 the 148 elements in **TPv148** are not tabulated here

For t=19 the 156 elements in **TPv156** are not tabulated here

For t=20 the 164 elements in **TPv164** are not tabulated here

Using sturdy element notation we might say the results tabulated in this document are

$\langle\langle 2 \rangle\rangle$ for set $1 + (1 + 2^t) \times (2^{t+1})$ for t=2,3,4,5,6,7,8

Chapter 9 – Sturdy element 3 and set $1+(-1+3^t)\times(3^{t+1})$

Consider the Proth space $1+(-1+3^t)\times(3^{t+1})$

We will be using generating element 3

The [sub]groups generated by 3 have low order [a lot lower than $n-1$]

Tabulating the elements of groups generated by 3 next.

Using the prefix ENp to avoid clashing with existing letter conventions for groups.

Prefer G or S? Replace them in your local copy.

Conjecture: Order of 3 mod N when N of the form $1+(-1+3^t)\times(3^{t+1})$ is $6\times(1+2\times t)$

When $t=2$ we have $P=1+8\times 27$ and the set of elements modulo P is a multiplicative group.

The subgroup generated by 3 has 30 elements

The elements in **ENp30** are as shown next

{ 3, 9, 27, 81, 26, 78, 17, 51, 153, 25,
75, 8, 24, 72, -1, 214, 208, 190, 136, 191,
139, 200, 166, 64, 192, 142, 209, 193, 145, 1 }

If **ENp30** is really a group then we need inverses so let us document those next.

- Inverse of 3 is 145 mod P
- Inverse of 9 is 193 mod P
- Inverse of 27 is 209 mod P
- Inverse of 81 is 142 mod P
- Inverse of 26 is 192 mod P
- Inverse of 78 is 64 mod P
- Inverse of 17 is 166 mod P
- Inverse of 51 is 200 mod P
- Inverse of 153 is 139 mod P
- Inverse of 25 is 191 mod P
- Inverse of 75 is 136 mod P
- Inverse of 8 is 190 mod P
- Inverse of 24 is 208 mod P
- Inverse of 72 is 214 mod P $\backslash 214 == \text{Mod}((3^{14}), pr)^{-1}$

We could alternatively write the group **ENp30** as follows:

{ 3, 9, 27, 81, 3^5 , 3^6 , 3^7 , 3^8 , 3^9 , 3^{10} , 3^{12} , 3^{13} , 3^{14} , -1
-3, -9, -27, -81, -3^5 , -3^6 , -3^7 , -3^8 , -3^9 , -3^{10} , -3^{11} , -3^{12} , -3^{13} , -3^{14} , 1 }

From $t=3$ the 42 elements in **ENp42** are as shown next

{ 3, 9, 27, 81, 243, 729, 80, 240, 720, 53
159, 477, 1431, 79, 237, 711, 26, 78, 234, 702,
-1, 2104, 2098, 2080, 2026, 1864, 1378, 2027, 1867, 1387,
2054, 1948, 1630, 676, 2028, 1870, 1396, 2081, 2029, 1873,

1405, 1 }

From t=4 the 54 elements in **ENp54** are as shown next

{ 3, 9, 27, 81, 243, 729, 2187, 6561, 242, 726
2178, 6534, 161, 483, 1449, 4347, 13041, 241, 723, 2169,
6507, 80, 240, 720, 2160, 6480, -1, 19438, 19432, 19414,
19360, 19198, 18712, 17254, 12880, 19199, 18715, 17263, 12907, 19280,
18958, 17992, 15094, 6400, 19200, 18718, 17272, 12934, 19361, 19201,
18721, 17281, 12961, 1 }

From t=5 the 66 elements in **ENp66** are as shown next.

{ 3, 9, 27, 81, 243, 729, 2187, 6561, 19683, 59049,
728, 2184, 6552, 19656, 58968, 485, 1455, 4365, 13095, 39285,
117855, 727, 2181, 6543, 19629, 58887, 242, 726, 2178, 6534,
19602, 58806, -1, 176416, 176410, 176392, 176338, 176176, 175690, 174232,
169858, 156736, 117370, 175691, 174235, 169867, 156763, 117451, 175934, 174964,
172054, 163324, 137134, 58564, 175692, 174238, 169876, 156790, 117532, 176177,
175693, 174241, 169885, 156817, 117613, 1 }

From t=6 the 78 elements in **ENp78** are not tabulated here

From t=7 the 90 elements in **ENp90** are not tabulated here

From t=8 the 102 elements in **ENp102** are not tabulated here

From t=9 the 114 elements in **ENp114** are not tabulated here

For t=10 the 126 elements in **ENp126** are not tabulated here

For t=11 the 138 elements in **ENp138** are not tabulated here

For t=12 the 150 elements in **ENp150** are not tabulated here

For t=13 the 162 elements in **ENp162** are not tabulated here

For t=14 the 174 elements in **ENp174** are not tabulated here

For t=15 the 186 elements in **ENp186** are not tabulated here

For t=16 the 198 elements in **ENp198** are not tabulated here

For t=17 the 210 elements in **ENp210** are not tabulated here

For t=18 the 222 elements in **ENp222** are not tabulated here

For t=19 the 234 elements in **ENp234** are not tabulated here

For t=20 the 246 elements in **ENp246** are not tabulated here

Using sturdy element notation we might say the results tabulated in this document are

$\langle\langle 3 \rangle\rangle$ for set $1 + (-1 + 3^t) \times (3^{t+1})$ for t=2,3,4,5

Chapter 10 – Sturdy element 3 and set $1+(1+3^t)\times(3^{t+1})$

Consider the Proth space $1+(1+3^t)\times(3^{t+1})$

We will be using generating element 3

The [sub]groups generated by 3 have low order [a lot lower than $n-1$]

Tabulating the elements of groups generated by 3 next.

Using the prefix EPr to avoid clashing with existing letter conventions for groups.

Prefer G or S? Replace them in your local copy.

Conjecture: Order of 3 mod N when N of the form $1+(1+3^t)\times(3^{t+1})$ is $6\times(1+2\times t)$

When $t=2$ we have $P=1+10\times 27$ and the set of elements modulo P is a multiplicative group.

The subgroup generated by 3 has 30 elements

The elements in **EPr30** are as shown next

{ 3, 9, 27, 81, 243, 187, 19, 57, 171, 242,
184, 10, 30, 90, -1, 268, 262, 244, 190, 28,
84, 252, 214, 100, 29, 87, 261, 241, 181, 1 }

If **EPr30** is really a group then we need inverses so let us document those next.

- Inverse of 3 is 181 mod P
 - Inverse of 9 is 241 mod P
 - Inverse of 27 is 261 mod P
 - Inverse of 81 is 87 mod P
 - Inverse of 243 is 29 mod P
 - Inverse of 187 is 100 mod P
 - Inverse of 19 is 214 mod P
 - Inverse of 57 is 252 mod P
 - Inverse of 171 is 84 mod P
 - Inverse of 242 is 28 mod P
 - Inverse of 184 is 190 mod P
 - Inverse of 10 is 244 mod P
 - Inverse of 30 is 262 mod P
 - Inverse of 90 is 268 mod P
- $\backslash 268 == \text{Mod}((3^{14}), \text{prp})^{-1}$

We could alternatively write the group **EPr30** as follows:

{ 3, 9, 27, 81, 3^5 , 3^6 , 3^7 , 3^8 , 3^9 , 3^{10} , 3^{11} , 3^{12} , 3^{13} , 3^{14} , -1,
-3, -9, -27, -81, -3^5 , -3^6 , -3^7 , -3^8 , -3^9 , -3^{10} , -3^{11} , -3^{12} , -3^{13} , -3^{14} , 1 }

From $t=3$ the 42 elements in **EPr42** are as shown next

{ 3, 9, 27, 81, 243, 729, 2187, 2023, 1531, 55,
165, 495, 1485, 2186, 2020, 1522, 28, 84, 252, 756,
-1, 2266, 2260, 2242, 2188, 2026, 1540, 82, 246, 738,
2214, 2104, 1774, 784, 83, 249, 747, 2241, 2185, 2017,

1513, 1 }

From t=4 the 54 elements in **EPr54** are as shown next

{ 3, 9, 27, 81, 243, 729, 2187, 6561, 19683, 19195,
17731, 13339, 163, 489, 1467, 4401, 13203, 19682, 19192, 17722,
13312, 82, 246, 738, 2214, 6642, -1, 19924, 19918, 19900,
19846, 19684, 19198, 17740, 13366, 244, 732, 2196, 6588, 19764,
19438, 18460, 15526, 6724, 245, 735, 2205, 6615, 19845, 19681,
19189, 17713, 13285, 1 }

From t=5 the 66 elements in **EPr66** are as shown next.

{ 3, 9, 27, 81, 243, 729, 2187, 6561, 19683, 59049,
177147, 175687, 171307, 158167, 118747, 487, 1461, 4383, 13149, 39447,
118341, 177146, 175684, 171298, 158140, 118666, 244, 732, 2196, 6588,
19764, 59292, -1, 177874, 177868, 177850, 177796, 177634, 177148, 175690,
171316, 158194, 118828, 730, 2190, 6570, 19710, 59130, 177390, 176416,
173494, 164728, 138430, 59536, 721, 2193, 6579, 19737, 59211, 177633,
177145, 175681, 171289, 158113, 118585, 1 }

From t=6 the 78 elements in **EPr78** are not tabulated here

From t=7 the 90 elements in **EPr90** are not tabulated here

From t=8 the 102 elements in **EPr102** are not tabulated here

From t=9 the 114 elements in **EPr114** are not tabulated here

For t=10 the 126 elements in **EPr126** are not tabulated here

For t=11 the 138 elements in **EPr138** are not tabulated here

For t=12 the 150 elements in **EPr150** are not tabulated here

For t=13 the 162 elements in **EPr162** are not tabulated here

For t=14 the 174 elements in **EPr174** are not tabulated here

For t=15 the 186 elements in **EPr186** are not tabulated here

For t=16 the 198 elements in **EPr198** are not tabulated here

For t=17 the 210 elements in **EPr210** are not tabulated here

For t=18 the 222 elements in **EPr222** are not tabulated here

For t=19 the 234 elements in **EPr234** are not tabulated here

For t=20 the 246 elements in **EPr246** are not tabulated here

Using sturdy element notation we might say the results tabulated in this document are

$\langle\langle 3 \rangle\rangle$ for set $1 + (1 + 3^t) \times (3^{t+1})$ for t=2,3,4,5

Chapter 11 – Sturdy element 2 and set $1+(-1+2^t)\times 2^t$

Consider the space $1+(-1+2^t)\times 2^t$

We will be using generating element 2

The [sub]groups generated by 2 have low order [a lot lower than $n-1$]

Tabulating the elements of groups generated by 2 next.

Using the prefix **NNa** to avoid clashing with existing letter conventions for groups.
Prefer G or S? Replace them in your local copy.

From $t=3$ the elements in **NNa18** are { 2, 4, 8, 16, 32, 7, 14, 28, -1, 55, 53, 49, 41, 25, 50, 43, 29, 1 }

Conjecture: Order of 2 mod N when N of the form $1+(-1+2^t)\times 2^t$ is $6\times t$

When $t=4$ we have $P=1+15\times 16$ and the set of elements modulo P is a multiplicative group.

The subgroup generated by 2 has 24 elements

The elements in **NNa24** are as shown next

{ 2, 4, 8, 16, 32, 64, 128, 15, 30, 60, 120, -1, 239, 237, 233, 225, 209, 177, 113, 226, 211, 181, 121, 1 }

If **NNa24** is really a group then we need inverses so let us document those next.

- Inverse of 2 is 121 mod P
- Inverse of 4 is 181 mod P
- Inverse of 8 is 211 mod P
- Inverse of 16 is 226 mod P
- Inverse of 32 is 113 mod P
- Inverse of 64 is 177 mod P
- Inverse of 128 is 209 mod P
- Inverse of 15 is 225 mod P
- Inverse of 30 is 233 mod P
- Inverse of 60 is 237 mod P
- Inverse of 120 is 239 mod P

We could alternatively write the group **NNa24** as follows:

{ 2, 4, 8, 16, 32, 64, (2^7) , (2^8) , (2^9) , (2^{10}) , (2^{11}) , -1, -2, -4, -8, -16, -32, -64, $-(2^7)$, $-(2^8)$, $-(2^9)$, $-(2^{10})$, $-(2^{11})$, 1 }

From $t=5$ the 30 elements in **NNa30** are as shown next

{ 2, 4, 8, 16, 32, 64, 128, 256, 512, 31, 62, 124, 248, 496, -1, 991, 989, 985, 977, 961, 929, 865, 737, 481, 962, 931, 869, 745, 497, 1 }

From $t=6$ the 36 elements in **NNa36** are as shown next

{ 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024,
2048, 63, 126, 252, 504, 1008, 2016, -1, 4031, 4029,
4025, 4017, 4001, 3969, 3905, 3777, 3521, 3009, 1985, 3970,
2907, 3781, 3529, 3025, 2017, 1 }

From t=7 the 42 elements in **NNa42** are as shown next.

{ 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024,
2048, 4096, 8192, 127, 254, 508, 1016, 2032, 4064, 8128,
-1, 16255, 16253, 16249, 16241, 16225, 16193, 16129, 16001, 15745,
15233, 14209, 12161, 8065, 16130, 16003, 15749, 15241, 14225, 12193,
8129, 1 }

From t=8 the 48 elements in **NNa48** are as shown next.

{ 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024,
2048, 4096, 8192, 16384, 32768, 255, 510, 1020, 2040, 4080,
8160, 16320, 32640, -1, 65279, 65277, 65273, 65265, 65249, 65217,
65153, 65025, 64769, 64257, 63233, 57089, 48897, 32513, 65026,
64771, 64261, 63241, 61201, 57121, 48961, 32641, 1 }

From t=9 the 54 elements in **NNa54** are as shown next.

{ 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024,
2048, 4096, 8192, 16384, 32768, 65536, 131072, 511, 1022, 2044,
4088, 8176, 16352, 32704, 65408, 130816, -1, 261631, 261629, 261625,
261617, 261601, 261569, 261505, 261377, 261121, 260609, 259585, 257537, 253441,
245249, 228865, 196097, 130561, 261122, 260611, 259589, 257545, 253457, 245281,
228929, 196225, 130817, 1 }

From t=10 the 60 elements in **NNa60** are as shown next.

{ 2, 4, 8, 16, 32, 64, 128, 256,
512, 1024, 2048, 4096, 8192, 16384, 32768, 65536,
131072, 262144, 524288, 1023, 2046, 4092, 8184, 16368,
32736, 65472, 130944, 261888, 523776, -1, 1047551, 1047549,
1047545, 1047537, 1047521, 1047489, 1047425, 1047297, 1047041, 1046529,
1045505, 1043457, 1039361, 1031169, 1014785, 982017, 916481, 785409,
523265, 1046530, 1045507, 1043461, 1039369, 1031185, 1014817, 982081,
916609, 785665, 523777, 1 }

For t=11 the 66 elements in **NNa66** are not tabulated here

For t=12 the 72 elements in **NNa72** are not tabulated here

For t=13 the 78 elements in **NNa78** are not tabulated here

For t=14 the 84 elements in **NNa84** are not tabulated here

For t=15 the 90 elements in **NNa90** are not tabulated here

For t=16 the 96 elements in **NNa96** are not tabulated here

For t=17 the 102 elements in **NNa102** are not tabulated here

For t=18 the 108 elements in **NNa108** are not tabulated here

For t=19 the 114 elements in **NNa114** are not tabulated here

For t=20 the 120 elements in **NNa120** are not tabulated here

Using sturdy element notation we might say the results tabulated in this document are

$\langle\langle 2 \rangle\rangle$ for set $1 + (-1 + 2^t) \times 2^t$ for t=3,4,5,6,7,8,9,10

Chapter 12 – Sturdy element 2 and set $1+(1+2^t)\times 2^t$

Consider the space $1+(1+2^t)\times 2^t$

We will be using generating element 2

The [sub]groups generated by 2 have low order [a lot lower than $n-1$]

Tabulating the elements of groups generated by 2 next.

Using the prefix NPb to avoid clashing with existing letter conventions for groups.
Prefer G or S? Replace them in your local copy.

Conjecture: Order of 2 mod N when N of the form $1+(1+2^t)\times 2^t$ is $3\times t$

When $t=3$ we have $P=1+9\times 8$ and the set of elements modulo P is a multiplicative group.

The subgroup generated by 2 has 9 elements

The elements in **NPb9** are as shown next

$\{ 2, 4, 8, 16, 32, 64, 55, 37, 1 \}$

If **NPb9** is really a group then we need inverses so let us document those next.

- Inverse of 2 is 37 mod P
- Inverse of 4 is 55 mod P
- Inverse of 8 is 64 mod P
- Inverse of 16 is 32 mod P

From 273 for $t=4$ the 12 elements in **NPb12** are as shown next

$\{ 2, 4, 8, 16, 32, 64, 128, 256, 239, 205, 137, 1 \}$

From 1057 for $t=5$ the 15 elements in **NPb15** are as shown next

$\{ 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 991, 925, 793, 529, 1 \}$

From 4161 for $t=6$ the 18 elements in **NPb18** are as shown next

$\{ 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 4031, 3901, 3641, 3121, 2081, 1 \}$

From 16513 for $t=7$ the 21 elements in **NPb21** are as shown next

$\{ 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384, 16255, 15997, 15481, 14449, 12385, 8257, 1 \}$

From 65793 for $t=8$ the 24 elements in **NPb24** are as shown next

$\{ 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536, 65279, 64765, 63737, 61681, 57569, 49345, 32897, 1 \}$

For t=9 the 27 elements in **NPb27** are as shown next

{ 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024,
2048, 4096, 8192, 16384, 32768, 65536, 131072, 262144, 261631, 260605,
258553, 254449, 264241, 229825, 196993, 131329, 1 }

For t=10 the 30 elements in **NPb30** are as shown next

{ 2, 4, 8, 16, 32, 64, 128,
256, 512, 1024, 2048, 4096, 8192,
16384, 32768, 65536, 131072, 262144,
524288, 1048576, 1047551, 1045501, 1041401, 1033201,
1016801, 984001, 918401, 787201, 524801, 1 }

For t=11 the 33 elements in **NPb33** are not tabulated here

For t=12 the 36 elements in **NPb36** are as shown next

{ 2, 4, 8, 16, 32, 64, 128,
256, 512, 1024, 2048, 4096, 8192,
16384, 32768, 65536, 131072, 262144,
524288, 1048576, 2097152, 4194304, 8388608, 16777216,
16773119, 16764925, 16748537, 16715761, 16650209, 16519105,
16256897, 15732481, 14683649, 12585985, 8390657, 1 }

For t=13 the 39 elements in **NPb39** are not tabulated here

For t=14 the 42 elements in **NPb42** are not tabulated here

For t=15 the 45 elements in **NPb45** are not tabulated here

For t=16 the 48 elements in **NPb48** are not tabulated here

For t=17 the 51 elements in **NPb51** are not tabulated here

For t=18 the 54 elements in **NPb54** are not tabulated here

For t=19 the 57 elements in **NPb57** are not tabulated here

For t=20 the 60 elements in **NPb60** are as shown next

{ 2, 4, 8, 16, 32,
64, 128, 256, 512, 1024,
2048, 4096, 8192, 16384, 32768,
65536, 131072, 262144, 524288, 1048576,
2097152, 4194304, 8388608, 16777216, 33554432,
67108864, 134217728, 268435456, 536870912, 1073741824,
2147483648, 4294967296, 8589934592, 17179869184, 34359738368,
68719476736, 137438953472, 274877906944, 549755813888, 1099511627776,
1099510579199, 1099508482045, 1099504287737, 1099495899121, 1099479121889,
1099445567425, 1099378458497, 1099244240641, 1098975804929, 1098438933505,
1097365190657, 1095217704961, 1090922733569, 1082332790785, 1065152905217,
1030793134081, 962073591809, 824634507265, 549756338177, 1 }

Using sturdy element notation we might say the results tabulated in this document are

$\langle\langle 2 \rangle\rangle$ for set $1 + (1 + 2^t) \times 2^t$ for t=3,4,5,6,7,8,9,10,12,20

Chapter 13 – Sturdy element 3 and set $1+(-1+3^t)\times 3^t$

Consider the space $1+(-1+3^t)\times 3^t$

We will be using generating element 3

The [sub]groups generated by 3 have low order [a lot lower than $n-1$]

Tabulating the elements of groups generated by 3 next.

Using the prefix NNe to avoid clashing with existing letter conventions for groups.
Prefer G or S? Replace them in your local copy.

Conjecture: Order of 3 mod N when N of the form $1+(-1+3^t)\times 3^t$ is $6\times t$

When $t=2$ we have $P=1+8\times 9$ and the set of elements modulo P is a multiplicative group.

The subgroup generated by 3 has 12 elements

The elements in **NNe12** are { 3, 9, 27, 8, 24, -1, 70, 64, 46, 65, 49, 1 }

If **NNe12** is really a group then we need inverses so let us document those next.

- Inverse of 3 is 49 mod P
- Inverse of 9 is 65 mod P
- Inverse of 27 is 46 mod P
- Inverse of 8 is 64 mod P
- Inverse of 24 is 70 mod P

We could alternatively write the group **NNe12** as follows:

{ 3, 9, 27, (3^4) , (3^5) , -1,
-3, -9, -27, $-(3^4)$, $-(3^5)$, 1, }

For 703 from $t=3$ the 18 elements in **NNe18** are as shown next

{ 3, 9, 27, 81, 243, 26, 78, 234, -1
700, 694, 676, 622, 460, 677, 625, 469, 1 }

For 6481 from $t=4$ the 24 elements in **NNe24** are as shown next

{ 3, 9, 27, 81, 243, 729, 2187, 80, 240, 720,
2160, -1, 6478, 6472, 6454, 6400, 6238, 5752, 4294, 6401,
6241, 5761, 4321, 1 }

For 58807 from $t=5$ the 30 elements in **NNe30** are as shown next

{ 3, 9, 27, 81, 243, 729,
2187, 6561, 19683, 242, 726, 2178,
6534, 19602, -1, 58804, 58798, 58780,
58726, 58564, 58078, 56620, 52246, 39124,
58565, 58081, 56629, 52273, 39205, 1 }

For 530713 from t=6 the 36 elements in **NNe36** are as shown next

{ 3, 9, 27, 81, 243, 729,
2187, 6561, 19683, 59049, 177147, 728,
2184, 6552, 19656, 58968, 176904, -1,
530710, 530704, 530686, 530632, 530470, 529984,
528526, 524152, 511030, 471664, 353566, 529985,
528529, 524161, 511057, 471745, 353809, 1 }

For 4780783 from t=7 the 42 elements in **NNe42** are as shown next

{ 3, 9, 27, 81, 243, 729,
2187, 6561, 19683, 59049, 177147, 531441,
1594323, 2186, 6558, 19674, 59022, 177066,
531198, 1593594, -1, 4780780, 4780774, 4780756,
4780702, 4780540, 4780054, 4778596, 4774222, 4761100,
4721734, 4603636, 4249342, 3186460, 4778597, 4774225,
4761109, 4721761, 4603717, 4249585, 3187189, 1 }

For t=8 the 48 elements in **NNe48** are not tabulated here

For t=9 the 54 elements in **NNe54** are not tabulated here

For t=10 the 60 elements in **NNe60** are not tabulated here

For t=11 the 66 elements in **NNe66** are not tabulated here

For t=12 the 72 elements in **NNe72** are not tabulated here

For t=13 the 78 elements in **NNe78** are not tabulated here

For t=14 the 84 elements in **NNe84** are not tabulated here

For t=15 the 90 elements in **NNe90** are not tabulated here

For t=16 the 96 elements in **NNe96** are not tabulated here

For t=17 the 102 elements in **NNe102** are not tabulated here

For t=18 the 108 elements in **NNe108** are not tabulated here

For t=19 the 114 elements in **NNe114** are not tabulated here

For t=20 the 120 elements in **NNe120** are not tabulated here

Using sturdy element notation we might say the results tabulated in this document are

$\langle\langle 3 \rangle\rangle$ for set $1 + (-1 + 3^t) \times 3^t$ for t=2,3,4,5,6,7

Chapter 14 – Sturdy element 3 and set $1+(1+3^t)\times 3^t$

Consider the space $1+(1+3^t)\times 3^t$

We will be using generating element 3

The [sub]groups generated by 3 have low order [a lot lower than $n-1$]

Tabulating the elements of groups generated by 3 next.

Using the prefix NPf to avoid clashing with existing letter conventions for groups.

Prefer G or S? Replace them in your local copy.

Conjecture: Order of 3 mod N when N of the form $1+(1+3^t)\times 3^t$ is $3\times t$

When $t=3$ we have $P=1+28\times 27$ and the set of elements modulo P is a multiplicative group.

The subgroup generated by 3 has 9 elements

The elements in **NPf9** are as shown next

{ 3, 9, 27, 81, 243, 729, 673, 505, 1 }

If **NPf9** is really a group then we need inverses so let us document those next.

- Inverse of 3 is 505 mod P
- Inverse of 9 is 673 mod P
- Inverse of 27 is 729 mod P
- Inverse of 81 is 243 mod P

For 6643 from $t=4$ the 12 elements in **NPf12** are as shown next

{ 3, 9, 27, 81, 243, 729,
2187, 6561, 6397, 5905, 4429, 1 }

For 59293 from $t=5$ the 15 elements in **NPf15** are as shown next

{ 3, 9, 27, 81, 243,
729, 2187, 6561, 19683, 59049,
58561, 57097, 52705, 39529, 1 }

For 532171 from $t=6$ the 18 elements in **NPf18** are as shown next

{ 3, 9, 27, 81, 243, 729,
2187, 6561, 19683, 59049, 177147, 531441,
529981, 525601, 512461, 473041, 354781, 1 }

For 4785157 from $t=7$ the 21 elements in **NPf21** are as shown next

{ 3, 9, 27, 81, 243, 729, 2187,
6561, 19683, 59049, 177147, 531441, 1594323, 4782969,
4778593, 4765465, 4726081, 4607929, 4253473, 3190105, 1 }

For 43053283 from t=8 the 24 elements in **NPf24** are as shown next

{ 3, 9, 27, 81, 243, 729,
2187, 6561, 19683, 59049, 177147, 531441,
1594323, 4782969, 14348907, 43046721, 43033597, 42994225,
42876109, 42521761, 41458717, 38269585, 28702189, 1 }

For 387440173 from t=9 the 27 elements in **NPf27** are as shown next

{ 3, 9, 27, 81, 243, 729,
2187, 6561, 19683, 59049, 177147, 531441,
1594323, 4782969, 14348907, 43046721, 129140163, 387420489,
387381121, 387263017, 386908705, 385845769, 382656961, 373090537,
344391265, 258293449, 1 }

For 3486843451 from t=10 the 30 elements in **NPf30** are as shown next

{ 3, 9, 27, 81, 243,
729, 2187, 6561, 19683, 59049,
177147, 531441, 1594323, 4782969, 14348907,
43046721, 129140163, 387420489, 1162261467, 3486784401,
3486666301, 3486312001, 3485249101, 3482060401, 3472494301,
3443796001, 3357701101, 3099416401, 2324562301, 1 }

For 31381236757 from t=11 the 33 elements in **NPf33** are as shown next

{ 3, 9, 27, 81, 243,
729, 2187, 6561, 19683, 59049,
177147, 531441, 1594323, 4782969, 14348907,
43046721, 129140163, 387420489, 1162261467, 3486784401,
10460353203, 31381059609, 31380705313, 31379642425, 31376453761,
31366887769, 31338189793, 31252095865, 30993814081, 30218968729,
27894432673, 20920824505, 1 }

For 282430067923 from t=12 the 36 elements in **NPf36** are as shown next

{ 3, 9, 27, 81, 243, 729, 2187, 6561, 19683, 59049,
177147, 531441, 1594323, 4782969, 14348907,
43046721, 129140163, 387420489, 1162261467, 3486784401,
10460353203, 31381059609, 94143178827, 282429536481, 282428473597,
282425284945, 282415718989, 282387021121, 282300927517, 282042646705,
281267804269, 278943276961, 271969695037, 251048949265, 188286711949,
1 }

For t=13 the 39 elements in **NPf39** are not tabulated here

For t=14 the 42 elements in **NPf42** are not tabulated here

For t=15 the 45 elements in **NPf45** are not tabulated here

For t=16 the 48 elements in **NPf48** are not tabulated here

For t=17 the 51 elements in **NPf51** are not tabulated here

For t=18 the 54 elements in **NPf54** are not tabulated here

For t=19 the 57 elements in **NPf57** are not tabulated here

For t=20 the 60 elements in **NPf60** are not tabulated here

Using sturdy element notation we might say the results tabulated in this document are

$\langle\langle 3 \rangle\rangle$ for set $1 + (1 + 3^t) \times 3^t$ for t=3,4,5,6,7,8,9,10,11,12

Chapter 15 – Sturdy element 5 and set $1+(-1+5^t)\times 5^t$

Consider the space $1+(-1+5^t)\times 5^t$

We will be using generating element 5

The [sub]groups generated by 5 have low order [a lot lower than $n-1$]

Tabulating the elements of groups generated by 5 next.

Using the prefix **NNd** to avoid clashing with existing letter conventions for groups.
Prefer G or S? Replace them in your local copy.

Conjecture: Order of 5 mod N when N of the form $1+(-1+5^t)\times 5^t$ is $6\times t$

When $t=2$ we have $P=1+24\times 25$ and the set of elements modulo P is a multiplicative group.

The subgroup generated by 5 has 12 elements

The elements in **NNd12** are { 5, 25, 125, 24, 120, -1, 596, 576, 476, 577, 481, 1 }

If **NNd12** is really a group then we need inverses so let us document those next.

- Inverse of 5 is 481 mod P
- Inverse of 25 is 577 mod P
- Inverse of 125 is 476 mod P
- Inverse of 24 is 576 mod P
- Inverse of 120 is 596 mod P

We could alternatively write the group **NNd12** as follows:

{ 5, 25, 125, (5^4) , (5^5) , -1,
-5, -25, -125, $-(5^4)$, $-(5^5)$, 1, }

For 15501 from $t=3$ the 18 elements in **NNd18** are as shown next

{ 5, 25, 125, 625, 3125, 124, 620, 3100, -1,
15496, 15476, 15376, 14876, 12376, 15377, 14881, 12401, 1 }

For 390001 from $t=4$ the 24 elements in **NNd24** are as shown next

{ 5, 25, 125, 625, 3125, 15625, 78125, 624,
3120, 15600, 78000, -1, 389996, 389976, 389876, 389376,
386876, 374376, 311876, 389377, 386881, 374401, 312001, 1 }

For 9762501 from $t=5$ the 30 elements in **NNd30** are as shown next

{ 5, 25, 125, 625, 3125, 15625,
78125, 390625, 1953125, 3124, 15620, 78100,
390500, 1952500, -1, 9762496, 9762476, 9762376,
9761876, 9759376, 9746876, 9684376, 9371876, 7809376,
9759377, 9746881, 9684401, 9372001, 7810001, 1 }

For 244125001 from t=6 the 36 elements in **NNd36** are as shown next

{ 5, 25, 125, 625, 3125, 15625,
78125, 390625, 1953125, 9765625, 48828125, 15624,
78120, 390600, 1953000, 9765000, 48825000, **-1**,
244124996, 244124976, 244124876, 244124376, 244121876, 244109376,
244046876, 243734376, 242171876, 234359376, 195296876, 244109377,
244046881, 243734401, 242172001, 234360001, 195300001, 1 }

For 6103437501 from t=7 the 42 elements in **NNd42** are as shown next

{ 5, 25, 125, 625, 3125, 15625,
78125, 390625, 1953125, 9765625, 48828125, 244140625,
1220703125, 78124, 390620, 1953100, 9765500, 48827500,
244137500, 1220687500, **-1**, 6103437496, 6103437476, 6103437376,
6103436876, 6103434376, 6103421876, 6103359376, 6103046876, 6101484376,
6093671876, 6054609376, 5859296876, 4882734376, 6103359377, 6103046881,
6101484401, 6093672001, 6054610001, 5859300001, 4882750001, 1 }

For t=8 the 48 elements in **NNd48** are not tabulated here

For t=9 the 54 elements in **NNd54** are not tabulated here

For t=10 the 60 elements in **NNd60** are not tabulated here

For t=11 the 66 elements in **NNd66** are not tabulated here

For t=12 the 72 elements in **NNd72** are not tabulated here

For t=13 the 78 elements in **NNd78** are not tabulated here

For t=14 the 84 elements in **NNd84** are not tabulated here

For t=15 the 90 elements in **NNd90** are not tabulated here

For t=16 the 96 elements in **NNd96** are not tabulated here

For t=17 the 102 elements in **NNd102** are not tabulated here

For t=18 the 108 elements in **NNd108** are not tabulated here

For t=19 the 114 elements in **NNd114** are not tabulated here

For t=20 the 120 elements in **NNd120** are not tabulated here

Using sturdy element notation we might say the results tabulated in this document are

$\langle\langle 5 \rangle\rangle$ for set $1 + (-1 + 5^t) \times 5^t$ for t=2,3,4,5,6,7

Chapter 16 – Sturdy element 5 and set $1+(1+5^t)\times 5^t$

Consider the space $1+(1+5^t)\times 5^t$

We will be using generating element 5

The [sub]groups generated by 5 have low order [a lot lower than $n-1$]

Tabulating the elements of groups generated by 5 next.

Using the prefix NPh to avoid clashing with existing letter conventions for groups.
Prefer G or S? Replace them in your local copy.

Conjecture: Order of 5 mod N when N of the form $1+(1+5^t)\times 5^t$ is $3\times t$

When $t=1$ we have $P=1+6\times 5$ and the set of elements modulo P is a multiplicative group.

The subgroup generated by 5 has 3 elements

The elements in **NPh3** are { 5, 25, 1 }

If **NPh3** is really a group then we need inverses so let us document those next.

- Inverse of 5 is 25 mod P

For 651 from $t=2$ the 6 elements in **NPh6** are as shown next

{ 5, 25, 125, 625, 521, 1 }

For 15751 from $t=3$ the 9 elements in **NPh9** are as shown next

{ 5, 25, 125, 625, 3125, 15625, 15121, 12601, 1 }

For 391251 from $t=4$ the 12 elements in **NPh12** are as shown next

{ 5, 25, 125, 625, 3125, 15625,
78125, 390625, 388121, 375601, 313001, 1 }

For 9768751 from $t=5$ the 15 elements in **NPh15** are as shown next

{ 5, 25, 125, 625, 3125, 15625,
78125, 390625, 1953125, 9765625, 9753121, 9690601,
9378001, 7815001, 1 }

For 244156251 from $t=6$ the 18 elements in **NPh18** are as shown next

{ 5, 25, 125, 625, 3125, 15625,
78125, 390625, 1953125, 9765625, 48828125, 244140625,
244078121, 243765601, 242203001, 234390001, 195325001, 1 }

For 6103593751 from $t=7$ the 21 elements in **NPh21** are as shown next

{ 5, 25, 125, 625, 3125, 15625,
78125, 390625, 1953125, 9765625, 48828125, 244140625,
1220703125, 6103515625, 6103203121, 6101640601, 6093828001, 6054765001,
5859450001, 4882875001, 1 }

For 152588281251 from $t=8$ the 24 elements in **NPh24** are as shown next

{ 5, 25, 125, 625, 3125,
15625, 78125, 390625, 1953125, 9765625,
48828125, 244140625, 1220703125, 6103515625, 30517578125,
152587890625, 152586328121, 152578515601, 152539453001, 152344140001,
151367575001, 146484750001, 122070625001, 1 }

For $t=9$ the 27 elements in **NPh27** are not tabulated here

For $t=10$ the 30 elements in **NPh30** are not tabulated here

For $t=11$ the 33 elements in **NPh33** are not tabulated here

For $t=12$ the 36 elements in **NPh36** are not tabulated here

For $t=13$ the 39 elements in **NPh39** are not tabulated here

For $t=14$ the 42 elements in **NPh42** are not tabulated here

For $t=15$ the 45 elements in **NPh45** are not tabulated here

For $t=16$ the 48 elements in **NPh48** are not tabulated here

For $t=17$ the 51 elements in **NPh51** are not tabulated here

For $t=18$ the 54 elements in **NPh54** are not tabulated here

For $t=19$ the 57 elements in **NPh57** are not tabulated here

For $t=20$ the 60 elements in **NPh60** are not tabulated here

Using sturdy element notation we might say the results tabulated in this document are

$\langle\langle 5 \rangle\rangle$ for set $1 + (1 + 5^t) \times 5^t$ for $t=2,3,4,5,6,7,8$

Chapter 17 – Sturdy element 2^4 in set

$$1 + (-1 + 2^t) \times (2^{t+1})$$

Consider the Proth space $1 + (-1 + 2^t) \times (2^{t+1})$

We will be using generating element 2^4

The [sub]groups generated by 2^4 have order lower than $n-1$

Tabulating the elements of groups generated by 2^4 next.

Using the prefix TNj to avoid clashing with existing letter conventions for groups.
Prefer G or S? Replace them in your local copy.

From $t=1$ the 913 elements in **TNj913** are as shown next

(16, 256, 255, 239, 3824, 3569, 3330, 3347, 3619, 289
783, 1005, 716, 3774, 2769, 2053, 2120, 3192, 1139, 2860,
...
47, 752, 509, 462, 3551, 3042, 2580, 2870, 3669, 1089,
2060, 2232, 1143, 2924, 692, 3390, 466, 3615, 225, 3600,
3826, 3601, 1 }

If **TNj913** is really a group then we need inverses so let us document those next.

- Inverse of 16 is 3601 mod P
 - Inverse of 256 is 3826 mod P
 - Inverse of 255 is 3600 mod P
 - Inverse of 239 is 225 mod P
 - Inverse of 3824 is 3615 mod P
 - Inverse of 3569 is 466 mod P
 - Inverse of 3330 is 3390 mod P
 - Inverse of 3347 is 692 mod P
 - Inverse of 3619 is 2924 mod P
 - Inverse of 289 is 1143 mod P
 - Inverse of 783 is 2232 mod P
 - Inverse of 1005 is 2060 mod P
 - Inverse of 716 is 1089 mod P
 - Inverse of 3774 is 3669 mod P
 - Inverse of 2769 is 2870 mod P
 - Inverse of 2053 is 2580 mod P
 - Inverse of 2120 is 3042 mod P
 - Inverse of 3192 is 3551 mod P
 - Inverse of 1139 is 462 mod P
 - Inverse of 2860 is 509 mod P
- $\backslash 509 == \text{Mod}((2^{80}), 3841)^{-1}$

This group can be considered a sort of intersection group in that the first so many group elements also appear in $\langle \langle -1 + 2^t \rangle \rangle$ for set $1 + (-1 + 2^t) \times (2^{t+1})$

Using sturdy element notation we might say the results tabulated in this document are

$$\langle\langle 2^4\rangle\rangle \text{ for set } 1+(-1+2^t)\times(2^{t+1}) \text{ for } t=1$$

For t=2 the 31395 elements in **TNj31395** are not tabulated here
For t=3 the 516096 elements in **TNj516096** are not tabulated here
For t=4 the 2863267840 elements in **TNj2863267840** are not tabulated here
For t=5 the 879604268045 elements in **TNj879604268045** are not tabulated here
For t=6 the elements in **TNj1563741107235** are not tabulated here
For t=7 the elements in **TNj6004239801465717** are not tabulated here
For t=8 the elements in **TNj296546931945918360** are not tabulated here
For t=9 the elements in **TNj752819693853576159547** are not tabulated here
For t=10 the elements in **TNj1196152061292125583555** are not tabulated here

Chapter 18 – Sturdy element 2^4 in set $1+(1+2^t)\times(2^{t+1})$

Consider the Proth space $1+(1+2^t)\times(2^{t+1})$

We will be using generating element 2^4

The [sub]groups generated by 2^4 have order lower than $n-1$

Tabulating the elements of groups generated by 2^4 next.

Using the prefix TPk to avoid clashing with existing letter conventions for groups.
Prefer G or S? Replace them in your local copy.

From $t=1$ the 725 elements in **TPk725** are as shown next

(16, 256, 4096, 241, 3856, 754, 3358, 1492, 2107, 3241,
3973, 2626, 2839, 1894, 4186, 1681, 778, 3742, 3283, 292,
...
3385, 1924, 313, 655, 1774, 2266, 1432, 1147, 940, 1981,
1225, 2188, 184, 2944, 3574, 595, 814, 4318, 3793, 4099,
289, 271, 4336, 4081, 1 }

If **TPk725** is really a group then we need inverses so let us document those next.

- Inverse of 16 is 4081 mod P
- Inverse of 256 is 4336 mod P
- Inverse of 4096 is 271 mod P
- Inverse of 241 is 289 mod P
- Inverse of 3856 is 4099 mod P
- Inverse of 754 is 3793 mod P
- Inverse of 3358 is 4318 mod P
- Inverse of 1492 is 814 mod P
- Inverse of 2107 is 595 mod P
- Inverse of 3241 is 3574 mod P
- Inverse of 3973 is 2944 mod P
- Inverse of 2626 is 184 mod P
- Inverse of 2839 is 2188 mod P
- Inverse of 1894 is 1225 mod P
- Inverse of 4186 is 1981 mod P
- Inverse of 1681 is 940 mod P
- Inverse of 778 is 1147 mod P
- Inverse of 3742 is 1432 mod P
- Inverse of 3283 is 2266 mod P
- Inverse of 292 is 1774 mod P

$$\backslash \backslash 1774 == \text{Mod}((2^80), 4353)^{-1}$$

This group can be considered a sort of intersection group in that the first so many group elements also appear in $\langle\langle 1+2^t \rangle\rangle$ for set $1+(1+2^t)\times(2^{t+1})$

Using sturdy element notation we might say the results tabulated in this document are $\langle\langle 2^4 \rangle\rangle$ for set $1+(1+2^t)\times(2^{t+1})$ for $t=1$

For t=2 the 175445 elements in **TPk175445** are not tabulated here
For t=3 the 44750165 elements in **TPk44750165** are not tabulated here
For t=4 the 260305020 elements in **TPk260305020** are not tabulated here
For t=5 the 4442475460 elements in **TPk4442475460** are not tabulated here
For t=6 the elements in **TPk187583588638745** are not tabulated here
For t=7 the elements in **TPk122266184687010** are not tabulated here
For t=8 the elements in **TPk49191317541345383765** are not tabulated here
For t=9 the elements in **TPk210444133885212645** are not tabulated here
For t=10 the elements in **TPk7198009101644858676245** are not tabulated here

Chapter 19 – Sturdy element 3^6 in set

$$1 + (-1 + 3^t) \times (3^{t+1})$$

Consider the Proth space $1 + (-1 + 3^t) \times (3^{t+1})$

We will be using generating element 3^6

The [sub]groups generated by 3^6 have order lower than $n-1$

Tabulating the elements of groups generated by 3^6 next.

Using the prefix ENI to avoid clashing with existing letter conventions for groups.
Prefer G or S? Replace them in your local copy.

From $t=1$ the 700535 elements in **ENI700535** are as shown next

(729, 531441, 531440, 530711, 386888319, 386356879,
385826168, 385826898, 386359068, 532900, 1595051, 2125032,
...
8482665, 380527050, 4771317, 383177701, 2650651, 384768383,
1590682, 385829080, 1060697, 386359064,
529984, 386358336, 386888321, 386358337, 1 }

If **ENI700535** is really a group then we need inverses so let us document those next.

- Inverse of 729 is 386358337 mod P
- Inverse of 531441 is 386888321 mod P
- Inverse of 531440 is 386358336 mod P
- Inverse of 530711 is 529984 mod P
- Inverse of 386888319 is 386359064 mod P
- Inverse of 386356879 is 1060697 mod P
- Inverse of 385826168 is 385829080 mod P
- Inverse of 385826898 is 1590682 mod P
- Inverse of 386359068 is 384768383 mod P
- Inverse of 532900 is 2650651 mod P
- Inverse of 1595051 is 383177701 mod P
- Inverse of 2125032 is 4771317 mod P \ \ 4771317==Mod((3^72),386889049)^-1

This group can be considered a sort of intersection group in that the first so many group elements also appear in $\langle \langle -1 + 3^t \rangle \rangle$ for set $1 + (-1 + 3^t) \times (3^{t+1})$

Using sturdy element notation we might say the results tabulated in this document are

$$\langle \langle 3^6 \rangle \rangle \text{ for set } 1 + (-1 + 3^t) \times (3^{t+1}) \text{ for } t=1$$

For t=2 the 51471794373481 elements in **ENI51471794373481** are not tabulated here

For t=3 the 2176380868150248 elements in **ENI2176380868150248** are not tabulated here

For t=4 the elements in **ENI3607817647748386329405865** are not tabulated here

For t=5 the elements in **ENI17883727159311165957331633472** are not tabulated here

For t=6 **ENI68430013617752741820051994454987067** is not tabulated here

For t=7 **ENI181707258973221807091901987412589460453225** is not tabulated here

For t=8 **ENI1159599421646749661461790540529837038823116734321** is not tabulated here

For t=9 **ENI49122068395903519082509051092628313045079453473823655** is not tabulated here

For t=10 **ENI122937343416764879794294217425047880764053692573181368234** is not tabulated here

Chapter 20 – Sturdy element 3^6 in set $1+(1+3^t)\times(3^{t+1})$

Consider the Proth space $1+(1+3^t)\times(3^{t+1})$

We will be using generating element 3^6

The [sub]groups generated by 3^6 have order lower than $n-1$

Tabulating the elements of groups generated by 3^6 next.

Using the prefix EPM to avoid clashing with existing letter conventions for groups.
Prefer G or S? Replace them in your local copy.

From $t=1$ the 5386126 elements in **EPM5386126** are as shown next

(729, 531441, 387420489, 530713, 386889777, 1593596,
385827622, 3186463, 383171872, 6904368, 377861100, 14870890,
...
383165329, 2134521, 4258085, 528517, 385288893, 386356884,
1066530, 1596508, 387950470, 386886862,
387420492, 532900, 532169, 387951201, 387419761, 1 }

If **EPM5386126** is really a group then we need inverses so let us document those next.

- Inverse of 729 is 387419761 mod P
- Inverse of 531441 is 387951201 mod P
- Inverse of 387420489 is 532169 mod P
- Inverse of 530713 is 532900 mod P
- Inverse of 386889777 is 387420492 mod P
- Inverse of 1593596 is 386886862 mod P
- Inverse of 385827622 is 387950470 mod P
- Inverse of 3186463 is 1596508, mod P
- Inverse of 383171872 is 1066530 mod P
- Inverse of 6904368 is 386356884 mod P
- Inverse of 377861100 is 385288893 mod P
- Inverse of 14870890 is 528517 mod P $\setminus 528517 == \text{Mod}((3^72), 387951931)^{-1}$

This group can be considered a sort of intersection group in that the first so many group elements also appear in $\langle\langle 1+3^t \rangle\rangle$ for set $1+(1+3^t)\times(3^{t+1})$

Using sturdy element notation we might say the results tabulated in this document are

$\langle\langle 3^6 \rangle\rangle$ for set $1+(1+3^t)\times(3^{t+1})$ for $t=1$

For t=2 the 189368764575 elements in **EPm189368764575** are not tabulated here

For t=3 the 1507545917798102 elements in **EPm1507545917798102** are not tabulated here

For t=4 the elements in **EPm806220813676060322261530** are not tabulated here

For t=5 the elements in **EPm143002068656319880828367052247** are not tabulated here

For t=6 **EPm4429127095000177394859605604527083** is not tabulated here

For t=7 **EPm29280455314283959475068482357591163365** is not tabulated here

For t=8 **EPm21473741659833750070095442629055780111082474875** is not tabulated here

For t=9 **EPm188691222598784991721868041563740633590000013880** is not tabulated here

For t=10 **EPm6005674821512041823019868864371284407630415986849347390051** is not tabulated here

Chapter 21 Other Conjectures in Group/Number theory

Conjecture: Factors of N when t is prime and N of the form $1+(-1+2^t)*(2^{t+1})$ and $1+2^t$ is prime must be either 5 or of the form $1+4*k*(1+2^t)$ where k is a positive integer

Example for $t=11$ $pr=8384513$ we have the factors 277 and 30269 where $1+2^t$ is 23

$$277=1+4*3*23$$

$$30269=1+4*7*47*23$$

$$8384513==277*30269$$

Conjecture: For P of the form $1+(-1+2^t)\times 2^{t+3}$ where t is a positive integer, when $\frac{p-1}{2^4} \equiv -1 \pmod{p}$ then P is prime.

Conjecture: Order of $b \pmod{N}$ when N of the form $1+(-1+b^t)\times b^t$ is $6\times t$ where b and t are positive integers ≥ 2

Conjecture: Order of $b \pmod{N}$ when N of the form $1+(1+b^t)\times b^t$ is $3\times t$ where b and t are positive integers ≥ 2

Conjecture: There are an infinite number of cyclic groups having finite order.

The previous chapters provides an abundant source of cyclic groups.

Chapter 22 – Analysis of output from rho(u,v,x)

In this chapter we will focus on $u=5467$ case and introduce the 3 variable function $\rho_{11}(u,v,x)$

The $\rho_{11}()$ here is one instance of what is likely to be several classes of similar 3 variable function.

In this paper we limit things to just $\rho_{11}()$ and from here forward refer to it as just $\rho()$

The output from $\rho(u,v,x)$ is a count of steps until finished, but behind the scenes during our analysis we record the values of each result of the mod [after dividing it by 11] and store in `divided_list`

That `divided_list` may be just a single entry as in the example shown next:

- $1 == \rho(5467, 479, 100)$ `divided_list = [363]`

Some examples of x values that produce $2 == \rho()$ \\ two

- $2 == \rho(5467, 479, 105)$ `divided_list [453, 11]`
- $2 == \rho(5467, 479, 112)$ `divided_list [100, 363]`
- $2 == \rho(5467, 479, 125)$ `divided_list [334, 264]`

Some examples of x values that produce $3 == \rho()$ \\ three

- $3 == \rho(5467, 479, 432)$ `divided_list [112, 100, 363]`
- $3 == \rho(5467, 479, 911)$ `divided_list [112, 100, 363]`

Typically when running the algorithm to tabulate stepcount results [and divided list] we decide a maximum for (i) x ... the input number (ii) maximum result

Usually I choose these the same and use a limit approx that is twice v or a convenient power of 10 or both. In results I have already tabulated, I used 1000 for that maximum (i and ii)

Stop conditions for the function algorithm are:

- Result of the modding is divisible by 11^2
- Result of the modding after 11 division is $>$ maximum (ii)
- [optional] Result of the modding after 11 division is a value already in `divided_list`

Here we define the lower level function $\Delta(u,v,x)$ which gives `divided_list` as output

How does this help us with $\rho()$? ... $\rho() = \text{length}(\Delta(u,v,x))$

Algorithm pseudo code for $\Delta(u,v,x)$

DELTA(u, v, x)

INPUT: An integer x in the range $1..(v-1)$

OUTPUT: A non-empty List of integers in the range $1..(v-1)$

Set L to be an empty list

Set d to be same integer value as x

repeat

 Modded = $(d * u) \% (11 * v)$

 d = Modded/11

 Append d to the list L

until $d \% 11 = 0$

return L

Next we show the $\Delta()$ function where u is fixed at 5467 and v is fixed as 479 for illustration

DELTA(5467, 479, x)

INPUT: An integer x in the range 1..478

OUTPUT: A non-empty List of integers in the range 1..478

Set L to be an empty list

Set d to be same integer value as x

repeat

 Modded = (d*5467)%(11*479)

 d = Modded/11

 Append d to the list L

until d%11 = 0

return L

Example output for $\Delta()$ and $\rho()$ for input x=378

$\Delta(5467,479,378)$ gives divided_list=[98, 327, 138, 89, 165]

$\rho(5467,479,378)$ is 5

Maximum value for $\rho()$

The maximum value for $\rho(5467,479,x)$ is 56

Currently I iterate all input x to obtain that maximum. It may be there are less labour intensive ways of calculating it.

Maximum value for $\rho()$ - why must there be a maximum?

There is exclusivity at play in the divided_list output of the $\rho()$ function.

On the final page we have divided_list tabulated for x={456,935,382,841}

Our observations are based on that very limited tabulation

Factors produce an exclusivity behaviour

Example $382=2*191$. Look at the values in divided_list tabulated on the final page.

There is no overlap in the entries of divided_list for x=381,x=2,x=191

In this early analysis I just think of this as a partition of an integer set

We throw in 479 or 1000 input values [of x] and $\rho()$ partitions our number set in to subsets.

Where the input values are composite, there are no overlapping entries in the output from `divided_list(composite)` and `divided_list(factor1 of composite)+divided_list(factor1 of composite)`

Returning to the question of maximum entries $p()$ - why must there be a maximum
Because of the exclusivity and partitioning behaviour in rough terms we might suggest:

- Small primes tend to short lists of elements
- Large numbers [prime or composite] tend to longer lists
- Because of the above and the limited input range, by combinatorics there will be a maximum number of elements for all input values to $p(1..478)$ and $p(1..1000)$

More tabulations required to verify that the exclusivity I suggest is a rule for this $p(5467,479,x)$ case. These tabulations have been completed but have not been examined in detail to support this assertion of exclusivity.

Distribution of $p() = \text{length}(\text{divided_list})$ for inputs $x==1..478$

Value of $p()$	Number of x values having this result
1	43
2	38
3	32
4	31
5	28
6	25
7	25
8	23
9	21
10	18
11	13
12	10
13	9
14	8
15	8
16	7
17	6
18	6
19	6
20	6
21	6
22	6
23	5
24	5

Value of $p()$	Number of x values having this result
25	5
26	5
27	5
28	5
29	5
30	4
31	4
32	4
33	4
34	4
35	4
36	3
37	3
38	3
39	3
40	3
41	3
42	3
43	3
44	3
45	2
46	2
47	2
48	2
49	2 (x=351, 418
50	1 (x=259
51	1 (x=41
52	1 (x=295
53	1 (x=43
54	1 (x=508
55	1 (x=454
56	1 (x=451
Sum() of number of x values ->	478

478==1+1+1+1+1+1+1+2+2+2+2+2+3+3+3+3+3+3+3+3+3+4+4+4+4+4+4+5+5+5+5+5+5+5+6+6+6+6+6+6+6+7+8+8+9+10+13+18+21+23+25+25+28+31+32+38+43

Reducing the addition a little above we might instead summarise the total as ...

- $478 = 7 + 10 + 27 + 24 + 35 + 36 + 7 + 16 + 9 + 10 + 13 + 18 + 21 + 23 + 50 + 28 + 31 + 32 + 38 + 43$

Looking at set partitioning another way – The tau function $\tau(u,v,y)$:

Here I do not define the function in pseudo code, but instead describe its properties

From a complete iteration of $\rho(u,v,x)$, we say $\tau(u,v,y)$ is the set of integer x that produce a divided_list ending in $11*y$.

(Here we are using fixed 11 scalar as our $\rho()$ in this paper is always $\rho_{11}()$ as described in opening paragraphs.)

Tabulation of $\tau(5467,479,y)$ for $y=1..43$:

Because $43 = 479 \setminus 11$ we need go no higher than $y=43$

y	$\tau(5467,479,y)$ [ordered]	# int in $\tau()$	$\tau(5467,479,y)$ [ordered by steps]
1	105,121,262,405,453	5	453,105,405,262,121
2	45,210,242,331,427	5	427,210,331,45,242
3	257,307,315,363,401	5	401,315,257,307,363
4	5,32,55,90,97,183,293,309,375,420	10	375,420,183,90,5,293,309,97,32,55
5	46,109,349,352	4	349,46,109,352
6	35,135,151,200,224,247,323,385	8	323,151,35,135,247,200,224,385
7	297	1	297
8	10,64,107,110,139,180,194,271,361,366	10	271,361,366,180,10,107,139,194,64,110
9	4,44,72,131,245,292,300,313,336,338,343,365,426,442,466	15	245,466,292,442,131,300,336,338,72,4,426,343,365,313,44
10	3,14,54,80,92,154,218,219,225,252,377	11	219,92,218,225,252,14,54,3,80,377,154
11	8,88,144,147,193,197,207,251,373	9	193,197,144,8,373,207,251,147,88
12	15,70,96,165,167,270,291,302,400,448	10	167,302,70,270,15,400,448,291,96,165
13	141,407	2	141,407
14	33,115	2	115,33
15	21,81,89,98,120,138,231,326,327,378	11	89,138,327,98,378,21,81,244,120,326,231
16	63,243,253	3	63,243,253
17	37,143,179,348	4	37,348,179,143
18	198	1	198
19	31,79,188,314,341,383,390,464	8	464,79,31,188,383,314,390,341
20	6,25,28,108,160,184,275,436,438,450	10	438,184,436,450,25,28,108,6,160,275
21	2,36,146,150,168,169,213,221,233,289,305,362,396,411,412,422	16	412,289,362,146,221,305,150,168,169,36,2,213,411,422,396
22	16,23,176,267,288,294,386,394,414	9	386,394,288,16,267,414,23,294,176
23	20,128,214,220,278,360,388	7	360,20,214,278,388,128,220

y	$\tau(5467,479,y)$ [ordered]	# int in $\tau()$	$\tau(5467,479,y)$ [ordered by steps]
24	30,61,103,125,140,192,321,330,334,417	10	334,125,140,61,30,321,417,103,192,330
25	275	1	275
26	38,47,78,102,106,113,116,118,145,164,172,205,208,215,222,227,228,254,260,261,272,282,285,299,318,325,332,335,337,339,340,354,364,367,369,372,379,387,391,399,415,418,425,446,455,465,469,471,476	49	282,335,471,106,272,228,332,391,208,118,113,299,469,372,340,285,415,369,260,387,261,254,227,465,425,476,399,102,325,364,446,78,164,222,172,116,379,367,47,455,318,337,205,38,215,145,354,339,418
27	256,440	2	256,440
28	66,230	2	230,66
29	26,34,76,87,94,95,123,124,129,133,155,156,157,171,195,199,204,229,232,249,255,268,273,279,281,290,298,316,328,344,357,374,395,404,406,410,413,419,430,431,444,461,468,478	44	204,171,249,413,156,328,444,344,232,279,255,94,431,157,195,410,76,430,290,229,199,357,419,316,124,273,95,298,123,406,129,87,404,395,155,461,478,133,34,268,281,468,26,374
30	9,42,162,173,175,178,196,240,276,277,462	11	178,276,175,196,277,42,162,9,240,173,462
31	29,41,43,52,57,65,67,68,83,85,91,93,101,117,119,148,152,153,174,185,190,191,201,212,226,235,236,237,246,248,258,259,265,266,269,295,303,310,311,329,333,351,359,381,398,416,434,443,451,454,456,457,458,459,463,477	56	152,381,101,458,398,235,359,153,248,67,190,117,246,333,258,174,329,311,310,443,477,266,68,57,83,457,52,269,148,434,237,93,85,191,463,212,65,456,185,303,416,236,226,119,459,265,201,91,351,259,41,295,43,29,454,451
32	7,27,40,77,126,241,428	7	126,7,27,241,40,428,77
33	24,100,112,142,161,264,274,432,441	9	100,112,432,24,161,142,274,441,264
34	74,217,286,358	4	74,217,358,286
35	1,18,48,49,60,69,73,75,84,122,163,181,189,198,206,211,250,280,284,322,324,346,350,355,356,384,392,403,445	29	48,322,284,69,403,49,189,250,280,122,60,163,355,206,384,181,356,73,350,392,75,84,324,18,1,346,445,211,198
36	396	1	396
37	39,51,53,58,59,82,86,104,111,114,127,130,136,166,170,182,186,223,238,296,353,370,382,389,402,424,429,433,435,439,447,452,472,474,475	35	475,53,136,114,166,435,104,59,296,389,474,186,170,382,447,424,130,433,370,127,353,472,452,238,439,51,402,182,223,39,82,111,86,58,429
38	13,17,62,134,149,158,187,202,203,234,239,283,287,301,304,306,317,376,380,437,449,470	22	449,158,62,376,287,149,301,203,304,283,202,437,317,470,239,306,17,134,380,234,13,187
39	19,159,177,209,263,312,342,347,408,409,423,467	12	423,263,467,159,408,342,19,347,312,177,409,209
40	12,50,56,71,132,137,216,368,393,397,421,460	13	397,368,393,421,50,56,216,12,320,71,137,460,132
41	371,473	2	371,473
42	99,345	2	345,99
43	319	1	319

478==5+5+5+10+4+8+1+10+15+11+9+10+2+2+11+3+4+1+8+10+16+9+7+10+1+49+2+2+44+11+**56**+7+9+4+29+1+35+22+12+13+2+2+1

478==1*5+2*6+3*1+4*3+5*3+10+8+10+15+11+9+10+11+8+10+16+9+7+10+49+44+11+56+7+9+29+35+22+12+13

478==1*5+2*6+3*1+4*3+5*3+7*2+8*2+9*3+10*5+11*3+15+16+49+44+56+29+35+22+12+13

The inverse of $\tau(5467,479,y)$ for $y=1..43$ gives you a Surjective map onto $1..43$

Supposing we defined that inverse in a program as `tauinv()` and it was designed to [surjective] map $1..478$ onto $1..43$

How might that work for say $x=473$?

If we define δ (uppercase) as the divided_list underpinning $\rho()$, and perhaps δ (lowercase) as the final element of the divided_list for a given x , then ...

- $\rho(,473)$ gives 2
- $\Delta(,473)$ gives [371,451]
- $\delta(,473)$ gives 451

The value we seek `tauinv()` can be obtained as $(1/11)$ of $\delta(,473)$

- $41==(1/11)*\delta(5467,479,473)$

To clarify the ranges for the different functions we have illustrated above:

- $\rho()$ produces a value in the range $1..56$
- $(1/11)$ of $\delta()$ produces a value in the range $1..43$

Implementing a Surjective map onto the range $1..43$ in an existing program that already implements $\rho()$, could be done using one of the following options:

- Implement $\Delta()$ and change $\rho()$ to be a count of the new $\Delta()$ function output
- Create an inner function / class for $\rho()$ and retain the final value of divided_list

An additional injective mapping function ϵ might be defined that returns the smallest integer whose divided_list contains the input z

This would be computationally intensive as we need to generate and iterate lots of divided_lists to support that Injective map at run time.

Chapter 23 – Probable prime hunting with Pari

On the second page I give a guide to the filters that are included in the code below.

```
b2(tee) = { \
  dp=1+2*tee; \
  mc2=2*dp; \
  t1=1+tee; \
  b=2 ; \
  \\ ordb=2*b*dp \
  lead=(-1+b^tee); \
  \\ next is nmo/2
  nmo2=lead*(b^tee); \
  pr=1+2*nmo2; \
  kra=kronecker(-1+2^(5*tee),pr); \
  krb=kronecker(-1+2^(3+5*tee),pr); \
  krc=kronecker(-1+2^(4+tee),pr); \
  krd=kronecker(1+2^(4+tee),pr); \
  kre=kronecker(-1+2^(2+tee),pr); \
  krf=kronecker(1+2^(2+tee),pr); \
  krj=kronecker(-1+2^(2*t1),pr); \
  krk=kronecker(1+b^(2*(t1)),pr); \
  krp=kronecker(1+b^(t1),pr); \
  krs=kronecker(-1+b^(2+3*tee),pr); \
  krt=kronecker(1+b^tee,pr); \
  kru=kronecker(-1+b^(tee-1),pr); \
  krv=kronecker(1+2^(tee*2),pr); \
  krw=kronecker(1+2^(2*tee),pr); \
  krx=kronecker(1+2^(mc2-2),pr); \
  krz=kronecker(-1+2^(mc2-2),pr); \
  kraa=kronecker(-1+2^(1+3*tee),pr); \
  krab=kronecker(1+2^(1+3*tee),pr); \
  krac=kronecker(-1+2^(3+3*tee),pr); \
  krad=kronecker(1+2^(3+3*tee),pr); \
  kcount=0; \
  if(kra==(-1),kcount++); \
  if(krb==(-1),kcount++); \
  if(krc==(-1),kcount++); \
  if(krd==(-1),kcount++); \
  if(kre==(-1),kcount++); \
  if(krf==(-1),kcount++); \
  if(krj==(-1),kcount++); \
  if(krk==(-1),kcount++); \
  if(krp==(-1),kcount++); \
  if(krs==(-1),kcount++); \
  if(krt==(-1),kcount++); \
  if(kru==(-1),kcount++); \
  if(krv==(-1),kcount++); \
  if(krw==(-1),kcount++); \
  if(krx==(-1),kcount++); \
  if(krz==(-1),kcount++); \
  if(kraa==(-1),kcount++); \
  if(krab==(-1),kcount++); \
  if(krac==(-1),kcount++); \
  if(krad==(-1),kcount++); \
  prim2=0; \
  if(kcount++>=16,prim2=isprime(dp);print("t=",tee," **sixteen**")); \
  if(kcount++>=18,print("t=",tee," ****eighteen****")); \
  modded=0; \
  m3=0; \
  moddp=2; \
  if(prim2>0,moddp=(2*nmo2)%dp); \
```

```

        if(0==moddp, print("t=", tee, " isprime(", dp, ")=", prim2, ". Remainder
nmo%dp=", moddp, ". Testing modded next.."); modded=Mod(lead, pr)^dp); \
        if(-1==modded, m3=Mod(3, pr)^nmo2); \
        if(-1==m3, print("t=", tee, " *ONE* using 3 as halfmaximal witness")); \
        kcount;
    }

starter=125000;
for(k=starter, starter+5001, t1=1+k; \
if(k%2>0, b2(k)); \
);

```

The largest part of the above script is concerned with using the kronecker() function to identify candidates [for probable prime testing] that have -1 for a series of elements

That filtering is based on loose analysis and is very specific to set $1 + (-1 + 2^t) \times (2^{t+1})$

We keep a count of the kronecker -1 results in variable kcount

We reject anything that cannot achieve a kcount of 16 or more.

kronecker() is inexpensive so this filtering costs us very little.

Next filter %dp is based on conjecture that n-1 must be a multiple of $1 + 2^t$

Next filter seeks -1 for $(-1 + 2^t)^{dp}$ which is often the case when n is prime

Next filter uses $3^{((n-1)/2)}$ being -1 as a probable prime indicator

Taken together all of these filters narrow the number space significantly

What is not known is whether any primes of the form $1 + (-1 + 2^t) \times (2^{t+1})$ exist for $t > 1520$.

By searching a narrow number space we are saving effort, but we may be looking for primes that do not exist or missing some by being too narrow in our search.

Chapter 24 – Brave enough?

Perhaps Mathematical Physics folk are brave.

After all they readily argue the case for and against the Einstein-Rosen bridge, even though some may say that Mathematically it is unstable and unobservable.

Being both Physicists and Mathematicians allows them to detach themselves from the Mathematical models and ask questions even though the Mathematics is difficult or non-existent.

Working in Abstract Algebra there are lots of brave people who have done good research.

Much of the important terminology and set theory foundations were laid 1800 to 1920 and are still with us today.

Since 1920 and beyond the advent of computers, Abstract Algebra has been developing as a descriptive system for the integers and real world shapes.

It is not a perfect system, how could it be?

We have in Abstract Algebra a set of Mathematical structures and a whole series of named integer groups on which to conduct [Mathematical] operations.

Is it a goal of Abstract Algebra to map the real world [of integers]?

Is it a goal of Abstract Algebra to map the real world of shapes?

Should we be as brave as the Physicists and consider shapes that are unobservable or tricky to model?

Have we been brave enough [yet] with our naming of integer groups.

Have we stopped considering new models because we believe our maps are very neat or complete for the integers?

Some of this might be the weight of past research in the subject.

Good research is very welcome, it moves the subject forward.

However that research might bring with it a quotable weight that is a challenge to new ideas / maps of collections of integers.

How does asking questions online require bravery?

Do any of those questions receive responses that seem weighed down with the past?

So there may well be some bravery required to ask difficult mathematics questions online.

Chapter 25 – Phases of Mathematics

For the purposes of stimulating debate, I define three phases for Mathematics [of a subject]

1. Analysis and Definition
2. Counting
3. Super Counting

Most subjects spend years in Phase 1. Some will spend decades.

“Analysis and Definition” usually ends when most Mathematicians believe that the subject is well understood, and that, there are complete definitions for all of the important aspects.

“Counting” is when we then become more interested in how many and where.

“Super Counting” is when the subject is not being actively analysed any more, and we are using advanced Statistical Analysis to extract advanced counts and trends. We might be engaged in trying to estimate limits from these results.

There are problems when most Mathematicians believe the “Analysis and Definition” stage is complete and we fully understand everything about the subject, but then later a new definition emerges.

For Group Theory [including subgroups] we have reached the “Super Counting” phase.

However the sturdy element has not been included during the “Analysis and Definition” phase.

Counts cannot be complete

Super Counting is happening already.

Is this a problem and does the problem have a solution?

If the solution is to argue the case for a sturdy element definition?

Chapter 26 – Referencing becomes tricky when large

Providing P is prime, we can refer to a [multiplicative] subgroup easily and in keeping with convention.

Let G be the multiplicative group modulo 390001

Let S be the [multiplicative] subgroup generated by 5.

S has 24 elements as shown next

{ 5, 25, 125, 625, 3125, 15625, 78125, 624,
3120, 15600, 78000, -1, 389996, 389976, 389876, 389376,
386876, 374376, 311876, 389377, 386881, 374401, 312001, 1 }

There are two problems potentially as we look at larger / other examples

1. The first part G can involve some very large numbers – what happens when you reach 12 digits or more?
2. The second part where we talk of subgroups* might be problematic when the modulo is not prime.

*When talking of multiplicative subgroups we are usually doing this in the context of a multiplicative main group.

However when the modulo is composite, there is no group under multiplication from which to subgroup from.

Using sturdy element notation we might refer to the above group instead as

$$\langle\langle 5 \rangle\rangle \text{ for set } 1 + (-1 + 5^t) \times 5^t \text{ for } t=4$$

It really is a matter of preference as to which you consider easier.

For this next 24 element example, we are hitting problem 1 (getting large) and problem 2 (composite N) so will not use a G and S way of navigating.

The 24 element multiplicative group

{ 5, 25, 125, 625, 3125,
15625, 78125, 390625, 1953125, 9765625,
48828125, 244140625, 1220703125, 6103515625, 30517578125,
152587890625, 152586328121, 152578515601, 152539453001, 152344140001,
151367575001, 146484750001, 122070625001, 1 }

can only properly be described (in my opinion) using sturdy element notation as shown next.

$$\langle\langle 5 \rangle\rangle \text{ for set } 1 + (1 + 5^t) \times 5^t \text{ for } t=8$$

Where we to try to talk in modulo terms we would be saying modulo 152588281251 for any attempt to describe a main group G. But we do not have a multiplicative group G?

Chapter 27 – Sure it's structure preserving

An isomorphism is said to be structure preserving

In fact relationships between elements are maintained even if the elements are renamed or reordered

But what if a finite multiplicative cyclic group has a secondary feature?

Allowing both relabelling and reordering means this secondary feature is no longer accessible or usable.

This prevents the mapping being structure preserving.

A truly structure preserving mapping would allow the use of the secondary feature even after reordering and relabelling.

Best illustrated with examples.

Using a generating element of 65 and working modulo 8321 we obtain the 52 element multiplicative group shown next.

{ 65,4225,32,**2080**,2064,1024,8313,7801,7805,8065,
2,**130**,129,64,4160,4128,2048,8305,7281,**7289**,
7809,4,260,258,128,8320,8256,**4096**,8289,6241,
6257,7297,8,520,516,**256**,8319,8191,8192,8257,
4161,4193,6273,**16**,1040,1032,512,**8317**,8061,8063,
8193,1 }

There is a secondary feature in that group that allows us to jump to a portion of our group and be at most 7 elements from the element we require.

Every eighth element after 16 from the end of the group is a power of 2.

In order we would write them as follows

$2^4, 2^8, 2^{12}, 2^{16}, 2^{20}, 2^{24}, 2^{28}, 2^{32}, 2^{36}, 2^{40}$

Writing them longhand we might say

eight from last is 16

sixteenth from last is 2^8

twentyfourth from last is 2^{12}

thirtysecond from last is 2^{16}

fortieth from last is 2^{20}

fortyeighth from last is 2^{24}

The fourth item is in bold in the group listing above and represents $2^{24} \bmod 8321$

Using sturdy element notation we might say the group we tabulated above beginning 65 is

$$\langle\langle 1+2^t \rangle\rangle \text{ for set } 1+(1+2^t)\times(2^{t+1}) \text{ for } t=6$$

Current theory tells us that there exists an isomorphism between this finite abelian cyclic group and Z52.

Such an isomorphism would use both relabelling and reordering.

The problem then becomes how to access the secondary feature?

We are now [after isomorphism] the group Z52 whose elements are:

{ 1,2,3,4,5,6,7,8,9,10,11,12,13,
14,15,16,17,18,19,20,21,22,23,24,25,26,
27,28,29,30,31,32,33,34,35,36,37,38,39,
40,41,42,43,44,45,46,47,48,49,50,51,52 }

By allowing reordering without being specific about tracking each element and how it maps individually, we have no way of locating an element of the secondary feature once in Z52

This prevents us from jumping to a section of the group and navigating a maximum of seven elements from that jump destination.

That secondary feature is part of our original multiplicative cyclic group.

We are unable to use that secondary feature.

Therefore we are not truly structure preserving.

Next a further example.

Using a generating element of 257 and working modulo 131585 we obtain the 68 element multiplicative group shown next.

{ 257, 66049, 128, **32896**, 32832, 16384, 131553, 123361, 123377, 127489,
8, **2056**, 2052, 1024, 131583, 131071, 131072, 131329, 65793, **65921**,
98817, 64, 16448, 16416, 8192, 131569, 127473, **127481**, 129537, 4
1028, 1026, 512, **-1**, 131328, **65536**, 131457, 98689, 98753, 115201,
32, 8224, 8208, **4096**, 131577, 129529, 129533, 130561, 2, 514
513, **256**, 65792, 65664, 32768, 131521, 115137, 115169, 123393, **16**,
4112, 4104, 2048, **131581**, 130557, 130559, 131073, 1 }

Using sturdy element notation we might say the group we tabulated above beginning 257 is

$$\langle\langle 1+2^t \rangle\rangle \text{ for set } 1+(1+2^t)\times(2^{t+1}) \text{ for } t=8$$

Labelling that 68 element multiplicative cyclic group as TPy68.

With a jump or secondary feature similar to our previous example

eight from last is 16

sixteenth from last is 2^8

twentyfourth from last is 2^{12}

thirtysecond from last is 2^{16}

fortieth from last is 2^{20}

fortyeighth from last is 2^{24}

fiftysixth from last is 2^{28}

sixtyfourth from last is 2^{32}

$$\backslash\backslash 32896 == \text{Mod}(2^{32}, 131585)$$

The fourth item is in bold in the group listing above and represents $2^{32} \bmod 131585$.

Current theory tells us that there exists an isomorphism between this finite abelian cyclic group and Z_{68} .

Such an isomorphism would use both relabelling and reordering.

The problem then becomes how to access the secondary feature?

We are now [after isomorphism] the group Z_{68} whose elements are

{ 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,
18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,
35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,
52,53,54,55,56,57,58,59,60,61,62,63,64,65,66,67,68 }

By allowing reordering without being specific about tracking each element and how it maps individually, we have no way of locating an element of the secondary feature once in Z_{68}

This prevents us from jumping to a section of the group and navigating a maximum of seven elements from that jump destination.

That secondary feature is part of our original multiplicative cyclic group TPy_{68} .

We are unable to use that secondary feature.

Therefore we are not truly structure preserving.

If the jump feature is an essential part of the multiplication operation, then you cannot have a structure preserving map.

Do we make a special case for this type of group, or do we modify or qualify current theory?

A question that might be hard to answer is do we in fact have the jump feature in the Z group and just need to add something to the labelling to allow it to operate [again]?

Want to try and highlight in bold the elements in the Z group? Would that be enough?

Chapter 28 – Element 2 and set $1+(-1+2^t)\times(2^{t+3})$

Consider the Proth space $1+(-1+2^t)\times(2^{t+3})$

Conjecture: For P of the form $1+(-1+2^t)\times 2^{t+3}$ where t is a positive integer, when order of 2 modulo P is $(2^{t+2})\times(-1+2^t)$ then P is prime.

Using the above conjecture we have established the following

$$1+(-1+2^{16224})\times(2^{16227}) \text{ is Prime}$$

By tabulating the order of groups next we provide examples where order follows the conjecture and other examples where the Proth number used is composite.

We will be using generating element 2.

When $t=1$ we have $P=1+1\times 16$ and the set of elements modulo P is a multiplicative group.

The subgroup generated by 2 has 8 elements

The elements in **TNz8** are $\{ 2, 4, 8, -1, 15, 13, 9, 1 \}$

If **TNz8** is really a group then we need inverses so let us document those next.

- Inverse of 2 is 9 mod P
- Inverse of 4 is 13 mod P
- Inverse of 8 is 15 mod P

Later we look at $1921=17*113$ and see order is 56 so does not follow the rule established in the conjecture as the Proth number is composite.

For 97 from $t=2$ the 48 elements in **TNz48** are as shown next.

$\{ 2, 4, 8, 16, 32, 64, 31, 62, 27, 54, 11, 22, 44, 88, 79, 61, 25, 50, 3, 6, 12, 24, 48, -1, 95, 93, 89, 81, 65, 33, 66, 35, 70, 43, 86, 75, 53, 9, 18, 36, 72, 47, 94, 91, 85, 73, 49, 1 \}$

For 449 from $t=3$ the 224 elements in **TNz224** are as shown next.

$\{ 2, 4, 8, 16, 32, 64, 128, 256, 63, 126, 252, 55, 110, 220, 440, 431, 413, 377, 305, 161, 322, 195, 390, 331, 213, 426, 403, 357, 265, 81, 162, 324, 199, 398, 347, 245, 41, 82, 164, 328, 207, 414, 379, 309, 169, 338, 227, 5, 10, 20, 40, 80, 160, 320, 191, 382, 315, 181, 362, 275, 101, 202, 404, 359, 269, 89, 178, 356, 263, 77, 154, 308, 167, 334, 219, 438, 427, 405, 361, 273, 97, 194, 388, 327, 205, 410, 371, 293, 137, 274, 99, 198, 396, 343, 237, 25, 50, 100, 200, 400, 351, 253, 57, 114, 228, 7, 14, 28, 56, 112, \}$

224, -1, 447, 445, 441, 433, 417, 385, 321, 193,
 386, 323, 197, 394, 339, 229, 9, 18, 36, 72,
 144, 288, 127, 254, 59, 118, 236, 23, 46, 92,
 184, 368, 287, 125, 250, 51, 102, 204, 408, 367,
 285, 121, 242, 35, 70, 140, 280, 111, 222, 444,
 439, 429, 409, 369, 289, 129, 258, 67, 134, 268,
 87, 174, 348, 247, 45, 90, 180, 360, 271, 93,
 186, 372, 295, 141, 282, 115, 230, 11, 22, 44,
 88, 176, 352, 255, 61, 122, 244, 39, 78, 156,
 312, 175, 350, 251, 53, 106, 212, 424, 399, 349,
 249, 49, 98, 196, 392, 335, 221, 442, 435, 421,
 393, 337, 225, 1 }

For 1921 from $t=4$ the 56 elements in **TNz56** are as shown next.

{ 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024,
 127, 254, 508, 1016, 111, 222, 444, 888, 1776, 1631,
 1341, 761, 1522, 1123, 325, 650, 1300, 679, 1358, 795,
 1590, 1259, 597, 1194, 467, 934, 1868, 1815, 1709, 1497,
 1073, 225, 450, 900, 1800, 1679, 1437, 953, 1906, 1891,
 1861, 1801, 1681, 1441, 961, 1 }

For 7937 from $t=5$ the 3968 elements in **TNz3968** are not tabulated here

For 32257 from $t=6$ the 16128 elements in **TNz16128** are not tabulated here

For 130049 from $t=7$ the 10603 elements in **TNz10603** are not tabulated here

For 522241 from $t=8$ the 14457 elements in **TNz14457** are not tabulated here

For 2093057 from $t=9$ the 20520 elements in **TNz20520** are not tabulated here

For 8380417 from $t=10$ the 4190208 elements in **TNz4190208** are not tabulated here

For 33538049 from $t=11$ the 16769024 elements in **TNz16769024** are not tabulated here

For 134184961 from $t=12$ the 246480 elements in **TNz246480** are not tabulated here

Conjecture: For P of the form $1 + (-1 + 2^t) \times 2^{t+3}$ where t is a positive integer, when

$2^{\frac{p-1}{4}} \equiv -1 \pmod{p}$ then P is prime.

Chapter 29 – Element 2 and set $1+(1+2^t) \times (2^{t+3})$

Consider the Proth space $1+(1+2^t) \times (2^{t+3})$

Conjecture: For P of the form $1+(1+2^t) \times 2^{t+3}$ where t is a positive integer, when order of 2 modulo P is $(2^{t+1}) \times (1+2^t)$ then P is prime.

Using the above conjecture we have established the following

$$1+(1+2^{639}) \times (2^{642}) \text{ is Prime}$$

By tabulating the order of groups next we provide examples where order follows the conjecture and other examples where the Proth number used is composite.

We will be using generating element 2.

When $t=3$ we have $P=1+9 \times 64$ and the set of elements modulo P is a multiplicative group.

The subgroup generated by 2 has 144 elements

Order is $(2^4) \times (1+2^3)$ so we are a [probable] prime.

The elements in **TPc144** are as shown next

{ 2, 4, 8, 16, 32, 64, 128, 256, 512, 447,
317, 57, 114, 228, 456, 335, 93, 186, 372, 167,
334, 91, 182, 364, 151, 302, 27, 54, 108, 216,
432, 287, 574, 571, 565, 553, 529, 481, 385, 193,
386, 195, 390, 203, 406, 235, 470, 363, 149, 298,
19, 38, 76, 152, 304, 31, 62, 124, 248, 496,
415, 253, 506, 435, 293, 9, 18, 36, 72, 144,
288, -1, 575, 573, 569, 561, 545, 513, 449, 321,
65, 130, 260, 520, 463, 349, 121, 242, 484, 391,
205, 410, 243, 486, 395, 213, 426, 275, 550, 523,
469, 361, 145, 290, 3, 6, 12, 24, 48, 96,
192, 384, 191, 382, 187, 374, 171, 342, 107, 214,
428, 279, 558, 539, 501, 425, 273, 546, 515, 453,
329, 81, 162, 324, 71, 142, 284, 568, 559, 541,
505, 433, 289, 1 }

Next we look at $2177=7 \times 311$ and see order is 465 so does not follow the rule established in the conjecture as the Proth number is composite.

For 2177 from $t=4$ the 465 elements in **TPc465** are not tabulated here

For 8449 from $t=5$ the 840 elements in **TPc840** are not tabulated here

For 33281 from $t=6$ the 7953 elements in **TPc7953** are not tabulated here

For 132097 from $t=7$ the 6972 elements in **TPc6972** are not tabulated here

For 526337 from $t=8$ the 17688 elements in **TPc17688** are not tabulated here

For 2101249 from $t=9$ the 525312 elements in **TPc525312** are not tabulated here

For 8396801 from $t=10$ the 298680 elements in **TPc298680** are not tabulated here

Conjecture: For P of the form $1 + (1 + 2^t) \times 2^{t+3}$ where t is a positive integer, when $\frac{p-1}{8} = -1 \pmod{p}$ then P is prime.

Chapter 30 – Mathematical discovery

There are many ways that Mathematical discovery can happen.

Doing an Undergraduate degree or Masters or PhD are ways that discoveries can be made.

Working in Algebra for many years and asking “what if” is another way.

My discovery, depending on your point of view, is one or more of the following:

- Discovered a strong probable prime or ‘is prime’ test for a particular set
- “fixed the b” so same base used all the time for a prime test of Proth numbers
- Discovered a set in which a probable prime test behaves strongly.

Thought it worth describing the process that has allowed that to happen and will talk subjectively about that next.

Have spent many years working in the set $1 + (-1 + 2^t) \times (2^{t+1})$

Documented lots of algebraic observations, and through them, was able to come up with an order conjecture involving a least common multiple.

Nothing too exciting so far.

Through thinking about order of two elements in particular, began to see the importance of thinking lengthwise about things with decreasing and increasing values of t .

This is in contrast to thinking about isomorphisms primarily, where we tend to view order as an important separator and then move laterally between [groups].

Went so far as to propose a new definition “sturdy element” to facilitate this thinking.

Tabulated [a lot] of group examples using those elements.

[See chapters 2 to 5 and other earlier chapters for examples.]

Adjusted the set definition slightly from $1 + (-1 + 2^t) \times (2^{t+1})$ to nearby sets.

This was a key step.

Broke away from considering only sets we can describe as Proth numbers and considered other sets.

Still thinking about order and patterns and came up with some new conjectures.

To try and add a few chapters, returned to sets of Proth numbers but considered slightly different powers.

This was another key step.

During this time was always asking “what if” and “suppose” type questions of what I was seeing.

This supposing and enquiring was another key step.

Spotted something interesting when working with groups in set $1+(-1+2^t)\times(2^{t+3})$

Factored the order of a couple of groups to see if there was anything to see.

Made a supposition and tested it for a couple of examples.

Found that the pattern did not apply in all cases.

Asked the question did it only apply to primes.

There was the discovery.

Conjecture: For P of the form $1+(-1+2^t)\times 2^{t+3}$ where t is a positive integer, when order of 2 modulo P is $(2^{t+2})\times(-1+2^t)$ then P is prime.

Created a script to test things out.

Used a computer algebra package to run the script to see it work with larger examples.

The largest prime found [9769 digits] using this probable prime test as a filter is next.

$$1+(-1+2^{16224})\times(2^{16227}) \text{ is Prime}$$

Looked for a further set with something that looked algebraic

Conjecture: For P of the form $1+(1+2^t)\times 2^{t+3}$ where t is a positive integer, when order of 2 modulo P is $(2^{t+1})\times(1+2^t)$ then P is prime.

The largest prime found [386 digits] using this probable prime test as a filter is next.

$$1+(1+2^{639})\times(2^{642}) \text{ is Prime}$$

Stronger conjectures of the above are shown next

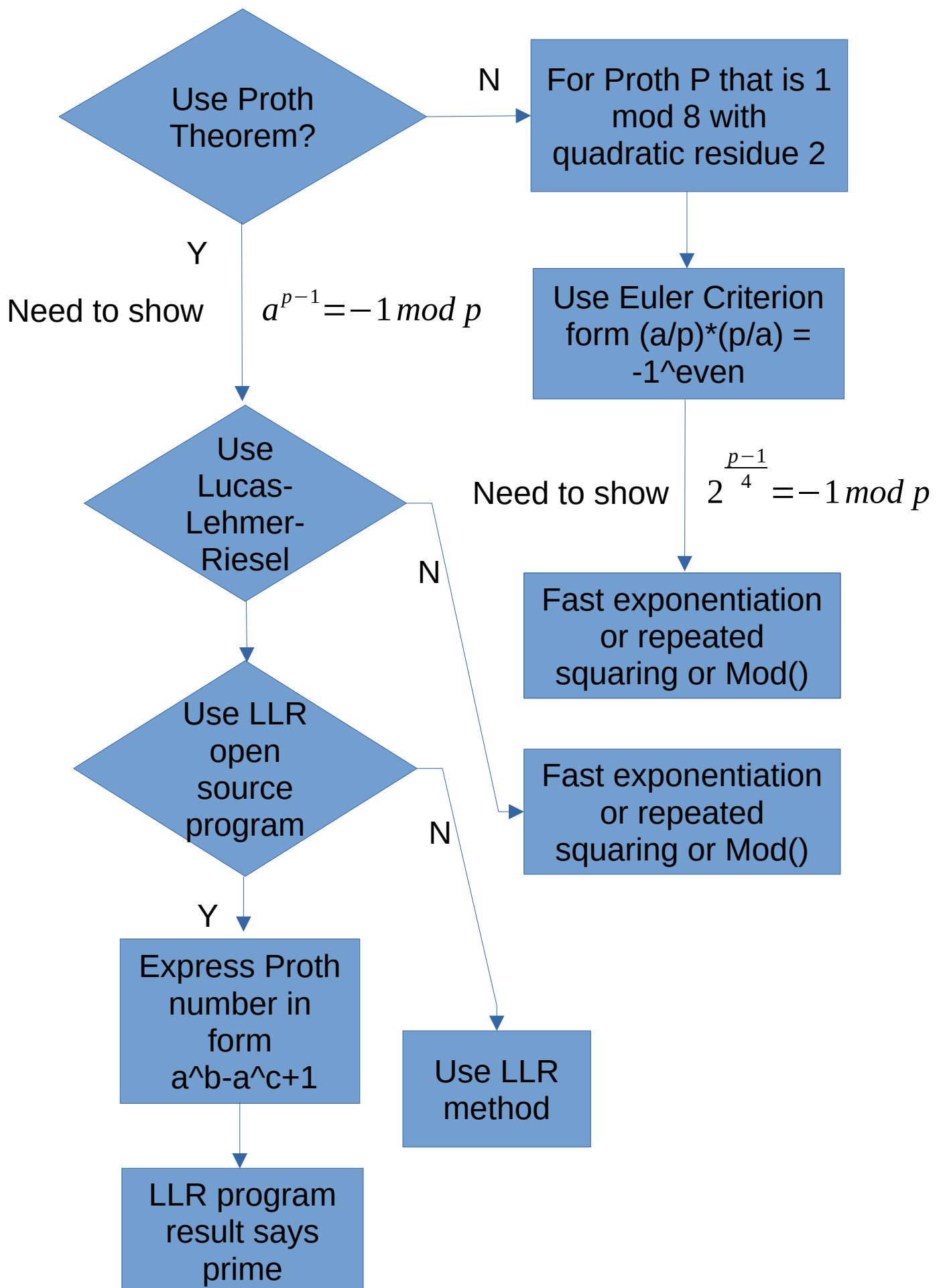
Conjecture: For P of the form $1+(-1+2^t)\times 2^{t+3}$ where t is a positive integer, when $2^{\frac{p-1}{4}} = -1 \pmod{p}$ then P is prime.

Conjecture: For P of the form $1+(1+2^t)\times 2^{t+3}$ where t is a positive integer, when $2^{\frac{p-1}{8}} = -1 \pmod{p}$ then P is prime.

Chapter 31 – Proving Proth Number is Prime

There are at least two ways of proving a Proth number is prime.

The flowchart on the next page shows the decisions involved in choosing which way to go.



Conjecture: For P of the form $1 + (-1 + 2^t) \times 2^{t+3}$ where t is a positive integer, when $2^{\frac{p-1}{4}} = -1 \pmod{p}$ then P is prime.

Numbers of this form are 1 mod 8 so the base 2 is always a quadratic residue

This can be checked with issquare(Mod(2,p)) or jacobi symbol

Necessity: If P is prime then $2^{\frac{p-1}{2}} = 1 \pmod{p}$

Using Euler Criterion

$\left(\frac{2}{p}\right) = 2^{\frac{p-1}{2}} \pmod{p}$ and extra/stronger requirement $2^{\frac{p-1}{4}} = -1 \pmod{p}$

Since P is 1 mod 8 according to the law of quadratic reciprocity* it follows that $\left(\frac{2}{p}\right) = 1$

Because P is an odd prime and P is 1 mod 4 we know $(2/p) = (p/2)$ so $\left(\frac{p}{2}\right) = 1$

Sufficiency: If $2^{\frac{p-1}{4}} = -1 \pmod{p}$ then Proth number P is prime

Have $\left(\frac{2}{p}\right) = 1$ and this can be equated to $2^{\frac{p-1}{2}} = 1 \pmod{p}$ when P is prime

Euler criterion does not apply if P is composite**

Because our base (2) is a quadratic residue, achieving $2^{\frac{p-1}{4}} = -1 \pmod{p}$ implies P is prime when $\left(\frac{2}{p}\right) = 1$

Achieving any other result mod p implies that P is composite or subject to further testing

* Have (p-1) is even and divisible by 8 and 2-1 is 1 and $\Rightarrow (q-1)/4$ is even
So $p/q * q/p$ is 1 (-1 to even power is 1) $\Rightarrow (2/p)$ must be 1

** Only for P prime can we equate to $\left(\frac{2}{p}\right)$

Proth number $1 + (-1 + 2^{16224}) \times (2^{16227})$ is Prime as checked $2^{\frac{p-1}{4}} = -1 \pmod{p}$

Chapter 32 – Proving Proth Number is Prime: extra step

An early version of the previous chapter offered a partial answer to proving a Proth Number is prime.

Conjecture: For P of the form $1 + (-1 + 2^t) \times 2^{t+3}$ where t is a positive integer, when $2^{\frac{p-1}{4}} = -1 \pmod{p}$ then P is prime.

It is not difficult to rule out most *Euler Pseudoprimes having $\left(\frac{2}{p}\right) = 1$, we just need to consider half the power so (p-1)/4 instead of just looking for the traditional $2^{\frac{p-1}{2}} = 1 \pmod{p}$

Next OEIS sequence A047713 Pseudoprimes along with the results of $2^{\frac{p-1}{4}} \pmod{p}$

*More specifically we might call these Euler-Jacobi Pseudoprimes

Pseudoprime n	$2^{\frac{p-1}{2}} = 1 \mod p$	$2^{\frac{p-1}{4}} \mod p$	(p-1)%4	Composite or pass
561	1	67	0	Composite
1105	1	781	0	Composite
1729	1	1	0	Composite
1905	1	1	0	Composite
2047	1	Incalculable	2	Incalculable
2465	1	1	0	Composite
3277	n/a	n/a	n/a	n/a
4033	1	1	0	Composite
4681	1	1	0	Composite
6601	1	4059	0	Composite
8321	1	1	0	Composite
8481	1	7195	0	Composite
10585	1	10294	0	Composite
12801	1	1	0	Composite
15841	1	1	0	Composite
16705	1	1	0	Composite
18705	1	1	0	Composite
25761	1	1	0	Composite
29341	n/a	n/a	n/a	n/a
30121	1	18357	0	Composite
33153	1	1	0	Composite
34945	1	1	0	Composite
41041	1	1	0	Composite
42799	1	Incalculable	2	Incalculable
46657	1	1	0	Composite
49141	n/a	n/a	n/a	n/a
52633	1	1	0	Composite
62745	1	25099	0	Composite
65281	1	1	0	Composite
74665	1	74664	0	pass
75361	1	1	0	Composite
80581	1	47813	0	Composite
85489	1	1	0	Composite
87249	1	1	0	Composite
88357	n/a	n/a	n/a	n/a
90751	1	Incalculable	2	Incalculable
104653	n/a	n/a	n/a	n/a

74665 is not a Proth Number. Is 74665 a strong Euler-Jacobi Pseudoprime?

See next page for counts and conclusions based on the table above

Of the 37 initial terms in OEIS sequence A047713 we found the following:

- One Pseudoprime passed the filter – 74665 (which is not a Proth number)
- Three were Incalculable as $p-1$ not divisible by 4
- Five were marked not applicable as we can only apply our filter when $\left(\frac{2}{p}\right) = 1$

One in twenty-nine passed the filter which means we eliminated 96% of the Pseudoprimes using this extra filter.

If you count the 8 for which our filter could not be used then we still eliminated $\frac{3}{4}$ of the Pseudoprimes.

We would for the context in which we apply our filter always be dealing with $(p-1)$ divisible by 8 and $2^{\frac{p-1}{2}} = 1 \pmod{p}$

So our filter would likely achieve near the 96% we achieved here.

Having amended the previous chapter, this filter is already incorporated into our prime test.

Chapter 33 – Ruling out Pseudoprimes – part 2

In this Chapter we continue through the OEIS 047713 Pseudoprimes tabulating the results of power $(p-1)/4$ as a filter

Pseudoprime n	$2^{\frac{p-1}{2}} = 1 \mod p$	$2^{\frac{p-1}{4}} \mod p$	$(p-1)\%4$	Composite or pass
113201	1	1	0	Composite
115921	1	963	0	Composite
126217	1	9710	0	Composite
129921	1	1	0	Composite
130561	1	1	0	Composite
149281	1	1	0	Composite
158369	1	1	0	Composite
162401	1	1	0	Composite
164737	1	108969	0	Composite
172081	1	1	0	Composite
188057	1	57050	0	Composite
196093	n/a	n/a	n/a	n/a
208465	1	96881	0	Composite
215265	1	1	0	Composite
220729	1	1	0	Composite
223345	1	1	0	Composite
233017	1	1	0	Composite
252601	1	252600	0	pass
253241	1	253240	0	pass
256999	1	Incalculable	2	Incalculable
266305	1	1	0	Composite
271951	1	Incalculable	2	Incalculable
278545	1	196621	0	Composite
280601	1	280600	0	pass
294409	1	262144	0	Composite
314821	n/a	n/a	n/a	n/a
323713	1	1	0	Composite
334153	1	1635	0	Composite
340561	1	140232	0	Composite
348161	1	1	0	Composite

Pseudoprime n	$2^{\frac{p-1}{2}} = 1 \mod p$	$2^{\frac{p-1}{4}} \mod p$	(p-1)%4	Composite or pass
357761	1	1	0	Composite
390937	1	390936	0	pass
399001	1	170067	0	Composite
410041	1	202211	0	Composite
427233	1	1	0	Composite
448921	1	157730	0	Composite
449065	1	120784	0	Composite
458989	1	126806	0	Composite
476971	1	Incalculable	2	Incalculable
486737	1	1	0	Composite
488881	1	1	0	Composite
489997	1	249759	0	Composite
493697	1	1	0	Composite
514447	1	Incalculable	2	Incalculable
526593	1	1	0	Composite
530881	1	1	0	Composite
552721	1	422670	0	Composite
580337	1	1	0	Composite
588745	1	185494	0	Composite
625921	1	1	0	Composite
635401	1	635400	0	pass
647089	1	1	0	Composite
656601	1	636703	0	Composite
658801	1	387531	0	Composite
665281	1	662974	0	Composite
670033	1	1	0	Composite
683761	1	532676	0	Composite
711361	1	1	0	Composite
721801	1	719398	0	Composite
741751	1	Incalculable	2	Incalculable

252601, 253241, 280601, 390937, 635401 are not Proth Numbers.
Are they strong Euler-Jacobi Pseudoprime?

See next page for counts and conclusions based on the table above

Of the 60 terms tabulated from OEIS sequence A047713 we found the following:

- Five Pseudoprimes passed the filter – (none of which are Proth numbers)
- Five were Incalculable as $p-1$ not divisible by 4
- Two were marked not applicable as we can only apply our filter when $\left(\frac{2}{p}\right) = 1$

Five in 60 passed the filter which means we eliminated 91% of the Pseudoprimes using this extra filter.

If you count the 7 for which our filter could not be used then we still eliminated 4/5 of the Pseudoprimes.

We would for the context in which we apply our filter always be dealing with $(p-1)$ divisible

by 8 and $2^{\frac{p-1}{2}} = 1 \pmod{p}$

Chapter 34 – Ruling out Pseudoprimes – part 3

In this Chapter we continue through the OEIS 047713 Pseudoprimes tabulating the results of power $(p-1)/4$ as a filter

Pseudoprime n	$2^{\frac{p-1}{2}} = 1 \mod p$	$2^{\frac{p-1}{4}} \mod p$	$(p-1)\%4$	Composite or pass
745889	1	1	0	Composite
748657	1	250706	0	Composite
800605	n/a	n/a	n/a	n/a
818201	1	818200	0	pass
825265	1	485451	0	Composite
838201	1	6343	0	Composite
838861	n/a	n/a	n/a	n/a
841681	1	1	0	Composite
852481	1	1	0	Composite
852841	1	1	0	Composite
873181	n/a	n/a	n/a	n/a
875161	1	544454	0	Composite
877099	n/a	n/a	n/a	n/a
916327	1	Incalculable	2	Incalculable
976873	1	976872	0	pass
983401	1	1	0	Composite
997633	1	1	0	Composite
1004653	n/a	n/a	n/a	n/a
1016801	1	1	0	Composite
1018921	1	45086	0	Composite
1023121	1	1	0	Composite
1050985	1	353534	0	Composite
1052929	1	1	0	Composite
1053761	1	1	0	Composite
1082401	1	1	0	Composite
1082809	1	999517	0	Composite
1132657	1	628506	0	Composite
1145257	1	1	0	Composite
1157689	1	181375	0	Composite
1168513	1	1	0	Composite

Pseudoprime n	$2^{\frac{p-1}{2}} = 1 \mod p$	$2^{\frac{p-1}{4}} \mod p$	(p-1)%4	Composite or pass
1194649	1	1194648	0	pass
1207361	1	1207360	0	pass
1246785	1	1	0	Composite
1251949	n/a	n/a	n/a	n/a
1252697	1	1252696	0	pass
1275681	1	1	0	Composite
1302451	n/a	n/a	n/a	n/a
1306801	1	1	0	Composite
1325843	n/a	n/a	n/a	n/a
1357441	1	1	0	Composite
1373653	n/a	n/a	n/a	n/a
1397419	n/a	n/a	n/a	n/a
1441091	n/a	n/a	n/a	n/a
1461241	1	100084	0	Composite
1472065	1	1	0	Composite
1472353	1	1197362	0	Composite
1472505	1	883504	0	Composite
1485177	1	1393072	0	Composite
1489665	1	1	0	Composite
1493857	1	1	0	Composite
1507561	1	1255563	0	Composite
1507963	n/a	n/a	n/a	n/a
1509709	n/a	n/a	n/a	n/a
1529185	1	1	0	Composite
1530787	n/a	n/a	n/a	n/a
1533601	1	1	0	Composite
1569457	1	553927	0	Composite
1608465	1	1	0	Composite
1615681	1	1	0	Composite
1620385	1	573366	0	Composite

818201, 976873, 1194649, 1207361, 1252697 are not Proth Numbers.
Are they strong Euler-Jacobi Pseudoprime?

See next page for counts and conclusions based on the table above

Of the 60 terms tabulated from OEIS sequence A047713 we found the following:

- Five Pseudoprimes passed the filter – (none of which are Proth numbers)
- One was Incalculable as $p-1$ not divisible by 4
- 14 were marked not applicable as we can only apply our filter when $\left(\frac{2}{p}\right) = 1$

Five in 60 passed the filter which means we eliminated 91% of the Pseudoprimes using this extra filter.

If you count the 15 for which our filter could not be used then we still eliminated $\frac{3}{4}$ of the Pseudoprimes.

We would for the context in which we apply our filter always be dealing with $(p-1)$ divisible

by 8 and $2^{\frac{p-1}{2}} = 1 \pmod{p}$

Chapter 35 – Ruling out Pseudoprimes – part 4

In this Chapter we continue through the OEIS 047713 Pseudoprimes tabulating the results of power $(p-1)/4$ as a filter

Pseudoprime n	$2^{\frac{p-1}{2}} = 1 \mod p$	$2^{\frac{p-1}{4}} \mod p$	$(p-1)\%4$	Composite or pass
1678541	n/a	n/a	n/a	n/a
1719601	1	505766	0	Composite
1730977	1	1	0	Composite
1735841	1	1	0	Composite
1746289	1	1258297	0	Composite
1773289	1	1	0	Composite
1811573	n/a	n/a	n/a	n/a
1815465	1	366904	0	Composite
1827001	1	623855	0	Composite
1857241	1	995318	0	Composite
1876393	1	1876392	0	pass
1896961	1	1	0	Composite
1907851	n/a	n/a	n/a	n/a
1908985	1	352429	0	Composite
1909001	1	1909000	0	pass
1969417	1	1	0	Composite
1987021	n/a	n/a	n/a	n/a
1993537	1	6917	0	Composite
2004403	n/a	n/a	n/a	n/a
2077545	1	1868179	0	Composite
2081713	1	1	0	Composite
2089297	1	1	0	Composite
2113665	1	1	0	Composite
2113921	1	1	0	Composite
2144521	1	1938881	0	Composite
2163001	1	7205	0	Composite
2171401	1	1588831	0	Composite
2181961	1	2181960	0	pass
2205967	1	Incalculable	2	Incalculable
2213121	1	1	0	Composite

Pseudoprime n	$2^{\frac{p-1}{2}} = 1 \mod p$	$2^{\frac{p-1}{4}} \mod p$	(p-1)%4	Composite or pass
2232865	1	1	0	Composite
2233441	1	1	0	Composite
2261953	1	1	0	Composite
2264369	1	1	0	Composite
2269093	n/a	n/a	n/a	n/a
2284453	n/a	n/a	n/a	n/a
2299081	1	1916812	0	Composite
2304167	1	Incalculable	2	Incalculable
2327041	1	1	0	Composite
2387797	n/a	n/a	n/a	n/a
2419385	1	2419384	0	pass
2433601	1	1	0	Composite
2455921	1	1	0	Composite
2510569	1	2510568	0	pass
2626177	1	1265974	0	Composite
2628073	1	1207494	0	Composite
2670361	1	1247040	0	Composite
2704801	1	1	0	Composite
2722681	1	1884934	0	Composite
2746477	n/a	n/a	n/a	n/a
2748023	1	Incalculable	2	Incalculable
2757241	1	2757240	0	pass
2811271	1	Incalculable	2	Incalculable
2909197	n/a	n/a	n/a	n/a
2953711	1	Incalculable	2	Incalculable
2976487	1	Incalculable	2	Incalculable
3020361	1	1	0	Composite
3048841	1	1549792	0	Composite
3057601	1	1	0	Composite
3090091	n/a	n/a	n/a	n/a

1876393, 1909001, 2181961, 2419385, 2510569, 2757241 are not Proth Numbers.
Are they strong Euler-Jacobi Pseudoprime?

See next page for counts and conclusions based on the table above

Of the 60 terms tabulated from OEIS sequence A047713 we found the following:

- Six Pseudoprimes passed the filter – (none of which are Proth numbers)
- Six were Incalculable as $p-1$ not divisible by 4
- 11 were marked not applicable as we can only apply our filter when $\left(\frac{2}{p}\right) = 1$

Six in 60 passed the filter which means we eliminated 90% of the Pseudoprimes using this extra filter.

If you count the 17 for which our filter could not be used then we still eliminated 71% of the Pseudoprimes.

We would for the context in which we apply our filter always be dealing with $(p-1)$ divisible

by 8 and $2^{\frac{p-1}{2}} = 1 \pmod{p}$

Chapter 36 – Ruling out Pseudoprimes – part 5

In this Chapter we continue through the OEIS 047713 Pseudoprimes tabulating the results of power $(p-1)/4$ as a filter

Pseudoprime n	$2^{\frac{p-1}{2}} = 1 \mod p$	$2^{\frac{p-1}{4}} \mod p$	$(p-1)\%4$	Composite or pass
3094273	1	1	0	Composite
3116107	n/a	n/a	n/a	n/a
3125281	1	1	0	Composite
3224065	1	1	0	Composite
3225601	1	1	0	Composite
3363121	1	5187	0	Composite
3370641	1	3172369	0	Composite
3375041	1	1	0	Composite
3400013	n/a	n/a	n/a	n/a
3429037	n/a	n/a	n/a	n/a
3539101	n/a	n/a	n/a	n/a
3567481	1	1	0	Composite
3581761	1	1	0	Composite
3605429	n/a	n/a	n/a	n/a
3656449	1	1	0	Composite
3664585	1	2299844	0	Composite
3679201	1	1	0	Composite
3755521	1	1	0	Composite
3763801	1	824191	0	Composite
3828001	1	1	0	Composite
3898129	1	1	0	Composite
3985921	1	1	0	Composite
4014361	1	5667	0	Composite
4069297	1	1359122	0	Composite
4072729	1	1	0	Composite
4154161	1	1	0	Composite
4154977	1	3794928	0	Composite
4181921	1	1	0	Composite
4188889	1	1	0	Composite
4229601	1	1	0	Composite

Pseudoprime n	$2^{\frac{p-1}{2}} = 1 \mod p$	$2^{\frac{p-1}{4}} \mod p$	(p-1)%4	Composite or pass
4259905	1	3014701	0	Composite
4335241	1	4335240	0	pass
4360621	n/a	n/a	n/a	n/a
4463641	1	3974216	0	Composite
4469471	1	Incalculable	2	Incalculable
4502485	n/a	n/a	n/a	n/a
4513841	1	1	0	Composite
4650049	1	1863247	0	Composite
4682833	1	1	0	Composite
4767841	1	737296	0	Composite
4835209	1	1	0	Composite
4863127	1	Incalculable	2	Incalculable
4869313	1	1	0	Composite
4877641	1	1336339	0	Composite
4903921	1	1	0	Composite
4909177	1	3776291	0	Composite
4984001	1	1	0	Composite
5016191	1	Incalculable	2	Incalculable
5044033	1	1	0	Composite
5049001	1	1	0	Composite
5095177	1	1701402	0	Composite
5133201	1	770320	0	Composite
5148001	1	1	0	Composite
5173169	1	1	0	Composite
5173601	1	5173600	0	pass
5176153	1	5169718	0	Composite
5256091	n/a	n/a	n/a	n/a
5271841	1	1907710	0	Composite
5310721	1	1	0	Composite
5351537	1	11333	0	Composite

4335241, 5173601 are not Proth Numbers.
Are they strong Euler-Jacobi Pseudoprime?

See next page for counts and conclusions based on the table above

Of the 60 terms tabulated from OEIS sequence A047713 we found the following:

- Two Pseudoprimes passed the filter – (none of which are Proth numbers)
- Three were Incalculable as $p-1$ not divisible by 4
- 8 were marked not applicable as we can only apply our filter when $\left(\frac{2}{p}\right) = 1$

Two in 60 passed the filter which means we eliminated 96% of the Pseudoprimes using this extra filter.

If you count the 11 for which our filter could not be used then we still eliminated 78% of the Pseudoprimes.

We would for the context in which we apply our filter always be dealing with $(p-1)$ divisible

by 8 and $2^{\frac{p-1}{2}} = 1 \pmod{p}$

Chapter 37 Sufficiency of (p-1)/4 testing

Here we reflect on the 277 Euler-Jacobi Pseudoprimes we tested $2^{\frac{p-1}{4}} = -1 \pmod{p}$

For Proth Numbers that satisfy $2^{\frac{p-1}{2}} = 1 \pmod{p}$ we assume there are some Euler-Jacobi Pseudoprimes to base 2.

Considering Proth Numbers ≥ 1000 we are always $1 \pmod{8}$ and have $\left(\frac{2}{p}\right) = 1$

No Proth Numbers that are Euler-Jacobi Pseudoprimes [to base 2] passed the filter in our 277 item sample.

The empirical evidence suggests that in our limited context that

There are no Proth Numbers that satisfy $2^{\frac{p-1}{4}} = -1 \pmod{p}$ that are Euler-Jacobi Pseudoprimes [to base 2]

Hence for Proth Numbers ≥ 1000 satisfying $2^{\frac{p-1}{4}} = -1 \pmod{p}$ implies P is Prime.

To disprove the above you would need to find a Proth Number that satisfies

$2^{\frac{p-1}{4}} = -1 \pmod{p}$ that is Composite.

A narrower and more context specific version of the above is the following conjecture

Conjecture: For P of the form $1 + (-1 + 2^t) \times 2^{t+3}$ where t is a positive integer, when

$2^{\frac{p-1}{4}} = -1 \pmod{p}$ then P is prime.

Proofs for that conjecture are available in 2026

Trying to disprove the above would involve finding a Proth Number of the form

$1 + (-1 + 2^t) \times 2^{t+3}$ that is composite but achieves $2^{\frac{p-1}{4}} = -1 \pmod{p}$

This is non-trivial*

*No counter-examples exist for $t \leq 30,000$ in our limited testing.

The following conjecture might be easier to disprove

Conjecture: For Proth Numbers of the form $1 + (-1 + 2^t) \times 2^{t+3}$ there are no Euler-Jacobi Pseudoprimes

Chapter 38 – Pari scripts for Conjectures

This chapter contains two scripts which I used to support / verify conjectures

The script below relates to the $2^{\frac{p-1}{4}} = -1 \pmod{p}$ conjecture at the end of Chapter 28
[Element 2 and set $1 + (-1 + 2^t) \times (2^{t+3})$]

```
t=10;t3=3+t;lead=-1+2^t;dp=1+2*t;d4=4*dp;pr=1+lead*(2^t3)
starter=16000;
for(k=starter,starter+1000,t2=2+k; \
    lead=(-1+2^k); \
    nmo=lead*(2*2^t2); \
    pr=1+nmo; \
    pow2=((2^t2)*(-1+2^k)); \
    pow2halved=pow2/2; \
    if(-1==Mod(2,pr)^pow2halved,print("t=",k," gives -1 for 2^pow2halved")); \
    if(k>starter&&0==k%500,print("-- loop marker -- t=",k)); \
);
```

The next script relates to the $2^{\frac{p-1}{8}} = -1 \pmod{p}$ conjecture at the end of Chapter 29
[Element 2 and set $1 + (1 + 2^t) \times (2^{t+3})$]

```
t=9;t3=3+t;leadplus=1+2^t;dp=1+2*t;d4=4*dp;prp=1+leadplus*(2^t3)
starter=1;
for(k=starter,starter+1000,t1=1+k;t2=2+k; \
    leadplus=(1+2^k); \
    nmo=leadplus*(2*2^t2); \
    prp=1+nmo; \
    pow2=((2^t1)*(1+2^k)); \
    pow2adjusted=pow2/2; \
    if(-1==Mod(2,prp)^pow2adjusted,print("t=",k," gives -1 for 2^pow2adjusted")); \
    if(k>starter&&0==k%500,print("-- loop marker -- t=",k)); \
);
```

The scripts are designed to work in Pari/GP and were tested in Pari version 2.17