MATH 4573: Elementary Number Theory We're online now!

Claire Merriman

February 5, 2024

Contents

Preclass assignment for March 23 4
Participation assignment for March 23 5
Euler ϕ function: number of relatively prime positive integers less than n 5
Other common number theory functions 6
March 25–Primitive roots and quadratic residues 7
Review facts about primitive roots 7
Review facts about quadratic residues 8
Quadratic reciprocity 10
March 27 – Lemma's for quadratic reciprocity 11
March 30–Proof of quadratic reciprocity 18
April 1–Möbius inversion formula 23
April 3–Diophantine equations 28
Linear Diophantine equations 28
Nonlinear Diophantine equations 30
April 6–Pythagorean triples and Fermat's Last Theorem 32
Pythagorean triples 32
Fermat's Last Theorem 33
April 8–Sums of squares 37
Sum of Two Squares 37
April 10–Sums of squares 42
Sum of three squares 42
Sum of four squares 43
April 13–Decimal expansions 47
A very different look at decimal numbers 50
April 15–Continued fractions 52
Continued fractions 52
A very different look at decimal numbers 55
Back to continued fractions 56
April 17–Continued fractions calculations and theorems 58
April 20–Farey sequence 64

April 22–n-ary expansions and Gaussian integers 69
n-ary expansions 69
Back to Gaussian Integers and Divisibilty 71

Preclass assignment for March 23

This assignment is designed to give you practice using this format.

This format allows you to answer questions directly in your browser. It will also grade some of the questions immediately. Let's test it out!

Question 1 *Did you find this page?*

Multiple Choice:

(a) *Yes* ✓

(b) *No*

We can also do math!

Question 2 *Find the smallest, nonnegative solution to* $x \equiv 10 \pmod 6$. $x =$ $\boxed{4}$.

Learning outcomes:
Author(s): Claire Merriman

Participation assignment for March 23

This assignment looks at arithmetic functions in number theory. We have already seen the examples $\phi(n) = \#\{x : 0 < x < n, (x, n) = 1\}$ and the floor/ greatest integer function $\lfloor x \rfloor$ =greatest integer less than x. So far, we have a formula for the value of $\phi(n)$ when n is prime or the product of two distinct primes. We will prove a general formula for the ϕ function and look at some other functions.

Euler ϕ function: number of relatively prime positive integers less than n

Recall from before break that $\phi(p) = p - 1$ if and only if p is prime. We also proved that $\phi(pq) = (p-1)(q-1)$ for primes p and q.

On the homework, you will prove that for relatively prime positive integers m and n, $\phi(mn) = \phi(m)\phi(n)$. Since Ximera can really only handle numerical answers, let's prove this is true for a particular example:

Question 3 *Let us prove that $\phi(20) = \phi(4)\phi(5)$. First, note that $\phi(4) =$ $\boxed{2}$ and $\phi(5) =$ $\boxed{4}$, so $\phi(20) =$ $\boxed{8}$.*

(a) *A number a is relatively prime to 20 if and only if a is relatively prime to $\boxed{4}$ and $\boxed{5}$ (first blank should be smaller than second blank for the automatic grading to work, both should be relevant to what we are trying to show).*

(b) *We can partition the positive integers less that 20 into*

$$0 \equiv \boxed{4} \equiv \boxed{8} \equiv \boxed{12} \equiv \boxed{16} \pmod 4$$
$$1 \equiv \boxed{5} \equiv \boxed{9} \equiv \boxed{13} \equiv \boxed{17} \pmod 4$$
$$2 \equiv \boxed{6} \equiv \boxed{10} \equiv \boxed{14} \equiv \boxed{18} \pmod 4$$
$$3 \equiv \boxed{7} \equiv \boxed{11} \equiv \boxed{15} \equiv \boxed{19} \pmod 4$$

For any b in the range $0, 1, 2, 3$, define s_b to be the number of integers a in the range $0, 1, 2, \ldots, 19$ such that $a \equiv b \pmod 4$ and $\gcd(a, 20) = 1$. Thus, $s_0 =$ $\boxed{0}$, $s_1 =$ $\boxed{4}$, $s_2 =$ $\boxed{0}$, and $s_3 =$ $\boxed{4}$.

We can see that when $(b, 4) = 1$, $s_b = \phi($ $\boxed{5}$ $)$ and when $(b, 4) > 1$, $s_b =$ $\boxed{0}$.

Learning outcomes:
Author(s): Claire Merriman

(c) $\phi(20) = s_0 + s_1 + s_2 + s_3$. *Why?*

All of the positive integers less than or equal to 20 *is in exactly one of the congruence classes above. The* s_i *count how many integers in each congruence class are relatively prime to* 20*. If we add them up, we have counted all positive integers less than or equal to* 20*.*

(d) *We have seen that* $\phi(20) = s_0 + s_1 + s_2 + s_3$*, that when* $(b, 4) = 1$*,* $s_b = \phi(5)$*, and that when* $(b, 4) > 1$*,* $s_b = 0$*. Thus, we can say that* $\phi(20) = 0 + \phi(\boxed{5}) + 0 + \phi(\boxed{5})$*. To finish the "proof" we show that there are* $\phi(\boxed{4})$ *integers* b *where* $(b, 4) = 1$*.*

There are $\boxed{4}$ *congruence classes modulo 4. Of these,* $\boxed{2} = \phi(\boxed{4})$ *have elements that are relatively prime to* 20*. Thus,* $\phi(20) = \phi(4)\phi(5)$*.*

Other common number theory functions

We are going to look at some other functions that show up in analytic number theory.

- $d(n)$ is the number of positive divisors of n. For example, $d(12) = \boxed{6}$. We introduce the notation $\sum_{d|n}$ as "the sum over the divisors of n," called the *divisor sum*. For the normal sum: $\sum_{i=1}^{n} 1 = \boxed{n}$. Then, $\sum_{d|n} 1 = \boxed{d(n)}$.

- $\sigma(n)$ is the sum of positive divisors of n. For example, $\sigma(12) = \boxed{28}$. Then $\sum_{d|n} \boxed{d} = \sigma(n)$.

- $\sigma_k(n)$ is sum of the k^{th} powers of positive divisors of n. For example, $\sigma_2(12) = 1^2 + 2^2 + 3^2 + 4^2 + 6^2 + 12^2 = 210$. Generally, $\sum_{d|n} \boxed{d^k} = \sigma_k(n)$.

- $\omega(n)$ is the number of distinct prime divisors of n. For example, $\omega(12) = \boxed{2}$. We can modify the divisor sum to sum over prime divisors of n, $\sum_{p|n}$. Then, $\sum_{p|n} \boxed{1} = \omega(n)$.

- $\Omega(n)$ is the number of primes dividing n counting multiplicity. For example, $\Omega(12) = \boxed{3}$. Then $\sum_{\boxed{p^\beta}|n} 1 = \Omega(n)$.

March 25–Primitive roots and quadratic residues

We will review a some points about primitive roots, quadratic residues, and the Legendre symbol from before break, then finish those sections.

Review facts about primitive roots

Question 4 *For a prime p, a primitive root there exists modulo p.*

Multiple Choice:

(a) *Always* ✓

(b) *Sometimes*

(c) *Never*

Question 5 *If $n = pq$ where p and q are distinct primes, then there exists a primitive root modulo n.*

Multiple Choice:

(a) *Always*

(b) *Sometimes* ✓

(c) *Never*

Question 6 *If $n = 2^k$ and $k \geq 3$, then there exists a primitive root modulo n.*

Multiple Choice:

(a) *Always*

Learning outcomes:
Author(s): Claire Merriman

(b) *Sometimes*

(c) *Never* ✓

Question 7 *If $n = km$ where k and m are relatively prime and greater than 2, then there exists a primitive root modulo n.*

Multiple Choice:

(a) *Always*

(b) *Sometimes*

(c) *Never* ✓

Question 8 *There exists primitive roots modulo n when for $n =$*

Select All Correct Answers:

(a) *1* ✓

(b) *p a prime* ✓

(c) *4* ✓

(d) *2^m for $m \geq 3$*

(e) *p^m for p an odd prime* ✓

(f) *$2p^m$ for p an odd prime* ✓

(g) *n a composite number with at least two distinct odd prime factors*

Review facts about quadratic residues

Question 9 *Let $p > 2$ be a prime, and let a be an integer between 0 and $p - 1$.*

- *If a is a quadratic residue modulo p, then $a^{\frac{p-1}{2}} = \boxed{1}$.*
- *If a is a quadratic nonresidue modulo p, then $a^{\frac{p-1}{2}} = \boxed{-1}$.*

- *Otherwise,* $a^{\frac{p-1}{2}} = \boxed{0}$.

Question 10 *Euler's identity: Let* $p > 2$ *be a prime, and let* a *be an integer. Then* $\left(\boxed{\frac{a}{p}}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

Theorem 1. *Let* $p > 2$ *be prime.*

- *If* $p \equiv 1 \pmod 4$*, then* -1 *is a quadratic residue modulo* p*.*
- *If* $p \equiv 3 \pmod 4$*, then* -1 *is a quadratic nonresidue modulo* p*.*

Proof For an arbitrary prime $p > 2$, Euler's identity tells us that $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$. Note that, we have that $\left(\frac{-1}{p}\right)$ is either $+1$ or -1 by definition, and $(-1)^{\frac{p-1}{2}}$ is also either $+1$ or -1. Since $1 \not\equiv -1 \pmod{p}$, the two sides of the congruence are actually equal. That is, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

The completion of the proof involves applying the answer to the preclass assignment, and the proof is on homework 9. ■

Question 11 *Let* $p > 2$ *be prime, and let* a *and* b *be integers between* 1 *and* $p - 1$.

- *If* ab *is a quadratic residue, then*

  Select All Correct Answers:

  (a) *a and b are both quadratic residues* ✓
  (b) *a and b are both quadratic nonresidues* ✓
  (c) *One of a and b is a quadratic residue and the other is a quadratic nonresidue*

- *If* ab *is a quadratic nonresidue, then*

  Select All Correct Answers:

  (a) *a and b are both quadratic residues* ✓
  (b) *a and b are both quadratic nonresidues* ✓
  (c) *One of a and b is a quadratic residue and the other is a quadratic nonresidue*

Quadratic reciprocity

We are going to explore the relationship between $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$. Let's look at an example:

Question 12 *We want to know if* 3 *is a quadratic residue modulo* 107. *It would be a lot easier to check if* 107 *is a quadratic residue modulo* 3. *We know that* $107 \equiv \boxed{2} \pmod 3$, *so* $\left(\frac{107}{3}\right) = \boxed{-1}$. *It would be nice if this also gave us* $\left(\frac{3}{107}\right)$.

Question 13 *Another example: Find* $\left(\frac{p}{5}\right)$ *and* $\left(\frac{5}{p}\right)$.

p	3	5	7	11	13
$\left(\frac{p}{5}\right)$	$\boxed{-1}$	$\boxed{0}$	$\boxed{-1}$	$\boxed{1}$	$\boxed{-1}$
$\left(\frac{5}{p}\right)$	-1	0	-1	1	-1

Question 14 *Another example: Find* $\left(\frac{p}{7}\right)$ *and* $\left(\frac{7}{p}\right)$.

p	3	5	7	11	13
$\left(\frac{p}{7}\right)$	$\boxed{-1}$	$\boxed{-1}$	0	$\boxed{1}$	$\boxed{-1}$
$\left(\frac{7}{p}\right)$	$\boxed{1}$	$\boxed{-1}$	0	-1	-1

This gives some evidence for our theorem:

Theorem 2. *Let* p *and* q *be odd primes with* $p \neq q$.

- *if* $p \equiv 1 \pmod 4$ *or* $q \equiv 1 \pmod 4$, *then* $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$
- *if* $p \equiv q \equiv 3 \pmod 4$, *then* $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$

Our goal for Friday is to prove this.

March 27 – Lemma's for quadratic reciprocity

We will prove the two lemmas needed in order to prove quadratic reciprocity.

We want to prove

Theorem 1 (Quadratic reciprocity)**.** *Let p and q be primes with $p \neq q$, then*

- *if* $p \equiv 1 \pmod 4$ *or* $q \equiv 1 \pmod 4$, *then* $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$.
- *if* $p \equiv q \equiv 3 \pmod 4$, *then* $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

Let's try some examples:

Question 15 $\left(\frac{11}{47}\right) = \boxed{-1} * \left(\frac{47}{11}\right)$. *We can reduce* $47 \equiv \boxed{3} \pmod{11}$, *which*

Multiple Choice:

(a) *is* ✓

(b) *is not*

a quadratic residue modulo 11. Thus, $\left(\frac{11}{47}\right) = \boxed{-1}$ *and* $\left(\frac{47}{11}\right) = \boxed{1}$.

Question 16 $\left(\frac{3}{107}\right) = \boxed{-1} * \left(\frac{107}{3}\right)$. *We can reduce* $107 \equiv \boxed{2} \pmod{3}$, *which*

Multiple Choice:

(a) *is*

(b) *is not* ✓

Learning outcomes:
Author(s): Claire Merriman

a quadratic residue modulo 3. Thus, $\left(\frac{107}{3}\right) = \boxed{-1}$ *and* $\left(\frac{3}{107}\right) = \boxed{1}$.

We are going to restate quadratic reciprocity as

Theorem 2 (Restatement of quadratic reciprocity)**.** *Let p and a be odd primes with $p \neq q$. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Theorem 3. *The restatement of quadratic reciprocity implies quadratic reciprocity.*

Proof Let p and q be odd primes with $p \neq q$. We assume that $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ is true. Then we have two cases:

- $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$ [To show $\left(\frac{p}{q}\right) = \boxed{1} * \left(\frac{q}{p}\right)$.]

  Without loss of generality, we assume $p \equiv 1 \pmod 4$. Then there exists a $k \in \mathbb{Z}$ such that $p = 4k + 1$. This implies that $\frac{p-1}{2} = 2k$. Thus,

  $$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = 1^{\frac{q-1}{2}} = 1.$$

  Thus, we have that $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ must either both be $+1$ or both be -1.

- $p \equiv q \equiv 3 \pmod 4$[To show $\left(\frac{p}{q}\right) = \boxed{-1} * \left(\frac{q}{p}\right)$.] There exists $k, m \in \mathbb{Z}$ such that $p = 4k + 3$ and $q = 4m + 3$. This implies that $\frac{p-1}{2} = 2k + 1$ and $\frac{q-1}{2} = 2k + 1$. Thus,

  $$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = (-1)^{\frac{q-1}{2}} = -1.$$

  Thus, we have that exactly one of $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ is $+1$ and the other is -1.

■

In order to prove this, we first need to prove two rather technical lemmas. Then we will use a geometric proof to finish.

Theorem 4 (Gauss's lemma)**.** *Let p be an odd prime number and let $a \in \mathbb{Z}$ with $p \nmid a$. Let n be the number of least positive residues of the integers $a, 2a, \ldots, \frac{p-1}{2}a$ that are greater than $\frac{p}{2}$. Then*

$$\left(\frac{a}{p}\right) = (-1)^n.$$

Question 17 *Use Gauss's lemma to find $\left(\frac{6}{11}\right)$. We need to find n, the number of least nonnegative positive residues of the integers $6, 2*6, 3*6, 4*6, 5*6$ greater that $\boxed{5.5}$ We have*

$$\begin{aligned} 6 &\equiv \boxed{6} \pmod{11} \\ 2*6 &\equiv \boxed{1} \pmod{11} \\ 3*6 &\equiv \boxed{7} \pmod{11} \\ 4*6 &\equiv \boxed{2} \pmod{11} \\ 5*6 &\equiv \boxed{8} \pmod{11} \end{aligned}$$

Thus, $n = \boxed{3}$ and $(-1)^n = \boxed{-1}$.

We now prove Gauss's lemma.

Proof Let $r_1, r_2, \ldots r_n$ be the least nonnegative residues of the integers $a, 2a, \ldots, \frac{p-1}{2}a$ that are greater than $\frac{p}{2}$ and $s_1, s_2, \ldots, s_m$ be the least nonnegative residues that are less that $\frac{p}{2}$. Note that no r_i or s_j is 0, since p does not divide any of $a, 2a, \ldots \frac{p-1}{2}$. Consider the $\frac{p-1}{2}$ integers given by

$$p - r_1, p - r_2, \ldots, p - r_n, s_1, s_2, \ldots, s_m.$$

We want to show that these integers are the integers from 1 to $\frac{p-1}{2}$ inclusive in some order. Since each integer is less than or equal to $\frac{p-1}{2}$, it suffices to show that no two of these integers are congruent modulo p.

If $p - r_i \equiv p - r_j \pmod{p}$ for some $i \neq j$, then $r_i \equiv r_j \pmod{p}$, but this implies that there exists some $k_i, k_j \in \mathbb{Z}$ such that $r_i = k_i a \equiv k_j a = r_j \pmod{p}$ with $k_i \neq k_j$ and $1 \leq k_i, k_j \leq \boxed{\frac{p-1}{2}}$. Since

Multiple Choice:

(a) $p \nmid a$ ✓

(b) $p \mid a$

we know that the multiplicative inverse of a modulo p

Multiple Choice:

(a) exists ✓

(b) does not exist

and thus $k_i \equiv k_j \pmod{p}$, a contradiction. Thus, no two of the first n integers are congruent modulo p.

Similarly, no two of the second m integers are congruent. Now, if $p - r_i \equiv s_j \pmod{p}$, for some i and j, then $-r_i \equiv s_j \pmod{p}$. Thus, there exists $k_i, k_j \in \mathbb{Z}$ such that $-r_i = -k_i a \equiv k_j a = s_j \pmod{p}$ with $k_i \neq k_j$ and $1 \leq k_i, k_j \leq \frac{p-1}{2}$. Since $p \nmid a$, we know that the multiplicative inverse of a modulo p exists, and thus $-k_i \equiv k_j \pmod{p}$, a contradiction. Thus, the $\frac{p-1}{2}$ integers $p - r_1, p - r_2, \ldots, p - r_n, s_1, s_2, \ldots, s_m$ are the integers $1, 2, \ldots, \frac{p-1}{2}$ in some order.

Then,

$$(p - r_1)(p - r_2) \cdots (p - r_n) s_1 s_2 \cdots s_m \equiv \frac{p-1}{2}! \pmod{p}$$

implies that

$$(-1)^n r_1 r_2 \cdots r_n s - 1 s_2 \cdots s_m \equiv \frac{p-1}{2}! \pmod{p}.$$

By the definition of r_i and s_j, we have

$$(-1)^n a(2a)(3a) \cdots (\frac{p-1}{2}a) \equiv \frac{p-1}{2}! \pmod{p}.$$

By reordering, we have

$$(-1)^n a^{\frac{p-1}{2}} \frac{p-1}{2}! \equiv \frac{p-1}{2}! \pmod{p}.$$

Thus, $(-1)^n a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, and $a^{\frac{p-1}{2}} \equiv (-1)^n \pmod{p}$. By Euler's criterion, we get that $\left(\frac{a}{p}\right) \equiv (-1)^n \pmod{p}$. Since both sides of the congruence must be ± 1, we have $\left(\frac{a}{p}\right) = (-1)^n$. ■

We are going to prove a result about $\left(\frac{2}{p}\right)$ before our next technical lemma.

Theorem 5. *Let p be an odd prime. Then*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & if\ p \equiv 1,7 \pmod 8 \\ -1 & if\ p \equiv 3,5 \pmod 8. \end{cases}$$

Proof By Gauss's Lemma, we have that $\left(\frac{2}{p}\right) = (-1)^n$, where n is the number of least positive residues of the integers $2, 2*2, 2*3, \ldots, \frac{p-1}{2}$ that are greater than $\frac{p}{2}$. Let $k \in \mathbb{Z}$ with $1 \leq k \leq \frac{p-1}{2}$. Then $2k < \left\lceil \frac{p}{2} \right\rceil$ if and only if $k < \frac{p}{4}$; so $\left\lfloor \left\lceil \frac{p}{4} \right\rceil \right\rfloor$ of the integers $2, 2*2, 2*3, \ldots, \frac{p-1}{2}$ that are less than $\frac{p}{2}$, where $\lfloor \cdot \rfloor$ is the greatest integer (or floor) function. So, $\frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor$ of these integers are greater than $\frac{p}{2}$, from which

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor}$$

by Gauss's Lemma. For the first equality, it suffices to show that

$$\frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor \equiv \frac{p^2-1}{8} \pmod 2.$$

If $p \equiv 1 \pmod 8$, the $p = 8k+1$ for some $k \in \mathbb{Z}$. That gives us

$$\frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor = \frac{(8k+1)-1}{2} - - \left\lfloor \frac{8k+1}{4} \right\rfloor = 4k - 2k = 2k \equiv 0 \pmod 2$$

and

$$\frac{p^2-1}{8} = \frac{8k+1)^2-1}{8} = 8k^2 + 2k \equiv 0 \pmod 2.$$

Thus, holds when $p \equiv 1 \pmod 8$. The rest of the cases are part of homework 9. ■

Theorem 6 (Rephrased textbook Theorem 3.3)**.** *Let p be an odd prime number and let $a \in \mathbb{Z}$ with $p \nmid a$ and a odd. If*

$$N = \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor,$$

then

$$\left(\frac{a}{p}\right) = (-1)^N.$$

Where $\lfloor \cdot \rfloor$ is the greatest integer (or floor) function. This gives us another way of computing Legendre symbols. Let's look at an example before diving into the technical proof.

Question 18 *Use this lemma to find* $\left(\frac{7}{11}\right)$. *We have*

$$\begin{aligned} N &= \sum_{j=1}^{\boxed{5}} \left\lfloor \frac{j7}{11} \right\rfloor = \left\lfloor \frac{7}{11} \right\rfloor + \left\lfloor \frac{14}{11} \right\rfloor + \left\lfloor \frac{21}{11} \right\rfloor + \left\lfloor \frac{28}{11} \right\rfloor + \left\lfloor \frac{35}{11} \right\rfloor \\ &= \boxed{0} + \boxed{1} + \boxed{1} + \boxed{2} + \boxed{3} \\ &= \boxed{7} \end{aligned}$$

So $\left(\frac{7}{11}\right) = (-1)^{\boxed{7}} = \boxed{-1}$.

Proof Let $r_1, r_2, \ldots, r_n$ are the least nonnegative representatives of $a, 2a, 3a, \ldots, \frac{p-1}{2}a$ modulo p which are greater than $\frac{p}{2}$ and $s_1, s_2, \ldots, s_m$ be the least nonnegative representatives of $a, 2a, 3a, \ldots, \frac{p-1}{2}a$ modulo p which are less than $\frac{p}{2}$. Then for each $j = 1, 2, \ldots, \frac{p-1}{2}$ we have that

$$ja = p\left\lfloor \frac{ja}{p} \right\rfloor + (\text{remainder depending on } j)$$

where each of $r_1, r_2, \ldots, r_n, s_1, s_2, \ldots, s_m$ appears exactly once as a remainder. By adding the $\frac{p-1}{2}$ equations above, we get

$$\sum_{j=1}^{\frac{p-1}{2}} ja = \sum_{j=1}^{\frac{p-1}{2}} p\left\lfloor \frac{ja}{p} \right\rfloor + \sum_{j=1}^{n} r_j + \sum_{j=1}^{m} s_j \tag{1}$$

The integers $p - r_1, p - r_2, \ldots, p - r_n, s_1, s_2, \ldots, s_m$ are precisely the integers from 1 to $\frac{p-1}{2}$ in some order, so we have

$$\sum_{j=1}^{\frac{p-1}{2}} j = \sum_{j=1}^{n}(p - r_j) + \sum_{j=1}^{m} s_j = pn - \sum_{j=1}^{n} r_j + \sum_{j=1}^{m} s_j \tag{2}$$

We subtract (2) from (1) to get

$$\sum_{j=1}^{\frac{p-1}{2}} ja - \sum_{j=1}^{\frac{p-1}{2}} j = \sum_{j=1}^{\frac{p-1}{2}} p\left\lfloor \frac{ja}{p} \right\rfloor + \sum_{j=1}^{n} r_j + \sum_{j=1}^{m} s_j - \left(pn - \sum_{j=1}^{n} r_j + \sum_{j=1}^{m} s_j \right)$$
$$= \sum_{j=1}^{\frac{p-1}{2}} p\left\lfloor \frac{ja}{p} \right\rfloor - pn + 2\sum_{j=1}^{n} r_j.$$

Now, we can factor the left hand side to get

$$(\boxed{a-1}) \sum_{j=1}^{\frac{p-1}{2}} j = \sum_{j=1}^{\frac{p-1}{2}} p\left\lfloor \frac{ja}{p} \right\rfloor - pn + 2\sum_{j=1}^{n} r_j.$$

Reducing both sides of the equation modulo 2 gives

$$0 \equiv \sum_{j=1}^{\frac{p-1}{2}} p\left\lfloor \frac{ja}{p} \right\rfloor - n \pmod 2$$

since $p \equiv \boxed{1} \pmod 2$. Equivalently $n \equiv \sum_{j=1}^{\frac{p-1}{2}} p\left\lfloor \frac{ja}{p} \right\rfloor \pmod 2$.

Thus, $n \equiv N \pmod 2$, thus $\left(\frac{a}{p}\right) = (-1)^n = (-1)^N$. ■

March 30–Proof of quadratic reciprocity

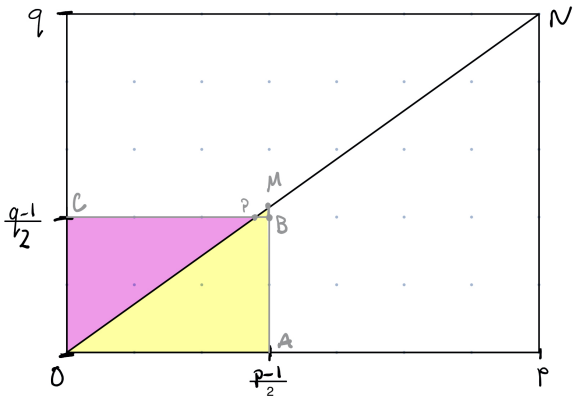
We finally prove quadratic reciprocity!

Theorem 7 (Restatement of quadratic reciprocity)**.** *Let p and a be odd primes with $p \neq q$. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Definition 1. *A* lattice point *is a point $(x, y) \in \mathbb{R}^2$ where $x, y \in \mathbb{Z}$. We can write this as $(x, y) \in \mathbb{Z}^2$.*

Proof Without loss of generality, assume that $p > q$. We draw the rectangle $O = (0, 0), A = \left(\frac{p-1}{2}, 0\right), B = \left(\frac{p-1}{2}, \frac{q-1}{2}\right)$, and $C = \left(0, \frac{q-1}{2}\right)$, like in the graphic below:



The participation assignment is to count the lattice points in the rectangle $OABC$ outlined in grey, including those on the lines AB and BC, but not those on OA or OC.

In order to count these lattice points another way, we are going to show that there are N_1 lattice points in the triangle OPC not including OC(pink) and N_2 lattice points in in OAM not including OA (yellow), thus the total number of lattice points is $N_1 + N_2$. We will find that $N_1 = \sum_{j=1}^{\frac{q-1}{2}} \left\lfloor \frac{jp}{q} \right\rfloor$ and $N_2 = \sum_{j=1}^{\frac{-1}{2}} \left\lfloor \frac{jq}{p} \right\rfloor$.

Learning outcomes:
Author(s): Claire Merriman

Thus, by the previous lemma, $\left\lfloor \frac{p}{q} \right\rfloor = (-1)^{N_1}$ and $\left\lfloor \frac{q}{p} \right\rfloor = (-1)^{N_2}$, which will let us finish the proof.

We will do an examples first:

Example 1. *We look at the example above with $p = 7$ and $q = 5$.*

a) The line ON has slope $\boxed{\frac{5}{7}}$. Since p and q are distinct primes, there are no lattice points on ON except the endpoints.

b) The x-coordinate of M is $\boxed{3}$, y-coordinate of M is $\boxed{\frac{15}{7}}$.

c) The y-coordinate of M lies between two consecutive integers $\boxed{2}$ and $\boxed{3}$.

Thus, the triangle PMB has no lattice points except possibly those on PB. We can then count the number of lattice points in $OABC$ by adding the number of lattice points in OCP to those in OAM.

To find N_1, the number of lattice points in OPC, not including those on OC, we count how many lattice points on the line $y = j$ are to the left of ON for $j = 1, 2, \ldots, \frac{q-1}{2}$ (in our case, this is only $j = 1, 2$.) Another was of saying this is for each j, we want the number of nonnegative integers less than

Multiple Choice:

(a) $\frac{7j}{5}$ ✓

(b) $\frac{5j}{7}$

Thus, we have for each j, there are

Multiple Choice:

(a) $\left\lfloor \frac{7j}{5} \right\rfloor$ ✓

(b) $\left\lfloor \frac{5j}{7} \right\rfloor$

lattice points in OPC. Then $N_1 =$

Multiple Choice:

(a) $\sum_{j=1}^{2} \left\lfloor \frac{7j}{5} \right\rfloor$ ✓

(b) $\sum_{j=1}^{2} \left\lfloor \frac{5j}{7} \right\rfloor$

To find N_2, we use a similar counting method on OAM. Now, we count the lattice points on $x = j$ for $j = 1, 2, \ldots, \frac{p-1}{2}$. Thus, for each j, we want the number of nonnegative integers less than

Multiple Choice:

(a) $\frac{7j}{5}$

(b) $\frac{5j}{7}$ ✓

Thus, we have for each j, there are

Multiple Choice:

(a) $\left\lfloor \frac{7j}{5} \right\rfloor$

(b) $\left\lfloor \frac{5j}{7} \right\rfloor$ ✓

l attice points in OPC. Then $N_2 =$

Multiple Choice:

(a) $\sum_{j=1}^{3} \left\lfloor \frac{7j}{5} \right\rfloor$ ✓

(b) $\sum_{j=1}^{3} \left\lfloor \frac{5j}{7} \right\rfloor$

Now we generalize this idea to any odd primes p and q with $p > q$.

a) The line ON has slope $\frac{q}{p}$. Since p and q are distinct primes, there are no lattice points on ON except the endpoints.

b) The x-coordinate of M is $\frac{p-1}{2}$, y-coordinate of M is $\frac{(p-1)}{2}\frac{q}{p} = \frac{q}{2} - \frac{q}{2p}$.

c) The y-coordinate of M lies between two consecutive integers $\frac{q-1}{2}$ and $\frac{q+1}{2}$, since

$$\frac{q-1}{2} = \frac{q}{2} - \frac{1}{2} < \frac{q}{2} - \frac{q}{2p} < \frac{q}{2} < \frac{q+1}{2}$$

Thus, the triangle PMB has no lattice points except possibly those on PB. We can then count the number of lattice points in $OABC$ by adding the number of lattice points in OCP to those in OAM.

To find N_1, the number of lattice points in OPC, not including those on OC, we count how many lattice points on the line $y = j$ are to the left of ON for $j = 1, 2, \ldots, \frac{q-1}{2}$. Another was of saying this is for each j, we want the number of nonnegative integers less than

Multiple Choice:

(a) $\frac{jp}{q}$ ✓

(b) $\frac{jq}{p}$

Thus, we have for each j, there are

Multiple Choice:

(a) $\left\lfloor \frac{jp}{q} \right\rfloor$ ✓

(b) $\left\lfloor \frac{jq}{p} \right\rfloor$

lattice points in OPC. Then $N_1 =$

Multiple Choice:

(a) $\sum_{j=1}^{2} \left\lfloor \frac{jp}{q} \right\rfloor$ ✓

(b) $\sum_{j=1}^{2} \left\lfloor \frac{jq}{p} \right\rfloor$

To find N_2, we use a similar counting method on OAM. Now, we count the lattice points on $x = j$ for $j = 1, 2, \ldots, \frac{p-1}{2}$. Thus, for each j, we want the number of nonnegative integers less than

Multiple Choice:

(a) $\dfrac{jp}{q}$

(b) $\dfrac{jq}{p}$ ✓

Thus, we have for each j, there are

Multiple Choice:

(a) $\left\lfloor \dfrac{jp}{q} \right\rfloor$

(b) $\left\lfloor \dfrac{jq}{p} \right\rfloor$ ✓

lattice points in OPC. Then $N_2 =$

Multiple Choice:

(a) $\displaystyle\sum_{j=1}^{2} \left\lfloor \frac{jp}{q} \right\rfloor$

(b) $\displaystyle\sum_{j=1}^{2} \left\lfloor \frac{jq}{p} \right\rfloor$ ✓

From the previous Lemma, $\left(\dfrac{p}{q}\right) = (-1)^{N_1}$ and $\left(\dfrac{q}{p}\right) = (-1)^{N_2}$. Thus,

$$\begin{aligned}\left(\frac{p}{q}\right)\left(\frac{p}{q}\right) &= (-1)^{N_1}(-1)^{N_2} \\ &= (-1)^{N_1+N_2} \\ &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\end{aligned}$$

with the result from the participation assignment. ■

Quadratic reciprocity means that determining all quadratic residues (perfect squares) modulo an odd prime is a finite problem. In terms of Legendre symbol, this is finding all a where $\left(\dfrac{a}{p}\right) = 1$ for a given p. For example, when $p = 11$, we can check all positive integers a. However, what about the reverse? Quadratic reciprocity allows us to find all odd primes p where $\left(\dfrac{11}{p}\right) = 1$, even though there are infinitely many odd primes. This idea is the last homework problem.

April 1–Möbius inversion formula

We revisit some arithmetic functions, introduce the Möbius function, and prove the Möbius inversion formula.

Definition 2. *A function f is* arithmetic *if it is defined on all positive integers.*

We have seen many arithmetic functions: the Euler ϕ-function, $d(n)$ is the number of positive divisors of n, $\sigma(n)$ is the sum of positive divisors of n, $\omega(n)$ is the number of distinct prime divisors of n, $\Omega(n)$ is the number of primes dividing n counting multiplicity.

Definition 3. *An arithmetic function f is* multiplicative *if for any relatively prime $m, n \in \mathbb{Z}$, $f(mn) = f(m)f(n)$. The function is* completely multiplicative *if $f(mn) = f(m)f(n)$ for all positive integers m and n.*

Question 19 *The Euler ϕ-function is:*

Multiple Choice:

(a) *not multiplicative*

(b) *multiplicative* ✓

(c) *completely multiplicative*

The function $f(n) = n^2$ is:

Multiple Choice:

(a) *not multiplicative*

(b) *multiplicative*

(c) *completely multiplicative* ✓

Multiplicative functions are completely defined by their value on powers of primes. If $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, then for any multiplicative function f, $f(n) = f(p_1^{a_1}) f(p_2^{a_2} \cdots f(p_r^{a_r})$ by repeatedly applying the definition of a multiplicative function.

Learning outcomes:
Author(s): Claire Merriman

Theorem 8. *Let f be an arithmetic function and for $n \in \mathbb{Z}$ with $n > 0$, let*

$$F(n) = \sum_{d|n} f(d).$$

If f is multiplicative, then so is $F(n)$.

Proof Let m and n be relatively prime positive integers. To prove that $F(n)$ is multiplicative, we need to show that $F(mn) = F(m)F(n)$. We have that $F(mn) = \sum_{d|mn} f(d)$. Since $(m, n) = 1$, each divisor $d > 0$ of mn can be written as $d_1 d_2$ where $d_1 \mid m, d_2 \mid n$, and $(d_1, d_2) = 1$ and each such product corresponds to a divisor d of mn (see homework 10). We have

$$\begin{aligned} F(mn) &= \sum_{d_1|m, d_2|n} f(d_1 d_2) \\ &= \sum_{d_1|m, d_2|n} f(d_1) f(d_2) \\ &= \sum_{d_1|m} f(d_1) \sum_{d_2|n} f(d_2) \\ &= F(m)F(n) \end{aligned}$$

■

Example 1. *To clarify the previous proof, we look at an example: Let $m = 3$ and $n = 4$. We need to show that $F(3 \cdot 4) = F(3)F(4)$. We have*

$$\begin{aligned} F(12) &= \sum_{d|12} f(d) \\ &= f(\boxed{1}) + f(\boxed{2}) + f(\boxed{3}) + f(\boxed{4}) + f(\boxed{6}) + f(\boxed{12}) \end{aligned}$$

Regroup so that the first 3 terms are factors of 4 and the last 3 terms are factors of 3.

$$= f(\boxed{1}) + f(\boxed{2}) + f(\boxed{4}) + f(\boxed{3}) + f(\boxed{6}) + f(\boxed{12})$$

The factor each term

$$\begin{aligned} &= f(1 \cdot 1) + f(1 \cdot 2) + f(1 \cdot 4) + f(3 \cdot 1) + f(3 \cdot 2) + f(3 \cdot 4) \\ &= f(\boxed{1} f(\boxed{1}) + f(\boxed{1} f(\boxed{2}) + f(\boxed{1} f(\boxed{4}) + f(\boxed{3} f(\boxed{1}) + f(\boxed{3} f(\boxed{2}) + f(\boxed{3} f(\boxed{4}) \\ &= [f(\boxed{1}) + f(\boxed{3}][f(\boxed{1}) + f(\boxed{2}) + f(\boxed{4})] \\ &= \sum_{d_1|3} f(d_1) \sum_{d_2|4} f(d_2) \\ &= F(3)F(4) \end{aligned}$$

Definition 4. *An integer n is* square-free *if it is not divisible by p^2 for any prime p.*

Definition 5. *Let $n \in \mathbb{Z}$ with $n > 0$. The* Möbius μ-function*, denoted $\mu(n)$, is*

$$\mu(n) = \begin{cases} 1 & if\ n = 1 \\ 0 & if\ p^2 \mid n,\ p\ prime \\ (-1)^r & if\ n = p_1 p_2 \cdots p_r,\ p_i\ prime \end{cases} = \begin{cases} 1 & if\ n = 1\ or \\ & n\ square\text{-}free,\ even\ number\ of\ prime\ factors \\ 0 & if\ n\ not\ square\text{-}free \\ -1 & if\ n\ square\text{-}free,\ odd\ number\ of\ prime\ factors. \end{cases}$$

Question 20 *Since $504 = 2^3 3^2 7$, $\mu(504)$ is*

Multiple Choice:

(a) *1*

(b) *0* ✓

(c) *-1*

Since $30 = 2 \cdot 3 \cdot 5$, $\mu(30)$ is

Multiple Choice:

(a) *1*

(b) *0*

(c) *-1* ✓

Theorem 9. *The Möbius μ function is multiplicative.*

Proof Let m and n be relatively prime positive integers. We must show that $\mu(mn) = \mu(m)\mu(n)$. If $m = 1$ or $n = 1$, then we are done (see participation assignment).

Either m or n is divisible by p^2 for some prime p if and only if mn is divisible by p^2. Then $\mu(mn) = 0$ and either $\mu(m) = 0$ or $\mu(n) = 0$, so $\mu(m)\mu(n) = 0$.

If m and n are both square-free, then $m = p_1 p_2 \cdots p_r$ and $n = q_1 q_2 \cdots q_s$ with $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s$ distinct primes. Then

$$\begin{aligned} \mu(mn) &= \mu(p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s) = (-1)^{r+s} \\ &= (-1)^r (-1)^s \\ &= \mu(m)\mu(n) \end{aligned}$$

■

Theorem 10. *Let $n \in \mathbb{Z}$ with $n > 0$. Then*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & if\ n = 1 \\ 0 & otherwise \end{cases}$$

Proof Since $\mu(n)$ is multiplicative, the first theorem from this section says that $\sum_{d|n} \mu(d)$ is also multiplicative. Thus, the value of this function is determined by it's value on power of primes. Now, $F(1) = \boxed{1}$. If p is prime, then

$$\begin{aligned} F(p^a) &= \sum_{d|p^a} F(d) \\ &= \mu(1) + \mu(p) + \mu(p^2) + \cdot + \mu(p^{a-1}) + \mu(p^a) \\ &= \boxed{1} + \boxed{-1} + \boxed{0} + \cdots + \boxed{0} \\ &= 0. \end{aligned}$$

■

Theorem 11 (Möbius Inversion Formula)**.** *Let f and g be arithmetic functions. Then*

$$f(n) = \sum_{d|n} g(d)$$

if and only if

$$g(n) = \sum_{d|n} \mu(d) f(\frac{n}{d}) = \sum_{d|n} \mu(\frac{n}{d}) f(d).$$

Proof Note that $\sum_{d|n} \mu(d) f(\frac{n}{d}) = \sum_{d|n} \mu(\frac{n}{d}) f(d)$ since $\frac{n}{d}$ and d are both on the list of all divisors of d.

($\Rightarrow$) Assume that $f(n) = \sum_{d|n} g(d)$. Then

$$\begin{aligned} \sum_{d|m} \mu(d) f(\frac{n}{d}) &= \sum_{d|n} \left(\mu(d) \sum_{c|\frac{n}{d}} g(c) \right) \\ &= \sum_{c|n} \left(g(c) \sum_{d|\frac{n}{d}} \mu(d) \right) \text{ why?} \end{aligned}$$

By the previous theorem, $\sum_{d|n} \mu(d) = 0$ unless $\frac{n}{c} = 1$, ie $c = n$. Thus, the only term in the summation is $g(c)$.

($\Leftarrow$) Assume that $g(n) = \sum_{d|n} \mu(\frac{n}{d}) f(d)$. Then

$$\begin{aligned}\sum_{d|n} g(d) &= \sum_{d|n} \left(\sum_{c|d} \mu(\frac{d}{c}) f(c) \right) \\ &= \sum_{d|n} \left(f(c) \sum_{d=cm|n} \mu(\frac{d}{c}) \right) \text{ why?} \\ &= \sum_{c|n} \left(f(c) \sum_{m|\frac{n}{c}} \mu(m) \right) \text{ why?}\end{aligned}$$

Again, $\sum_{m|\frac{n}{c}} \mu(d) = 0$ unless $\frac{n}{c} = 1$, ie $c = n$. Thus, the only term left is $f(n)$. ■

Example 2. *Let $n \in \mathbb{Z}$ with $n > 0$, and $g(n) = n$. We have*

$$g(n) = n = \sum_{d|n} \phi(n).$$

By the Möbius inversion formula

$$\phi(n) = \sum_{d|n} \mu(d) g(\frac{n}{d}) = \sum_{d|n} \mu(\frac{n}{d}) g(d).$$

Equivalently,

$$\phi(n) = \sum_{d|n} \mu(d) \frac{n}{d} = \sum_{d|n} \mu(\frac{n}{d}) d.$$

Example 3. *Let $n \in \mathbb{Z}$ with $n > 0$. We have*

$$d(n) = \sum_{d|n} 1 = \sum_{d|n} g(d),$$

where $g(n) = 1$ for all $n > 0$. By the Möbius inversion formula

$$1 = g(n) = \sum_{d|n} \mu(d) d(\frac{n}{d})$$

April 3–Diophantine equations

Good news, everyone! We are starting Diophantine equations, which are the type of problems that Ximera can actually check. We will pause to give people a chance to solve the problem themselves.

Definition 6. *A* Diophantine equation *is any equation in one or more variables to be solved in the integers.*

Linear Diophantine equations

Definition 7. *Let $a_1, a_2, \ldots, a_n, b \in \mathbb{Z}$ with $a_1, a_2, \ldots, a_n$ not zero. A Diophantine equation of the form*

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$$

is a linear Diophantine equation in the n variable $x_1, \ldots, x_n$.

The participation assignment classifies linear Diophantine equations in one variable.

The question of whether there are solutions to Diophantine equations becomes harder when there is more than one variable. Then next step is to classify Diophantine equations in two variables.

Theorem 12. *Let $ax+by = c$ be a linear Diophantine equation in the variables x and y. Let $d = (a, b)$. If $d \nmid c$, then the equation has no solutions; if $d \mid c$, then the equation has infinitely many solutions. Furthermore, if x_0, y_0 is a particular solution of the equation, then all solution are given by $x = x_0 + \frac{b}{d}n$ and $y = y_0 - \frac{a}{d}n$ where $n \in \mathbb{Z}$.*

Proof Since $d \mid a, d \mid b$, we have that $d \mid \boxed{c}$. So, if $d \nmid c$, then the given linear Diophantine equation has no solutions.

Assume that $d \mid c$. Then, there exists $r, s \in \mathbb{Z}$ such that

$$d = (a, b) = ar + bs.$$

Furthermore, $d \mid c$ implies $c = de$ for some $e \in \mathbb{Z}$. Then

$$c = de = (ar + bs)e = a(re) + b(se).$$

Learning outcomes:
Author(s): Claire Merriman

Thus, $x = re$ and $y = se$ are integer solutions.

Let x_0, y_0 be a particular solution to $ax + by = c$ Then, if $n \in \mathbb{Z}, x = x_0 + \frac{b}{d}n$ and $y = y_0 - \frac{a}{d}n$,

$$ax + by = a(x_0 + \frac{b}{d}n) + b(y_0 - \frac{a}{d}n) = ax_0 + \frac{abn}{d} + by_0 - \frac{abn}{d} = c.$$

We now need to show that every solution has this form. Let x and y be any solution to $ax + by = c$. Then

$$(ax + by) - (ax_0 + by_0) = c - c = 0.$$

Rearranging, we get

$$a(x - x_0) = b(y_0 - y).$$

Dividing both sides by d gives

$$\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y).$$

Now $\frac{b}{d} \mid \frac{a}{d}(x - x_0)$ and $(\frac{a}{d}, \frac{b}{d}) = 1$, so $\frac{b}{d} \mid x - x_0$. Thus, $x - x_0 = \frac{b}{d}n$ for some $n \in \mathbb{Z}$. The proof for y is similar. ■

Example 4. *Is* $24x + 60y = 15$ *is solvable?*

Multiple Choice:

(a) *Yes*

(b) *No* ✓

Example 5. *Find all solutions to* $803x + 154y = 11$.

Using the Euclidean Algorithm, we find:

$$\begin{aligned} 803 &= 154 * \boxed{5} + \boxed{33} \\ 154 &= \boxed{33} * \boxed{4} + \boxed{22} \\ \boxed{33} &= \boxed{22} * 1 + \boxed{11} \end{aligned}$$

Thus

$$\begin{aligned} (803, 154) &= \boxed{33} - \boxed{22} \\ &= \boxed{33} - (154 - \boxed{33} * \boxed{4}) = \boxed{33} * \boxed{5} - 154 \\ &= (803 - 154 * \boxed{5}) * \boxed{5} - 154 = 803 * \boxed{5} - 154 * \boxed{26} \end{aligned}$$

Thus, all solutions to the Diophantine equation have the form $x = \boxed{5} + \frac{\boxed{154}}{\boxed{11}}n$ *and* $y = \boxed{-26} - \frac{\boxed{803}}{\boxed{11}}n$.

Example 6. *There is a famous riddle about Diophantus: "God gave him his boyhood one-sixth of his life, One twelfth more as youth while whiskers grew rife; And then yet one-seventh ere marriage begun; In five years there came a bouncing new son. Alas, the dear child of master and sage After attaining half the measure of his father's life chill fate took him. After consoling his fate by the science of numbers for four years, he ended his life."*

That is: Diophantus's childhood was $1/6^{th}$ *of his life, adolescence was* $1/12^{th}$ *of his life, after another* $1/7^{th}$ *of his life he married, his son was born 5 years after he married, his son then died at half the age that Diophantus died, and 4 years later Diophantus died.*

The Diophantine equation that let's us solve this riddle is:

$$x = \frac{x}{6} + \frac{x}{12} + \frac{x}{7} + 5 + \frac{x}{2} + 4.$$

Then, Diophantus's childhood was $\boxed{14}$ *years, his adolescence was* $\boxed{7}$ *years, he married when he was* $\boxed{33}$*, his son was born when he was* $\boxed{38}$ *and died* $\boxed{42}$ *years later, then Diophantus died when he was* $\boxed{84}$.

Nonlinear Diophantine equations

Definition 8. *A Diophantine equation is* nonlinear *if it is not linear.*

Example 7. (a) *The Diophantine equation* $x^2 + y^2 = z^2$ *is our next section. Solutions are called Pythagorean triples.*

(b) *Let* $n \in \mathbb{Z}$ *with* $n \geq 3$*. The Diophantine equation* $x^n + y^n = z^n$ *is the subject of the famous Fermat's Last Theorem. We will also prove one case of this.*

(c) *Let* $n \in \mathbb{Z}$*. The Diophantine equation* $x^2 + y^2 = n$ *tells us which integers can be represented as the sum of two squares.*

(d) *Let* $d, n \in \mathbb{Z}$*. The Diophantine equation* $x^2 - dy^2 = n$ *is known as Pell's equation.*

Sometimes we can use congruences to show that a particular nonlinear Diophantine equation has no solutions.

Example 8. *Prove that* $3x^2 + 2 = y^2$ *is not solvable.*

Assume that there is a solution. Then any solution to the Diophantine equation is also a solution to the congruence $3x^2 + 2 \equiv y^2 \mod 3$*, which implies* $2 \equiv y^2 \mod 3$*, which we know is false. Thus there are no integer solutions to* $3x^2 + 2 = y^2$*.*

Note: viewing the same equation modulo 2 says $x^2 \equiv y^2 \mod 2$, which does not give us enough information to prove a solution does not exist.

Pythagorean triples

One of the most famous math equations is $x^2 + y^2 = z^2$, probably because we learn it in high school. We are going to classify all integer solutions to the equation.

Definition 9. *A triple* (x, y, z) *of positive integers satisfying the Diophantine equation* $x^2 + y^2 = z^2$ *is called* Pythagorean triple.

Select the Pythagorean triples:

Select All Correct Answers:

(a) 3,4,5 ✓

(b) 5,12,13 ✓

(c) -3,4,5

(d) 6,8,10 ✓

(e) 0,1,1

It is actually possible to classify all Pythagorean triples, just like we did for linear Diophantine equations in two variables. To simplify this process, we will work with $x, y, z > 0$, and $(x, y, z) = 1$. For any given solution of this form, we have that $(-x, y, z), (x, -y, z), (x, y, -z), (-x, -y, z), (x, -y, -z), (-x, y, -z)$, and $(-x, -y, -z)$ are also solutions to the Diophantine equation, as is (nx, ny, nz) for any integer n. Thus, we call such a solution a *primitive Pythagorean triple*. We call $(0, n, \pm n)$ and $(n, 0, \pm n)$ the *trival solutions*.

Theorem 13. *For a primitive Pythagorean triple* (x, y, z)*, exactly one of* x *and* y *is even.*

Proof If x and y are both even, then z must also be even, contradicting that $(x, y, z) = 1$.

If x and y are both odd, then z is even. Now we can work modulo 4 to get a contradiction. Since x and y are odd, we have that $x^2 \equiv y^2 \equiv \boxed{1} \pmod 4$. Since z is even, we have that $z^2 \equiv \boxed{0} \pmod 4$, but $x^2 + y^2 \equiv \boxed{2} \pmod 4$.

Thus, the only remaining option is exactly one of x and y is even. ■

April 6–Pythagorean triples and Fermat's Last Theorem

We will prove a formula for generating Pythagorean triples. We will also prove some cases of Fermat's Last Theorem.

Pythagorean triples

From last time, we have that *primitive Pythagorean triples* are solutions to $x^2 + y^2 = z^2$ with $x, y, z > 0$ and $(x, y, z) = 1$. For a primitive Pythagorean triple (x, y, z), exactly one of x and y is even.

Theorem 14. *There are infinitely many primitive Pythagorean triples x, y, z with y even. Furthermore, they are given precisely by the equations*

$$\begin{aligned} x &= m^2 - n^2 \\ y &= 2mn \\ z &= m^2 + n^2 \end{aligned}$$

where $m, n \in \mathbb{Z}, m > n > 0, (m, n) = 1$ and exactly one of m and n is even.

Before proving this theorem, we illustrate it with some examples:

Example 9. (a) *$m = 2$ and $n = 1$ satisfy the conditions of m and n in the theorem. This gives $x = \boxed{3}, y = \boxed{4}, z = \boxed{5}$.*

(b) *$m = 3$ and $n = 2$ gives $x = \boxed{5}, y = \boxed{12}, z = \boxed{13}$.*

(c) *Try with your own values of m and n.*

Proof We first show that given a primitive Pythagorean triple with y even, there exist m and n as described. Since y is even, y and z are both odd. Moreover, $(x, y) = 1, (y, z) = 1$, and $(x, z) = 1$. Now,

$$y^2 = z^2 - x^2 = (x + z)(z - x)$$

implies that

$$\left(\frac{y}{2}\right)^2 = \frac{(x + z)}{2}\frac{(z - x)}{2}.$$

Learning outcomes:
Author(s): Claire Merriman

To show, $\left(\frac{(x+z)}{2}, \frac{(z-x)}{2}\right) = 1$, let $\left(\frac{(x+z)}{2}, \frac{(z-x)}{2}\right) = d$. Then $d \mid \frac{z+x}{2}$ and $d \mid \frac{z-x}{2}$. Thus, $d \mid \frac{z+x}{2} + \frac{z-x}{2} = z$ and $d \mid \frac{z+x}{2} - \frac{z-x}{2} = x$. Since $(x, z) = 1$, we have that $d = 1$. Thus, $\frac{(x+z)}{2}$ and $\frac{(z-x)}{2}$ are perfect squares. Let

$$m^2 = \frac{(x+z)}{2}, \quad n^2 = \frac{(z-x)}{2}.$$

Then $m > n > 0, (m, n) = 1, m^2 - n^2 = x, 2mn = y$, and $m^2 + n^2 = z$. Also, $(m, n) = 1$ implies that not both m and n are both even. If both m and n are odd, we have that z and x are both even, but $(x, z) = 1$. This proves that every primitive Pythagorean triple has this form.

Now we prove that given any such m and n, we have a primitive Pythagorean triple. First, $(m^2 - n^2)^2 + (2mn)^2 = m^4 - 2m^2n^2 + n^4 + 4m^2n^2 = (m^2 + n^2)^2$. We need to show that $(x, y, z) = 1$. Let $(x, y, z) = d$. Since exactly one of m and n is even, we have that x and z are both odd. Then d is odd, and thus $d = 1$ or d is divisible by some odd prime p. Assume that $p \mid d$. Thus, $p \mid x$ and $p \mid z$. Thus, $p \mid z + x$ and $p \mid z - x$. Thus, $p \mid (m^2 + n^2) + (m^2 - n^2) = 2m^2$ and $p \mid (m^2 + n^2) - (m^2 - n^2) = 2n^2$. Since p is odd, we have that $p \mid m^2$ and $p \mid n^2$, but $(m, n) = 1$, so $d = 1$. ■

While this proof is not obvious, it does not use any concepts beyond chapter 1. Thus, this proof is considered *elementary*. Such elementary proofs often involve deep insights and intricate calculations, but no concepts beyond what we are learning in this course (and often not including things like divisor sums).

Fermat's Last Theorem

After the Diophantine equation $x^2 + y^2 = z^2$, one generalization is $x^n + y^n = z^n$ for $n \geq 3$. Fermat's Last Theorem was first conjectured in 1637 and proven in 1995 by Andrew Wiles. Attempts to solve this problem through the centuries have created new branches of mathematics.

Theorem 15 (Fermat's Last Theorem)**.** *The Diophantine equation $x^n + y^n = z^n$ has no nonzero integer solutions for $n \geq 3$.*

We will show that it suffices to prove Fermat's Last Theorem for the cases of n and odd prime and $n = 4$.

Theorem 16. *The Diophantine equation $x^n + y^n = z^n$ has a solution no solutions for $n \geq 3$ if and only if there are no solutions for n and odd prime or $n = 4$.*

Proof Let $n \in \mathbb{Z}$ and $n \geq 3$. Let $n = ab$ where $a, b \in \mathbb{Z}$ and b is either an odd prime or 4. If x, y, z is a solution to $x^n + y^n = z^n$, then x^a, y^a, z^a is a solution to $x^b + y^b = z^b$. By contraposition, if $x^b + y^b = z^b$ has no solutions, then $x^n + y^n = z^n$ has no solutions. ■

We will prove the case where $n = 4$ using the *method of decent.* This is the only case that Fermat proved. The next 400+ years were spent proving the theorem for odd primes.

The idea of the method of decent for proving no solution exists for a Diophantine equation is to assume a solution exists. Then use this solution to construct one that has one component that is strictly smaller than the original solution. This process could be repeated indefinitely, but it is not possible to construct an infinitely decreasing list of positive integers. Thus, no solution exists.

Theorem 17. *The Diophantine equation $x^4 + y^4 = z^2$ has not solutions in nonzero integers x, y, z.*

Note: If x, y, z is a solution to $x^4 + y^4 = z^4$, then

Multiple Choice:

(a) x, y, z

(b) x, y, z^2 ✓

is a solution to $x^4+y^4 = z^4$. By contraposition, if $x^4+y^4 = z^2$ has no solutions, then $x^4 + y^4 = z^4$ has no solutions.

Proof Assume by way of contradiction, that $x^4 + y^4 = z^2$ has a solution x_1, y_1, z_1 nonzero integers. Without loss of generality, we may assume $x_1, y_1, z_1 > 0$ and $(x_1, y_1) = 1$. We will show that there is another solution x_2, y_2, z_2 positive integers such that $(x_2, y_2) = 1$ and $0 < z_2 < z_1$. Now, $(x_1)^2, (y_1)^2, z_1$ is a Pythagorean triple with $(x_1^2, y_1^2, z_1) = 1$, and without loss of generality, y_1^2 is even. Thus, by the first theorem of the day says that there exists $m, n \in \mathbb{Z}$ such that $(m, n) = 1, m > n > 0$, and exactly one of m and n is even such that $x_1^2 = m^2 - n^2, y_1^2 = 2mn, z_1 = m^2 + n^2$. Now, $x_1^2 = m^2 - n^2$ implies $x_1^2 + n^2 = m^2$ and x_1, m, n is a Pythagorean triple with $(x_1, m, n) = 1$ and n is even. Applying the same theorem again, we get that there exists $a, b \in \mathbb{Z}$ with $(a, b) = 1, a > b > 0$, exactly one of a and b is even, with $x_1 = a^2 - b^2, n = 2ab, m = a^2 + b^2$.

We want to show that m, a and b are perfect squares. Now, $y_1^2 = 2mn = m(2n)$ and $(m, 2n) = 1$, we have that

Select All Correct Answers:

(a) m ✓

(b) n

(c) 2n ✓

are perfect squares. Thus, there exists $c \in \mathbb{Z}$ such that $2n = 4c^2$ or, equivalently, $n = 2c^2$. Now, $n = 2ab$ and $(a, b) = 1$, we have that

Select All Correct Answers:

(a) a ✓

(b) b ✓

(c) 2b

are perfect squares.

There exists x_2, y_2, z_2 such that $m =$

Multiple Choice:

(a) x_2^2

(b) y_2^2

(c) z_2^2 ✓

$a =$

Multiple Choice:

(a) x_2^2 ✓

(b) y_2^2

(c) z_2^2

and $b =$

Multiple Choice:

(a) x_2^2

(b) y_2^2 ✓

(c) z_2^2.

Without loss of generality, we may assume $x_2, y_2, z_2 > 0$. Then $m^2 = a^2 + b^2$ implies $z_2^2 = x_2^4 + y_2^4$, so that x_2, y_2, z_2 is a solution with positive integers to $x^4 + y^4 = z^2$. Also $(x_2, y_2) = 1$ and $0 < z_2 \leq z_2^2 = m \leq m^2 < m^2 + n^2 = z_1$.

Thus, we have constructed another solution as desired. That is, we assumed the existence of a solution to $x^4 + y^4 = z^2$ in the positive integers, we can construct another solution with a strictly smaller value of z. This is a contradiction sine there are only finitely many positive integers between a given positive integer and zero. So $x64 + y^4 = z^2$ has no solutions on nonzero x, y, z. ■

April 8–Sums of squares

We finally determine which integers can be written as the sum of two squares of integers!

Sum of Two Squares

Which integers can be represented as the sum of two perfect squares?

Select All Correct Answers:

(a) 1 ✓

(b) 2 ✓

(c) 3

(d) 4 ✓

(e) 5 ✓

(f) 6

(g) 7

(h) 8 ✓

(i) 9 ✓

(j) 10 ✓

(k) 11

(l) 12

(m) 13 ✓

(n) 14

(o) 15

Select All Correct Answers:

(a) 16 ✓

Learning outcomes:
Author(s): Claire Merriman

(b) 17 ✓

(c) 18 ✓

(d) 19

(e) 20 ✓

(f) 21

(g) 22

(h) 23

(i) 24

(j) 25 ✓

(k) 26 ✓

(l) 27

(m) 28

(n) 29 ✓

(o) 30

Note that this sum is not necessarily unique: $25 = 5^2 + 0^2 = 4^3 + 3^2$. Try to conjecture whether or not 374^{695} can be written as the sum of two squares. We found back in the congruences chapter that n cannot be written written as the sum of two squares if $n \equiv 3 \pmod 4$. In order to establish which integers are expressible as the sum of two squares, we will find necessary and sufficient conditions for the Diophantine equation $x^2 + y^2 = n$ to have solutions.

Theorem 18. *Let $n_1, n_2 \in \mathbb{Z}$ with $n_1, n_2 > 0$. If n_1 and n_2 are expressible as the sum of two squares of integers, then $n_1 n_2$ is expressible as the sum of two squares of integers.*

Proof Participation assignment ■

Example 10. *Since $13 = \boxed{3}^2 + \boxed{2}^2$ and $17 = \boxed{4}^2 + \boxed{1}^2$ are each expressible as the sum of two squares, $13 * 17 = 221 = \boxed{14}^2 + \boxed{-5}^2$.*

We will finally prove that every prime that congruent to 1 (mod 4) is expressible as the sum of two squares.

Theorem 19 (Primes as sums of squares)**.** *If p is a prime such that $p \equiv 1 \pmod 4$, then there exists $x, y \in \mathbb{Z}$ such that $x^2 + y^2 = kp$ for some $k \in \mathbb{Z}$ and $0 < k < p$.*

Proof Since $p \equiv 1 \pmod 4$, we have that $\left(\frac{-1}{p}\right) = 1$. Thus, there exists $x \in \mathbb{Z}$ with $0 < x \leq \frac{p-1}{2}$ such that $x^2 \equiv -1 \pmod p$. Then, $p \mid x^2 + 1$, and we have that $x^2 + 1 = kp$ for some $k \in \mathbb{Z}$. Thus, we found x and $y = 1$. Since $x^2 + 1$ and p are positive, so is k. Also,

$$kp = x^2 + y^2 < \left(\frac{p}{2}\right)^2 + 1 < p^2$$

implies $k < p$. ■

The next theorem will finally prove that primes $p \equiv 1 \pmod 4$ and $p = 2$ can be written as the sum of two square integers.

Theorem 20. *If p is a prime number such that $p \not\equiv 3 \pmod 4$, then p is expressible as the sum of two squares of integers.*

Proof When $p = 2 = 1^2 + 1^2$, we are done.

Assume that $p \equiv 1 \pmod 4$. Let m be the least integer such that there exists $x, y \in \mathbb{Z}$ with $x^2 + y^2 = mp$ and $0 < m < p$ as in the previous theorem. We show that $m = 1$. Assume, by way of contradiction, that $m > 1$. Let $a, b \in \mathbb{Z}$ such that

$$a \equiv x \pmod m, \quad \frac{-m}{2} < a \leq \frac{m}{2}$$

and

$$b \equiv y \pmod m, \quad \frac{-m}{2} < b \leq \frac{m}{2}.$$

Then

$$a^2 + b^2 \equiv x^2 + y^2 = mp \equiv 0 \pmod m,$$

and so there exists $k \in \mathbb{Z}$ with $k > 0$ such that $a^2 + b^2 = km$. (Why?)

Now,

$$(a^2 + b^2)(x^2 + y^2) = (km)(mp) = km^2p.$$

By the participation assignment, $(a^2 + b^2)(x^2 + y^2) = (ax + by)^2 + (ay - bx)^2$, so $(ax + by)^2 + (ay - bx)^2 = km^2p$. Since $a \equiv x \pmod m$ and $b \equiv y \pmod m$,

$$ax + by \equiv x^2 + y^2 \equiv 0 \pmod m$$

and

$$ay - bx \equiv xy - yx \equiv 0 \pmod m$$

so $\frac{ax + by}{m}, \frac{ay - bx}{m} \in \mathbb{Z}$ and

$$\left(\frac{ax + by}{m}\right)^2 + \left(\frac{ay - bx}{m}\right)^2 = \frac{km^2p}{m^2} = kp.$$

Now, $\frac{-m}{2} < a \leq \frac{m}{2}$ and $\frac{-m}{2} < b \leq \frac{m}{2}$ imply that $a^2 \leq \frac{m^2}{4}$ and $b^2 \leq \frac{m^2}{4}$. Thus, $km = a^2 + b^2 \leq \frac{m^2}{2}$. Thus, $k \leq \frac{m}{2} < m$, but this contradicts that m is the smallest such integer.

Thus, $m = 1$. ■

We finish with a characterization of which integers are expressible as the sum of two square integers and some examples.

Theorem 21. *Let $n \in \mathbb{Z}$ with $n > 0$. Then n is expressible as the sum of two squares if and only if every prime factor congruent to 3 modulo 4 occurs to an even power in the prime factorization of n.*

Proof ($\Rightarrow$) Assume that p is an odd prime number and that $p^{2i+1}, i \in \mathbb{Z}$ occurs in the prime factorization of n. We will show that $p \equiv 1 \pmod 4$. Since n is expressible as the sum of two squares of integers, there exist $x, y \in \mathbb{Z}$ such that $n = x^2 + y^2$. Let $(x, y) = d, a = \frac{x}{d}, b = \frac{y}{d}$ and $m = \frac{n}{d^2}$. Then $(a, b) = 1$ and $a^2 + b^2 = m$. Let $p^j, j \in \mathbb{Z}$ be the largest power of p dividing d. Then $p^{(2i-1)-2j} \mid m$; since $(2i + 1) - 2j) \geq 1$, we have $p \mid m$. Now, $p \nmid a$ since $(a, b) = 1$. Thus, there exists $z \in \mathbb{Z}$ such that $az \equiv b \pmod p$. Then $m = a^2 + b^2 \equiv a^2 + (az)^2 \equiv a^2(1 + z^2) \pmod p$.

Since $p \mid m$, we have

$$a^2(1 + z^2) \equiv 0 \pmod p$$

or $p \mid a^2(1 + z^2)$ or $z \equiv -1 \pmod p$. Thus, -1 is a quadratic residue modulo p, so $p \equiv 1 \pmod 4$. By contrapositive, any prime factor congruent to 3 modulo 4 occurs to an even power in the prime factorization of n as desired.

($\Leftarrow$) Assume that every prime factor of n congruent to 3 modulo 4 occurs to an even power in the prime factorization of n. Then n can be written as $n = m^2 p_1 p_2 \dots p_r$ where $m \in \mathbb{Z}$ and $p_1, p_2, \dots, p_r$ are distinct prime numbers equal to 2 or equivalent to 1 modulo 4. Now, $m^2 = m^2 + 0^2$, so is expressible as the sum of two squares, and each p_1 is also expressible as the sum of two squares by the theorem labeled Primes as Sums of Squares. Thus, by the first theorem of the day, n is expressible as the sum of two squares. ■

Example 11. *Determine whether 374^{695} is expressible as the sum of two squares. The prime factorization of 374 is $2 * 11 * 17$. So $374^{695} = 2^{695}11^{695}17^{695}$ Thus, 374^{695}*

Multiple Choice:

(a) *is*

(b) *is not* ✓

expressible as the sum of two squares.

Example 12. *Express* 4410 *as the sum of two squares by splitting into factors that can be written as the sum of two squares.*

The prime factorization of 4410 *is* $2 * 3^2 * 5 * 7^2$. *We group this into* $4410 = (\boxed{2} * \boxed{7}^2)(\boxed{3}^2 * \boxed{5}) = \boxed{98} * \boxed{45}$. *By inspection, the larger of these factors is* $\boxed{98} = \boxed{7}^2 + \boxed{7}^2$ *and the smaller is* $\boxed{45} = \boxed{6}^2 + \boxed{3}^2$.

The method from the participation assignment gives $4410 = \boxed{63}^2 + \boxed{21}^2$.

April 10–Sums of squares

We prove that all integers can be written as the sum of four squares.

Sum of three squares

We finish out the sums of squares section by classifying which integers can be written as the sum of three squares and sum of four squares. These cases are more difficult than the sum of two squares since there is no formula analogous to the April 8 participation assignment.

Theorem 22 (Sum of three squares necessary condition)**.** *Let $m, n \in \mathbb{Z}$ with $m, n \geq 0$. If $N = 4^m(8n+7)$, then N can not be written as the sum of 3 squares.*

Proof We start by proving the $m = 0$ case. In order to get a contradiction, assume that $N = 8n + 7$ can be written as the sum of three squares. Thus, there exists $x, y, z \in \mathbb{Z}$ such that

$$8n + 7 = x^2 + y^2 + z^2.$$

Now, $8n + 7 \equiv 7 \pmod 8$ and $x^2 + y^2 + z^2 \not\equiv 7 \pmod 8$ (by participation assignment), which gives the contradiction we are looking for.

Now we assume $m > 0$. and again assume $N = 4^m(8n + 7)$ can be written as the sum of three squares. As before, there exist $x, y, z \in \mathbb{Z}$ such that

$$4^m(8n + 7) = x^2 + y^2 + z^2$$

and x, y, z are even (by participation assignment). So there exists x', y' and z' such that $x = 2x', y = 2y'$, and $z = 2z'$. Substituting into our definition of N, we get

$$4^{m-1}(8n + 7) = (x')^2 + (y')^2 + (z')^2.$$

Repeating this process $m - 1$ times, we find $8n + 7$ is expressible as a sum of three squares, a contradiction. Thus, $N = 4^m(8n + 7)$ cannot be written as the sum of three squares. ■

Now, the converse is true. Legendre proved this in 1798, but is much harder to prove, due to the lack of formula like the one from April 8 participation assignment. Note that any integer that cannot be written as the sum of three squares cannot be written as the sum of two squares.

Learning outcomes:
Author(s): Claire Merriman

Example 13. *Determine whether* 1584 *is expressible as the sum of three squares.*

The highest power of 4 *that divides* 1584 *evenly is* $\boxed{16}$*, leaving* $\boxed{99} \equiv \boxed{3} \pmod 8$*. Thus,* 1584 *can be written as the sum of three squares:*

Multiple Choice:

(a) *True* ✓

(b) *False*

(c) *Not enough information*

Since this also allows us to factor 1584*, we also know* 1584 *can be written as the sum of two squares:*

Multiple Choice:

(a) *True*

(b) *False* ✓

(c) *Not enough information*

Sum of four squares

We now prove that all positive integers can be written as the sum of four squares. The new few results are similar to the proof of the sum of two squares. Some of these calculations are even more involved, but still use multiplication and factoring. I will upload a scan of the sums of squares section from *Elementary Number Theory* by James K. Strayer. All of the missing calculations are expanding and refactoring polynomial expression.

Theorem 23 (Euler)**.** *Let* $n_1, n_2 \in \mathbb{Z}$ *with* $n_1, n_2 > 0$*. If* n_1 *and* n_2 *are expressible as the sum of four squares, then so is* $n_1 n_2$*.*

Proof Let $a, b, c, d, w, x, y, u \in \mathbb{Z}$ such that

$$n_1 = a^2 + b^2 + c^2 + d^2$$

and

$$n_1 = w^2 + x^2 + y^2 + z^2.$$

Then

$$n_1 n_2 = (aw+bx+cy+dz)^2+(-ax+bw-cz+dy)^2+(-ay+bz+cw-dx)^2+(-az-by+cx+dw)^2$$

as desired. ■

Theorem 24 (Also Euler)**.** *If p is an odd prime number, then there exist $x, y \in \mathbb{Z}$ such that $x^2 + y^2 + 1 = kp$ for some $k \in \mathbb{Z}$ with $0 < k < p$.*

Proof We consider two cases.

Case 1: $p \equiv 1 \pmod 4$. Then $\left(\dfrac{-1}{p}\right) = 1$, so there exists $x \in \mathbb{Z}$ with $0 < x \leq \dfrac{p-1}{2}$ such that $x^2 \equiv -1 \pmod p$. Then, $p \mid x^2 + 1$, and we have that $x^2 + 1 = kp$ for some $k \in \mathbb{Z}$. Thus, we found x and $y = \boxed{0}$. Since $x^2 + 1$ and p are positive, so is k. Also,

$$kp = x^2 + 1 < \left(\frac{p}{2}\right)^2 + 1 < p^2$$

implies $k < p$.

Case 2: $p \equiv 3 \pmod 4$. Let a be the least positive quadratic nonresidue modulo p. Note that $a \geq 2$. Then

$$\left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right) = (-1)(-1) = 1$$

and so there exists $x \in \mathbb{Z}$ with $0 < x \leq \dfrac{p-1}{2}$ such that $x^2 \equiv -a \pmod p$. Now, $a - 1$ is positive and less than a, then $a - 1$ is a quadratic residue modulo p. Thus, there exists $y \in \mathbb{Z}$ with $0 < y \leq \dfrac{p-1}{2}$ such that $y^2 \equiv a - 1 \pmod p$. Thus,

$$x^2 + y^2 + 1 \equiv (-a) + (a-1) + 1 \equiv 0 \pmod p$$

or, equivalently, $x^2 + y^2 + 1 = kp$ for some $k \in \mathbb{Z}$. Again, $k > 0$. Furthermore,

$$kp = x^2 + y^2 + 1 < \left(\frac{p}{2}\right)^2 + \left(\frac{p}{2}\right)^2 + 1 < p^2$$

implies $k < p$. ■

We will prove that every prime number can be written as the sum of four squares.

Theorem 25 (Lagrange, 1770)**.** *All prime numbers can be written as the sum of four squares.*

Proof When $p = 2 = 1^2 + 1^2 + 0^2 + 0^2$, we are done. In fact, we can also writes a prime p where $p \equiv 1 \pmod 4$ as $p = x^2 + y^2 + 0^2 + 0^2$, but the following method works for all odd primes.

Let m be the least positive integer where $x^2 + y^2 + z^2 + w^2 = mp$ and $0 < m < p$. We want to show that $m = 1$. To get a contradiction, assume $m > 1$. We consider two cases.

Case 1: m even. There are three posibilities: w, x, y, z are all even; w, x, y, z are all odd; two of w, x, y, z are odd and the other two are even. In all three cases, we can assume $w \equiv x \pmod 2$ and $y \equiv z \pmod 2$. Then $\frac{w+x}{2}, \frac{w-x}{2}, \frac{y+z}{2}, \frac{y-z}{2}$ are integers and

$$\left(\frac{w+x}{2}\right)^2 + \left(\frac{w-x}{2}\right)^2 + \left(\frac{y+z}{2}\right)^2 + \left(\frac{y-z}{2}\right)^2 = \frac{mp}{2}$$

which contradicts the fact that m is minimal.

Case 2: m is odd.

Then $m \geq 3$. Let $a, b, c, d \in \mathbb{Z}$ such that

$$\begin{aligned} a &\equiv w \pmod m, \frac{-m}{2} < a < \frac{m}{2} \\ b &\equiv x \pmod m, \frac{-m}{2} < b < \frac{m}{2} \\ c &\equiv y \pmod m, \frac{-m}{2} < c < \frac{m}{2} \\ d &\equiv z \pmod m, \frac{-m}{2} < d < \frac{m}{2}. \end{aligned}$$

Then $a^2 + b^2 + c^2 + d^2 \equiv w^2 + x^2 + y^2 + z^2 \equiv mp \equiv 0 \pmod m$ and so there exists $k \in \mathbb{Z}$ with $k > 0$ such that $a^2 + b^2 + c^2 + d^2 = km$. Now

$$(a^2 + b^2 + c^2 + d^2)(w^2 + x^2 + y^2 + z^2) = (km)(mp) = km^2p.$$

By theorem 2 from today, we can rewrite $a^2+b^2+c^2+d^2)(w^2+x^2+y^2+z^2)$ as the sum of four squares $(aw + bx + cy + dz)^2 + (-ax + bw - cz + dy)^2 + (-ay + bz + cw - dx)^2 + (-az - by + cx + dw)^2 = km^2p$. Since $a \equiv w \pmod m, b \equiv x \pmod m, c \equiv y \pmod m, \frac{-m}{2} < c < \frac{m}{2}, d \equiv z \pmod m, \frac{-m}{2} < d < \frac{m}{2}$, we have

$$\begin{aligned} aw + bx + cy + dz \equiv w^2 + x^2 + y^2 + z^2 &\equiv 0 \pmod m \\ -ax + bw - cz + dy \equiv -wx + xw - yz + zy &\equiv 0 \pmod m \\ -ay + bz + cw - dx \equiv -wy + yw + xz - zx &\equiv 0 \pmod m \\ -az - by + cx + dw \equiv -wx + zw - xy + yx &\equiv 0 \pmod m \end{aligned}$$

Let $W = \frac{w^2 + x^2 + y^2 + z^2}{m}, X = \frac{-wx + xw - yz + zy}{m}, Y = \frac{-wy + yw + xz - zx}{m}, Z = \frac{-wx + zw - xy + yx}{m}$. Then $W^2 + X^2 + Y^2 + Z^2 = \frac{km^2p}{m^2} = kp$. Since $\frac{-m}{2} < a, b, c, d < \frac{m}{2}$, then $a^2, b^2, c^2, d^2 < \frac{m^2}{4}$. Thus,

$$km = a^2 + b^2 + c^2 + d^2 < \frac{4m^2}{4}$$

and $k < m$. This contradicts that m is the smallest such integers.

Thus, $m = 1, w^2 + x^2 + y^2 + z^2 = p$. ■

Theorem 26 (Lagrange)**.** *All positive integers can be written as the sum of four squares.*

Proof Let $n \in \mathbb{Z}$ with $n > 1$. If $n = 1 = 1^2 + 0^2 + 0^2 + 0^2$. If $n > 1$, then n is the product of primes by the Fundamental Theorem of Arithmetic. By the previous theorem, every prime number can be written as the sum of four squares. By theorem 2 from today, n is can be written by the sum of four squares. ■

We finish this section with a few famous problems.

Example 14 (Waring's Problem, 1770)**.** *Let $k \in \mathbb{Z}$ with $k > 0$. Does there exist a minimum integer $g(k)$ such that every positive integer can be written as the sum of at most $g(k)$ nonnegative integers to the k^{th} power?*

For example, $g(1) = \boxed{1}$. Today we showed that $g(2) = \boxed{4}$. The next step would be to find if $g(3)$ exists and what it equals.

Theorem 27 (Hilbert, 1906)**.** *Let $k \in \mathbb{Z}$ with $k > 0$. There exists a minimal integer $g(k)$ such that every positive integer can be written as the sum of at most $g(k)$ nonnegative integers to the k^{th} power.*

The proof of Hilbert's theorem does not provide a formula for $g(k)$, merely proves it exists. Numerical evidence suggests $g(k) = \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor + 2^k - 2$. It's been proven that there are only finitely many (or 0) k where the formula does not hold, and the formula holds when $k \leq 471,600,000$. Thus, $g(3) = \boxed{9}, g(4) = 19$, and $g(5) = 37$. Proofs of these facts come from analytic number theory.

April 13–Decimal expansions

We take a number theoretic view of decimal (ie, regular) expansion of numbers.

We are going to look at our regular, decimal expansions of numbers from a number theory perspective in order to study something familiar as an analogy for continued fractions. We start with some familiar definitions.

Definition 10. *Let $\alpha \in \mathbb{R}$. Then α is a* rational number *(or $\alpha \in \mathbb{Q}$) if $\alpha = \frac{a}{b}$ where $a, b \in \mathbb{Z}$ and $b \neq 0$. Otherwise α is irrational.*

Example 15. (a) $0.5 = \frac{5}{10} = \frac{1}{2}$

(b) 0.666..... *where the 6s repeat forever is rational since* $0.666\cdots = \boxed{\frac{2}{3}}$. *We will actually prove that the decimal expansion of a rational number either repeats or terminates.*

(c) *The real number $\sqrt{2}$ is irrational. This is our first proof.*

(d) *The real constants π and e are irrational. We will prove that e is irrational in the homework. The proof that π is irrational is much harder.*

(e) *The real numbers $2^{\sqrt{2}}, e^{\pi}$, and πe are irrational. These were not proven until 1929.*

(f) *We still do not know if $\pi^{\sqrt{2}}, \pi^e$ or 2^e are rational or irrational.*

Theorem 28. $\sqrt{2} \notin \mathbb{Q}$.

Proof In order to get a contradiction, assume that $\sqrt{2} \in \mathbb{Q}$. Then $\sqrt{2} \in \frac{a}{b}$ for some $a, b \in \mathbb{Z}$, with $b \neq 0$. Without loss of generality, assume $(a, b) = 1$. By squaring both sides, we get $2 = \frac{a^2}{b^2}$, so $2b^2 = a^2$. Thus, $2 \mid a^2$ and $2 \mid a$. Thus, there is some integer c where $a = 2c$. Then $2b^2 = 4c^2$, so $b^2 = 2c^2$. Now we get that $2 \mid b$. Thus $2 \mid a$ and $2 \mid b$, which contradicts $(a, b) = 1$. So $\sqrt{2} \notin \mathbb{Q}$. ■

Proof by contradiction is a useful technique for proving a number is irrational.

Theorem 29. *Let $\alpha, \beta \in \mathbb{Q}$. Then $\alpha \pm \beta, \alpha\beta \in \mathbb{Q}$, and if $\beta \neq 0$, then $\frac{\alpha}{\beta} \in \mathbb{Q}$.*

Learning outcomes:
Author(s): Claire Merriman

Proof The participation assignment covers $\alpha+\beta, \alpha\beta$. Replacing β with $-\beta$ gives $\alpha-\beta$. If $\beta \neq 0$, then there exists $a, b, c, d \in \mathbb{Z}$ where $\alpha = \dfrac{a}{b}$ and $\beta = \dfrac{c}{d}$ where none of b, c, d are zero.

$$\frac{\alpha}{\beta} = \frac{\frac{a}{b}}{\frac{c}{d}} = \frac{ad}{bc}.$$

■

The analogous statement for irrational numbers does not hold. For example $\sqrt{2}\sqrt{2} = 2$. The participation assignment is to find an example that does not work for addition.

Theorem 30. *Let $\alpha \in \mathbb{R}$ be the root of the polynomial*

$$f(x) = x^n + c_{n-1}x^{n-1} + \cdot + c_1 x + c_0$$

where $c_i \in \mathbb{Z}$ and $c_0 \neq 0$. Then $\alpha \in \mathbb{Z}$ or α is irrational.

Proof Assume that $\alpha \in \mathbb{Q}$. We must show that $\alpha \in \mathbb{Z}$. Now $\alpha = \dfrac{a}{b}$ for some integers a and $b \neq 0$. Without loss of generality, $(a, b) = 1$. Then for $f(\alpha) = 0$ implies

$$\left(\frac{a}{b}\right)^n + c_{n-1}\left(\frac{a}{b}\right)^{n-1} + c_{n-2}\left(\frac{a}{b}\right)^{n-2} + \cdots + c_1\left(\frac{a}{b}\right) + c_0 = 0.$$

■

Multiplying both sides by b^n, we get

$$a^n + c_{n-1}a^{n-1}b + c_{n-2}a^{n-2}b^2 + \cdots + c_1 ab^{n-1} + c_0 b^n = 0.$$

Then

$$a^n = b(-c_{n-1}a^{n-1} - c_{n-2}a^{n-2}b - \cdots - c_1 ab^{n-2} - c_0 b^{n-1}.$$

Thus, $b \mid a^n$. Since $(a, b) = 1$, we have that $b = \pm 1$. Then $\alpha = \dfrac{a}{\pm 1} = \pm a \in \mathbb{Z}$.

Example 16. (a) *$\sqrt{3}$ is a root of the polynomial $f(x) = x^2 - 3$. Since $\sqrt{3} \notin \mathbb{Z}$, then $\sqrt{3}$ is irrational.*

(b) *$2 + \sqrt{7}$ is a root of the polynomial $f(x) = x^2 - 4x - 3$ and $\sqrt{7} \notin \mathbb{Z}$, $2 + \sqrt{7}$ is irrational.*

(c) *$\sqrt[3]{5}$ is a root of the polynomial $f(x) = x^3 - 5$. Since 5 is between the perfect cubes $\boxed{1^3}$ and $\boxed{2^3}$, we have that $\boxed{1} < \sqrt[3]{5} < \boxed{2}$. Thus, $\sqrt[3]{5}$ is not an integer, and thus is irrational.*

Using this theorem involves finding a polynomial where x is a root. Sometimes this is basic algebra, like rewriting $x = 3 + \sqrt{2}$ as $0 = \boxed{x^2 - 6x + 7}$. However, for numbers like π and e, no such polynomial exists.

Every real number has a decimal expansion, which is how we are used to writing numbers.

Definition 11. *Let $\alpha \in \mathbb{R}$ with $0 \leq \alpha < 1$ and let $\displaystyle\sum_{n=1}^{\infty} \frac{a_n}{10^n} = 0.a_1a_2a_3\ldots$ be a decimal representation of α. If there exist a positive integer ρ and N such that $a_n = a_{n+\rho}$ for all $n \geq N$, then 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

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

This is a formalized definition of a repeating decimal.

Example 17. (a) *A decimal representation of $\frac{1}{2}$ is $0.5 = 0.5\overline{0}$, so $\frac{1}{2}$ is eventually periodic with period $\boxed{0}$ and length $\boxed{1}$. Any terminating decimal can be considered periodic with the same period and length.*

(b) *A decimal representation of $\frac{2}{3}$ is $0.\overline{6}$ is eventually periodic with period $\boxed{6}$ and length $\boxed{1}$.*

(c) *A decimal representation of $\sqrt{2}$ to 20 digits is $1.41421356237309504880\ldots$ which does not* appear *to be eventually periodic, but maybe we have not computed enough digits.*

(d) *A decimal representation of π to 20 digits is $3.14159263558979323846\ldots$ which does not* appear *to be eventually periodic but maybe we have not computed enough digits.*

You have probably heard that the decimal expansion of a ration number either terminates or repeats. We have formalized the definition of repeats to "eventually periodic," and show that terminating decimals are also eventually periodic. Now we prove that fact.

Theorem 31. *Let $\alpha \in \mathbb{R}$ with $0 \leq \alpha < 1$. Then $\alpha \in \mathbb{Q}$ if and only if α is eventually periodic.*

Proof ($\Rightarrow$) Assume that $\alpha \in \mathbb{Q}$. The $\alpha = \frac{a}{b}$ for some integers a and $b \neq 0$. Since, $0 \leq \alpha <$, we also have that $0 \leq a < b$. Now divide b into a by using long

division; let the resulting decimal representation of α be

$$\sum_{n=1}^{\infty} \frac{q_n}{10^n} = 0.q_1q_2q_3\ldots$$

By the division algorithm, the possible remainders when dividing a by b are $0, 1, 2, \ldots, b-1$. At each stage of the long-division process, b is being divided by one of these remainders times 10 (ie, $0, 10, 20, \ldots, (b-1)10$). The first such remainder is a. Accordingly, let $r_1 = a, r_2, r_3, \ldots$ be the sequence of remainders corresponding to the quotients $q_1, q_2, q_3 \ldots$ (so that $\frac{a}{b} = 0.q_1q_2q_3\ldots$). Since the number of possible remainders is finite, $r_N = r_M$ for some N and M with $N < M$. If $p = M - N$, then $r_n = r_n + p$ for all $n \geq N$, from which $q_n = q_{n+p}$ for all $n \geq N$, and α is eventually periodic.

($\Leftarrow$) Assume that α is eventually periodic. Then there exists positive integers p and N such that $\alpha = 0.a_1a_2a_3\ldots a_{N-1}\overline{a_Na_{N+1}\cdots a_{N+\rho-1}}$ Now

$$10^{N-1}\alpha = a_1a_2a_3\ldots a_{N-1}.\overline{a_Na_{N+1}\cdots a_{N+\rho-1}}$$

and

$$10^p10^{N-1}\alpha = a_1a_2a_3\ldots a_{N-1}a_Na_{N+1}\cdots a_{N+\rho-1}.\overline{a_Na_{N+1}\cdots a_{N+\rho-1}}.$$

Furthermore, $10^p10^{N-1}\alpha - 10^{N-1}\alpha$ is an integer since the identical repeating blocks cancel (leaving $a_1a_2a_3\ldots a_{N-1}a_Na_{N+1}\cdots a_{N+\rho-1} - a_1a_2a_3\ldots a_{N-1}$). Since $10^p10^{N-1}\alpha - 10^{N-1}\alpha = (10^p-1)10^{N-1}\alpha$, we have that $(10^p-1)10^{N-1}\alpha = m \in \mathbb{Z}$. Then

$$\alpha = \frac{m}{(10^p-1)10^{N-1}}.$$

Since $(10^p-1)10^{N-1}$ is a nonzero integer, then $\alpha \in \mathbb{Q}$ as desired. ■

Homework: parallel this proof for specific numbers.

A very different look at decimal numbers

Here is a very different way of generating decimal expansions using ideas from dynamical systems. The idea is to divide the unit interval $[0, 1)$ into intervals $\left[\frac{i}{10}, \frac{i+1}{10}\right)$ where $i = 0, 1, 2, \ldots, 9$. If a number $x \in \left[\frac{i}{10}, \frac{i+1}{10}\right)$, then the first digit of the decimal expansion is i. For example, when $i = 1$, the interval is $\left(\boxed{\frac{1}{10}}, \boxed{\frac{2}{10}}\right)$ and the first digit of every x in the interval is $\boxed{1}$.

To get the second digit, we break each of these intervals into 10 smaller intervals $\left[\frac{i}{10} + \frac{j}{10^2}, \frac{i}{10} + \frac{j+1}{10^2}\right), 0 \leq i \leq 9, 0 \leq j \leq 9$. For each $x \in \left[\frac{i}{10} + \frac{j}{10^2}, \frac{i}{10} + \frac{j+1}{10^2}\right), x =$

$0.ij\ldots$. For example, when $i = 2, j = 3$, the interval is $\left(\boxed{\frac{2}{10} + \frac{3}{100}}, \boxed{\frac{2}{10} + \frac{4}{100}}\right)$ and the first digit of every $x = 0.\boxed{2}\boxed{3}\ldots$.

Determining the rest of the digits involves iterating this process.

April 15–Continued fractions

Continued fractions

Continued fractions are a way to represent positive real numbers as

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \dots}}},$$

$a_i \in \mathbb{Z}$ with $a_0 \geq 0$ and $a_i \geq 1$ for $i \geq 1$. For example, you may have heard that π is approximately $\frac{22}{7}$, which comes from the continued fraction approximation $\pi \approx 3 + \frac{1}{7} = 3.\overline{142857}$. In fact,

$$\pi = 3 + \cfrac{1}{7 + \cfrac{1}{15 + \dots}} \tag{3}$$

where $3 + \cfrac{1}{7 + \frac{1}{15}}$ agrees with π to four decimal places. In fact, for almost all numbers, the continued fraction converges faster than the decimal expansion.

Example 18. *Now, let's try an example using the Euclidean algorithm:*

$$\begin{aligned} 803 &= 154 * 5 + 33 \\ 154 &= 33 * 4 + 22 \\ 33 &= 22 * 1 + 11 \\ 22 &= 11 * 2 + 0 \end{aligned}$$

Instead of rewriting these equations to find 11 *as a linear combination of* 803 *and* 154*, like we have done in previous sections, we are going to find the continued*

Learning outcomes:
Author(s): Claire Merriman

fraction expansion of $\frac{803}{154}$.

$$\frac{803}{154} = 5 + \frac{33}{154} \tag{4}$$

$$\frac{154}{33} = \boxed{4} + \frac{\boxed{22}}{\boxed{33}} \tag{5}$$

$$\frac{33}{22} = \boxed{1} + \frac{\boxed{11}}{\boxed{22}} \tag{6}$$

$$\frac{22}{11} = \boxed{2} + \frac{\boxed{0}}{\boxed{22}} \tag{7}$$

The trick in combining (4)-(7) *is that* $\frac{a}{b} = \frac{1}{\frac{b}{a}}$.

$$\begin{aligned}
\frac{803}{154} &= 5 + \frac{1}{\frac{154}{33}} && \text{by (4)} \\
&= 5 + \frac{1}{\boxed{4} + \frac{1}{\frac{\boxed{33}}{\boxed{22}}}} && \text{by (5)} \\
&= 5 + \frac{1}{\boxed{4} + \frac{1}{\boxed{1} + \frac{1}{\frac{\boxed{22}}{\boxed{11}}}}} && \text{by (6)} \\
&= 5 + \frac{1}{\boxed{4} + \frac{1}{\boxed{1} + \frac{1}{\boxed{2}}}} && \text{by (7)} \quad \textit{or} \quad = 5 + \frac{1}{\boxed{4} + \frac{1}{\boxed{1} + \frac{1}{\boxed{1} + \frac{1}{\boxed{1}}}}}
\end{aligned}$$

We can skip explicitly writing the Euclidean algorithm step by using the floor/

greatest integer function (Note: this is implicitly using the Euclidean algorithm):

$$\begin{aligned}\frac{803}{154} &= \left\lfloor \frac{803}{154} \right\rfloor + \frac{1}{r_1} && \text{where } r_1 > 1 \\ &= 5 + \frac{1}{\frac{154}{33}} \\ &= 5 + \frac{1}{\left\lfloor \frac{154}{33} \right\rfloor + \frac{1}{r_2}} && \text{where } r_2 > 1\end{aligned}$$

continuing the process until it terminates.

The floor function method of generating continued fractions also works for irrational numbers like π where the Euclidean algorithm version does not make sense.

Definition 12. *Let $x \in \mathbb{R}, x > 0$, then a_0 is the largest integer less than x. If $a_0 = x$, then we are done. Otherwise,*

$$x = a_0 + \frac{1}{r_1} \quad \text{for } 1 < r_1.$$

Let a_1 be the largest integer less that r_1. If $x = a_0 + \dfrac{1}{a_1}$, we are done. Otherwise,

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{r_2}} \quad \text{for } 1 < r_2.$$

Continue this process,

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \dots}} = [a_0; a_1, a_2, \dots].$$

We use $x = [a_0; a_1, a_2, \dots]$ to save space. If this process ends, we say x has a finite continued fraction expansion*, otherwise it has an* infinite continue fraction expansion.

If $x \in \mathbb{R}, x < 0$ and $|x| = [a_0; a_1, a_2, \dots]$, then $x = -[a_0; a_1, a_2, \dots] = -\left(a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \dots}} \right)$.

You probably noticed in the example that we have an issue with uniqueness that come from the fact that $2 = 1 + \dfrac{1}{1}$ and in general, $n = n - 1 + \dfrac{1}{1}$. To deal with this, we typically require the last $a_i > 1$. Thus, $\dfrac{803}{154} = [\boxed{5}; \boxed{4}, \boxed{1}, \boxed{2}]$.

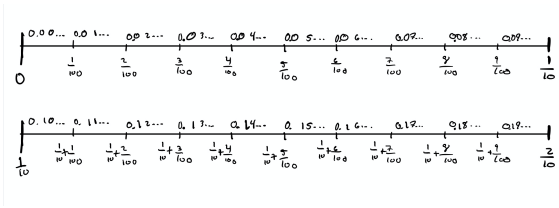
A very different look at decimal numbers

Here is a very different way of generating decimal expansions using ideas from dynamical systems. The idea is to divide the unit interval $[0,1)$ into intervals $\left[\frac{i}{10}, \frac{i+1}{10}\right)$ where $i = 0, 1, 2, \ldots, 9$. If a number $x \in \left[\frac{i}{10}, \frac{i+1}{10}\right)$, then the first digit of the decimal expansion is i. For example, when $i = 1$, the interval is $\left(\boxed{\frac{1}{10}}, \boxed{\frac{2}{10}}\right)$ and the first digit of the decimal expansion of every x in the interval is $\boxed{1}$.

On the following graph of the real line, I marked the endpoints of each interval, and about the interval, I write the decimal expansion for each x in the interval. ie, $0.0\ldots$ above the interval $\left(0, \frac{1}{10}\right)$.

To get the second digit of the decimal expansion of x, we break each of these intervals into 10 smaller intervals $\left[\frac{i}{10} + \frac{j}{10^2}, \frac{i}{10} + \frac{j+1}{10^2}\right), 0 \le i \le 9, 0 \le j \le 9$. For each $x \in \left[\frac{i}{10} + \frac{j}{10^2}, \frac{i}{10} + \frac{j+1}{10^2}\right), x = 0.ij\ldots$. For example, when $i = 2, j = 3$, the interval is $\left(\boxed{\frac{2}{10} + \frac{3}{100}}, \boxed{\frac{2}{10} + \frac{4}{100}}\right)$ and the first two digits of the decimal expansion of every $x = 0.\boxed{2}\boxed{3}\ldots$.

Here is a zoomed in version of the picture:



Determining the rest of the decimal expansion involves iterating this process. (Note: no dynamical system has actually appeared, but this idea comes from that area of mathematics that uses the function $T(x) = 10x - \lfloor 10x \rfloor = 10x - i$ if $x \in \left(\frac{i}{10}, \frac{i+1}{10}\right)$ to find the decimal expansion of x).

Back to continued fractions

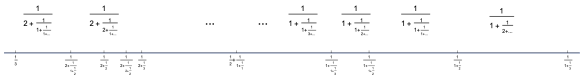
We can use a similar idea from dynamical systems for continued fractions. Now we break up based on the first digit of the continued fraction expansion, which can be any positive integer. Thus, we get an infinite number of intervals $\left(\frac{1}{i+1}, \frac{1}{i}\right)$ where each $x \in \left(\frac{1}{i+1}, \frac{1}{i}\right)$ has continued fraction expansion $\frac{1}{i+\ldots}$. For example, when $i = 1$, the interval is $\left(\boxed{\frac{1}{2}}, \boxed{\frac{1}{1}}\right)$ and the first digit of the continued fraction expansion every x in the interval is $\boxed{1}$.

On the following graph of the real line, I marked the endpoints of the largest six intervals, and about the interval, I write the continued fraction expansion for each x in the interval. ie, $\frac{1}{2+\ldots}$ above the interval $\left(\frac{1}{3}, \frac{1}{2}\right)$. Notice that these intervals shrink very quickly.

To get the second digit of the continued fraction expansion of x, we break each of these intervals into smaller intervals $\left[\frac{1}{i+\frac{1}{j+1}}, \frac{1}{i+\frac{1}{j}}\right), 0 \le i \le 9, 0 \le j \le 9$. For each $x \in \left[\frac{1}{i+\frac{1}{j}}, \frac{1}{i+\frac{1}{j+1}}\right), x = \cfrac{1}{i+\cfrac{1}{j+\ldots}}$. For example, when $i = 2, j = 3$, the interval is $\left(\cfrac{1}{\boxed{2}+\cfrac{1}{\boxed{3}}}, \cfrac{1}{\boxed{2}+\cfrac{1}{\boxed{4}}}\right)$ and the first two digits of the continued fraction expansion of every $x = \cfrac{1}{\boxed{2}+\cfrac{1}{\boxed{3}+\ldots}}$.

Here is the picture with some of the second level intervals:

and a zoomed in version with some of the third level:



Noticed that even zoomed in a lot, it becomes very difficult to draw the third level intervals.

April 17–Continued fractions calculations and theorems

We find the continued fraction expansions of some rational and irrational numbers, and prove some theorems about errors of estimates.

Before diving into irrational numbers, let's take one more look at the Euclidean algorithm to find the continued fraction expansion of $\frac{a}{b}$ for integers $a > b > 0$. First, we let $r_0 = a$ and $r_1 = b$.

$$a = r_0 = r_1 a_0 + r_2 \quad 0 \leq r_2 < r_1 = b$$

If $0 = r_2$, we stop. Otherwise,

$$b = r_1 = r_2 a_1 + r_3 \quad 0 \leq r_3 < r_2$$

Continuing until $0 = r_{n+1} < r_n < r_{n-1} < r_{n-2} < \cdots < r_1 = b < r_0 = a$. We know that $r_k = a_{k+1} r_{k+1} + r_{k+2}$ for $k \leq n-1$ and $(a, b) = r_n$

Then

$$\begin{aligned}
\frac{a}{b} = \frac{r_0}{r_1} &= a_0 + T_1, & a_0 &= \left\lfloor \frac{r_0}{r_1} \right\rfloor, T_1 = \frac{r_2}{r_1} \\
\frac{1}{T_1} &= a_1 + T_2, & a_1 &= \left\lfloor \frac{r_1}{r_2} \right\rfloor, T_2 = \frac{r_3}{r_2} \\
&\vdots & & \\
\frac{1}{T_{n-2}} &= a_{n-1} + T_{n-1}, & a_{n-1} &= \left\lfloor \frac{r_{n-2}}{r_{n-1}} \right\rfloor, T_{n-1} = \frac{r_n}{r_{n-1}} \\
\frac{1}{T_{n-1}} &= a_n + 0 & a_n &= \left\lfloor \frac{r_{n-1}}{r_n} \right\rfloor
\end{aligned}$$

and $\frac{a}{b} = [a_0; a_1, a_2, \ldots, a_n]$.

Definition 13. *Let $x = [a_0; a_1, a_2, \ldots]$. We call the rational approximations $\frac{p_i}{q_i} = [a_0; a_1, a_2, \ldots, a_i]$ are called* convergents*, where $(p_i, q_i) = 1$.*

Learning outcomes:
Author(s): Claire Merriman

Example 19. *Determine the continued fraction expansion and convergents for* $\frac{36}{13}$.

$$\frac{36}{13} = \boxed{2} + \frac{1}{\boxed{\frac{13}{10}}} = \boxed{2} + \frac{1}{\boxed{1} + \frac{1}{\boxed{\frac{10}{3}}}} = \boxed{2} + \frac{1}{\boxed{1} + \frac{1}{\boxed{3} + \frac{1}{\boxed{3}}}}$$

$$\frac{p_0}{q_0} = \frac{2}{1}, \frac{p_1}{q_1} = \frac{\boxed{3}}{\boxed{1}}, \frac{p_2}{q_2} = \frac{\boxed{11}}{\boxed{4}}, \frac{p_3}{q_3} = \frac{\boxed{36}}{\boxed{13}}$$

Here is a plot of the convergents

Example 20. *Determine the continued fraction expansion and convergents for* $\frac{5}{14}$

$$\frac{5}{14} = \boxed{0} + \frac{1}{\boxed{\frac{14}{5}}} = \boxed{0} + \frac{1}{\boxed{2} + \frac{1}{\boxed{\frac{5}{4}}}} = \boxed{0} + \frac{1}{\boxed{2} + \frac{1}{\boxed{1} + \frac{1}{\boxed{4}}}}$$

$$\frac{p_0}{q_0} = \frac{0}{1}, \frac{p_1}{q_1} = \frac{\boxed{1}}{\boxed{2}}, \frac{p_2}{q_2} = \frac{\boxed{1}}{\boxed{3}}, \frac{p_3}{q_3} = \frac{\boxed{5}}{\boxed{14}}$$

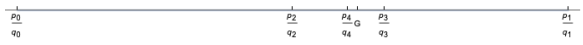
Here is a plot of the convergents

Example 21. *Now we do our first example of an irrational number, the golden ration* $G = \varphi = \dfrac{1+\sqrt{5}}{2}$*. Now,* G *is a root of* $\boxed{x^2 - x - 1}$*, so* $G = 1 + \dfrac{1}{G}$ *(check for yourself). Substituting in for* G*, we get* $G = 1 + \dfrac{1}{1 + \dfrac{1}{G}} = [1; \overline{1}]$ *where the* $\overline{\cdot}$ *indicates repeating digits, as with decimal expansions.*

Since every digit is 1*, this continued fraction expansion converges very slowly. Calculate a few of the convergents:*

$$\frac{p_0}{q_0} = \frac{1}{1}, \frac{p_1}{q_1} = \frac{\boxed{2}}{\boxed{1}}, \frac{p_2}{q_2} = \frac{\boxed{3}}{\boxed{2}}, \frac{p_3}{q_3} = \frac{\boxed{5}}{\boxed{3}}, \frac{p_4}{q_4} = \frac{\boxed{8}}{\boxed{5}}$$

Here is a plot of the convergents



Looking at all three plots, we can start to see that for $x \in \mathbb{R}, x > 0$, $\dfrac{p_0}{q_0} < x < \dfrac{p_1}{q_1}$ and $\dfrac{p_0}{q_0} < \dfrac{p_2}{q_2} < x < \dfrac{p_3}{q_3} < \dfrac{p_1}{q_1}$ (contrast this to the decimal expansion where $d_0 \leq d_0.d_1 \leq d_0.d_1d_2 \leq d_0.d_1d_2d_3 \leq \cdots$). In order to prove that this pattern continues (and holds for all positive real numbers), we need to prove a few more facts about p_i and q_i.

Theorem 32. *Let $p_{-1} = 1, q_{-1} = 0, p_0 = a_0, q_0 = 1$ (see that this matches with p_0, q_0 above). Then*

$$p_n = a_n p_{n-1} + p_{n-2} \tag{8}$$
$$q_n = a_n q_{n-1} + q_{n-2} \tag{9}$$

for $n \geq 1$.

Proof We start by checking $\frac{p_1}{q_1} = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1} = \frac{p_0 a_1 + p_{-1}}{q_0 a_1 + q_{-1}}$.

Next, we check $k = 2$, $\frac{p_2}{q_2} = a_0 + \frac{1}{a_1 + \frac{1}{a_2}} = a_0 + \frac{a_2}{a_2 a_1 + 1} = \frac{a_0(a_2 a_1 + 1) + a_2}{a_2 a_1 + 1} = \frac{a_2 p_1 + p_0}{a_2 q_1 + q_0}$.

Now we proceed by induction. Assume that these recurrence relations hold for $n \leq k$. Then

$$\frac{p_k}{q_k} = [a_0; a_1, a_2, \ldots, a_k] = \frac{a_k p_{k-1} + p_{k-2}}{a_k q_{k-1} + q_{k-2}}.$$

By definition,

$$\begin{aligned}
\frac{p_{k+1}}{q_{k+1}} &= [a_0; a_1, a_2, \ldots, a_k, a_{k+1}] = [a_0; a_1, a_2, \ldots, a_k + \frac{1}{a_{k+1}}] \\
&= \frac{\left(a_k + \frac{1}{a_{k+1}}\right) p_{k-1} + p_{k-2}}{\left(a_k + \frac{1}{a_{k+1}}\right) q_{k-1} + q_{k-2}} \text{(by induction hypothesis*)} \\
&= \frac{a_{k+1}\left(a_k p_{k-1} + p_{k-2}\right) + p_{k-1}}{a_{k+1}\left(a_k q_{k-1} + q_{k-2}\right) + q_{k-1}} \\
&= \frac{a_{k+1} p_k + p_{k-1}}{a_{k+1} q_k + q_{k-1}} \text{(by induction hypothesis)}
\end{aligned}$$

■

*Often the recurrence relations (8) and (9) are proven using matrix multiplication instead of justifying that it is ok to substitute $a_k + \frac{1}{a_{k+1}}$ for a_k. The matrix definition also allows us to prove the next theorem by taking determinants. Instead, we will use induction and the recurrence relations.

Theorem 33. *For all $n \geq 1$, $p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}$, which is equivalent to $\frac{p_n}{q_n} = \frac{(-1)^{n-1}}{q_n q_{n-1}} + \frac{p_{n-1}}{p_{n-1}}$.*

Proof The second equation is the first equation rewritten.

We start with $i = 1$, so from the previous theorem $p_1q_0 - p_0q_1 = (a_0a_1 + 1)1 - a_0a_1 = 1 = (-1)^0$.

Now we proceed by induction. Assume that these recurrence relations hold for $n \leq k$. Then $p_kq_{k-1} - p_{k-1}q_k = (-1)^{k-1}$. Substituting in the recurrence relations (8) and (9), we get

$$\begin{aligned} p_{k+1}q_k - p_kq_{k+1} &= (a_{k+1}p_k + p_{k-1})q_k - p_k(a_{k+1}q_k + q_{k-1}) \\ &= p_{k-1}q_k - p_kq_{k-1} \\ &= -(p_kq_{k-1} - p_{k-1}q_k) \\ &= -(-1)^{k-1} = (-1)^k \end{aligned}$$

■

Notice that $\dfrac{p_n}{q_n} = \dfrac{(-1)^{n-1}}{q_nq_{n-1}} + \dfrac{p_{n-1}}{p_{n-1}}$ is still a recurrence relation. Expanding this out, we get

$$\frac{p_n}{q_n} = a_0 + \frac{1}{q_0q_1} - \frac{1}{q_1q_2} + \cdots + \frac{(-1)^{n-1}}{q_nq_{n-1}} = a_0 + \sum_{k=1}^{n} \frac{(-1)^{k-1}}{q_{k-1}q_k}.$$

Thus $x = \lim\limits_{n\to\infty} \dfrac{p_n}{q_n} = a_0 + \lim\limits_{n\to\infty} \sum\limits_{k=1}^{n} \dfrac{(-1)^{k-1}}{q_{k-1}q_k} = a_0 + \sum\limits_{k=1}^{\infty} \dfrac{(-1)^{k-1}}{q_{k-1}q_k}$ which converges by the alternating series test. This shows that the continued fraction expansion of x really does converge to x for all $x \in \mathbb{R}, x > 0$.

Theorem 34. *For $x \in \mathbb{R}, x > 0$, $\dfrac{p_0}{q_0} < \dfrac{p_2}{q_2} < \cdots < x < \cdots < \dfrac{p_3}{q_3} < \dfrac{p_1}{q_1}$.*

Proof From (9), we find that $q_0 < q_1 < q_2 < \cdots$, since we have a recurrence relation that add positive integers to get a larger positive integer. Thus $\dfrac{1}{q_{n+1}q_n} < \dfrac{1}{q_nq_{n-1}}$.

For $n = 2k$, we have that

$$\begin{aligned} \frac{p_{2k}}{q_{2k}} &= \frac{(-1)^{2k-1}}{q_{2k}q_{2k-1}} + \frac{p_{2k-1}}{p_{2k-1}} = \frac{-1}{q_{2k}q_{2k-1}} + \frac{(-1)^{2k-2}}{q_{2k-1}q_{2k-2}} + \frac{p_{2k-2}}{p_{2k-2}} \\ &= \frac{-1}{q_{2k}q_{2k-1}} + \frac{1}{q_{2k-1}q_{2k-2}} + \frac{p_{2k-2}}{p_{2k-2}}, \end{aligned}$$

and $\dfrac{-1}{q_{2k}q_{2k-1}} + \dfrac{1}{q_{2k-1}q_{2k-2}} > 0$, so $\dfrac{p_0}{q_0} < \dfrac{p_2}{q_2} < \cdots < \dfrac{p_{2k}}{q_{2k}} < \cdots$. We also have that $\lim\limits_{k\to\infty} \dfrac{p_{2k}}{q_{2k}} = x$ (from analysis) $\dfrac{p_0}{q_0} < \dfrac{p_2}{q_2} < \cdots < \dfrac{p_{2k}}{q_{2k}} < \cdots < x$.

For $n = 2k + 1$, we have that

$$\begin{aligned}\frac{p_{2k+1}}{q_{2k+1}} &= \frac{(-1)^{2k}}{q_{2k+1}q_{2k}} + \frac{p_{2k}}{p_{2k}} = \frac{1}{q_{2k+1}q_{2k}} + \frac{(-1)^{2k-1}}{q_{2k}q_{2k-1}} + \frac{p_{2k-1}}{p_{2k-1}} \\ &= \frac{1}{q_{2k+1}q_{2k}} + \frac{-1}{q_{2k}q_{2k-1}} + \frac{p_{2k-1}}{p_{2k-1}},\end{aligned}$$

and $\frac{1}{q_{2k+1}q_{2k}} + \frac{-1}{q_{2k}q_{2k-1}} < 0$, so $\cdots < \frac{p_{2k-1}}{q_{2k-1}} < \frac{p_{2k+1}}{1_{2k+1}} \cdots < \frac{p_3}{q_3} < \frac{p_1}{q_1}$. We also have that $\lim_{k\to\infty} \frac{p_{2k+1}}{q_{2k+1}} = x$ (from analysis) $x < \cdots < \frac{p_{2k-1}}{q_{2k-1}} < \frac{p_{2k+1}}{1_{2k+1}} \cdots < \frac{p_3}{q_3} < \frac{p_1}{q_1}$. ■

April 20–Farey sequence

We explore the Farey sequence of rational numbers.

There are several equivalent ways of defining successive Farey sequences. We will show that these are equivalent, as well as prove some properties of these sequences.

Definition 14. *The* level n Farey fractions between 0 and 1 *is the set of reduced form fractions ordered from smallest to largest with*

$$S_n = \left\{ \frac{p}{q} : 0 \leq \frac{p}{q} \leq 1, (p,q) = 1, 1 \leq q \leq n \right\}.$$

So that every term in the sequence is a fraction, we write $0 = \frac{0}{1}$ *and* $1 = \frac{1}{1}$. *The first four Farey sequences are*

$$S_1 = \left\{ \frac{0}{1}, \frac{1}{1} \right\}$$
$$S_2 = \left\{ \frac{0}{1}, \boxed{\frac{1}{2}}, \frac{1}{1} \right\}$$
$$S_3 = \left\{ \frac{0}{1}, \boxed{\frac{1}{3}}, \boxed{\frac{1}{2}}, \boxed{\frac{2}{3}}, \frac{1}{1} \right\}$$
$$S_4 = \left\{ \frac{0}{1}, \boxed{\frac{1}{4}}, \boxed{\frac{1}{3}}, \boxed{\frac{1}{2}}, \boxed{\frac{2}{3}}, \boxed{\frac{3}{4}}, \frac{1}{1} \right\}$$

It is clear that each sequence S_n is ordered from smallest to largest and that each $(p,q) = 1$ (since these facts are both part of the definition). However, these facts are less obvious for the next definition, f_n:

Definition 15. *Construct a table using the following rules: In the first row, write* $\frac{0}{1}$ *and* $\frac{1}{1}$.

For the n^{th} *row, copy the* $(n-1)^{st}$ *row. For each* $\frac{a}{b}$ *and* $\frac{c}{d}$ *in the*$(n-1)^{st}$ *row, insert* $\frac{a+c}{b+d}$ *between* $\frac{a}{b}$ *and* $\frac{c}{d}$ *if* $b + d \leq n$. *The first four rows are*

Learning outcomes:
Author(s): Claire Merriman

f_1	$\frac{0}{1}$						$\frac{1}{1}$
f_2	$\frac{0}{1}$			$\boxed{\frac{1}{2}}$			$\frac{1}{1}$
f_3	$\frac{0}{1}$		$\boxed{\frac{1}{3}}$	$\boxed{\frac{1}{2}}$	$\boxed{\frac{2}{3}}$		$\frac{1}{1}$
f_4	$\frac{0}{1}$	$\boxed{\frac{1}{4}}$	$\boxed{\frac{1}{3}}$	$\boxed{\frac{1}{2}}$	$\boxed{\frac{2}{3}}$	$\boxed{\frac{3}{4}}$	$\frac{1}{1}$

We call the sequence in the n^{th} row of the table f_n.

It is clear that for each $\frac{a}{b}$ and $\frac{c}{d}$ in the$(n-1)^{st}$ row, we insert $\frac{a+c}{b+d}$ between $\frac{a}{b}$ and $\frac{c}{d}$ if $b+d \leq n$ (since this is the definition). This unusual (but easier) way of adding fractions gives what we call *median convergents.*

We are going to prove that $f_n = S_n$ for every n; that the n^{th} row of the table consists of all $\frac{p}{q}$ with $0 \leq \frac{p}{q} \leq 1, (p,q) = 1, 1 \leq q \leq n$; and that the fractions in each row are ordered from smallest to largest. From there, we get that for each $\frac{a}{b}$ and $\frac{c}{d}$ in the F_{n-1}, we insert $\frac{a+c}{b+d}$ between $\frac{a}{b}$ and $\frac{c}{d}$ if $b+d \leq n$

In both definitions, if $\frac{a}{b}$ and $\frac{c}{d}$ are next to each other in S_n (or f_n), then we say they are *consecutive fractions in S_n (or f_n).*

Theorem 35 (Textbook Theorem 6.1)**.** *If $\frac{a}{b}$ and $\frac{c}{d}$ are consecutive fractions in f_n with $\frac{c}{d}$ to the left of $\frac{a}{b}$, then $ad - bc = 1$.*

Proof We use induction. For $n = 1$, there are only two fractions, and $1(1) - 0(1) = 1$.

Assume that this fact holds for the $(n-1)^{st}$ row. That is, $ad - bc = 1$ for all $\frac{a}{b}$ and $\frac{c}{d}$ consecutive Farey fractions in F_{n-1} with $\frac{c}{d} < \frac{a}{b}$. For each pair, there are two options for the n^{th} row: either $b + d > n$, so $\frac{a}{b}$ and $\frac{c}{d}$ are still consecutive Farey fractions or $b + d \leq n$, so $\frac{a}{b}, \frac{a+c}{b+d}$ and $\frac{c}{d}$ are consecutive Farey fractions. If $b + d > n$, we are done. If $b + d \leq n$, then $\frac{c}{d}, \frac{a+c}{b+d}$, and $\frac{a}{b}$ are consecutive fractions, and we need to check both new pairs.

$$\begin{aligned}(a+c)d - (b+d)c &= ad + cd - bc - cd \\ &= ad - bc = 1 \quad \text{(by induction hypothesis)} \\ a(b+d) - b(a+c) &= ab + ad - ba - cb \\ &= ad - bc = 1 \quad \text{(by induction hypothesis)}\end{aligned}$$

■

Corollary 1 (Textbook Corollary 6.2)**.** *Every* $\frac{p}{a}$ *in the table is in reduced form, ie,* $(p, q) = 1$

Corollary 2 (Textbook Corollary 6.3)**.** *The fractions in each row are ordered from smallest to largest.*

Theorem 36 (Textbook Theorem 6.4)**.** *If* $\frac{a}{b}$ *and* $\frac{c}{d}$ *are consecutive fractions in any row, then for all* f_n *that contain* $\frac{a+c}{b+d}$, $\frac{a+c}{b+d}$ *has the smallest denominator of any rational number between* $\frac{a}{b}$ *and* $\frac{c}{d}$ *and is the unique rational number between* $\frac{a}{b}$ *and* $\frac{c}{d}$ *with denominator* $b + d$*.*

Proof From the definition, $\frac{a+c}{b+d}$ is the first fraction to appear between $\frac{a}{b}$ and $\frac{c}{d}$ in row $b + d$. Thus, $\frac{c}{d} < \frac{a+c}{b+d} < \frac{a}{b}$ by Corollary 6.3. Now consider any $\frac{x}{y}$ with $\frac{c}{d} < \frac{x}{y} < \frac{a}{b}$. Then

$$\begin{aligned}\frac{a}{b} - \frac{c}{d} &= \left(\frac{a}{b} - \frac{x}{y}\right) + \left(\frac{x}{y} - \frac{c}{y}\right) \\ &= \frac{ay - bx}{by} + \frac{xd - cd}{dy} \geq \frac{1}{by} + \frac{1}{dy} = \frac{b+d}{bdy}\end{aligned}$$

and thus

$$\frac{b+d}{bdy} \leq \frac{ad - bd}{bd} = \frac{1}{bd}$$

and $y \geq b+d$. If $y > b+d$, then $\frac{x}{y}$ does not have the least denominator of rational numbers between $\frac{a}{b}$ and $\frac{c}{d}$. If $y = b + d$, then $\frac{ay - bx}{by} + \frac{xd - cy}{dy} = \frac{1}{by} + \frac{1}{dy}$ and $ay - bx = xd - cy = 1$. By solving, we find $x = a + c$ and $y = b + d$, so $\frac{x}{y} = \frac{a+c}{b+d}$. ■

Theorem 37 (Textbook Theorem 6.5)**.** *If* $0 \leq x \leq y, (x, y) = 1$*, then the fraction* $\frac{x}{y}$ *appears in the* y^{th} *row of the table and all future rows.*

Proof The theorem is true by definition for $y = 1$. Assume that the theorem is true for $y = y_0 - 1$, with $y_0 > 1$. Then if $y = y_0 - 1$, then the fraction $\frac{x}{y}$ cannot be in the $(y-1)^{st}$ row by definition. Then $\frac{c}{d} < \frac{x}{y} < \frac{a}{b}$ for some $\frac{a}{b}, \frac{c}{d}$ in the $(y-1)^{st}$ row. Since $\frac{c}{d} < \frac{a+c}{b+d} < \frac{a}{b}$, and $\frac{a}{b}, \frac{c}{d}$ are consecutive fractions,

$\dfrac{a+c}{b+d}$ is not in the $(y-1)^{st}$ row. Thus $b+d > y-1$ by the induction hypothesis. By Theorem 6.4, $y \geq b+d$, so $y = b+d$. By the uniqueness part of Theorem 6.4, $x = a+c$. Thus, $\dfrac{x}{y}$ appears in the y^{th} row of the table and all future rows. ■

Corollary 3 (Textbook Corollary 6.6)**.** *The n^{th} row consists of all reduce fractions with $\dfrac{a}{b}$ such that $0 \leq \dfrac{a}{b} \leq 1$ and $0 < b \leq n$. The fractions are listed from smallest to largest.*

Now we have the definition of the Farey sequences which contain the level n Farey fractions between 0 and 1.

Definition 16. *The n^{th} Farey sequence*

$$F_n = \left\{ \frac{p}{q} : (p,q) = 1, 1 \leq q \leq n \right\}.$$

So that every term in the sequence is a fraction, we write $n = \dfrac{n}{1}$. The first four Farey sequences are

$$F_1 = \left\{ \ldots, -\frac{1}{1}, \frac{0}{1}, \frac{1}{1}, \ldots \right\}$$

$$F_2 = \left\{ \ldots, -\frac{1}{1}, -\boxed{\frac{1}{2}}, \boxed{\frac{0}{1}}, \boxed{\frac{1}{2}}, \frac{1}{1}, \ldots \right\}$$

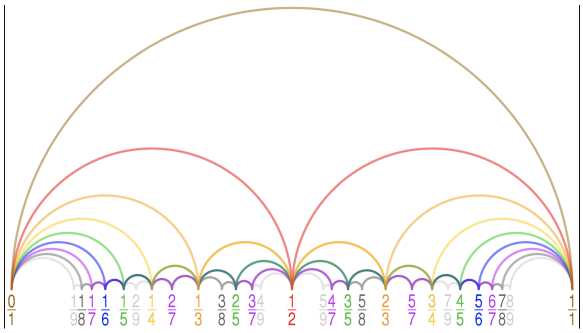
$$F_3 = \left\{ \ldots, -\frac{1}{1}, -\boxed{\frac{2}{3}}, -\boxed{\frac{1}{2}}, -\boxed{\frac{1}{3}}, \boxed{\frac{0}{1}}, \boxed{\frac{1}{3}}, \boxed{\frac{1}{2}}, \boxed{\frac{2}{3}}, \frac{1}{1}, \ldots \right\}$$

$$F_4 = \left\{ \ldots, -\frac{1}{1}, -\boxed{\frac{3}{4}}, -\boxed{\frac{2}{3}}, -\boxed{\frac{1}{2}}, -\boxed{\frac{1}{3}}, -\boxed{\frac{1}{4}}, \boxed{\frac{0}{1}}, \boxed{\frac{1}{4}}, \boxed{\frac{1}{3}}, \boxed{\frac{1}{2}}, \boxed{\frac{2}{3}}, \boxed{\frac{3}{4}}, \frac{1}{1}, \ldots \right\}$$

Depending on the source, Farey sequences may or may not be restricted to the interval $[0,1]$. However, if you look at the sets $f_n = S_n$, they aren't really sequences since they are finite.

Remark 1. *If $\dfrac{p}{q} = [a_0; a_1, a_2, \ldots, a_n]$ with $(p,q) = 1$, then the fractions on either side of $\dfrac{p}{q}$ in the q^{th} Farey sequence are $[a_0; a_1, a_2, \ldots, a_n - 1]$ and $[a_0; a_1, a_2, \ldots, a_{n-1}]$. For example, $\dfrac{2}{9}$ has continued fraction expansion $[\boxed{0}; \boxed{4}, \boxed{2}]$ and fractions on either side of $\dfrac{2}{9}$ in the 9^{th} Farey sequence are $\boxed{\dfrac{1}{5}} = [\boxed{0}; \boxed{4}, \boxed{1}]$ (smaller) and $\boxed{\dfrac{1}{4}} = [\boxed{0}; \boxed{4}]$ (larger).*

The following great image from Wikipedia highlights successive Farey fractions connected by semicircles. F_1 in brown, F_2 in red, F_3 in yellow, etc (the arc from 0 to $\frac{1}{n}$ tells you the color of the n^{th} Farey sequence). If you view the image on Wikipedia, hovering over a curve to highlights it and the terms in that Farey sequence (this seems to require a desktop browser) `https://upload.wikimedia.org/wikipedia/commons/9/91/Farey_diagram_horizontal_arc_9.svg`



April 22–n-ary expansions and Gaussian integers

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

n-ary expansions

Definition 17. *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

$$\sum_{k=-\infty}^{\infty} b_k n^k = \ldots b_2 b_1 b_0 . b_{-1} b_{-2} b_{-3} \ldots$$

$$= \cdots + b_2 n^2 + b_1 n + b_0 + \frac{b_{-1}}{n} + \frac{b_{-2}}{n^2} + \cdots, \quad b_k = b_k(x) \in \{0, 1, \ldots, n-1\},$$

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 22. *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}
2	3	1	4	1	2	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

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

Learning outcomes:
Author(s): Claire Merriman

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* $10, 11, 12, 13, 14, 15$*.*

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

Definition 18. *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*

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

is written

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

Theorem 38. *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 39. *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 19. *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 40. *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 41 (Contrapositive of Textbook Lemma 2.14)**.** $a^2+b^2 \not\equiv 3 \pmod 4$.

Theorem 42 (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 20. *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 21. *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 $N(-4-11i) = 137 < N(15-17i) = 514$.

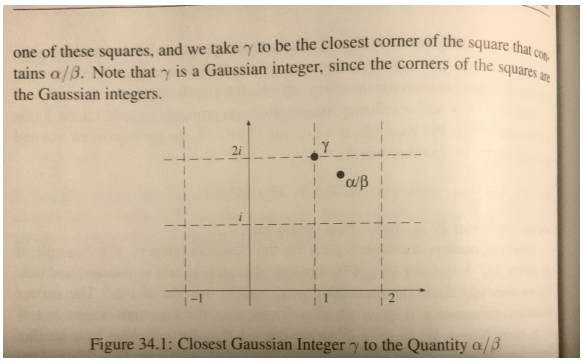
Theorem 43 (Division algorithm for Gaussian integers)**.** *Let $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$. Then there are Gaussian integers γ and ρ so that*

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

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.



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