TERNARY ARITHMETIC, FACTORIZATION, AND THE CLASS NUMBER ONE PROBLEM

ARAM BINGHAM

Abstract. Ordinary binary multiplication of natural numbers can be generalized in a non-trivial way to a ternary operation by considering discrete volumes of lattice hexagons. With this operation, a natural notion of '3-primality' – primality with respect to ternary multiplication – is defined, and it turns out that there are very few 3-primes. They correspond to imaginary quadratic fields $\mathbb{Q}(\sqrt{-n})$, $n > 0$, with odd discriminant and whose ring of integers admits unique factorization. We also present algorithms for determining representations of numbers as ternary products, as well as related algorithms for usual primality testing and integer factorization.

1. Breaking the Rules

When ideas become engrained, it can be hard to imagine any other possibility. Many students have this experience with arithmetic, so that the first time one encounters alternative number systems like finite fields or modular arithmetic, it seems sort of incredible.

In the spirit of questioning basic assumptions, this article will generalize integer arithmetic in another sideways fashion which is (hopefully) still grounded enough in geometry so as to not seem arbitrary. We will achieve this by examining the properties of the arithmetic operations themselves, and asking how one of these properties – symmetry – can be extended to a new kind of operation. Chasing down the consequences of this new operation a bit leads to a surprising new perspective on an old problem in number theory, and a few applications to standard arithmetic.

So let's start with the absolute basics. What is multiplication? That is, say you want to multiply two whole numbers, a and b. What do you do to find the product ab?

Two possibilities: add a to itself b many times, or add b to itself a many times. This is often taken as the definition of multiplication, by which one could regard $a \cdot b$ as simply shorthand notation rather than a separate algebraic operation. But the fact that either one of

$$\overbrace{a + a + \cdots + a}^{b \text{ times}} \qquad \text{or} \qquad \overbrace{b + b + \cdots + b}^{a \text{ times}}$$

works allows us to say that multiplication is **commutative**.

Another way to reproduce this operation is the following. Draw a parallel lines on a piece of paper. Now draw b lines which are parallel to each other but perpendicular to the a parallel lines you drew first. The

New Orleans, LA

E-mail address: `abingham@tulane.edu`.

Date: Jan. 2020.

2010 *Mathematics Subject Classification.* 11A05, 11H06, 11Y05.

number of intersection points of the two sets of lines is your product ab.[1] One sees the commutativity of multiplication in the fact that the number of intersection points doesn't change when you rotate the whole picture by $90°$.

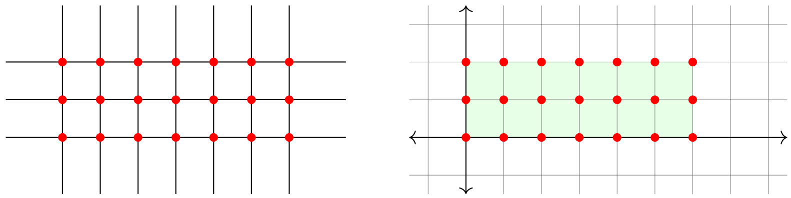


FIGURE 1. 3 times 7 is 21

Let's think of this a little bit differently. Pick two independent vectors $\vec{v}$, $\vec{w}$ in the plane $\mathbb{R}^2$. Then these vectors generate a **lattice** Λ in the plane by taking all integer linear combinations of the vectors $\vec{v}$ and $\vec{w}$, which are called the **basis** of the lattice. That is,

$$\Lambda = \{a\vec{v} + b\vec{w} \mid a, b \in \mathbb{Z}\}.$$

The next definition will allow us to interpret multiplication a kind of **discrete volume**.

Definition 1. Given a lattice $\Lambda \subset \mathbb{R}^2$, a **lattice polygon** is a polygon in the plane whose vertices are lattice points.

Since the directions and magnitudes of the basis vectors don't matter much for the purpose of studying whole-number multiplication, we might as well use the unit vectors in the x- and y-directions so that the resulting lattice is actually $\mathbb{Z}^2 = \{(a, b) \mid a, b \in \mathbb{Z}\}$. Then the product ab is realized as the number of lattice points inside (or on the boundary) of the lattice rectangle with corners at $(0, 0)$, $(b - 1, 0)$, $(0, a - 1)$ and $(a - 1, b - 1)$ Slightly restated, ab is the discrete volume of the lattice rectangle with a points along two opposite edges in the vertical direction and b lattice points along the opposite edges in the horizontal direction; see the right side of Figure 1. This view of multiplication allows us to codify the following simple observation.

Fact 1. A number is prime if and only if it cannot be represented as the discrete volume of a $\mathbb{Z}^2$ lattice rectangle with edges in the horizontal and vertical directions and where each edge contains at least two lattice points.

The problem of studying discrete volumes of general lattice polygons (or polytopes, in higher dimensions) leads to what is now called *Ehrhart theory*. However we are restricting away from this theory by using polygons with edges along particular directions – namely, those of the points *nearest* to a given lattice point[2] – and consequently some of the same symmetries as the lattice that houses them. Again, our purpose here is just to characterize multiplication in geometric terms so that we can see how it might be generalized.

[1] Of course, the angle between the two sets of parallel lines can vary, and we would still get the answer to the multiplication problem $ab =?$ as the number of intersection points of the two sets of lines.

[2] This idea is also useful for classifying 2-dimensional lattices.

With this model, the commutativity of multiplication could be viewed in the preservation of discrete volume when interchanging which lattice direction corresponds to which factor. The lattice $\mathbb{Z}^2$ is especially nice because then this change is also realized by a rotational symmetry. That is, we can rotate a $\mathbb{Z}^2$ lattice rectangle by 90° and view the result as the multiplication reversed: ba instead of ab. If we want to look for sensible alternatives to standard multiplication *and* maintain commutativity, it seems we might do well to stick to lattices with rotational symmetry. Guiding this search is the *crystallographic restriction theorem*, which says that lattices in $\mathbb{R}^2$ can only have rotational symmetry of order 2, 3, 4, or 6 [Cox69, p. 60-61]. This can also be seen as a restriction on which regular polygons can occur as lattice polygons.

Let us be greedy and opt for maximal symmetry: the 6-fold rotational symmetry offered by the **hexagonal lattice**. This means that a rotation of the plane by 60° about any lattice point sends lattice points to other lattice points. Furthermore, from any lattice point P there are six lattice points which are all nearest neighbors to P, and these six points come in pairs that are in opposite directions from P. Compare this (Figure 2) to the four nearest neighbors of a point in the $\mathbb{Z}^2$ lattice, neighbors which come in pairs in opposite directions along two lines through the point. The four-fold symmetry of $\mathbb{Z}^2$ lent itself to commutativity of the two arguments of the multiplication operation. But with 6-fold symmetry we might expect a higher order commutativity – commutativity of *three* arguments.

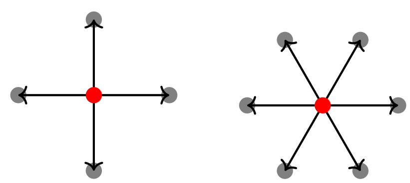


FIGURE 2. Nearest neighbors in a square ($\mathbb{Z}^2$) lattice and a hexagonal lattice.

Restriction. From now on, the sides of lattice polygons may only lie in the direction of nearest neighbors from the lattice points that are the vertices of the polygon.

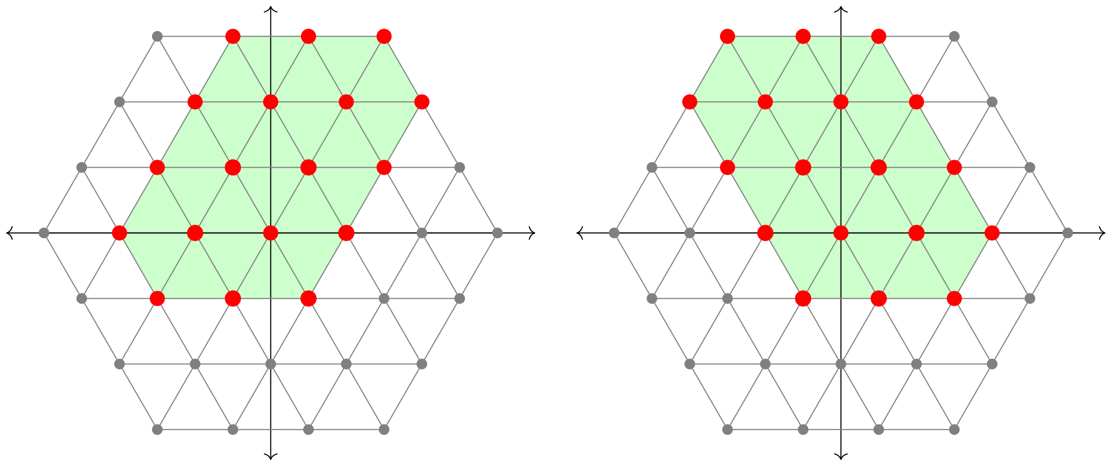
Recall that the **arity** of a function or algebraic operation refers to the number of inputs or arguments it takes. Ordinary addition and multiplication are *binary* operations, while other operations like the *successor* function which takes a natural number n and spits out $S(n) = n+1$ is *unary*.[3] Binary operations could simply be iterated to make operations of higher arity, and some of the algebraic properties that we study (e. g. associativity) are really about how the operation behaves in iteration.

However, let us introduce a true **ternary product**, which is not merely repeated multiplication, but bears some of the same nice properties: namely, commutativity, and the presence of a *multiplicative identity*, which naturally must be the number 1. We will denote this product as

$$\langle -, -, - \rangle : \mathbb{N}^3 \to \mathbb{N},$$

and define it, in analogy with our lattice model of binary multiplication, as the function which takes the triplet (a, b, c) to the number of lattice points inside the equiangular lattice hexagon with a points along two opposite edges, b points along the next pair of edges, and c points along the final pair. Illustrations are given in Figures 3 and 4.

[3]Throughout this manuscript, we take the set of natural numbers $\mathbb{N}$ does not include 0.



(A) $\langle 2, 3, 4\rangle = 18$ (B) $\langle 4, 3, 2\rangle = 18$

Figure 3. Commutativity of ternary multiplication under reflection.

2. Properties of Ternary Arithmetic

A lattice hexagon representing the product $\langle a, b, c\rangle$ can be acted upon by any of the symmetries of the lattice. If we consider only those symmetries which have fix the origin, then these are generated by a rotation by $60°$ and a reflection across the y-axis. This is the same as the group of symmetries of any regular lattice hexagon centered at the origin, and so the group generated is the dihedral group of order six which is also isomorphic to the symmetric group of permutations of three letters. Under this action, the discrete volume of any lattice hexagon is preserved, and so we have that $\langle -, -, -\rangle$ is fully commutative as a ternary product.

Notice that if we put a 1 into one of the arguments of this product, one of the pairs of sides of the hexagon degenerates to a single point and we instead have a parallelogram (see Figure 4). The discrete volume of this parallelogram is then just the value of the binary product of the other two arguments, so we observe ordinary multiplication as a specialization of the ternary product. Further, if we have a 1 appearing twice as an argument, then $\langle 1, 1, n\rangle$ leads to just a row of n points (with discrete volume n), showing that 1 indeed behaves as a multiplicative identity.

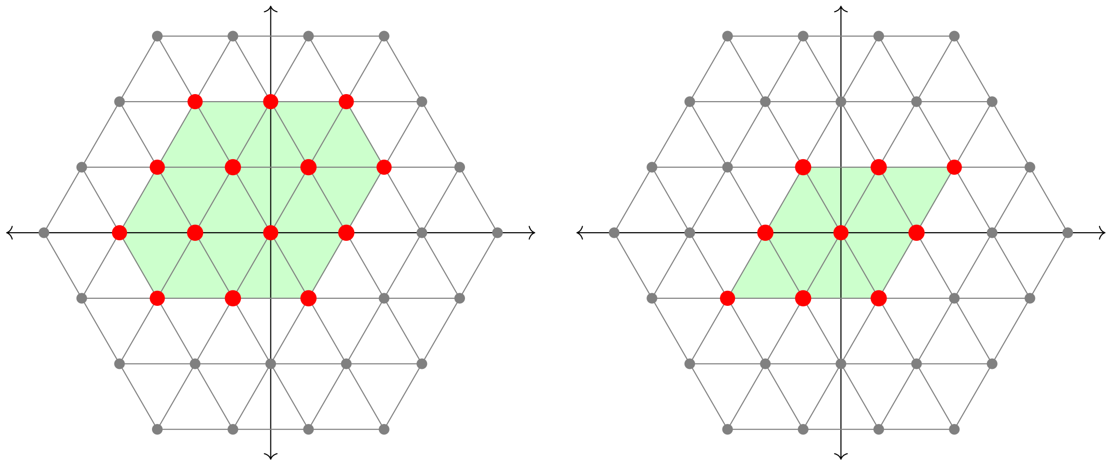
By analogy with Fact 1, we make the following definition.

Definition 2. We will say that a natural number n is **3-prime** if it can not be represented as the discrete volume of an equiangular lattice hexagon for which at least two pairs of opposing sides have at least two points. Equivalently, n is 3-prime if there is no choice of x, y, z such that $\langle x, y, z\rangle = n$ other than $\langle 1, 1, n\rangle = n$ and permutations of these inputs.

To avoid confusion with the usual definition of primality, from now on we will say that a natural number n is **2-prime** to mean that its only natural number factors are 1 and n.[4] We shall also say that a number is "2-composite" or "3-composite" to mean that it is not 2-prime or not 3-prime, respectively. An immediate consequence of this definition is that 3-primality implies 2-primality, but not the other way around.

[4]Under binary multiplication, of course.

For instance $\langle 2,2,2\rangle = 7$ is not 3-prime, but 2, 3 and 5 are still 3-prime, and with a little checking you can convince yourself that 11 is as well. This begs the following question.



(A) $\langle 2,3,3\rangle = 14$ (B) $\langle 1,3,3\rangle = 9$

FIGURE 4. Ternary multiplication includes binary multiplication.

Question: Which natural numbers are 3-prime?

To answer this question, first we need a better understanding of ternary multiplication. Since the operation is fully symmetric, it is natural to expect that it can be represented by a symmetric polynomial in three variables.

Proposition 1. *The ternary product can be written*

$$\langle x,y,z\rangle = xy + yz + zx - x - y - z + 1.$$

Proof. We have seen that $\langle x,y,1\rangle = xy$. Observe that if you increase the z argument to 2, you would add a strip of $x + y - 1$ points along two consecutive edges of the parallelogram given by $\langle x,y,1\rangle$ (see again Figure 4). If you increase z to 3, you add another strip of $x+y-1$ points beside the previous strip, and so on. We see then that

$$\langle x,y,z\rangle = xy + (z-1)(x+y-1) = xy + yz + xz - x - y - z + 1$$

as claimed. □

Scholars of symmetric polynomials will recognize this as an alternating sum of **elementary symmetric polynomials**,

$$\langle x,y,z\rangle = e_2(x,y,z) - e_1(x,y,z) + e_0(x,y,z).$$

However, if you want to mentally compute some ternary products, you may find the formula

$$\langle x,y,z\rangle = xyz - (x-1)(y-1)(z-1)$$

somewhat more manageable.

Now then, how can we determine if a number n is 3-prime? When studying 2-primes, the first method one usually learns is trial division. Trial division is souped up to give the **Sieve of Eratosthenes**, used to produce the list of 2-primes up to a given N by crossing off multiples of those 2-primes which are at most $\sqrt{N}$. For a 2-prime p, this amounts to eliminating all of the numbers greater than p in the congruence class 0 mod p.

The proof of Proposition 1 indicates how we might sieve for 3-primes. Suppose that $p = x + y - 1$ is a 2-prime, where x and y are natural numbers. We see that

$$\langle x, y, z\rangle = xy + (z-1)(x+y-1) = xy + (z-1)p$$

fails to be 3-prime for all $z \geq 2$, thus we can also eliminate all of the numbers of the congruence class xy mod p which are greater than xy by varying the choice of z in the product $\langle x, y, z\rangle$.

For example, the 2-prime 3 can be written as

$$3 = 3 + 1 - 1 \qquad \text{or} \qquad 3 = 2 + 2 - 1.$$

The first case corresponds the choice of $x = 3$, $y = 1$, which produces the class of ternary products $\langle 3, 1, z\rangle = 3z$ and eliminates numbers above $3 \cdot 1 = 3$ in the congruence class 0 mod 3 from 3-primality, as in the usual 2-primality sieve. But when we take $x = 2$, $y = 2$, the products of the form

$$\langle 2, 2, z\rangle = 4 + (z-1)(2+2-1) = 4 + (z-1)3$$

eliminate those numbers that are above 4 and in the congruence class of $4 \equiv 1 \bmod 3$ from possible 3-primality.

We see that for an odd 2-prime p, there are $\frac{p+1}{2}$ choices of (unordered) pairs x and y such that $p = x + y - 1$. The next proposition shows that each choice produces a distinct congruence class xy mod p.

Proposition 2. *Let x and w be distinct natural numbers between 1 and a 2-prime p, and $w \neq p + 1 - x$. Then the congruence classes of $x(p+1-x)$ and $w(p+1-w)$ modulo p are distinct.*

Proof. We will show the equivalent statement that $x(p+1-x) \equiv w(p+1-w) \bmod p$ implies that $x = w$ or $x = p + 1 - w$. Supposing we have

$$x(p+1-x) \equiv x - x^2 \bmod p \qquad \text{and} \qquad w(p+1-w) \equiv w - w^2 \bmod p,$$

satisfying $x - x^2 \equiv w - w^2 \bmod p$. Then

$$\begin{aligned} w^2 - x^2 - w + x &\equiv 0 \bmod p, \quad \text{so} \\ (w-x)(w+x-1) &\equiv 0 \bmod p. \end{aligned}$$

So either p divides $w - x$ or p divides $w + x - 1$. Since both x and w are between 1 and p, we have

$$1 - p \leq w - x \leq p - 1 \qquad \text{and} \qquad 1 \leq w + x - 1 \leq 2p - 1.$$

Then in the first case, it can only be that $w - x = 0$, while in the other case $w + x - 1 = p$. $\square$

This has major consequences for how many numbers can be 3-prime! Recall Dirichlet's theorem on arithmetic progressions.

Theorem (Dirichlet)**.** *Let p be a 2-prime and $1 \leq k < p$. Then there are infinitely many 2-primes of the form $k + mp$, where $m \in \mathbb{N}$.*

A fuller statement of Dirichlet's theorem says that there is the same "proportion" of primes in each nonzero congruence class modulo p [Apo76, Chap. 7]. There are $p-1$ such classes for each p, and Proposition 2 says that half of them are ruled out from the possibility of 3-primality, in addition to the congruence class 0 mod p.

To continue to develop our sieve, we have the the following lemma which tells us that the business of ruling out congruence classes only needs to happen at the 2-primes – nothing new comes from ternary products of the form $\langle x, y, z\rangle$ where $x+y-1$ is 2-composite.

Lemma 1. *Let $m = ab = x+y-1$. Then there are natural numbers v and w such that $v+w-1 = a$ and $xy \equiv vw \bmod a$.*

Proof. We can write

$$xy = x(ab+1-x) = xab + x - x^2 \equiv x - x^2 \bmod a.$$

Let v be the least natural number representative of the congruence class $x \bmod a$, and set $w = a+1-v$. Then

$$vw = v(a+1-v) = va + v - v^2 \equiv v - v^2 \bmod a.$$

Since v and x are in the same congruence class modulo a, the claim is proved. □

Now suppose we are trying to determine all of the 3-primes up to some number N. We know that first we can eliminate the 2-primes below N using the Sieve of Eratosthenes, and now Lemma 1 and Proposition 2 say that we further need to eliminate some congruence classes modulo p for some of the 2-primes below N. But how far do we need to go up in these 2-primes?

Let us write **TS**[5] to denote our sieve for 3-primes. We will view **TS** as consisting of a succession of stages TS_k where the Sieve of Eratosthenes is the "zeroth" step TS_0. To restate, the Sieve of Eratosthenes eliminates the products of the form $\langle 1, p, z\rangle$ for $z \geq 2$ by allowing us to add $(z-1)p$ to the product $p \cdot 1 = p$. Here's another small efficiency: starting from the first 2-prime 2 and as p increases towards $\sqrt{N}$, one only really needs to cross off products $\langle 1, p, z\rangle$ with $z \geq p$, as those for $z < p$ will already have been cancelled as products of lesser 2-primes.

The next stage (TS_1) of our sieve for 3-primes will eliminate products of the form $\langle 2, p-1, z\rangle$. Lemma 1 tells us that this can only possibly cross out new things if all of the sums

$$2 + (p-1) - 1, \qquad 2 + z - 1, \qquad \text{and} \qquad (p-1) + z - 1$$

are 2-primes. However, since we will also proceed through this stage using p's in increasing order from among the 2-primes produced by TS_0, the elimination of a product will be redundant if $2+z-1$ (which is possibly smallest among the three sums) is a 2-prime less than p. Thus, we can start from $z \geq p-1$ at this stage. Furthermore, this should be done only for those 2-primes p such that the first possible interesting product

$$\langle 2, p-1, p-1\rangle \leq N.$$

Writing

$$\langle 2, p-1, p-1\rangle = 2(p-1) + (p-2)p = p^2 - 2,$$

[5] For "ternary sieve."

we see that the TS_1 stage uses those 2-primes such that $p \leq \sqrt{N+2}$.

On to the next stage, TS_2, wherein we eliminate products of the form $\langle 3, p-2, z\rangle$. By considerations similar as in the previous case, this process only needs to start when $z \geq p-2$, and therefore only for 2-primes such that

$$\langle 3, p-2, p-2\rangle = 3(p-2) + (p-3)p = p^2 - 6 \leq N,$$

or $p \leq \sqrt{N+6}$.

One begins to see a pattern now: TS_3 eliminates numbers at least $\langle 4, p-3, p-3\rangle$ and in the same congruence class modulo p as this product for $p \leq \sqrt{N+12}$, and so on. We also see the triangular number $T_k = \frac{k(k+1)}{2}$ entering: TS_k starts at $\langle k+1, p-k, p-k\rangle$ and runs through all 2-primes $p \leq \sqrt{N+2T_k}$. The next question is how many stages do we need to complete **TS**?

To avoid further unnecessary redundancy, we should keep $k+1 \leq p-k$ in the product $\langle k+1, p-k, z\rangle$.[6] Since $z \geq p-k$ during TS_k, if we want to maximize k but not go past N we that the smallest possible product with large k satisfy

$$\langle k+1, k+1, k+1\rangle = 3k^2 + 3k + 1 \leq N.$$

Completing the square and solving the inequality, one finds that

$$k \leq \sqrt{\frac{4N-1}{12}} - \frac{1}{2} \tag{1}$$

is a sufficient bound, though possibly not necessary, as the product $\langle k+1, k+1, k+1\rangle$ will only eliminate a new congruence class if $p = 2k+1$ is 2-prime, again by Lemma 1. Now we can state the full ternary sieve.

Algorithm (Ternary Sieve)**.** To determine the 3-primes less than a given N, list the numbers from 2 to N and perform the following elimination procedure **TS**:

(1) TS_0: Perform the Sieve of Eratosthenes, and create the list auxiliary list $\Pi_2(N)$ of 2-primes at most N.
(2) For each $1 \leq k \leq \sqrt{\frac{4N-1}{12}} - \frac{1}{2}$ perform elimination step TS_k as follows. For each $p \in \Pi_2(N)$ such that $p \leq \sqrt{N+2T_k}$, eliminate the numbers up to N of the form $\langle k+1, p-k, p-k\rangle + mp$, for $m \in \mathbb{N}$.
(3) Those numbers that remain among the numbers from 2 to N constitute the list $\Pi_3(N)$ of 3-primes which are at most N.

This algorithm can be implemented on a computer without too much trouble, and a search for the 3-primes up to 10,000,000 reveals a very short list.

$$2,\ 3,\ 5,\ 11,\ 17,\ 41$$

A quick trip to OEIS (A014556) reveals that these are "Euler's 'Lucky' numbers," those 2-primes p such that

$$n^2 - n + p \tag{2}$$

[6]Otherwise, once $k+1$ becomes bigger than $p-k$ we start transiting the same choices of pairs for the first two inputs, but in the opposite direction.

is 2-prime for all $1 \leq n \leq p-1$. This is a happy coincidence, as it confirms somehow that 3-primes are "extra" prime. But theses numbers are significant for a deeper reason. We might add the number 1 to Euler's list, as it vacuously satisfies the condition $n^2 - n + 1$ is 2-prime for every n from (eek!) 1 to 0, so obtaining an "augmented lucky numbers" list. The augmented list is then exactly the list of integers k such that $4k - 1$ is a **Heegner number**. The full list of Heegner numbers is

$$1, 2, 3, 7, 11, 19, 43, 67, 163,$$

but to explain their full significance, we need to back up a bit.

3. The Class Number One Problem

The account here will flaunt chronology a bit, though we find this the more accessible approach. Since the ancients, 2-primes have been important mainly because of the *fundamental theorem of arithmetic*: every natural number factors uniquely into 2-primes. This marvelous fact is related to the existence of an algorithm to divide integers which can always produce remainders of magnitude smaller than the divisor; were it not the case, a larger remainder could be pushed and spackled about in various ways, one imagines, so that the decomposition of a number into irreducible pieces wouldn't always be unique.

Around 1830, Gauss introduced what we now call the **Gaussian integers**

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z},\ i = \sqrt{-1}\},$$

which is a commutative ring sitting inside the field of complex numbers $\mathbb{C}$. It's useful to think of $\mathbb{Z}[i]$ as the unit square lattice in the complex plane. Associated to this ring is a multiplicative **norm** $N : \mathbb{Z}[i] \to \mathbb{N} \cup \{0\}$ defined by

$$N(a + bi) = (a + bi)(a - bi) = a^2 + b^2,$$

which is useful because there is also a division algorithm for Gaussian integers which produces remainders with smaller norm than the divisors. That is, if one divides Gaussian integers z by w, there are s and r in $\mathbb{Z}[i]$ such that $z = sw + r$ where $N(r) < N(w)$. As a consequence, one learns in algebra, $\mathbb{Z}[i]$ is a principal ideal domain, and so all elements admit unique[7] factorization into a set of *Gaussian primes*.

Another set of "integers" with unique factorization! In asking how this idea can extend even further, it helps to recontextualize what $\mathbb{Z}[i]$ "is." Start with what i is: one of the roots of the irreducible polynomial $x^2 + 1$, conjured into existence to sate a desire that all polynomials factor completely. But there are zillions of irreducible quadratic polynomials (over the integers), and their roots, when presumed to exist, always come in conjugate pairs. What happens if we affix one of these other roots α onto the integers: for which other α's is $\mathbb{Z}[\alpha]$ a unique factorization domain?

With a bit more machinery, this question can be asked in a way so that the answer depends only on the **discriminant** ($b^2 - 4ac$) that appears when applying the quadratic formula to find the root α of the polynomial $ax^2 + bx + c \in \mathbb{Z}[x]$. To keep $\mathbb{Z}[\alpha]$ from getting unnecessarily big, it is desirable to restrict attention to monic polynomials[8] (which is the case when $a = 1$).

[7] Up to multiplication by units, which are powers of i.

[8] This choices preserves the analogy between $\mathbb{Z}$ and $\mathbb{Q}$, and further keeps $\mathbb{Z}[\alpha]$ finitely generated as an abelian group [Cox13, Prop. 5.3].

But this is not quite enough. Consider the two monic polynomials

$$x^2 + 3 \qquad \text{and} \qquad x^2 + x + 1,$$

both irreducible over the integers. The first has roots $\pm\sqrt{-3}$ while the latter has roots $\omega = -\frac{1}{2} + \frac{\sqrt{-3}}{2}$ and $\omega^2 = -\frac{1}{2} - \frac{\sqrt{-3}}{2}$. One can show that $\mathbb{Z}[\omega]$[9] is a UFD, while $\mathbb{Z}[\sqrt{-3}]$ is not, so even though both involve the square root of -3, here the particular polynomial makes a difference. Notice also that $\mathbb{Z}[\sqrt{-3}]$ is a subring of $\mathbb{Z}[\omega]$, and that both sit inside the **quadratic number field** $\mathbb{Q}(\sqrt{-3})$[10]. What makes $\mathbb{Z}[w]$ special is that it is largest in a sense which motivates the following definition.

Definition. The **ring of integers** of a quadratic number field $K = \mathbb{Q}(\sqrt{n})$ is the subset of elements which are roots of some monic polynomial with integer coefficients. It is denoted $\mathcal{O}_K$.

According to the definition, if $n = 0$ so that $K = \mathbb{Q}$, we recover the usual integers $\mathbb{Z} = \mathcal{O}_K$, making this the "right" definition of algebraic integers. Further, as the ring of integers of $\mathbb{Q}(\sqrt{n})$ is canonically defined, this reduces the important data to just the number n under the radical, which can be assumed to be square-free. Note that the integers $\mathbb{Z}$ themselves are always in $\mathcal{O}_K$ as roots of monic linear polynomials. Further, the only denominator that can appear among *quadratic integers* is a 2, due to the restriction to monic polynomials of degree at most two.

As a more interesting example, $\mathbb{Z}[\omega] = \mathcal{O}_K$ for $K = Q(\sqrt{-3})$. One can even obtain the following uniform description of rings of quadratic integers [IR90, p. 189].

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{n}] & \text{if } n \not\equiv 1 \bmod 4 \\ \mathbb{Z}\left[\frac{-1+\sqrt{n}}{2}\right] & \text{if } n \equiv 1 \bmod 4. \end{cases} \tag{3}$$

Now we can ask the question in the "right way."

For which n does the ring of integers of $\mathbb{Q}(\sqrt{n})$ have unique factorization?

Beyond the description of 3, there is a bifurcation in the approach to this question according to whether n is positive or negative; that is, whether the quadratic field is *real* or *imaginary*. These two types are of extremely different character. For starters, there are very few units (invertible elements) in the ring of integers of imaginary fields, while there are infinitely many in the real case. We are concerned here with the imaginary case, for which there is a complete answer to the question above.

Theorem 1. *For a natural number n, the ring of integers of $\mathbb{Q}(\sqrt{-n})$ has unique factorization if and only if n is a Heegner number: 1, 2, 3, 7, 11, 19, 43, 67, or 163.*

This theorem, which has origins in the study of quadratic forms (going back to Fermat, Lagrange, Legendre, Gauss) has a long, interesting history, recounted well in [Gol85]. The answer was guessed by Gauss

[9] These are the **Eisenstein integers**.

[10] For those that are unfamiliar, this means take the rational numbers, throw in $\sqrt{-3}$, and then throw in everything else you need so that it is closed under multiplication, addition and inverses, making it a field again. It is "quadratic" because it extends $\mathbb{Q}$ by the root of a quadratic polynomial.

(in distinct terms) and was proved by Heegner in 1952, but this proof was only accepted by the mathematical community after Heegner's death and the appearance of proofs in the 1960s by established mathematicians Baker and Stark. Moreover, the answer to the unique factorization problem is just one part of a larger problem called **Gauss' class number problem**, resolved by Goldfeld-Gross-Zagier in 1985. Theorem 1 above addresses just the "class number one" problem, with classes referring to equivalence classes either of ideals in $\mathcal{O}_K$ or of a related set of quadratic forms. When the class number of $\mathcal{O}_K$ is one, it implies that $\mathcal{O}_K$ has the unique factorization property; for background, see [Cox13].

Within the imaginary case, there are again two subcases which are treated differently. Remember that a quadratic number field is obtained by adjoining to $\mathbb{Q}$ a root α of a quadratic polynomial, $ax^2 + bx + c$, which root has formula

$$\alpha = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Since we are adjoining α to the rational numbers, the fractional part doesn't matter, and what comes out in the wash is really the $\sqrt{b^2 - 4ac}$ part, so this discriminant $D = b^2 - 4ac$ is what determines the number field. Now, $D \equiv b^2$ modulo 4, and so since D is a square mod 4 it can only be congruent to 0 or 1. When $D \equiv 0$, there is a factor of 4 that can be pulled out of the square root so that

$$\mathbb{Q}(\sqrt{D}) = \mathbb{Q}\left(\sqrt{\frac{D}{4}}\right).$$

When talking about quadratic fields $\mathbb{Q}(\sqrt{n})$, usually n is meant to be square-free, although it may come from a discriminant $D \equiv 0 \bmod 4$ (as in $n = \frac{D}{4}$), which is the reason for the following definition.

Definition. The **discriminant** d_K of the number field $K = \mathbb{Q}(\sqrt{n})$ is

$$d_K = \begin{cases} n & \text{if } n \equiv 1 \bmod 4 \\ 4n & \text{otherwise.} \end{cases}$$

It's easy to see that any member of the congruence class 1 modulo 4 can be realized as a discriminant $b^2 - 4ac$ for the right choice of b and c (we can assume $a = 1$). And the "otherwise" above really only means $n \equiv 2$ or $3 \bmod 4$ since we only look at square-free n. Going back to the list of Heegner numbers, we see that $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-2})$ are the only cases where $d_K \equiv 0 \bmod 4$; $-n \equiv 1 \bmod 4$ for every other Heegner number n. Often times, Theorem 1 will be stated by giving instead the list of negative *field discriminants* D such that $\mathbb{Q}(\sqrt{D})$ has **class number** $h(D)$ equal to one. Then, instead of the Heegner numbers, we have the slightly modified list

$$D = -3, -4, -7, -8, -11, -19, -43, -67, -163.$$

In 1902, Landau was able to prove that $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-2})$ are the only imaginary quadratic fields with even (divisible by 4) discriminant and unique factorization.[11] The proof of this fact is quite elementary, but the proofs of Heegner, Baker and Stark that cover the odd discriminant case require much more technology.[12] Nevertheless, Rabinowitsch provided another criterion in 1913, also by fairly elementary means.

[11] Actually, he proved a slightly broader statement in terms of quadratic forms; see [Cox13, Theorem 2.18].

[12] Heegner's and Stark's proofs use modular forms, while Baker's approach involves bounds on logarithms of linear forms of algebraic numbers.

Theorem 2 ([Rab13]). *Let $D < 0$ and $D \equiv 1 \bmod 4$. Then*

$$x^2 - x + \frac{1+|D|}{4} \quad \textit{is prime for each} \quad x = 1, 2, \ldots, \frac{|D|-3}{4}$$

if and only if the integers of the field $\mathbb{Q}(\sqrt{D})$ admit unique factorization.

This theorem does not appear to have been so useful for solving the class number one problem, but it does link it to the list of Euler's lucky primes from before, and so now to the list of 3-primes! One might even say that the integers of $\mathbb{Q}(\sqrt{-163})$ have unique factorization "because" $x^2 - x + 41$ is 2-prime for each x from 1 to 40, or vice versa. We then see that the augmented lucky numbers

$$1, 2, 3, 5, 11, 17, 41$$

account for all of the negative odd discriminants of class number one,

$$-3, -7, -11, -19, -43, -67, -163.$$

We have defined a number to be 3-prime if it is not representable by some non-degenerate hexagonal or parallelogrammatic configuration. In this sense, we might throw (at least for the time being) 1 into our collection of 3-primes. Now we can show the following.

Theorem 3. *A number is 3-prime if and only if it is among the augmented lucky numbers.*

Proof. If n is not 3-prime, then n dots can be arranged into a parallelogram or equiangluar hexagon in the hexagonal lattice such that two distinct pairs of sides have at least two points along the edge. When this is the case, one of the following two cases happens. Either n is already 2-composite, in which case a parallelogrammatic representation exists, or not, in which case a true hexagonal representation exists. Supposing the latter is the case, the hexagon can be "completed" to a parallelogram by adding two triangles along opposite edges. If the the sides abutting these triangles contain k points, then the completed parallelogram will have $n + 2T_{k-1}$ points (see Figure 5a).

Thinking of this in relief, if a number n is 3-prime, then the only representation it admits is a row of n dots. In other words, the smallest triangles that can be adjoined in order to obtain a parallelogram are those of size T_{n-1} (see Figure 5b). Equivalently, $n + 2T_k$ is 2-prime for $k = 1, 2, \ldots, n-1$, as is n itself.

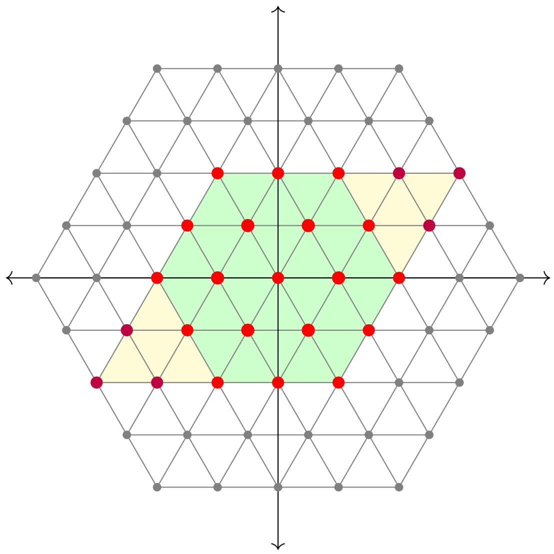
Now examine the polynomial $x^2 - x + n$, and observe that $x^2 - x = x(x-1) = 2T_{x-1}$ when x is a natural number.[13] Then, the condition that $x^2 - x + n$ is 2-prime for all x from 1 to $n-1$ is equivalent to statement that every number in the set

$$\{n, n + 2T_1, n + 2T_2, \ldots n + 2T_{n-1}\}$$

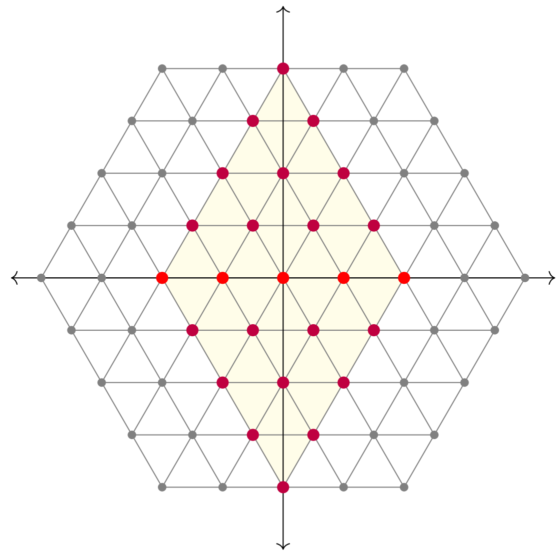
is 2-prime. This is plainly equivalent to the characterization of 3-primality given in the preceding paragraph. ∎

This establishes that the list produced by the ternary sieve is complete, and clarifies the coincidence with Euler's lucky numbers. Moreover, invoking the theorems of Rabinowitsch and Heegner/Baker/Stark, we have the following.

[13] Let $T_0 = 0$.



(A) $\langle 3,3,3\rangle = 19$ is not 3-prime because $19 + 2T_2 = 19 + 6 = 25$ is 2-composite.



(B) 5 is 3-prime because two T_4 triangles are the smallest that can be added to reach a 2-composite.

FIGURE 5. Relating 3-factorizations and 2-factorizations.

Corollary 1. *There are only finitely many 3-primes. Including 1, these are 1, 2, 3, 5, 11, 17, and 41.*

Proof. We see that if there were 3-primes beyond the list of augmented lucky numbers, they would give imaginary quadratic fields with unique factorization and odd discriminant. But there are only seven of these from the solution of the class number one problem. □

This is a very heavy-handed proof, especially if you compare this to typical proofs of the finitude of 2-primes. It would be marvelous to find an elementary proof of this corollary, as it would give a new proof of the solution to class number one problem. But it is perhaps greedy to expect that such a proof could be yielded from the vantage of ternary multiplication.

4. Applications

Besides determining which numbers are 2-prime and which are 2-composite, one of the most basic questions one can ask in number theory is how to determine the factorization of numbers which are 2-composite. The proof of Theorem 3 can be retooled to produce 3-factorizations of natural numbers. We return to the idea of attaching triangles to polygonal representations of a number, beginning with the example of the number 19.

From our short list of 3-primes, we know that 19 is 3-composite, but we might not know how to represent it as a lattice hexagon. To figure out how to do this, we can add twice a triangular number to 19 to see if we can get a 2-composite number. Then, since we know that a 2-composite of the form $19 + 2T_k$ can be represented by a parallelogram, there is an equation $19 + 2T_k = ab$ where neither of a and b is equal to 1.

All we have to do next is clip the corner triangles (consisting of $2T_k$ points) off of this parallelogram, and we get a hexagon whose sides give a non-trivial 3-factorization of 19.

The only complication here is that there may be several k for which $19 + 2T_k$ is 2-composite, and possibly multiple parallelograms that represent each of those 2-composites. For instance, $19 + 2 = 21 = 7 \cdot 3$. Clipping two points from the opposite corners of a 7 by 3 parallelogram, we get a hexagon with pairs of sides of lengths 2, 2 and 6, so $19 = \langle 2, 2, 6 \rangle$. But

$$19 + 2T_2 = 19 + 6 = 25 = 5 \cdot 5$$

as well, and clipping the T_2 triangles from the 5 by 5 parallelogram gives us the 3-factorization $19 = \langle 3, 3, 3 \rangle$ of Figure 5a. This idea easily generalizes to produce the following.

Proposition 3. *If $n + 2T_k = ab$ for $a, b > k$, then $n = \langle a - k, b - k, k + 1 \rangle$.*

Proof. Construct a lattice parallelogram which has a and b points along opposite pairs of edges. Since a and b are bigger than k, we can remove lattice triangles with k points along each edge from opposite corners of the parallelogram. If a and b are $k + 1$, then removal of these triangles yields n points in a row and the factorization $n = \langle 1, 1, n \rangle$. In case exactly one of a or b is $k + 1$ (assume it is a), the removal produces a new parallelogram and the factorization $n = \langle 1, b - k, k + 1 \rangle$. Otherwise this removal produces a true lattice hexagon. The number of points in opposite pairs of edges of this hexagon are $a - k$, $b - k$, and $k + 1$ which yields the factorization $n = \langle a - k, b - k, k + 1 \rangle$. □

We see that the proposition also covers "degenerate" 3-factorizations which are either trivial ($n = \langle 1, 1, n \rangle$) or become 2-factorizations, though we are most interested in the 3-factorizations where each factor is at least 2. One could obtain all of these hexagonal representations of n as follows.

Suppose n has 3-factorization $n = \langle x, y, z \rangle$, where z is the least among the three factors. This 3-factorization can be discovered by examining parallelograms which represent $n + 2T_{z-1}$ and "breaking off" the triangles in opposite corners. This indicates that every 3-factorization can be found in terms of 2-factorizations of n plus twice a trianglular number which is related to the smallest 3-factor. The smallest 3-factor of n is as large as possible when $n = \langle z, z, z \rangle$, meaning that one should examine the 2-factorizations of the numbers $n + 2T_k$ for $1 \le k \le z - 1$, where z is the largest number satisfying

$$\langle z, z, z \rangle = 3z^2 - 3z + 1 \le n.$$

Since ternary multiplication results in a number system with finitely many 3-primes, the fact that many numbers admit multiple 3-factorizations is not surprising. The question of exactly how many distinct 3-factorizations (up to reordering the factors) a number admits, and how this statistic may be further related to the class numbers of quadratic fields could be of interest for future research.

TABLE 1. Number of 3-factorizations of small natural numbers

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
3-factorizations	1	1	1	2	1	2	2	2	2	3	1	3	2	3	2	4	1	4	3	3

We will wrap up this discussion with a few applications of this line of thinking to elementary number theory. The first is a 2-primality test that comes as a consequence of the following partial converse of Proposition 2.

Proposition 4. *Let $n = pr$ be an odd 2-composite number and $p, r \geq 3$. Then there are distinct x and w where $1 \leq x, w \leq \frac{n+1}{2}$ such that $x(n+1-x) \equiv w(n+1-w) \bmod n$.*

Proof. We can assume $p \leq r$ by choosing p to be the smallest 2-prime factor of n. We will show that the claim is true for some $x \leq \frac{n+1}{2}$ and $w = x + p \leq \frac{n+1}{2}$, though the statement may be true for other choices of x and w as well. In order to obtain

$$x(n+1-x) \equiv w(n+1-w) \bmod n$$

we need

$$\begin{aligned} x(n+1-x) &\equiv (x+p)(n+1-x-p) \bmod n, \quad \text{so} \\ nx + x - x^2 &\equiv nx + x - x^2 - px + np + p - px - p^2 \bmod n. \end{aligned}$$

Subtracting and collecting terms, we have

$$2px + p^2 - p = p(2x + p - 1) \equiv 0 \bmod n.$$

This is satisfied if and only if $2x + p - 1 \equiv 0 \bmod r$. By varying x, we can arrange $2x + p - 1$ to take the value of any even number from

$$p + 1 \qquad \text{to} \qquad 2\left(\frac{n+1}{2} - p\right) + p - 1 = pr + 1 - 2p + p - 1 = pr - p.$$

By showing that the even number $2r$ lies in this range, we will establish the existence of x and w. First, $p + 1 \leq 2r$ because $r \geq p$ and both are at least 3. Next, the inequality $2r \leq pr - p$ holds if and only if

$$\begin{aligned} pr - 2r - p &\geq 0 \\ (p-2)r - p &\geq 0 \end{aligned}$$

which holds because $p \geq 3$ and $r \geq p$. □

The statement of this proposition seems to hold for any $r \geq 2$, and so for every 2-composite that is not a pure power of 2, rather than just for odd n. However, when testing 2-primality, one usually has an odd number in mind as even numbers are trivial to test, so these other cases are of less concern for us. Thus we have the following 2-primality test, which is an immediate consequence of Propositions 2 and 4.

Theorem 4. *Let n be and odd natural number. Then n is 2-prime if and only if the congruence classes of $x(n+1-x) \bmod n$ are distinct for every x between 1 and $\frac{n+1}{2}$.*

This test doesn't appear to be very efficient – on its face it requires about half as many computations as the size of the number n.[14] However there is a small speed-up which makes this test not too bad to perform by hand calculation, at least for 2-digit numbers. Recalling the familiar calculation

$$x(n+1-x) \equiv x - x^2 \bmod n,$$

[14]The best (deterministic) 2-primality testing algorithms require a number of computations which is polynomial in $\log n$, instead of polynomial in n as this one is.

and observing $x - x^2 = x(1-x) = -2T_{x-1}$, we have the following.

Lemma 2. *Let* $T_k = \frac{k(k+1)}{2}$ *for any* $k = 0, 1, 2, 3, \ldots$ *and let* n *and* x *be natural numbers with* $1 \le x \le n$. *Then* $x(n+1-x) \equiv -2T_{x-1} \bmod n$.

This lemma makes it quite easy to write down the congruence classes of interest for Theorem 4. To make the list, start from $x = 1$, in which case $x(n+1-x) \equiv -2T_0 \equiv 0 \bmod n$, and then to get from $-2T_k$ to $-2T_{k+1}$, all you have to do is subtract $2(k+1)$. We illustrate this now for $n = 15$:

$$15 \equiv 0 \bmod 15 \xrightarrow{\text{subtract } 2} 13 \xrightarrow{\text{subtract } 4} 9 \xrightarrow{\text{subtract } 6} 3 \xrightarrow{\text{subtract } 8} -5 \equiv 10 \xrightarrow{\text{subtract } 10} 0 \xrightarrow{\text{subtract } 12} 2 \xrightarrow{\text{subtract } 14} 3.$$

We see that the appearance of the congruence class 3 mod 15 at $x = 5$ and $x = 8$ indicates that 15 is 2-composite. Also notice the coincidence at $x = 1$ and $x = 6$, indicating that the type of repetition produced in the proof of Proposition 4 occurs not only at intervals of length equal to the smallest prime p. By the converse statement of Proposition 2, this collision could also be used to detect compositeness of 15.

The coincidence of congruence classes $-2T_k \equiv -2T_l \bmod n$ can be rephrased as saying that $2T_l - 2T_k$ is a multiple of n. And it appears that the difference $l - k$ has something to do with the 2-factorization of n. The next proposition confirms this, and suggests how to upgrade the 2-primality test to a 2-factorization algorithm.

Proposition 5. *With notation as before, if* $2(T_l - T_k) = mn$ *for* $0 \le k, l \le \frac{n-1}{2}$, *distinct and* $n > 3$, *then neither of the pairs* $(l-k, n)$ *nor* $(l+k+1, n)$ *has greatest common divisor (gcd) equal to 1.*

Proof. We have

$$2(T_l - T_k) = l^2 + l - k^2 - k = (l-k)(l+k+1) = mn.$$

If $\gcd(l-k, n) = 1$, then $l - k$ divides m and $l + k + 1 = sn$ for some integer s. But since $0 \le k, l \le \frac{n-1}{2}$, and k and l are distinct, we have

$$2 \le l + k + 1 \le n - 1,$$

so $l + k + 1 = sn$ is impossible.

On the other hand, if $\gcd(l+k+1, n) = 1$, then $l - k = tn$ for some integer t. But $-\frac{n}{2} < l - k < \frac{n}{2}$, so the only possibility is $t = 0$. This would imply $m = 0$, contradicting that l and k are distinct. □

Taking the gcd of natural numbers can be done efficiently by Euclid's algorithm, taught in many introductory discrete mathematics or number theory courses. Thus, the major cost in the following 2-factorization algorithm is generating the list of congruence classes $x(n+1-x) \equiv -2T_{x-1} \bmod n$.

Theorem 5 (2-factorization algorithm)**.** *Given an odd natural number* n, *one can obtain the factorization of* n *into 2-primes as follows.*

(1) *List the congruence classes* $-2T_k \bmod n$ *for* $k = 0, 1, 2 \ldots$ *until there is a repetition*

$$-2T_k \equiv -2T_l \bmod n, \quad k \ne l$$

In case there is no repetition up through $k = \frac{n-1}{2}$, *then conclude* n *is 2-prime.*

(2) *Otherwise compute either* $\gcd(l-k,n)$ *or* $\gcd(l+k+1,n)$. *The output will be a non-trivial divisor* d *of* n.
(3) *Repeat steps 1 and 2 with* d *and* $n_1 = \frac{n}{d}$. *Continue to iterate on the outputs of these steps until all divisors and quotients are determined to be 2-prime.*

At the end of this branching process of step 3, one obtains the 2-prime factorization of n *as the collection of* 2*-primes at which the algorithm dead-ends.*

One may recognize in this algorithm a formal similarity with *Pollard's rho algorithm*, which also finds a non-trivial factor of n by taking the gcd of numbers after finding a repetition in a sequence. However the discovery of a repetition in the algorithm of Theorem 5 does not mean that there is a "cycle" in the sequence as it does in Pollard's algorithm. Closer examination reveals that this algorithm actually has more in common with the *Fermat factorization method* which finds factors of n by representing it as a difference of squares, $n = a^2 - b^2$.[15] Let us explain.

From the list of products of the form $x(n+1-x) \bmod n$, let us call $u = \frac{n+1}{2}$. When $x = u$, we are computing the product $x(n+1-x) = u^2$. Then all of the other products in the list are $(u+a)(u-a) = u^2 - a^2$ for some a. In seeking a match

$$u^2 - a^2 \equiv u^2 - b^2 \bmod n,$$

we are also seeking a solution to $a^2 - b^2 \equiv 0 \bmod n$, or $a^2 - b^2 = mn$ for some integer m.

The ideas of the Fermat factorization form the basis of the fastest known integer factorization algorithms, the quadratic sieve and general number field sieve. It remains to be seen if the algorithm of Theorem 5 admits improvements that could make it competitive. For now, it is a curiousity which we hope encourages the reader to explore the plunder of simple ideas which may come from non-binary thinking.

Acknowledgements: The author is grateful to Craig Jensen for permission to think about this topic as a master's student, Ken Holladay for a helpful mathematical suggestion, Padi Fuster and Bradford Fournier for encouragement, and Mahir Can for reading a draft and suggesting improvements in the writing.

References

[Apo76] Tom M. Apostol. *Introduction to analytic number theory.* Undergraduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg, 1976, pp. xii+338.

[Bre89] David M. Bressoud. *Factorization and primality testing.* Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1989, pp. xiv+237. ISBN: 0-387-97040-1. DOI: 10.1007/978-1-4612-4544-5. URL: https://doi.org/10.1007/978-1-4612-4544-5.

[Cox13] David A. Cox. *Primes of the form* $x^2 + ny^2$. Second. Pure and Applied Mathematics (Hoboken). Fermat, class field theory, and complex multiplication. John Wiley & Sons, Inc., Hoboken, NJ, 2013, pp. xviii+356. ISBN: 978-1-118-39018-4. DOI: 10.1002/9781118400722. URL: https://doi.org/10.1002/9781118400722.

[Cox69] H. S. M. Coxeter. *Introduction to geometry.* Second. John Wiley & Sons, Inc., New York-London-Sydney, 1969, pp. xviii+469.

[15] See [Bre89, Ch. 5], for instance, for descriptions of these other algorithms.

[Gol85] Dorian Goldfeld. "Gauss's class number problem for imaginary quadratic fields". In: *Bull. Amer. Math. Soc. (N.S.)* 13.1 (1985), pp. 23–37. ISSN: 0273-0979. DOI: 10.1090/S0273-0979-1985-15352-2. URL: https://doi.org/10.1090/S0273-0979-1985-15352-2.

[IR90] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory.* Second. Vol. 84. Graduate Texts in Mathematics. Springer-Verlag, New York, 1990, pp. xiv+389. ISBN: 0-387-97329-X. DOI: 10.1007/978-1-4757-2103-4. URL: https://doi.org/10.1007/978-1-4757-2103-4.

[Rab13] Georg Rabinowitsch. "Eindeutigkeit der Zerlegung in Primzahlfaktoren in quadratischen Zahlkörpern". In: *J. Reine Angew. Math.* 142 (1913), pp. 153–164. ISSN: 0075-4102. DOI: 10.1515/crll.1913.142.153. URL: https://doi.org/10.1515/crll.1913.142.153.