April 22–n-ary expansions and Gaussian integers

We look at binary and other expansions of real numbers. We also return to Gaussian integers.

Definition 1. *Let $n \in \mathbb{Z}$ with $n \geq 2$. Then every real number $\alpha \in \mathbb{R}$ with $0 \leq \alpha < 1$. can be uniquely written as*

$$\sum_{k=1}^{\infty} \frac{a_k}{n^k} = 0.a_1a_2a_3\ldots, a_k = a_k(x) \in \{0, 1, \ldots, n-1\}.$$

We call this the n-ary expansion of α. When $n = 2$, we call this binary, when $n = 10$, we call this decimal, and when $n = 16$, we call this hexidecimal.

We can expand this definition to all real numbers x, but the sum notation is more awkward. Typically we write something like

$$\sum_{k=-\infty}^{\infty} b_k n^k = \ldots b_2b_1b_0.b_{-1}b_{-2}b_{-3}\ldots$$

$$= \cdots + b_2n^2 + b_1n + b_0 + \frac{b_{-1}}{n} + \frac{b_{-2}}{n^2} + \cdots, \quad b_k = b_k(x) \in \{0, 1, \ldots, n-1\},$$

except there will be some $K \in \mathbb{Z}$ where $b_k = 0$ for all $k \geq K$. The b_k (or a_k in the first definition) are called digits.

Example 1. *When we look at the decimal expansion of a number x, we ask how many 10^i add up to x. If $x = 2314.123$, there are two 10^3, three 10^2, one 10^1, four 10^0, one 10^{-1}, two 10^{-2}, and three 10^{-3} (this may give you elementary school flash backs). We use this information to fill out the chart:*

10^3	10^2	10^1	10^0	10^{-1}	10^{-2}	10^{-3}
$\boxed{2}$	$\boxed{3}$	$\boxed{1}$	$\boxed{4}$	$\boxed{1}$	$\boxed{2}$	$\boxed{3}$

Now, to calculate binary, we do a similar thing, but count how many 2^n are in a number. We started with something easier: x with decimal expansion 43.75. Remember all binary digits are 0 or 1

$2^5 = 32$	$2^4 = 16$	$2^3 = 8$	$2^2 = 4$	$2^1 = 2$	$2^0 = 1$	$2^{-1} = \frac{1}{2}$	$2^{-2} = \frac{1}{4}$	$2^{-3} = \frac{1}{8}$
$\boxed{1}$	$\boxed{0}$	$\boxed{1}$	$\boxed{0}$	$\boxed{1}$	$\boxed{1}$	$\boxed{1}$	$\boxed{1}$	$\boxed{0}$

Finally, we do a hexidecimal for x with decimal expansion 2314.125. Normally hexidecimal has $a = 10, b = 11, c = 12, d = 13, e = 14, d = 15$, since we need more than 10 characters, but the for the table, we will just use $10, 11, 12, 13, 14, 15$.

Learning outcomes:
Author(s):

$16^2 = 256$	$16^1 = 16$	$16^0 = 1$	$16^{-1} = \frac{1}{16}$	$16^{-2} = \frac{1}{256}$
$\boxed{9}$	$\boxed{0}$	$\boxed{10}$	$\boxed{2}$	$\boxed{0}$

Definition 2. *If there exist a positive integer ρ and N such that $a_k = a_{k+\rho}$ for all $k \geq N$, then the n-ary expansion of α is* eventually periodic*; the sequence $a_N a_{N+1} \cdots a_{N+\rho-1}$ with ρ minimal is the* period *of α and ρ is the* period length*. If the smallest such N is 1, then α is* periodic*. An eventually periodic real number*

$$\alpha = 0.a_1a_2a_3 \ldots a_{N-1}a_Na_{N+1}\cdots a_{N+\rho-1}a_Na_{N+1}\cdots a_{N+\rho-1}a_Na_{N+1}\cdots a_{N+\rho-1}\cdots$$

is written

$$\alpha = 0.a_1a_2a_3 \ldots a_{N-1}\overline{a_Na_{N+1}\cdots a_{N+\rho-1}}.$$

Theorem 1. *Let $\alpha \in \mathbb{R}$ with $0 \leq \alpha < 1$. If α had an finite or eventually periodic n-ary expansion for $n \geq 2$, then $\alpha \in \mathbb{Q}$.*

Theorem 2. *Let $n \in \mathbb{Z}, n \geq 2$ and $x \in [0, 1)$. Then*

(a) *x has a finite n-ary expansion if and only if there exist $p, q \in \mathbb{Z}^+, (p, q) = 1, x = \frac{p}{q}$, and $p_i \mid n$ for all $p_i \mid q$ for p_i prime.*

(b) *x has a purely-periodic n-ary expansion if and only if there exist $p, q \in \mathbb{Z}(p, q) = 1, x = \frac{p}{q}$, and $(q, n) = 1$.*

For $n \in \mathbb{Z}, n \geq 2$, divide the unit interval $[0, 1)$ into intervals $\left[\frac{i}{n}, \frac{i+1}{n}\right)$ where $i = 0, 1, 2, \ldots, n-1$. If a number $x \in \left[\frac{i}{n}, \frac{i+1}{n}\right)$, then the first digit of the n-art expansion is i

For example, binary divides partitions $[0, 1)$ into $[\boxed{0}, \boxed{\frac{1}{2}})$ and $[\boxed{\frac{1}{2}}, \boxed{1})$. 5-ary partitions $[0, 1)$ into $[\boxed{0}, \boxed{\frac{1}{5}})$,$[\boxed{\frac{1}{5}}, \boxed{\frac{2}{5}})$, $[\boxed{\frac{2}{5}}, \boxed{\frac{3}{5}})$,$[\boxed{\frac{3}{5}}, \boxed{\frac{4}{5}})$, and $[\boxed{\frac{4}{5}}, \boxed{1})$.

To get the second digit, we break each of these intervals into n smaller intervals $\left[\frac{i}{n} + \frac{j}{n^2}, \frac{i}{n} + \frac{j+1}{n^2}\right), 0 \leq i \leq n-1, 0 \leq j \leq n-1$. For each $x \in \left[\frac{i}{n} + \frac{j}{n^2}, \frac{i}{n} + \frac{j+1}{n^2}\right), x = 0.ij\ldots$. For example, the partition for the $(1/4)^{th}$ digit in binary is $[\boxed{0}, \boxed{\frac{1}{4}})$, $[\boxed{\frac{1}{4}}, \boxed{\frac{2}{4}})$, $[\boxed{\frac{1}{2}}, \boxed{\frac{3}{4}})$, and $[\boxed{\frac{3}{4}}, \boxed{1})$.

Determining the rest of the digits involves iterating this process.

Back to Gaussian Integers and Divisibilty

Instead of looking at other ways of writing real numbers, we can look at imaginary numbers. Remembering back to the January, the *Gaussian integers* $\mathbb{Z}[i]$ are the set of complex numbers $\{a + bi : a, b \in \mathbb{Z}, i^2 = -1\}$. We define addition and subtraction as normal:

$$a + bi + c + di = (a + c) + (b + d)i, \quad (a + bi)(c + di) = (ac - bd) + (ad + bc)i.$$

$ab = 1$ has four solutions: $a = b = \pm 1$ and $a = -b = \pm i$. In this new setting, it is not clear what it means for $1 < a + bi$. Is $1 < -1 + 2i$?

Definition 3. *A number $p \in \mathbb{Z}[i]$ is* prime *if $p \mid ab$ implies $p \mid a$ or $p \mid b$ for all $a, b \in \mathbb{Z}[i]$.*

Now, a quick note about the regular integers: $2 = (1 + i)(1 - i)$, so is not prime in $\mathbb{Z}[i]$. Our goal is to show which integers are prime in $\mathbb{Z}[i]$.

Theorem 3. *The primes in $\mathbb{Z}[i]$ have the form:*

- *$p \in \mathbb{Z}$ where p is a prime and $p \equiv 3 \pmod 4$*
- *$a + bi$ where $a^2 + b^2$ is prime.*

Theorem 4 (Contrapositive of Textbook Lemma 2.14)**.** *$a^2 + b^2 \not\equiv 3 \pmod 4$.*

Theorem 5 (Textbook Lemma 2.13)**.** *If p is prime and $p \equiv 1 \pmod 4$, then there exist $a, b \in \mathbb{Z}$ such that $a^2 + b^2 = p$.*

We can use this to see that $p = (a + bi)(a - bi)$. So our only candidates for primes $a + 0i$ are those congruent to 3 mod 4.

Definition 4. *A* unit *is a Gaussian (or regular) integer u where $u \mid 1$. The units in $\mathbb{Z}$ are $1, -1$, and the units in $\mathbb{Z}[i]$ are $1, -1, i, -i$.*

Definition 5. *The* Gaussian norm *is $N(a + bi) = a^2 + b^2$. The norm is completely multiplicative, since $N((a + bi)(c + di)) = (ac - bd)^2 + (ad + bc)^2 = (a^2 + b^2)(c^2 + d^2)$.*

How would we divide $237 + 504i$ by $15 - 17i$? Well, we could require that the remainder is less that $N(15 - 17i) = 514$. In this case,

$$237 + 504i = (-10 + 23i)(15 - 17i) + (-4 - 11i),$$

and $N(-4 - 11i) = 137 < N(15 - 17i) = 514$.

Theorem 6 (Division algorithm for Gaussian integers)**.** *Let $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$. Then there are Gaussian integers γ and ρ so that*

$$\alpha = \beta\gamma + \rho \quad N(\rho) < N(\beta).$$

Proof If with divide the equation we are trying to solve by β, it becomes

$$\frac{\alpha}{\beta} = \gamma + \frac{\rho}{\beta} \quad N(\frac{\rho}{\beta}) < 1.$$

If the ratio $\frac{\alpha}{\beta}$ is a Gaussian integer, then $\gamma = \frac{\alpha}{\beta}$ and $\rho = 0$. Otherwise, $\frac{\alpha}{\beta}$ is in a square with corners $a + bi, a + 1 + bi, a + (b + 1)i, a + 1 + (b + 1)i$. We set γ equal to the closest corner of the square to $\frac{\alpha}{\beta}$ as in the image.

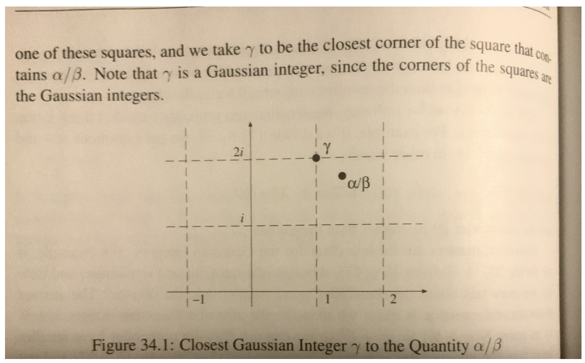
one of these squares, and we take γ to be the closest corner of the square that contains α/β. Note that γ is a Gaussian integer, since the corners of the squares are the Gaussian integers.

Figure 34.1: Closest Gaussian Integer γ to the Quantity α/β

The farthest that $\frac{\alpha}{\beta}$ can be from γ is when it is the middle of the circle (Distance from $\frac{\alpha}{\beta}$ to γ) $\leq \frac{\sqrt{2}}{2}$. Now, the norm is also the square of the distance function, so squaring both sides gives $N(\frac{\alpha}{\beta} - \gamma) \leq \frac{1}{2}$.

Multiplying both sides of the equation by $N(\beta)$, we get $N(\alpha - \beta\gamma) \leq \frac{N(\beta)}{2}$. Now, set $\rho = \alpha - \beta\gamma$, we get

$$\alpha = \beta\gamma + \rho \quad N(\rho) < N(\beta)$$

(and in fact $N(\rho) \leq \frac{N(\beta)}{2}$). ■