Using Idoneal Numbers to Find Large Primes.

An exposition on Euler's paper (E718)

Skyler Mao

1 Introduction

A number p is prime if the only numbers that divide it are 1 and itself. For example, 7 is prime because only 1 and 7 divide it. Prime numbers have been of interest to mathematicians for centuries and are the fundamental building block of number theory.

One may check whether p is prime by going through all potential factors, checking whether they evenly divide p. Before the advent of modern computing devices, this process is a tedious one, which made finding large prime numbers very difficult and time consuming. Euler was able to solve this issue by developing a method to find large primes, of which we will discuss below.

2 Idoneal Numbers

In his paper, Euler utilizes a set of numbers known as *numerous idoneous*, or *idoneal numbers*. Although there are several definitions for idoneal numbers, the most relevant one is the following:

Definition 2.1. A number n is an idoneal number if and only if the following holds: Let $m > 1$ be an odd number relatively prime to n which can be written in the form $x^2 + ny^2$ with $\gcd(x, y) = 1$. If the equation $m = x^2 + ny^2$ has exactly one solution with $x, y \geq 0$, then m is a prime number.

Example 2.2. The number 1 is a trivial idoneal number. If the relatively prime pair (x, y) satisfies $m = x^2 + y^2$, then (y, x) satisfies it as well. The only time there is exactly one solution is when $x = y = 1$, in which case $m = 2$ is even. Therefore, 1 is idoneal.

Example 2.3. The number 11 is the first non-idoneal number. We realize that $15 = 2^2 + 11 \cdot 1^2$ is the only way we can express 15 as $x^2 + 11y^2$, but 15 is composite. Therefore, 11 is non-idoneal.

There are currently 65 known idoneal numbers, conjectured by Euler and Gauss to be the only ones. Even now, it is unknown whether there are more idoneal numbers.

The intuition behind Euler's method was the fact that the number m in the definition is expressed in terms of squares. This means that we can deal with small numbers to generate a large m that we know is prime.

Euler's proceeded in an interesting way: he relied on the process of elimination to remove certain values that generated composite numbers, and took the remaining ones as primes. Indeed, he utilized the following statement.

Corollary 2.4. *If an odd m can be expressed as $x^2 + ny^2$ in at least two ways, where n is an idoneal number, then m is composite.*

We will now outline Euler's method below.

3 Euler's Method

Euler experimented with the expression $232a^2 + 1$. Since $232 = 29 \cdot 8$ is idoneal, the expression will yield a composite number if there exists x, y such that

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

which can be rearranged to

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

Since the prime factors of 29 and 2 must be on the right, Euler substituted $y = 58z \pm 1$, which eventually simplifies to

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

Euler then let $r = a + x$ and $s = a - x$, so $a = \frac{r+s}{2}$. The equation only has a solution if r and s share the same parity.

Euler then proceeded to plug in various values for z. For example, setting $z = 1$ gives us $rs = 14$ or 15. 14 doesn't work, while 15 gives us $r = 5$, $s = 3$, and $a = 4$.

Setting $z = 2$ yields $rs = 57, 59$. This gives us three more working solutions: $(r, s, a) = (19, 3, 11)$, $(57, 1, 29)$, $(59, 1, 30)$.

Setting $z = 3$ yields $rs = 129, 132$. We test the factors to get $(r, s, a) = (129, 1, 65)$, $(43, 3, 23)$, $(66, 2, 34)$, and $(22, 6, 14)$.

Euler continued his computation up until $z = 78$, of which the results are included below:

z	Exclusions	z	Exclusions	z	Exclusions
1	4, 8	22	84, 85, 96, 123, 276	46	191, 217, 257
2	11, 29, 30	23	90, 122, 178	47	184
3	14, 23, 34, 65	24	92, 140, 154	48	185, 241, 253
5	19, 21, 23, 33, 39,	25	98, 110, 154, 194	49	192, 260
	47, 91, 183	26	108,145	50	191, 193, 215,
6	23, 25, 41, 55, 88,	27	103, 105, 111, 125,		225, 279, 297
	89, 260, 263		129, 147, 165, 203,	51	196, 236, 292
7	54		209, 241	53	202, 223, 245,
8	32, 40, 80, 232, 234	29	122, 134, 166, 218,		260
9	70, 198		225	54	224
10	51, 56, 147, 148, 244	30	122, 131, 133, 146,	56	216, 240
11	42, 43, 51, 54, 63, 85,		187, 214	58	224, 236, 292
	93, 114, 222, 293	31	240	59	225, 231, 233,
13	51, 59, 60, 69, 101,	32	129, 224		273
	141, 179	33	256	61	239, 241, 282
14	54, 57, 58, 66, 78,	34	130, 141, 190, 202	62	237
	102, 135, 162,	35	137, 143, 162, 169,	63	240
	206, 207, 286		247, 271	64	246, 282
15	64, 68, 88, 116, 236	37	141, 145, 171, 287	65	252
16	61, 77, 103, 161, 191	38	212	66	274
17	120, 132, 168	39	154, 202	67	282
18	265, 266	40	156, 174, 178, 242	69	263, 265, 295
19	75, 80, 88, 117, 147,	41	162, 186	71	278
	243	42	160, 220, 268	73	286
21	80, 83, 85, 97, 103,	43	164, 181, 195, 199,	75	286, 290
	109, 128, 145, 163,		211, 284	78	298
	221, 235, 272	45	208		

The a that satisfy the equation make $232a^2 + 1$ composite, and the ones that are not covered gives us primes. Since the minimum a achieved when $n \geq 79$ is $\sqrt{z} > 300$ we have exhausted all the possibilities for numbers under 300. Thus, the a that weren't covered make $232a^2 + 1$ prime, giving us the following result:

Theorem 3.1. *The list of a that makes $232a^2 + 1$ prime is 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, 289, 291, 294, 299, ...*

This can be used to generate large primes; plugging in 299 gives us $232 \cdot 299^2 + 1 = 20,741,033$, which is prime.

Although this method requires a substantial amount of computation, it is much easier than checking divisibility. We are able to generate a list of many large prime numbers.