Presentation on an easy method for finding many very large prime numbers

Johan Vonk*

April 2, 2018

1 Introduction

In a letter during 1640, Fermat proved that an odd prime m can be written in the form $x^2 + y^2$ if and only if $p \equiv 1 \mod 4$. Later he discovered similar statements with $x^2 + 2y^2$ and $x^2 + 3y^2$. Namely:

$$m = x^2 + 2y^2 \iff m = 2 \text{or} m \equiv 1, 3 \mod 8$$

$$m = x^2 + 3y^2 \iff m = 3 \text{or} m \equiv 1 \mod 3$$

Later in 1750, 1774, and 1763, Euler proved these statements. He then went on to discuss for which numbers n the equation $x^2 + ny^2$ produced primes with a finite amount of exceptions. Euler called these n *numerus idoneus* or idoneal numbers.

Definition 1.0.1. *A number n is* **idonealif** *$x^2 + ny^2$ it produces primes with a finite amount of exceptions. More formally, an number n is idoneal when any integer is expressible in only one way as $x^2 \pm ny^2$ where x^2 is relatively prime to ny^2 must be a prime, a prime power, twice a prime power or prime, or a power of two.*

If n is idoneal, then if the equation $m = x^2 + ny^2$ has only one solution with $x, y \geq 0$ then m must be prime. Therefore, every idoneal number can generates a set containing infinitely many primes m. Unfortunately, it also misses infinitely many other primes.

Euler investigated primes of the form $232 \cdot a^2 + 1$. Since $232 = 8 \cdot 29$ is idoneal, some values from this formula will be composite and we will figure out which those are and the rest must be prime.

*Simon Rubinstein-Salzedo, and the rest of Euler Circle

1.1 What do we know about composite ms

We can now find primes m that are related to n given that it is idoneal.
Since 232 is idoneal, if $232 \cdot a^2 + 1$ is composite, then

$$m = 232a^2 + 1 = 232x^2 + y^2$$

This equals

$$232(a^2 - x^2) = y^2 - 1$$

Say

$$y = 1 \pm 58z$$

Put this in and divide by 232 to get

$$a^2 - x^2 = \frac{1}{2}z(29z \pm 1)$$

Next take all values for z in order
Since $\frac{1}{2}z(29z \pm 1)$ has more than 2 factors, then it can be represented in at least one way as rs where r and s are factors.
Since this has to equal $a^2 - x^2$ or $(a-x)(a+x)$, then $r = a + x$ and $s = a - x$
Therefore $r + s = (a + x) + (a - x) = 2a$ or

$$a = \frac{r+s}{2}$$

The values of a which are composite must be in this form. Clearly, r and s must both be even or odd because otherwise a is not going to be an integer, which doesn't work.

1.2 $z = 1$

Recall

$$a^2 - x^2 = \frac{1}{2}z(29z \pm 1)$$

When $z = 1$ this is

$$rs = \frac{29 \pm 1}{2}$$

Therefore $rs = 14$ or $rs = 15$
The first value is useless because either r is odd and s is even or vice versa. So we are left with

$$rs = 15$$

Either $r = 15$ and $s = 1$ or $r = 5$ and $s = 3$ Then $a = \frac{r+s}{2}$ which equals $\frac{15+1}{2} = 8$ or $\frac{5+3}{2} = 4$ Since for these a, $232 \cdot a^2 + 1$ must be composite, we can exclude these a.

1.3 $2 \leq z \leq 4$

Here we will do a couple more zs, but many more can be easily computed. When $z = 2$, then

$$rs = \frac{\cancel{2} \cdot (2 \cdot 29 \pm 1)}{\cancel{2}} = 58 \pm 1$$

So rs is either 57 or 59. For the first, $rs = 57$, either $r = 57$ and $s = 1$ or $r = 19$ and $s = 3$. For the second one, $rs = 59$, then $r = 59$ and $s = 1$.
Remember $a = \frac{r+s}{2}$. So either $a = \frac{57+1}{2} = 29$, $a = \frac{19+3}{2} = 11$, or $a = \frac{59+1}{2} = 30$.
So, for $n = 2$:

$$a = 11, a = 29, a = 30$$

When $z = 3$, then

$$rs = \frac{3 \cdot (3 \cdot 29 \pm 1)}{2} = \frac{3 \cdot (87 \pm 1)}{2} = 3 \cdot 43,\ 3 \cdot 4 = 129,\ 132$$

So rs is either 129 or 132. For $r = 132$ and $s = 1$ it doesn't work because $r + s$ is not even so the result is a fraction and a cannot be a fraction.

$$\begin{array}{cc|ccc} r = 129 & r = 43 & \cancel{r = 132} & r = 66 & r = 22 \\ s = 1 & s = 3 & \cancel{s = 1} & s = 2 & s = 6 \end{array}$$

For $r = 132$ and $s = 1$ it doesn't work because $r + s$ is not even so the result is a fraction and a cannot be a fraction.
Remember $a = \frac{r+s}{2}$. So either $a = \frac{129+1}{2} = 65$, $a = \frac{43+3}{2} = 23$, $a = \frac{66+2}{2} = 34$, or $a = \frac{22+6}{2} = 14$.
So, for $n = 3$:

$$a = 14, a = 23, a = 34, a = 65$$

When $z = 4$, unlike the previous cases (and practically all future cases), $rs = 230$ or $rs = 234$. Because these numbers are $\equiv 2 \pmod 4$, the resultant r and s turn out to never make a whole a, so this case doesn't produce any exceptions.

1.4 Put it all together

We can continue on like this (and Euler did), but it ends up being fairly repetitive. So here is a table with all of the values that $a < 42$ cannot be to form primes of the form

$$232 \cdot a^2 + 1$$

z	Exclusions							
1	4,	8,						
2	11,	29,	30,					
3	14,	$\underline{23}$,	34,	65,				
4								
5	19,	21,	$\underline{23}$,	33,	39,	47,	91,	183,
6	23,	25,	41,	55,	88,	89,	260,	263,
7	54							
8	32,	40,	80,	232,	234			
.	...	...	...	...	...	...	...	...

As we can see some numbers such as 23 occur multiple times because $232 \cdot a^2 + 1$ has more than 2 factors. For 23,

$$232 \cdot 23^2 + 1 = 232 \cdot 529 + 1 = 122729 = 31 \cdot 37 \cdot 107$$

Because of this, this value can be excluded for multiple z values. Another thing that can be fixed with this table is that it is not in order!

4, 8, 11, 14, 19, 21, 23, 25, 29, 30, 32, 33, 34, 39
40, 41, 42, 43, 47, 51, 54, 55, 56, 57, 58, 59, 60, 61
63, 64, 65, 66, 68, 69, 70, 75, 77, 78, 80, 83, 84, 85
88, 89, 90, 91, 92, 93, 96, 97, 98, 101, 102, 103, 105, 108
109, 110, 111, 114, 116, 117, 120, 122, 123, 125, 128, 129, 130, 131
132, 133, 134, 135, 137, 139, 140, 141, 143, 145, 146, 147, 148, 154
156, 160, 161, 162, 163, 164, 165, 166, 168, 169, 171, 174, 178, 179
181, 183, 184, 185, 186, 187, 190, 191, 192, 193, 194, 195, 196, 198
199, 202, 203, 206, 207, 208, 209, 211, 212, 214, 215, 216, 217, 218
220, 221, 222, 223, 224, 225, 231, 232, 233, 234, 235, 236, 237, 239
240, 241, 242, 243, 244, 245, 246, 247, 252, 253, 256, 257, 260, 263
265, 266, 268, 271, 272, 273, 274, 276, 278, 279, 282, 284, 286, ...

All the values that are not part of this list must form primes when substituted in $232 \cdot a^2 + 1$. Here is a list of them:

1, 2, 3, 5, 6, 7, 9, 10, 12, 13, 15, 16, 17, 18,
20, 22, 24, 26, 27, 28, 31, 35, 36, 37, 38, 44, 45, 46,
48, 49, 50, 52, 53, 62, 67, 71, 72, 73, 74, 76, 79, 81,
82, 86, 87, 94, 95, 99, 100, 104, 106, 107, 112, 113, 115, 118,
119, 121, 124, 126, 127, 136, 138, 142, 144, 149, 150, 151, 152, 153,
155, 157, 158, 159, 167, 170, 172, 173, 175, 176, 177, 180, 182, 188,
189, 197, 200, 201, 204, 205, 210, 213, 219, 226, 227, 228, 229, 230,
238, 248, 249, 250, 251, 254, 255, 258, 259, 261, 262, 264, 267, 269,
270, 275, 277, 280, 281, 283, 285, 288, ...