https://doi.org/10.15446/recolma.v55n2.102612

Revista Colombiana de Matemáticas
Volumen 55(2021)2, páginas 149-166

Ternary arithmetic, factorization, and the class number one problem

Aritmética ternaria, factorización, y el problema de número de clase uno

Aram Bingham

Centro de Ciencias Matemáticas (UNAM), Morelia, México

Abstract. Ordinary multiplication of natural numbers can be generalized 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 describe how to determine representations of numbers as ternary products and related algorithms for usual primality testing and integer factorization.

Key words and phrases. Factorization, primality testing, quadratic fields.

2020 Mathematics Subject Classification. 11A05, 11H06, 11Y05.

Resumen. La multiplicación usual de numeros naturales se puede generalizar a una operación ternaria en consideración de volúmenes discretos de hexágonos de retícula. Con esta operación, se define una noción de '3-primalidad' y resulta que hay muy pocos números que son 3-primos. Éstos corresponden a cuerpos cuadráticos imaginarios $\mathbb{Q}(\sqrt{-n})$, $n > 0$, de discriminante impar cuyos anillos de enteros admiten factorización única. También describimos cómo obtener representaciónes de números enteros como productos ternarios y algoritmos relacionados de chequeo de primalidad y factorización ordinaria.

Palabras y frases clave. Factorización, prueba de primalidad, campos cuadráticos.

1. Introduction

When ideas become engrained, it can be hard to imagine other possibilities. But in escaping from deep-seated notions, we may uncover pleasant surprises. In this spirit, this article will present a deformation of integer arithmetic which remains grounded in geometry and leads to new perspectives on old problems in number theory related to primality and factorization.

Let's start with the absolute basics. Say you want to multiply two whole numbers, a and b. What do you do to find the product ab?

One option 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 number of intersection points of the two sets of lines is your product ab. Further, the commutativity of multiplication is evident in the fact that the number of intersection points doesn't change when you rotate the whole picture by 90°.

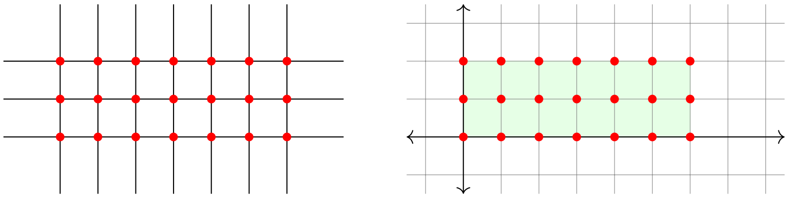


FIGURE 1. 3 times 7 is 21

Let's think of this slightly more formally. Given a lattice of points in the plane, we will define a **lattice polygon** to be a polygon whose vertices are lattice points and whose edges are only in the directions of nearest neighbors from a given vertex. Using the $\mathbb{Z}^2$ lattice, this means that edges are either in the horizontal or vertical directions. The product ab is then 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 $(a - 1, b - 1)$. Restated, ab is the **discrete volume** of the lattice rectangle with a points along two opposite edges in one direction and b lattice points along the opposite edges in the other direction; see the right side of Figure 1. This view of multiplication allows us to codify the following simple observation.

Fact 1.1. A positive integer 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) where each edge contains at least two lattice points.

In this model, the commutativity of multiplication is beheld in the preservation of discrete volume when interchanging which lattice direction corresponds to which factor in the product ab. This suggests that sensible alternatives to standard multiplication might then be found in by taking discrete volumes of other lattice polygons in other lattices.

Opting for maximal symmetry, we consider the **hexagonal lattice** [4, pp. 60-61]. In this lattice, rotation of the plane by 60° about any lattice point sends lattice points to other lattice points, arranging the nearest neighbors of any lattice point P in a regular hexagon. These six other points come in pairs along three lines through P as compared to the four nearest neighbors of a point in the $\mathbb{Z}^2$ lattice which come in pairs along two lines (Figure 2). Hence we gain an extra direction that can be assigned to a third factor.

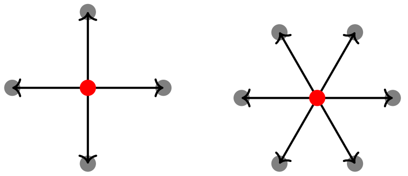


FIGURE 2. Nearest neighbors in a square ($\mathbb{Z}^2$) lattice and a hexagonal lattice.

Recall that the **arity** of a function or algebraic operation refers to the number of inputs (arguments) it takes. Binary operations can always be iterated to fabricate operations of higher arity, but we will introduce a true **ternary product** on the natural numbers.[1] While distinct from repeated multiplication, it bears some of the same nice properties: commutativity guaranteed by geometry, and the presence of a *multiplicative identity* element in the number 1. We will denote this product as

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

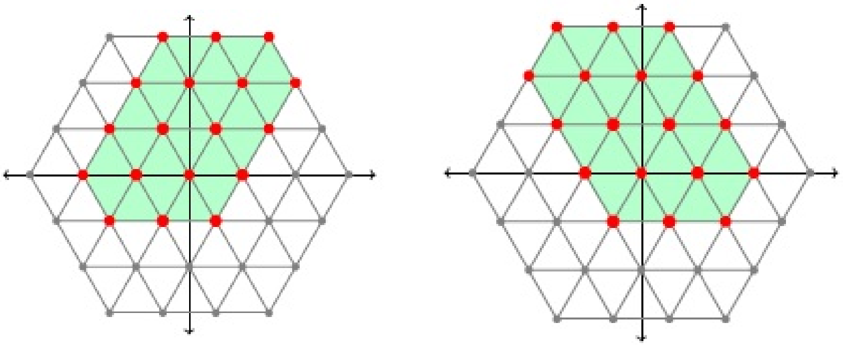
and define it, in analogy with our lattice model of binary multiplication, as the function which takes the triplet (a, b, c) to the number of lattice points inside the equiangular lattice hexagon with a points along two opposite edges, b points along the next pair of edges, and c points along the final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

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. Under this action, any lattice direction can be taken to any other while the discrete volume of a lattice hexagon is always preserved, implying that $\langle -, -, - \rangle$ is fully commutative as a ternary product.

Notice that if we put a 1 as an argument 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 1 appears 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.

[1] Throughout this manuscript, we take the set of natural numbers $\mathbb{N}$ to start at 1.



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

Figure 3. Commutativity of ternary multiplication under reflection.

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

Definition 2.1. 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 $x = 1$, $y = 1$, $z = n$, 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.[2] 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 vice versa. 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.

Question: Which natural numbers are 3-prime?

To answer this question, we need some preliminaries on ternary multiplication.

Proposition 2.2. *The ternary product can be written*

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

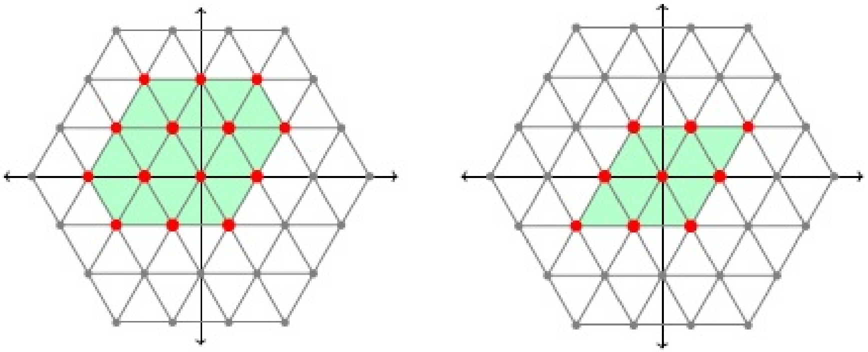
Proof. We have seen that $\langle x, y, 1\rangle = xy$. Increasing the third argument by 1 adds a hooked strip of $x + y - 1$ points along two consecutive edges opposite to

[2] Under binary multiplication, of course.

those with x and y points (see again Figure 4, where the argument increases from 1 to 2). This allows us to conclude the claimed equality,

$$\langle x, y, z\rangle = xy + (z-1)(x+y-1) = xy + yz + xz - x - y - z + 1. \qquad (2)$$

☑



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

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

FIGURE 4. Ternary multiplication includes binary multiplication.

Scholars of symmetric polynomials will recognize (1) as an alternating sum of **elementary symmetric polynomials**,[3]

$$\langle x, y, z\rangle = e_2(x, y, z) - e_1(x, y, z) + e_0(x, y, z). \qquad (3)$$

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

$$\langle x, y, z\rangle = xyz - (x-1)(y-1)(z-1) \qquad (4)$$

more convenient.

How can we determine if a number n is 3-prime? When studying 2-primes, the first method one usually learns is the **Sieve of Eratosthenes**, which produces the list of 2-primes up to a given N by crossing off multiples of those 2-primes which are at most $\sqrt{N}$. This amounts to eliminating all of the numbers greater than each 2-prime p in the congruence class 0 mod p.

The proof of Proposition 2.2 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

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

[3] This observation can be generalized to construct a family of n-ary operations with similar properties.

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 choice of $x = 3$, $y = 1$ 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 2.3. *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 $x = p+1-w$. Suppose 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

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

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 $w + x - 1 = p$. ☑

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

Theorem 2.4 (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 non-zero congruence class modulo p [1, Chap. 7]. There are $p-1$ such classes for each p, and Proposition 2.3 says that half of them are ruled out from the possibility of 3-primality, in addition to the congruence class 0 mod p. The following lemma further tells us that ruling out congruence classes only needs to happen at the 2-primes – nothing new is eliminated by ternary products of the form $\langle x, y, z\rangle$ where $x+y-1$ is 2-composite.

Lemma 2.5. Let $m = ab = x + y - 1$. Then there are natural numbers v and w such that $v + w - 1 = a$ and $xy \equiv vw \bmod a$. Hence if $n = \langle x, y, z\rangle$, then there exists z' such that $n = \langle v, w, z'\rangle$.

***Proof*.** We can write

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

Let v be the least 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. ☑

To list the 3-primes up to a given N, first we can eliminate the 2-primes below N using the Sieve of Eratosthenes, and now Proposition 2.3 and Lemma 2.5 say that we must further eliminate some congruence classes modulo p for some of the 2-primes below N. The full method is given in the following "ternary sieve" **TS**, by proceeding through numerous stages TS_k.

Algorithm 2.6 (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 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. Let $T_k = \frac{k(k+1)}{2}$ be the k^{th} triangular number. 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 $m \in \mathbb{N}$.

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.

Proof. 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 $p \cdot 1 = p$. As a small efficiency, starting from the first 2-prime 2 and as p increases towards $\sqrt{N}$, one only 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 eliminates products of the form $\langle 2, p-1, z\rangle$. Lemma 2.5 tells us that this can only possibly cross out new numbers 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

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

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

At the k^{th} stage TS_k, we eliminate products of the form $\langle k+1, p-k, z\rangle$. By considerations similar as in the previous case, this process only needs to happen for $z \geq p - k$, and therefore only for 2-primes such that (applying formula 2)

$$\langle k+1, p-k, p-k\rangle = (k+1)(p-k) + (p-k-1)p = p^2 - (k^2 + k) \leq N.$$

Rearranging, this condition becomes $p \leq \sqrt{N + 2T_k}$.

To obtain the bound on k, note that to avoid further unnecessary redundancy we should keep $k + 1 \leq p - k$ in the product $\langle k+1, p-k, z\rangle$.[4] Since $z \geq p - k$ during TS_k, the largest possible value of k must 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

$$k \leq \sqrt{\frac{4N-1}{12}} - \frac{1}{2} \tag{5}$$

is a sufficient bound. Note that by Lemma 2.5 $\langle k+1, k+1, k+1\rangle$ will only eliminate a new congruence class if $p = 2k + 1$ is 2-prime. ☑

[4] 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.

This algorithm is not hard to implement on a computer, and a search for the 3-primes up to 10,000,000 reveals a very short list.

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

At OEIS (A014556) one learns that these are "Euler's 'lucky' numbers," those 2-primes p such that

$$n^2 - n + p \tag{6}$$

is 2-prime for all $1 \leq n \leq p-1$. This confirms that 3-primes are somehow "extra" prime, but these numbers are significant for a deeper reason. We might add the number 1 to Euler's list, as it vacuously satisfies the defining condition, so obtaining an "augmented lucky numbers" list. The augmented list is then exactly the set of integers k such that $4k-1$ is a **Heegner number**. The full list of Heegner numbers is

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

We next explain their significance.

3. The Class Number One Problem

Recall that a **quadratic number field** $\mathbb{Q}(\sqrt{n})$ is an extension of the rational numbers $\mathbb{Q}$ obtained by adjoining a root of an irreducible degree-two polynomial. Just as the integers $\mathbb{Z}$ sit inside the rationals, each quadratic number field has its own set of integers.

Definition 3.1. 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 coefficients in $\mathbb{Z}$. It is denoted $\mathcal{O}_K$.

Classic examples include the *Gaussian integers* $\mathbb{Z}[i]$ inside $\mathbb{Q}(i)$, and the *Eisenstein integers* $\mathbb{Z}[\omega]$ inside $\mathbb{Q}(\sqrt{-3})$, where $\omega = -\frac{1}{2} + \frac{\sqrt{-3}}{2}$. In general one has the following uniform description of rings of *quadratic integers* [7, p. 189].

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{n}] & \text{if } n \not\equiv 1 \bmod 4 \\ \mathbb{Z}\left[\frac{-1+\sqrt{n}}{2}\right] & \text{if } n \equiv 1 \bmod 4. \end{cases} \tag{7}$$

It is well-known that both the Gaussian integers and the Eisenstein integers admit unique factorization into irreducible elements, just as the ordinary integers admit unique factorization into 2-primes. But other rings of quadratic integers do not. To cite a common example, in $\mathbb{Z}[\sqrt{-5}]$ the number 6 admits decompositions as both $2 \cdot 3$ and $(1+\sqrt{-5})(1-\sqrt{-5})$. This leads to the following natural question.

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

Beyond the description of (7), 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 instance, 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 a complete answer to the question above is known.

Theorem 3.2. *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, has a long, interesting history with origins in the study of quadratic forms going back to Fermat, Lagrange, Legendre, Gauss, etc.[5] The answer was guessed by Gauss 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 1960's 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 3.2 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 [3].

Within the class number one problem, the two cases of (7) are treated differently. Remember that a quadratic number field is obtained by adjoining to $\mathbb{Q}$ a root α of some 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, everything other than $\sqrt{b^2 - 4ac}$ can be disregarded, and in fact the discriminant $D = b^2 - 4ac$ determines the number field. Since $D \equiv b^2$ modulo 4 it can only be congruent to 0 or 1. When $D \equiv 0 \bmod 4$, there is a factor of 4 that can be pulled out of the square root so that

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

This is to say that for a quadratic field $\mathbb{Q}(\sqrt{n})$, n is usually understood to be square-free, although it may come by adjoining the root of a polynomial with discriminant $D = 4n$. This motivates the following definition.

[5] See, for instance, [5].

Definition 3.3. The **field discriminant** d_K of $K = \mathbb{Q}(\sqrt{n})$ is

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

Returning to the list of Heegner numbers, we see that $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-2})$ are the only cases where $d_K \equiv 0 \bmod 4$. That is, $-n \equiv 1 \bmod 4$ for every other Heegner number n. Often, Theorem 3.2 is 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, really) discriminant and unique factorization.[6] 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 sophistication.[7] In 1913, Rabinowitsch provided another elementary characterization of the odd case.

Theorem 3.4 ([9])**.** *Let $D < 0$ and $D \equiv 1 \bmod 4$. Then*

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

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

This theorem does not appear to have been directly useful for solving the class number one problem, but it does link it to the list of Euler's lucky primes, and so to the list of 3-primes. Just as we augmented Euler's lucky primes by adding 1, from now on we will consider 1 as a 3-prime in the sense that it is not representable by a non-degenerate hexagonal or parallelogrammatic configuration. We then see that the augmented lucky numbers/known 3-primes

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

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

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

Next we show that the 3-primes known from the ternary sieve exactly coincide with the augmented lucky numbers.

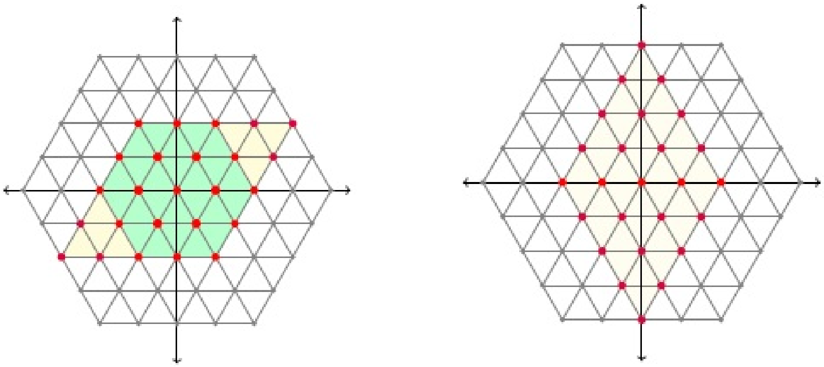
[6] Actually, he proved a slightly broader statement in terms of quadratic forms; see [3, Theorem 2.18].

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

Theorem 3.5. *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 lattice parallelogram or hexagon such that two distinct pairs of sides have at least two points along the edge. Then 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 5).

On the other hand, 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 5). Equivalently, $n + 2T_k$ is 2-prime for $k = 1, 2, \ldots, n-2$, as is n itself.



(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.

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. 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

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

is 2-prime. This is plainly equivalent to the characterization of 3-primality just given. ☑

Invoking the theorems of Rabinowitsch and Heegner/Baker/Stark, we conclude the following.

Corollary 3.6. *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 compared to common proofs of the finitude of 2-primes. While it would be extremely desirable to find a proof that relied only upon ternary multiplication, the historical difficulty of the class number one problem suggests that this might be out of reach.

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 3.5 can be retooled to produce **3-factorizations** of natural numbers, by which we mean representations of a number as a ternary product.

For example, by Corollary 3.6, we know that 19 is 3-composite. To find its 3-factorizations, we can add twice a triangular number to 19 to see if we obtain 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. Removing the corner triangles (consisting of $2T_k$ points) from this parallelogram, we get a hexagon whose sides give a non-trivial 3-factorization of 19.

Note that there may be several k's for which $19 + 2T_k$ is 2-composite and multiple parallelograms that represent each of those 2-composites. For instance, $19 + 2 = 21 = 7 \cdot 3$. Removing 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 removing the T_2 triangles from the 5 by 5 parallelogram gives us the 3-factorization $19 = \langle 3, 3, 3\rangle$ of Figure 5. In general, we have the following.

Proposition 4.1. *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 points 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 reduce to binary products, 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 removing the triangles in opposite corners. The smallest 3-factor of n is as large as possible when $n = \langle z, z, z\rangle$, meaning that to recover all 3-factorizations, one needs to examine the 2-factorizations of all the numbers $n + 2T_k$ for $1 \leq k \leq z-1$, where z is the largest number satisfying

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

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.

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

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

We will close this discussion with a few applications of this line of thinking to elementary number theory. The first is a 2-primality test that comes from the following partial converse of Proposition 2.3.

Proposition 4.2. *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 be true 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, 2-primality tests usually are usually only meant for odd numbers since even numbers can be tested instantly, so we ignore this other case. Thus we have the following 2-primality test, which is an immediate consequence of Propositions 2.3 and 4.2.

Theorem 4.3. *Let n be an 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 – as stated it requires about half as many computations as the size of the number n.[8] However a simple observation makes it slightly more suitable for hand calculation with small numbers.

Lemma 4.4. *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 $1 \leq x \leq n$. Then $x(n+1-x) \equiv -2T_{x-1} \bmod n$.*

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

Proof. Recall that $x(n+1-x) \equiv x - x^2 \bmod n$ and $x - x^2 = x(1-x) = -2T_{x-1}$. ☑

This lemma makes it quite easy to write down the congruence classes of interest for Theorem 4.3. 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 $-2T_x$ to $-2T_{x+1}$, just subtract $2(x+1)$. We illustrate this now for $n = 15$:

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

We see that the appearance of the congruence class $3 \bmod 15$ at $x = 4$ and $x = 7$ 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 4.2 occurs not only at intervals of length equal to the smallest prime p.

The coincidence of congruence classes $-2T_k \equiv -2T_l \bmod n$ means that $2T_l - 2T_k$ is a multiple of n. The next proposition goes further, relating the value $l - k$ to the 2-factorization of n.

Proposition 4.5. *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 both of the pairs $(l-k, n)$ and $(l+k+1, n)$ have greatest common divisor (gcd) greater than 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 $t = 0$ contradicting that l and k are distinct. ☑

Taking the gcd of natural numbers can be done efficiently by Euclid's algorithm. 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 4.6 (2-factorization algorithm)**.** *Given an odd natural number n, one can obtain a non-trivial 2-divisor of n as follows.*

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

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

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.

Steps 1 and 2 can then be iterated on d *and* $n_1 = \frac{n}{d}$ *to obtain a complete 2-factorization of* n.

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 4.6 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, $n = a^2 - b^2$.[9] To see this, let $u = \frac{n+1}{2}$, so that when $x = u$ the product $x(n+1-x)$ is 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 really 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 method form the basis of the fastest known integer factorization algorithms, the *quadratic sieve* and *general number field sieve* [8]. It remains to be seen whether the algorithm of Theorem 4.6 admits improvements that could make it competitive. For now, it is a curiosity which we hope encourages the reader to explore the plunder of ideas which may come from non-binary thinking.

Acknowledgements. I thank an anonymous referee for helpful comments and criticisms. I'm also grateful to Craig Jensen for permission to think about this topic as a master's student, Ken Holladay for a helpful suggestion, Padi Fuster and Bradford Fournier for encouragement, and Mahir Can and Joseph Silverman for comments on a draft of this manuscript.

[9] See [2, Ch. 5] or [6, Ch. 3], for instance, for descriptions of these other algorithms.

References

[1] T. M. Apostol, *Introduction to analytic number theory*, Undergraduate Texts in Mathematics, Springer-Verlag, New York-Heidelberg, 1976. MR 0434929

[2] D. M. Bressoud, *Factorization and primality testing*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1989. MR 1016812

[3] D. A. Cox, *Primes of the form* $x^2 + ny^2$, second ed., Pure and Applied Mathematics (Hoboken), John Wiley & Sons, Inc., Hoboken, NJ, 2013, Fermat, class field theory, and complex multiplication. MR 3236783

[4] H. S. M. Coxeter, *Introduction to geometry*, second ed., John Wiley & Sons, Inc., New York-London-Sydney, 1969. MR 0346644

[5] D. Goldfeld, *Gauss's class number problem for imaginary quadratic fields*, Bull. Amer. Math. Soc. (N.S.) **13** (1985), no. 1, 23–37. MR 788386

[6] J. Hoffstein, J. Pipher, and J. H. Silverman, *An introduction to mathematical cryptography*, second ed., Undergraduate Texts in Mathematics, Springer, New York, 2014. MR 3289167

[7] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, second ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990. MR 1070716

[8] C. Pomerance, *A tale of two sieves*, Notices Amer. Math. Soc. **43** (1996), no. 12, 1473–1485. MR 1416721

[9] G. Rabinowitsch, *Eindeutigkeit der Zerlegung in Primzahlfaktoren in quadratischen Zahlkörpern*, J. Reine Angew. Math. **142** (1913), 153–164. MR 1580865

(Recibido en mayo de 2019. Aceptado en mayo de 2021)

Centro de Ciencias Matemáticas
Universidad Nacional Autónoma de México
Campus Morelia
Antigua Carretera a Pátzcuaro # 8701
Morelia, Michoacán, México
e-mail: aram@matmor.unam.mx