Euler's Primality Test Through Sums of Two Squares

Julian Schennach

August 20, 2023

1 Introduction

For large positive integers, it is quite difficult to prove that a number is prime, as we must check each possible prime divisor up to the square root of said number. While computers have sped this process up in the past decades, no such aid existed in the 18-th century, and therefore mathematicians had to manually find the possible divisors. Fortunately, Euler devised a more efficient method to check for primes that are equivalent to 1 (mod 4): If a number n can only be written as the sum of two squares for *one* unique pair of squares, n is prime, and otherwise, if there are at least two sums, or even none at all, n is composite. This is quite an unintuitive result, as, at first, there seems to be no connection between primes and squares, and yet there is actually an interesting relationship between them.

More specifically, in his 1758 paper, *On numbers which are the sum of two squares* (E228), Euler starts by proving some simple properties of sums of two squares: For instance, the product of two sums of two squares is also a sum of two squares, and if a product is a sum of two squares and has one prime factor that is a sum of two squares, the complementary factor is also a sum of two squares. Using these results, Euler is then able to prove that sums of two relatively prime squares can only be divided by sums of two squares. Finally, in addition to the aforementioned test for primes, Euler partially proves Fermat's Theorem on Sums of Two Squares as another major result of his paper. Euler displays the importance of his primality test by determining whether large numbers with remainder 1 (mod 4) are prime and, if they are not, finds their factors. He accomplishes this substantially faster than mathematicians of his century would have otherwise been able to. This new criterion has served as a starting point to the search of more efficient methods, now used to factor large numbers with the help of computers.

In our paper, we will be following in Euler's footsteps and prove his theorems, hopefully in a clearer and more concise fashion (such as by combining similar cases in proofs together, or by explaining unclear manipulations and results). Additionally, we will also be looking at another one of Euler's papers (E241) in order to complete his proof of Fermat's Theorem on Sums of Two Squares. Like Euler, we will end our paper by demonstrating the usefulness of his primality test, with an implementation in Python — which, of course, did not exist in Euler's time.

2 Fundamentals

We begin by investigating some fundamental properties of sums of two squares, which will, for instance, allow us to only consider odd sums of two squares.

As a simple definition, a sum of two squares is defined as a number that can be written as x^2+y^2, where x, y are nonnegative integers. Also, the sum x^2+y^2 is considered equivalent to y^2+x^2. Using this definition, Euler lists the numbers less than 200 that are sum of two squares, but there is no pattern other than the definition that creates the list.

However, at the very least, we know what remainder the numbers in the list have when divided by 4 or 8. The squares x^2 and y^2 can only be both even, both odd, or one square is even and the other is odd. Notice that squares can only be $0 \pmod 4$ or $1 \pmod 8$: When x^2 is even, x is too, meaning $x^2 = (2n)^2 = 4n^2$, a multiple of 4. When x^2 is odd, though, x is odd too, so $x^2 = (2n+1)^2 = 4n^2 + 4n + 1$. As $n^2 + n$ can only be even (the sum is either even plus even, or odd plus odd), x^2 must be 1 more than a multiple of 8. Hence, $x^2 + y^2$ is either $0 \pmod 4 + 0 \pmod 4 \equiv 0 \pmod 4$, $0 \pmod 4 + 1 \pmod 8 \equiv 1 \pmod 4$, or $1 \pmod 8 + 1 \pmod 8 \equiv 2 \pmod 8$. However, not all numbers with those remainders are necessarily the sum of two squares.

There are some other useful relations between sum of squares. One quite obvious result is that n^2p is a sum of squares if p is, as $n^2p = n^2(x^2+y^2) = (nx)^2 + (ny)^2$. Similarly, $2p$ is a sum of two squares as well, as $2p = 2x^2 + 2y^2 = (x+y)^2 + (x-y)^2$. The converse of the previous result is true too: If $2p$ is a sum of two squares, p is. Indeed, if $2p = x^2 + y^2$, $p = \left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 = \frac{x^2+2xy+y^2}{4} + \frac{x^2-2xy+y^2}{4} = \frac{x^2+y^2}{2}$, as desired.

The last two relations between sums of squares means that we must only analyze odd sums of squares, since all even sums of squares can be derived from them: All even sums of squares can be divided by 2 continuously to get other sums of squares, eventually giving us an odd sum of squares. And all odd sums of squares generate even sums of squares by repeated doubling.

3 Initial Theorems

In the following theorems, p and q are not prime unless it is mentioned.

Theorem 1. *Let p and q be sums of squares. Then, pq is a sum of squares too.*

Proof. Let $p = x_p^2 + y_p^2$ and $q = x_q^2 + y_q^2$. Then, we simply expand pq:

$$pq = (x_p^2 + y_p^2)(x_q^2 + y_q^2) = x_p^2x_q^2 + x_p^2y_q^2 + y_p^2x_q^2 + y_p^2y_q^2.$$

If we add and subtract $2x_px_qy_py_q$ on the right side, we can get a sum of squares:

$$\begin{aligned}pq &= x_p^2x_q^2 + x_p^2y_q^2 + y_p^2x_q^2 + y_p^2y_q^2 + 2x_px_qy_py_q - 2x_px_qy_py_q \\ &= (x_p^2x_q^2 + 2x_px_qy_py_q + y_p^2y_q^2) + (y_p^2x_q^2 - 2x_px_qy_py_q + x_p^2y_q^2) \\ &= (x_px_q + y_py_q)^2 + (y_px_q + x_py_q)^2.\end{aligned}$$

□

Example 1. *We proved earlier that if p is the sum of two squares, n^2p is too. This is a specific case of Theorem 1, where we let $q = 0^2 + n^2$. Similarly, letting $q = 1^2 + 1^2$, we find that if p is a sum of two squares, $2p$ is too. The last result is a case of a future theorem that acts like the reverse of Theorem 1.*

The converse of Theorem 1 (that if pq is a sum of squares, p and q are too) would be nice, but this is easily disproven by 18 (which, in fact, is the smallest counterexample): We have $18 = 3^2 + 3^2$, but the divisors 3 and 6 are not sums of squares. However, there is a result that is *almost* the converse of Theorem 1:

Theorem 2. *If p (a prime number) and pq are sums of squares, then q is too.*

Proof. Let $p = x_p^2 + y_p^2$ and $pq = x^2 + y^2$. Then $q = \frac{x^2+y^2}{x_p^2+y_p^2}$. Clearly, $x^2 + y^2$ is a multiple of $x_p^2 + y_p^2$, and thus $x_p^2x^2 + x_p^2y^2$ is too. Obviously, $x^2x_p^2 + x^2y_p^2$ is another multiple of $x_p^2 + y_p^2$, so $(x_p^2x^2 + x_p^2y^2) - (x^2x_p^2 + x^2y_p^2)$ is a multiple as well. Simplifying and using the difference of squares factorization, we find that $x_p^2y^2 - x^2y_p^2 = (x_py - xy_p)(x_py + xy_p)$ is divisible by $x_p^2 + y_p^2$.

As $p = x_p^2 + y_p^2$ is a prime, one of the two factors, $x_py - xy_p$ or $x_py + xy_p$, is divisible by $x_p^2+y_p^2$. Thus, $x_py \pm xy_p = nx_p^2+ny_p^2$ for some n. Now, we can let $x = \mp ny_p+a$ and $y = nx_p+b$, where a and b may be negative if necessary, and where $\mp$ denotes the opposite sign of $\pm$. Then we must have $x_p(nx_p+b) \pm y_p(\mp ny+a) = nx_p^2+x_pb+ny_p^2 \pm y_pa = nx_p^2+ny_p^2$, so $x_pb \pm y_pa = 0$. Hence, $\frac{x_p}{y_p} = \pm\frac{a}{b}$, and since x_p and y_p are relatively prime (otherwise, $p = x_p^2+y_p^2$ is not prime), we have $a = mx_p$ and $b = my_p$ for some m. Therefore, $x = \mp ny_p \pm mx_p$ and $y = nx_p + my_p$, and $pq = x^2 + y^2 = n^2y_p^2 - 2mnx_py_p + m^2x_p^2 + m^2x_p^2 + 2mnx_py_p + n^2y_p^2 = (n^2 + m^2)(x_p^2 + y_p^2)$. Since $p = x^2 + y^2$, the remaining factor must be q. As $q = n^2 + m^2$, we conclude that q is indeed a sum of two squares. □

Example 2. *Again, we can prove one of our initial results using Theorem 2. Suppose $2p$ is a sum of two squares. As $2 = 1^2 + 1^2$ is a prime number, we know that p must also be a sum of two squares.*

Corollary 1. *It is limiting that we can only use a prime number for p, but fortunately, by repeatedly applying Theorem 2, we can generalize the result. Suppose that $n = qp_1p_2\cdots$ is a sum of two squares, where $p_1, p_2, \cdots$ are primes and sums of two squares. By Theorem 2, $qp_2p_3\cdots$ has to be a sum of two squares. Similarly, $qp_3p_4\cdots$ is a sum of two squares. Repeating this reasoning, we can conclude that q is also a sum of two squares.*

The contrapositive of Theorem 2 and Corollary 1 is true, although this is obvious by the rules of logic:

Theorem 3. *If pq is a sum of two squares, but q is not, then at least one of the prime factors of p is not a sum of two squares.*

Remark 1. *Euler proved the case where p is prime separately, although the proof can be condensed into one single case by letting $p = p_1p_2\cdots$. If all prime factors p_k are sums of two squares, p is also, by Theorem 1. However, as pq and p are sums of two squares, Theorem 2 implies that q is also a sum of two squares, which is a contradiction. Thus, one of the p_k cannot be a sum of two squares.*

Example 3. *An extension of Theorem 3 is that if a composite number n is a sum of two squares and has a factor that is not a sum of two squares, n must have at least two prime factors that are not sums of two squares. Indeed, letting q be the factor that is not a sum of two squares, we find that $\frac{n}{q}$ has at least one prime factor that is not a sum of two squares. Then, q must have at least one prime factor that is not a sum of two squares, as otherwise, the product q of the sums of two squares is a sum of two squares too.*

Lemma 1. *Let $p^2 + q^2$ be a sum of two relatively prime squares that is divisible by some prime n. Then we can find r and s such that $r^2 + s^2 \leq \frac{n^2}{2}$ is divisible by n.*

Before proceeding with the proof, notice that we can in fact write $r^2 + s^2 < \frac{n^2}{2}$ instead of $r^2 + s^2 \leq \frac{n^2}{2}$ whenever n is an odd prime, since then $\frac{n^2}{2}$ is not an integer and $r^2 + s^2$ cannot be equal to it.

Proof. Evidently, p and q cannot both be divisible by n. If p were, then q would have to be too as $p^2 + q^2$ has to be a multiple of n, and vice-versa. So we can write $p = an \pm r$ and $q = bn \pm s$, where r and s are positive. In fact, including the ± means that r and s can be at most $\frac{1}{2}n$, since when they are negative, we consider the cases where the remainder mod n is greater than $\frac{1}{2}n$.

So $p^2 + q^2 = (a^2n^2 + 2an + r^2) + (b^2n^2 + 2bn + s^2) = (a^2n^2 + b^2n^2 + 2an + 2bn) + r^2 + s^2$ is a multiple of n, meaning $r^2 + s^2$ is too. Also, since $r, s \leq \frac{1}{2}n$, $r^2, s^2 \leq \frac{1}{4}n^2$ and $r^2 + s^2 \leq \frac{1}{2}n^2$. Hence, we have found r and s such that $r^2 + s^2$ is divisible by n and is at most $\frac{1}{2}n^2$. □

This lemma seems very specific, and indeed it is. We will only be using this theorem to prove the following, much more versatile statement:

Theorem 4. *If a number is a sum of two relatively prime squares, it cannot be divided by a number that is not a sum of two squares.*

Proof. We can use a proof by contradiction. Suppose that $p_1^2 + q_1^2$, where $\gcd(p_1, q_1) = 1$, can actually be divided by a prime n_1 that is not a sum of two squares. We must not look at composite n_1, as if we prove that all prime factors are sum of two squares, the composite factors must be too by Theorem 1.

By Lemma 1, we can find different p_2 and q_2 such that $p_2^2 + q_2^2$ is divisible by n_1, and $p_2^2 + q_2^2 < \frac{n_1^2}{2}$. Let $p_2^2 + q_2^2 = n_1 n_2$, which gives us $n_2 < \frac{n_1}{2}$. Now we can use a technique known as "infinite descent:" As $p_2^2 + q_2^2$ is a divisible by n_2, there exist p_3 and q_3 such that $p_3^2 + q_3^2$ is divisible by n_2 and is less than $\frac{n_2^2}{2}$. If $p_3^2 + q_3^2 = n_2 n_3$, $n_3 < \frac{n_2}{2} < \frac{n_1}{4}$. We can repeat this reasoning infinitely, creating infinitely many n_k that are less than $\frac{n_1}{2}$ that divide sums of two squares but are themselves not sums of two squares. Obviously, this is impossible, as n_1 is finite. Thus, through this contradiction, we conclude that a sum of two relatively prime squares cannot be divided by numbers that are not sums of two squares too. □

4 Major Results

Finally, after these initial theorems and investigations of sums of two squares, we can prove the desired statement: When a number can only be written as a unique sums of two squares, it is prime; otherwise, it is composite.

Notice that we only consider numbers with a remainder of 1 (mod 4) here, as these are the only primes (except $2 = 1^2 + 1^2$) that can be written as a sum of two squares in the first place. Also, $1 = 0^2 + 1^2$ is neither a prime nor a composite, so it is an exception that we ignore.

Theorem 5 (Fermat's Theorem on the Sum of Two Squares)**.** *All primes that have remainder* 1 (mod 4) *can be written as a sum of two squares.*

Proof. Let the prime p equal $4n + 1$ for some n. From Fermat's Little Theorem, $a^{4n} \equiv 1 \pmod{p}$ and $b^{4n} \equiv 1 \pmod{p}$ whenever a, b are relatively prime to p (in other words, are not multiples of the prime p). So $a^{4n} - b^{4n}$ is a multiple of p. Factoring, we find that $(a^{2n} - b^{2n})(a^{2n} + b^{2n})$ is divisible by p. Since $2b^{2n}$ is not divisible by p, only one of the two factors is a multiple of p. Euler assumed that $a^{2n} - b^{2n}$ is not divisible by p, but was at first unable to prove that a and b exist that allows this to be the case. Regardless, with this assumption, we can find that $a^{2n} + b^{2n}$ must be divisible by p. Let $c = a^n$ and $d = b^n$, which gives us a sum of two squares, $c^2 + d^2$, that is divisible by p. Neither square is divisible by p, as the original a and b are not. So $m = \gcd(c, d)$ cannot be divisible by p. As $c^2 + d^2 = m^2(e^2 + f^2)$, where $c = me$ and $d = mf$, we know that $e^2 + f^2$ is divisible by p *and* $\gcd(e, f) = 1$. Using Theorem 4, we conclude that $e^2 + f^2$ cannot be divisible by any number that is not a sum of two squares. So $e^2 + f^2$ couldn't be divisible by p if p is not a sum of two squares, so, by proof by contradiction, p must always be a sum of two squares.

We still need to prove that a and b can be found such that $a^{2n} - b^{2n}$ is not divisible by p. Euler published the following proof for this in *Proof of a theorem of Fermat that every prime number of the form* $4n + 1$ *is a sum of two squares* (E241):

We use a proof by contradiction: Suppose no such a and b exist. Then, we can select $a = 2$ and $b = 1$, $a = 3$ and $b = 2$, and so on until $a = 4n$ and $b = 4n - 1$. All $a^{2n} - b^{2n}$, their differences, the differences of the differences, etc. are multiples of p.

Notice that this sequence consists of the differences of consecutive terms of the sequence $1^{2n}, 2^{2n}, 3^{2n}, \cdots$. We will prove that if we subtract consecutive terms k times (using the resulting sequence for the next difference) of the sequence $1^k, 2^k, 3^k, \cdots$, we get the constant term $k!$.

The first difference sequence is $(x+1)^k - x^k$, the second is $(x+2)^k - 2(x+1)^k + x^k$, the third is $(x+3)^k - 3(x+2)^k + 3(x+1)^k - x^k$, and so on. Ultimately, the k-th difference is $(x+k)^k - \binom{k}{1}(x+k-1)^k + \binom{k}{2}(x+k-2)^k + \cdots$. In particular, the first difference has degree $k-1$, the second $k-2$, and the k-th has degree 0 - i.e. the k-th differences are constant and do not depend on x.

We have $m = (k+1)^k - \binom{k}{1}(k)^k + \binom{k}{2}(k-1)^k + \cdots$ as the k-th difference of the sequence $1^k, 2^k, 3^k, \cdots$, where $x = 1$, and $n = (k+1)^{k+1} - \binom{k+1}{1}(k)^{k+1} + \binom{k+1}{2}(k-1)^{k+1} + \cdots$ for the $(k+1)$-th difference of the sequence $1^{k+1}, 2^{k+1}, 3^{k+1}, \cdots$ where $x = 0$. Note that because the k-th and $(k+1)$-th differences of either sequence are constant, we can use any x we desire, in this case $x = 0$ and $x = 1$. Comparing the terms $\binom{k}{\ell}(k+1-\ell)^k$ in m and $\binom{k+1}{\ell}(k+1-\ell)^{k+1}$

in n, we find that the terms for n are $(k+1)$ times as great as the terms of m:

$$\begin{aligned}\binom{k+1}{\ell}(k+1-\ell)^{k+1} &= \frac{(k+1)\cdot k\cdot\dots\cdot(\ell+1)}{(k+1-\ell)!}(k+1-\ell)^{k+1} \\ &= (k+1)\frac{k\cdot(k-1)\cdot\dots\cdot(\ell+1)}{(k-\ell)!}(k+1-\ell)^{k} \\ &= (k+1)\binom{k}{\ell}(k+1-\ell)^{k}.\end{aligned}$$

So $n=(k+1)m$. In other words, the first term in the $(k+1)$-th difference sequences of $1^{k+1}, 2^{k+1}, 3^{k+1}, \cdots$ are always $k+1$ times the first term in the k-th difference sequences of $1^k, 2^k, 3^k, \cdots$. The first term in the 1st difference sequence of $1, 2, 3, \cdots$ is 1, so the first term in the 2nd difference sequence is 2, in the 3rd difference sequence is 6, etc. Ultimately, the first term in the k-th difference sequence of $1^k, 2^k, 3^k, \cdots$ is $k!$.

Therefore, the first term in the $(2n)$-th difference sequence of the sequence $1^{2n}, 2^{2n}, 3^{2n}, \cdots$ is $(2n)!$. The first term of the $(2n-1)$-th difference sequence of our original sequence $2^{2n}-1^{2n}, 3^{2n}-2^{2n}, \cdots$, which is also equal to $(2n)!$, must clearly be divisible by $p=4n+1$, but $(2n)!$ is not divisible by $4n+1$ as the prime is not included in the factorial product. Due to this contradiction, we conclude that there must exist some a and b such that $a^{2n}-b^{2n}$ is not divisible by p. □

However, this theorem is not very useful on its own, as we already need to know the prime that the theorem is applied on. Therefore, we would like to find a simple method to check whether a number is prime. The long-winded proof above is still worthwhile, since Theorem 5, in conjunction with Theorems 6 and 7 that we will prove now, allows us to find *all* primes of the form $1 \pmod 4$.

Theorem 6. *If a number with remainder* $1 \pmod 4$ *is a unique sum of two squares that are relatively prime to each other, it is a prime.*

Proof. Instead of proving this theorem directly, we instead prove the equivalent contrapositive: If the number n has a remainder $1 \pmod 4$ and is a composite, it can only be written as two different sums of two relatively prime squares or it cannot be written as a sum of such squares at all. By Theorem 5, we know that n cannot be divided by numbers that are not sums of two squares. So $n=(p^2+q^2)(r^2+s^2)$, where all p, q, r, s are nonzero.

However, we must show that we can actually find nonzero p, q, r, s that can factor n like this. If p is 0 and q is 1 for every factorization, n cannot be factored into sums of two squares that are not 1 or n, even though these should be the only types of factors by Theorem 5. Thus, n is prime, which is a contradiction. If $p=0$ but $q \neq 1$, then n can only be written as a sum of two squares that are not relatively prime. This still satisfies the contrapositive. The same reasoning works for r and s.

Assuming now that p, q, r, s are non-zero, we have two possible squares from our work in Theorem 1:

$$n=(pr+qs)^2+(qr-ps)^2$$

$$n=(pr-qs)^2+(qr+ps)^2.$$

As $pr - qs$, $pr + qs$ and $qr + ps$, $qr - ps$ cannot be equal to each other (as p, q, r, s are nonzero), the only way for the two sums to be the same is when $pr + qs = \pm(qr + ps)$ and $qr - ps = \pm(pr - qs)$, which both simplify to $pr + qs - qr - ps = (p - q)(r - s) = 0$ or $pr + qs + qr + ps = (p + q)(r + s) = 0$. So $p = \pm q$ or $r = \pm s$, but then n is divisible by $p^2 + q^2 = 2p^2$ or $r^2 + s^2 = 2r^2$. n is one more than a multiple of 4, i.e. odd, so it cannot be divisible by these even numbers. Thus, our two sums of two squares are always different when n is composite and our proof is complete. □

However, we *still* cannot find with absolute certainty all primes 1 (mod 4) using Theorem 6. For instance, there might be a prime that is the sum of two squares in two different ways. Fortunately, we can prove that this is impossible with the following theorem, which coincidentally gives us a condition for composite numbers too:

Theorem 7. *If a number can be written as two different sums of two squares, then it is a composite number.*

Proof. Assume that $n = a^2 + b^2 = c^2 + d^2$. We can assume that the two squares in a sum cannot be equal to each other, as otherwise n is divisible by 2. Without loss of generality, we let $a > b$ and $c > d$. In addition, $a \neq c$ and $b \neq d$ as we need two *different* sums.

If $a > c$, then $b < d$ such that $a^2 + b^2 = c^2 + d^2$. So let $a = c + x$ and $d = b + y$, where $x, y \neq 0$. Then n equals both $(c+x)+b^2 = c^2+b^2+2cx+x^2$ and $c^2+(b+y)^2 = c^2+b^2+2by+y^2$, so $2cx + x^2 = 2by + y^2$. Let $2cx + x^2 = 2cy + y^2 = xyz$, since the expressions are multiples of x and y. Then $c = \frac{xyz-x^2}{2x} = \frac{yz-x}{2}$ and $b = \frac{xz-y}{2}$, and therefore $a = \frac{yz-x}{2} + x = \frac{yz+x}{2}$ and $d = \frac{xz-y}{2} + y = \frac{xz+y}{2}$. Therefore:

$$\begin{aligned} n = a^2 + b^2 &= (\frac{yz + x}{2})^2 + (\frac{xz - y}{2})^2 \\ &= \frac{y^2z^2 + 2xyz + x^2}{4} + \frac{x^2z^2 - 2xyz + y^2}{4} \\ &= \frac{(x^2 + y^2)z^2 + x^2 + y^2}{4} = \frac{(x^2 + y^2)(z^2 + 1)}{4}. \end{aligned}$$

As squares can only be 0 or 1 (mod 4), $z^2 + 1$ cannot be a multiple of 4. Thus, $x^2 + y^2$ must be a multiple of 4. As $x, y \neq 0$, $x^2 + y^2$ cannot be equal to 4, so when we simplify the fraction for n, we will have $z^2 + 1$ times the remaining factor of $x^2 + y^2$, which is not 1. In other words, n has two factors and is composite. □

However, knowing that a number is composite is not very useful on its own. We would much prefer to know at least one divisor of the composite number, so that we may begin finding its prime factorization. Fortunately, with the help of Theorem 4, we are able to do so.

Assume that $n = a^2 + b^2 = c^2 + d^2$. We know that n is composite. If a and b (or c and d) are not relatively prime, we can write $x = \frac{a}{m}$ and $y = \frac{b}{m}$, where $m = \gcd(a, b)$. So $\frac{n}{m^2}$ is a sum of relatively prime squares, meaning we can apply Theorem 4. Thus, $\frac{n}{m^2}$ cannot be divided by any number that is not a sum of two squares. We can write $\frac{n}{m^2} = (t^2+u^2)(r^2+s^2)$, or $n = ((mt)^2 + (mu)^2)(r^2 + s^2) = (p^2 + q^2)(r^2 + s^2)$. r and s are made to be relatively prime here.

Due to Theorem 1, we know that $a = pr + qs$, $b = ps - qr$, $c = ps + qr$, and $d = pr - qs$ work as values. In particular, a and b (and c and d) are both divisible by m, as we assumed before. Thus, we can actually solve for r and s: $c - b = ps + qr - (ps - qr) = 2qr$ and $a - d = pr + qs - (pr - qs) = 2qs$, meaning $\frac{c-b}{a-d} = \frac{r}{s}$. Since r and s were assumed to be relatively prime, we should simplify $\frac{c-b}{a-d}$ as much as we can before computing r and s. After finding r and s, we now know that $r^2 + s^2$ is a factor of n.

Note that if $r^2 + s^2$ happens to be even, but n is not, we halve $r^2 + s^2$ to get a true factor of n. This is because $4n$ would give us $(2a)^2 + (2b)^2 = (2c)^2 + (2d)^2 = 4n$, meaning that $r^2 + s^2$ (where $\frac{r}{s}$ is still $\frac{2c-2b}{2a-2d} = \frac{c-b}{a-d}$) is a factor of $4n$. So $\frac{r^2+s^2}{2}$ has to be a factor of n. Also, $r^2 + s^2$ cannot be a multiple of 4 as the only way to have the remainder $0 \pmod 4$ is when r and s are both even, which is never the case as r and s are defined to be relatively prime.

In addition, we could switch the a and b, and the c and d in order to get some other factors. This technique to find factors is known, unsurprisingly, as Euler's factorization method.

Finally, if the number has remainder $1 \pmod 4$, but cannot be written as a sum of two squares, it must be composite, or else the number would contradict Theorem 5. Unfortunately, no factors can be found without relying on the typical trial and error.

5 Some Final Experimentation!

This method is quite useful, as we can not only determine whether a number is prime or not, but also compute at least one factor. However, it can be tedious to check all squares up to $\sqrt{\frac{n}{2}}$ (if $a, b > \sqrt{\frac{n}{2}}$, then $a^2 + b^2 > \frac{n}{2} + \frac{n}{2} = n$). Fortunately, we know that squares can only end in the units digits of $0, 1, 4, 5, 6$, and 9. So if we subtract a square from the number we are analyzing and we get a number that ends in $2, 3, 7$, or 8, we know that we cannot get a sum of squares with that subtracted square. In fact, if we know the units digit of the number we are testing, we can narrow down the possible units digits of our subtracted square even more.

If the number has an even units digit, it is even and therefore a composite (with the obvious exception of 2). A units digit of 5 also means that our number is divisible by 5. If the number ends in 1, the square can only end in $0, 1, 5$, or 6. If the number has a units digit of 3, the square must end in 4 or 9. If 7 is the units digit of our number, the square ends in 1 or 6. Finally, with a units digit of 9, the square can only end in $0, 4, 5$, or 9.

Euler wasn't satisfied with this, however, as squaring numbers in the first place can be difficult. Thus, he devised a method that only requires addition and subtraction of terms after squaring an initial number. To speed up the square computations, we can begin with the largest possible numbers n with the correct units digits to be squared. Then, $(n - 10k)^2$ has the same units digit, for any positive integers k such that $n - 10k > 0$. To go from $(n - 10k)^2$ to $(n - 10k - 10)^2$, we add $(n - 10k - 10)^2 - (n - 10k)^2 = (-10)(n - 10k - 10 + n - 10k) = -20n + 200k + 100$, meaning we can subtract $20n - 200k - 100$ from the previous square subtraction to get the next. This is much easier than computing the next squares, and the resulting differences, manually.

Euler ends his paper by applying his method to a variety of large primes and composites, which, even to this day, is a quite impressive accomplishment. For instance, Euler showed that 82421, 100981, and 262657 are prime, while $1000009 = 292 \cdot 3413$ and $32129 = 19^2 \cdot 89$ are composite. He also proved that 233033 is composite, although he was only able to find the factorization $467 \cdot 499$ by testing because 233033 is not a sum of two squares.

However, for the sake of length, we will be using a much smaller number as an example: We will deduce whether 1853 (which is $1 \pmod 4$), since Euler's method is only useful for such numbers) is a prime or not. No primes less than 10 are divisors, as we can see with our typical divisibility rules. While we could test all primes up to about 45, let's use Euler's method to speed up the process. We must only check the numbers up to $\sqrt{\frac{1853}{2}}$, or about 30. Squares with unit digits of 1, 5, 6, or 0 do not work, as otherwise we are left with a number with units digits of 2, 3, 7, or 8, which is not a square. Thus, we only check the squares $4, 9, 49, 64, 144, 169, 289, 324, 484, 529, 729,$ and 784. Subtracting, we get the possible squares $1849, 1844, 1804, 1789, 1709, 1684, 1564, 1529, 1369, 1324, 1124,$ and 1069. By comparing these numbers with known squares ($30^2 = 900$ and $40^2 = 1600$), we find that $1849 = 43^2$ and $1369 = 37^2$, so we have the sums $2^2 + 43^2$ and $22^2 + 37^2$ for 1853. Hence, 1853 is composite.

We can also find a factor $r^2 + s^2$ of 1853 using our formula $\frac{r}{s} = \frac{c-b}{a-d}$. Plugging in $a = 2$, $b = 43$, $c = 22$, and $d = 37$, we get $\frac{c-b}{a-d} = \frac{-21}{-35} = \frac{3}{5}$, meaning $\frac{3^2+5^2}{2} = 17$ is a factor. Knowing this, we find that $1853 = 17 \cdot 19$. Admittedly, we could have found these factors rapidly through trial and error with primes in this simple example, but for much larger primes and composites, this method is very useful.

While Euler's primality test is especially useful for manual computations, it can also be implemented into programs that check for primes in order to make them run faster and more efficiently. For instance, the following Python code can deduce that 3543553 is a composite number with a factor of $2^2 + 3^2 = 13$, and indeed $3543553 = 13 \cdot 272581$. Running the program again for 272581, we find that it is prime. So $13 \cdot 272581$ is the prime factorization for 3543553.

```python
import math

def euler_prime_test(n):
    squares = []

    for p in range(math.floor((n/2)**0.5)+1):
        q = (n-p**2)**0.5

        #This tests whether q is an integer.
        if q == math.floor(q):
            squares.append([p, math.floor(q)])

        if len(squares) == 2:
            break

    if len(squares) == 1:
        return 'prime'
    elif len(squares) == 2:
        return 'composite factors: ' + \
               str(abs((squares[1][0]- squares[0][1])// \
               math.gcd(squares[1][0]-squares[0][1],squares[0][0]-squares[1][1]))) + \
               ' ' + str(abs((squares[0][0]-squares[1][1])// \
               math.gcd(squares[1][0]-squares[0][1],squares[0][0]-squares[1][1])))
    else:
        return 'composite'
```

Even though this code is not optimized with the units digits test we found earlier, it is able to state whether 3543553 and 272581 are prime in just two seconds! Note that this program only works for numbers equivalent to 1 (mod 4), since our original conditions only work, or at least are only useful, for this remainder.

6 Conclusion

Ultimately, one of the most fundamental issues in number theory is finding primes, and Euler's discovery allows us to find them. In addition, the factors of composites can be found in about two thirds ($\frac{1}{\sqrt{2}} \approx 0.707$) the time we would otherwise need. While more efficient primality tests have been found since, such as the elliptic curve or Miller-Rabin primality tests, although they are far beyond the scope of this paper, this method is a nice introduction to the deep, interesting search for primes, not only on paper, but also on screens.