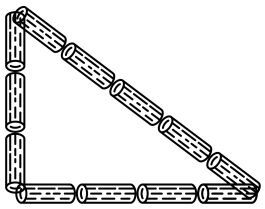
PYTHAGOREAN TRIPLES

DEFINITION: A triple (a, b, c) of natural numbers is a **Pythagoran triple** if they form the side lengths of a right triangle, where c is the length of the hypotenuse.



$(3, 4, 5)$ is a Pythagorean triple.

Our goal today is to find all Pythagoran triples. We will use a couple of tools that whose relevance might not be clear at first:

FUNDAMENTAL THEOREM OF ARITHMETIC: Every natural number $n \geq 1$ can be written as a product of prime numbers:

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}.$$

This expression is unique up to reordering. □

We call the number e_i the **multiplicity** of the prime p_i in the prime factorization of n.

DEFINITION: Let m, n be integers and $K \geq 1$ be a natural number. We say that m **is congruent to** n **modulo** K, written as $m \equiv n \pmod{K}$, if $m - n$ is a multiple of K.

THEOREM: Let n be an integer and $K \geq 1$ a natural number. Then n is congruent to exactly one nonnnegative integer between 0 and $K-1$: this number is the "remainder" when you divide n by K. □

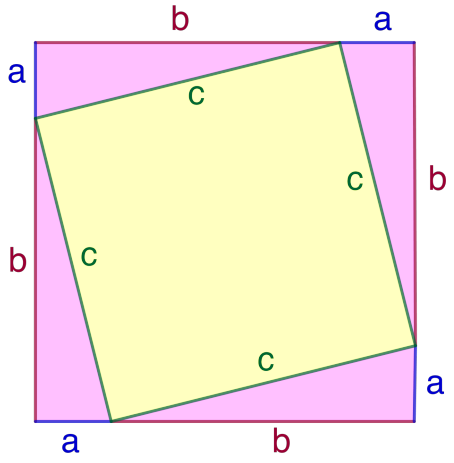
PROPOSITION: Let m, m', n, n' and K be natural numbers. Suppose that

$$m \equiv m' \pmod{K} \quad \text{and} \quad n \equiv n' \pmod{K}.$$

Then

$$m + n \equiv m' + n' \pmod{K} \quad \text{and} \quad mn \equiv m'n' \pmod{K}.$$ □

(1) Without writing too much, use the picture below to deduce the
PYTHAGOREM THOREM: If a, b, c are the side lengths of a right triangle, where c is the length of the hypotenuse, then $a^2 + b^2 = c^2$.



(2) Creating Pythagorean triples from others:
   (a) Show that if (a, b, c) is a Pythagorean triple and d is a natural number, then (da, db, dc) is a Pythagorean triple. Deduce that there are infinitely many Pythagorean triples.
   (b) Show that if (a, b, c) is a Pythagorean triple and d is a common factor of a, b, and c, then $(a/d, b/d, c/d)$ is a Pythagorean triple.

DEFINITION: A triple (a, b, c) of natural numbers is a **primitive Pythagoran triple (PPT)** if $a^2 + b^2 = c^2$, and there is no common factor of a, b, c greater than 1; equivalently, a, b, c have no common prime factor.

Based on (1) and (2), finding all Pythagorean triples boils down to finding all PPTs.

(3) Let a be a natural number. Show that if a is even, then $a^2 \equiv 0 \pmod 4$, and if a is odd, then $a^2 \equiv 1 \pmod 4$.

(4) Suppose that (a, b, c) is a Pythagorean triple. We want to examine the parity (even vs. odd) of the numbers a, b, c.
   (a) Suppose that a and b are both even. Show that c is even too. Deduce that there are no PPTs with a and b both even.
   (b) Suppose now that a and b are both odd. Consider the equation $a^2 + b^2 = c^2$ modulo 4, and use the problem (3) to get a contradiction.
   (c) Conclude that if (a, b, c) is a PPT, then one of a, b is odd, and the other is even, and that c is odd.

(5) Let m and n be natural numbers.
   (a) Show that n is a perfect square if and only if the multiplicity of each prime in its prime factorization is even.
   (b) Suppose that m and n have no common prime factors. Show that if mn is a perfect square, then m and n are both perfect squares.

(6) Consider a PPT (a, b, c). Following (4c), without loss of generality we can assume that a is odd and b is even. Rewrite the equation $a^2 + b^2 = c^2$ as $a^2 = c^2 - b^2$.
   (a) By definition, there is no prime factor common to all three of a, b, and c. Show that there is no prime factor common to just b and c.
   (b) Factor $c^2 - b^2$ as $(c-b)(c+b)$. Show that[1] there is no prime factor common to $c-b$ and $c+b$.
   (c) Show that $c - b$ and $c + b$ are perfect squares.
   (d) Show[2] that any PPT can be written in the form
$$(a, b, c) = \left(st, \frac{s^2 - t^2}{2}, \frac{s^2 + t^2}{2}\right)$$
   for some odd integers $s > t \geq 1$ with no common factors.
   (e) Check the other direction: show that any triple of the form $(st, \frac{s^2-t^2}{2}, \frac{s^2+t^2}{2})$, where $s > t \geq 1$ are odd integers with no common factors, is a PPT.

[1] Hint: If there is a (prime) number that divides these, it divides their sum and difference too.

[2] Hint: Start with writing $c + b = s^2$, $c - b = t^2$ and solve for a, b, c.

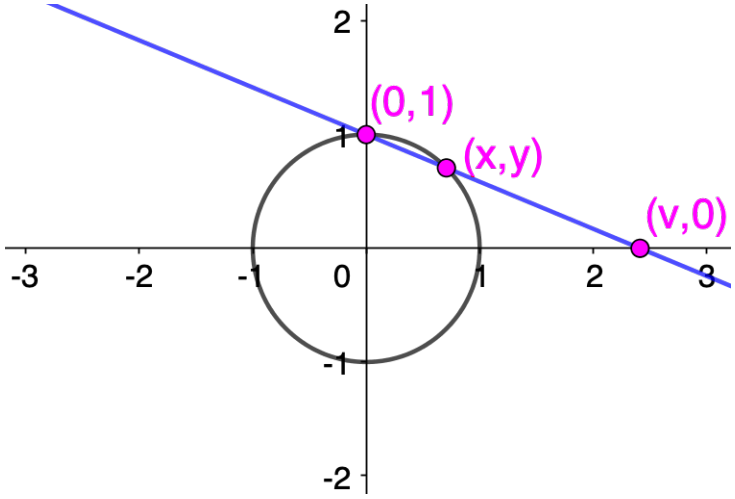
You have proven the following:

THEOREM: The set of primitive Pythagorean triples (a, b, c) with a odd is given by the formula

$$a = st, \quad b = \frac{s^2 - t^2}{2}, \quad c = \frac{s^2 + t^2}{2},$$

where $s > t \geq 1$ are odd integers with no common factors.

These mysterious formulas have a geometric explanation.



(7) (a) Show that if (a, b, c) is a Pythagorean triple, then $\left(\frac{a}{c}, \frac{b}{c}\right)$ is a point on the circle with positive rational coordinates, and vice versa.

(b) Given a rational number $v > 1$, the line L through $(0, 1)$ and $(v, 0)$ intersects the unit circle in two points (one of which is $(0, 1)$). As a first step towards finding this point, find an equation for L.

(c) Use the equation you found in (7b) and the equation for the unit circle to solve for x and y in terms of v.

(d) Use (b) to solve for v in terms of x and y and this to show that if x and y are rational, then v is rational.
Conclude the following theorem:

THEOREM: The set of points on the unit circle $x^2 + y^2 = 1$ with positive rational coordinates is given by the formula

$$(x, y) = \left(\frac{2v}{v^2 + 1}, \frac{v^2 - 1}{v^2 + 1}\right)$$

where v ranges through rational numbers greater than one.

(e) Take the expressions for x and y from the Theorem above in terms of v, and plug in $v = s/t$ and simplify each expression for x and y into a single fraction.

(f) Plug these expressions back into $x^2 + y^2 = 1$, clear denominators, and divide through by 4. What do you notice?

(8) Use similar techniques[3] to find rational points on:
   (a) The circle $x^2 + y^2 = 2$.
   (b) The hyperbola $x^2 - y^2 = 1$.
   (c) The hyperbola $x^2 - 2y^2 = 1$.
   (d) The circle $x^2 + y^2 = 3$.

(9) Use this to find integer solutions (a, b, c) to the equations:
   (a) The circle $a^2 + b^2 = 2c^2$.
   (b) The hyperbola $a^2 - b^2 = c^2$.
   (c) The hyperbola $a^2 - 2b^2 = c^2$.
   (d) The circle $a^2 + b^2 = 3c^2$.

   Are these all of the integer solutions?

Key Points:

- Using the Fundamental Theorem of Arithmetic for basic divisibility arguments.
- Definition of congruence, and using congruences to rule out solutions of equations.
- Using geometry to find rational points.

[3]Hint: You many have to change your starting point and/or target line. You might find it useful to take new coordinates in which your starting point is the origin, i.e., $x' = x - a$, $y' = y - b$ if your starting point is (a, b).

THE EUCLIDEAN ALGORITHM AND LINEAR EQUATIONS

DEFINITION: The **greatest common divisor** of two integers a and b, denoted $\gcd(a, b)$, is the largest integer that divides a and b. Two integers a and b are **coprime** if $\gcd(a, b) = 1$.

The **Euclidean algorithm** is an algorithm to find the greatest common divisor of two integers $a \geq b \geq 1$. Here is how it works:

(I) Start with $a_0 := a$, $b_0 := b$, and $n = 0$.
(II) Apply long division / division algorithm to write $a_n := q_n b_n + r_n$ with $0 \leq r_n < b_n$.
(III) If $r_n = 0$, STOP; the greatest common divisor of a and b is b_n.
Else, set $a_{n+1} := b_n$, $b_{n+1} := r_n$, and return to Step (II).

It is a THEOREM from Math 310 that the Euclidean algorithm terminates and outputs the correct value.

An expression of the form $ra + sb$ with $r, s \in \mathbb{Z}$ is a **linear combination** of a and b.

COROLLARY: If a, b are integers, then $\gcd(a, b)$ can be realized as a linear combination of a and b. Concretely, we can use the Euclidean algorithm to do this.

(1) Warumup with GCDs:
  (a) Let a, b be nonzero integers. Explain why[1] that $\gcd(a, b) = \gcd(|a|, |b|)$.
  (b) Let a, b be nonzero integers and $d = \gcd(a, b)$. Show that a/d and b/d are coprime.
  (c) Given prime factorizations of two positive integers a and b, explain[2] how to find $\gcd(a, b)$ using the prime factorizations (not the Euclidean algorithm).

(2) The following calculations correspond to running the Euclidean algorithm with 524 and 148:

(i)	$524 = 148 \cdot 3 + 80$	$0 \leqslant 80 < 148$
(ii)	$148 = 80 \cdot 1 + 68$	$0 \leqslant 68 < 80$
(iii)	$80 = 68 \cdot 1 + 12$	$0 \leqslant 12 < 68$
(iv)	$68 = 12 \cdot 5 + 8$	$0 \leqslant 8 < 12$
(v)	$12 = 8 \cdot 1 + 4$	$0 \leqslant 4 < 8$
(vi)	$8 = 4 \cdot 2 + 0$	

  (a) Identify the numbers a_n and b_n in the notation of the Euclidean algorithm as stated above.
  (b) What is the greatest common divisor of 524 and 148?

(3) Continuing this example...
  (a) Use equation (i) to express 80 as a linear combination of 524 and 148.
  (b) Use equation (ii) to express 68 as a linear combination of 148 and 80. Use this and the previous part to express 68 as a linear combination of 524 and 148.
  (c) Express 12 as a linear combination of 524 and 148.
  (d) Express $4 = (524, 148)$ as a linear combination of 524 and 148.

(4) Use the Euclidean algorithm to find the GCD of 184 and 99, and to express this GCD as a linear combination of 184 and 99.

[1] Hint: How are the divisors of a and $|a|$ related?
[2] Explain how, but don't write a careful proof for now.

We now know everything we need to solve all equations of the form $ax + by = c$ over the integers! A equation of this form considered over $\mathbb{Z}$ is called a **linear Diophantine equation**.

THEOREM: Let a, b, c be integers. The equation

$$ax + by = c$$

has an integer solution if and only if c is divisible by $d := \gcd(a, b)$. If this is the case, there are infinitely many solutions. If (x_0, y_0) is a one particular solution, then the general solution is of the form

$$x = x_0 - (b/d)n, \quad y = y_0 + (a/d)n$$

as n ranges through all integers.

(4) Proof of the first sentence/finding one particular solution:
   (a) Explain why if $ax + by = c$ has an integer solution (x_0, y_0) then c is a multiple of d.
   (b) What technique[3] would you use to find a particular solution of $ax + by = d$?
   (c) Given an integer m how could you find a particular solution for $ax + by = md$?
   (d) Observe that you have proven the first sentence of the Theorem above.

(5) Find all integer solutions (x, y) of the following equations:
   - $21x + 56y = 222$.
   - $21x + 56y = 224$.

(6) A farmer wishes to buy 100 animals and spend exactly \$200. Cows are \$20, sheep are \$6, and pigs are \$1. Is this possible? If so, how many ways can he do this?

(7) Conclusion of the proof of the Theorem: Suppose that c is divisible by $d := \gcd(a, b)$ and that (x_0, y_0) is a particular solution to $ax + by = c$.
   (a) Show that, for any integer n, $(x_0 - (b/d)n, y_0 + (a/d)n)$ is also a solution.
   (b) Suppose that (x_1, y_1) is another solution. Show that $(x_0 - x_1, y_0 - y_1)$ is a solution to $ax + by = 0$.
   (c) Take the equation $a(x_0 - x_1) = -b(y_0 - y_1)$ and divide through by d. Show that a/d divides $y_0 - y_1$ and b/d divides $x_0 - x_1$. Conclude the proof of the Theorem.

---

(8) In the next few problems we outline how to solve linear equations

(†) $$a_1x_1 + \cdots + a_nx_n = b$$

in multiple variables over $\mathbb{Z}$. First we deal with the easy cases.
   (a) Show that if $\gcd(a_1, \ldots, a_n)$ does not divide b, then (†) has no solution.
   (b) Show that if $a_1 = 1$, then $x_2, \ldots, x_n$ can be chosen to be *any* integers, with x_1 determined uniquely by the other values.
   (c) Solve $6x_1 + 10x_2 + 12x_3 = 13$ over $\mathbb{Z}$.
   (d) Solve $x_1 + 7x_2 + 9x_3 = 3$ over $\mathbb{Z}$.

(9) Now we discuss how to reduce the general equation to the easy cases. We start with two examples:
   (a) Take the equation

$$5x_1 + 35x_2 + 45x_3 = 15.$$

   Divide through to get to a settled case.

[3] Just name the relevant algorithm for now.

(b) Take the equation:

$$3x + 7y + 8z + 9w = 10.$$

We replace x by $u = x + 2y$, so $x = u - 2y$. Rewrite the equation above in terms of u, y, z, w and solve. Then express (x, y, z, w) in terms of the free parameters u, y, z.

(c) Here's how to generalize the last example: if a_i is the coefficient with smallest absolute value (say it's positive) and a_j is another coefficient that is *not* a multiple of a_i, apply long division to write $a_j = qa_i + r$ with $0 \leq r < |a_i|$. Replace x_i with $x_i' := x_i + qx_j$. Show that the coefficient of x_j in the new system is smaller than $|a_i|$.
Repeating this step and dividing all coefficients through by a common factor keeps decreasing the smallest coefficient until it becomes 1*, or until it is clear there is no solution.*

(d) Solve the equation $4x + 11y + 9z = 35$ over $\mathbb{Z}$.

(e) Solve the equation $8x - 4y + 10z - 12w = 28$ over $\mathbb{Z}$.

(f) Challenge your neighbor with a multivariate linear Diophantine equation!

Key Points:

- Computing GCD and GCD as a linear combination by Euclidean Algorithm.
- How to solve linear equations over $\mathbb{Z}$.

THE RING $\mathbb{Z}_n$, MODULAR UNITS, AND CRT

DEFINITION: A **congruence class** modulo K is a set of the form

$$[a] := \{n \in \mathbb{Z} \mid n \equiv a \pmod{K}\}$$

for some $a \in \mathbb{Z}$. We might also write $[a]_K$ to make clear what K is. A **representative** for a congruence class is an element of the congruence class.

PROPOSITION: Given $K > 0$, the set of integers $\mathbb{Z}$ is the disjoint union of K congruence classes:

$$\mathbb{Z} = [0] \sqcup [1] \sqcup \cdots \sqcup [K-1]. \qquad \square$$

The ring $\mathbb{Z}_K$ is the set of congruence classes modulo K:

$$\{[0], [1], \ldots, [K-1]\}$$

equipped with the operations

$$[a] + [b] = [a+b] \quad \text{and} \quad [a][b] = [ab].$$

(1) Warmup with congruence classes:
   (a) Find three distinct representatives of the congruence class $[13]$ in $\mathbb{Z}_5$.
   (b) Write a formula for all of the elements in the congruence class $[13]_5$.
   (c) Find the smallest nonnegative representative of the congruence class $[228]_{13}$.
   (d) True or false: $[5]_4$ is an element of $\mathbb{Z}_4$.
   (e) Fill in the blank: $a \equiv b \pmod{n}$ if and only if _____ in $\mathbb{Z}_n$.

(2) Fill out the following $+$ and $\times$ table for $\mathbb{Z}_4$. Write all of your entries in the form $[0]$, $[1]$, $[2]$, or $[3]$:

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$				
$[1]$				
$[2]$				
$[3]$				

$\times$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$				
$[1]$				
$[2]$				
$[3]$				

Explain the entry in the $[3]$ row and $[2]$ column of each table as a statement about integers and congruence modulo 4 (instead of about elements of $\mathbb{Z}_4$).

(3) Translating between congruence equations in $\mathbb{Z}$ and literal equations in $\mathbb{Z}_K$: Consider the equation

(†) $$x^2 + 3x \equiv 6 \pmod{n}.$$

   (a) Since we can add and multiply elements of $\mathbb{Z}_n$, the equation

(‡) $$y^2 + [3]y = [6]$$

   makes sense in $\mathbb{Z}_n$. Show that $x = a$ is a solution of (†) if and only if $y = [a]$ is a solution of (‡). Conclude that the set of solutions to (†) is the union of the congruence classes

$$\{[a] \mid y = [a] \text{ is a solution of (‡)}\}.$$

   (b) What was special about the equation (†)? Formulate a general principle.

DEFINITION: We say that a number a is a **unit modulo** K if there is an integer solution x to $ax \equiv 1 \pmod{K}$, and we say that such a number x is an **inverse modulo** K to a.

We say that a congruence class $[a]$ is a **unit in** $\mathbb{Z}_K$ if there is a congruence class $x \in \mathbb{Z}_K$ such that $[a]x = [1]$, and we say that such a class x is an **inverse** to $[a]$ in $\mathbb{Z}_K$.

(4) Warmup with units and inverses:
   (a) Check that 4 is an inverse for 16 modulo 21. Find two more inverses for 16 modulo 21.
   (b) Explain the following: b is an inverse for a modulo K if and only if $[b]$ is an inverse for $[a]$ in $\mathbb{Z}_K$.
   (c) Explain the following: a is a unit modulo K if and only if $[a]$ is a unit in $\mathbb{Z}_K$.
   (d) Show that if x has an inverse in $\mathbb{Z}_K$ then this inverse is unique.

THEOREM: Let a and n be integers, with n positive. Then a is a unit modulo n if and only if a and n are coprime.

(5) Proof of the Theorem / how to find inverses.
   (a) Use the definition of congruent modulo n to rewrite the statement $ax \equiv 1 \pmod{n}$ as a statement just about integers.
   (b) Prove the Theorem above.
   (c) Find an inverse for 24 modulo 149.

THEOREM (THE CHINESE REMAINDER THEOREM): Given $m_1, \ldots, m_k > 0$ integers such that m_i and m_j are coprime for each $i \neq j$, and $a_1, \ldots, a_k \in \mathbb{Z}$, the system of congruences

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \qquad\quad \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

has a solution $x \in \mathbb{Z}$. Moreover, the set of solutions forms a unique congruence class modulo $m_1 m_2 \cdots m_k$.

(6) Proof of CRT:
   (a) Set $m_i' = m_1 \cdots m_{i-1} m_{i+1} \cdots m_k$ to be the product of all of the m's except the i-th. Explain why m_i and m_i' are coprime.
   (b) Let m_i^* be an inverse of m_i' modulo m_i. (Why does one exist?) Show that

$$m_i' m_i^* \equiv 1 \pmod{m_i} \quad \text{and} \quad m_i' m_i^* \equiv 0 \pmod{m_j} \text{ for } j \neq i.$$

   (c) Find a solution in terms of $a_1, \ldots, a_k$ and $m_1' m_1^*, \ldots, m_k' m_k^*$.
   (d) Show that if $x' \equiv x \pmod{m_1 m_2 \cdots m_k}$, then x' is a solution as well.
   (e) Show[1] that if x' is another solution, then $x' \equiv x \pmod{m_1 m_2 \cdots m_k}$.

[1] The following LEMMA may be useful: if a and b are coprime, and a and b both divide c, then ab divides c.

(7) Solve the following systems:

(a)
$$\begin{cases} x & \equiv 4 \pmod{11} \\ x & \equiv 3 \pmod{17} \end{cases}$$

(b) Find[2] a number that leaves remainder 1 when divided by 3, a remainder of 2 when divided by 5, and a remainder of 3 when divided by 7.

(c)
$$\begin{cases} x \equiv 4 \pmod{6} \\ x \equiv 13 \pmod{15} \end{cases}$$

---

(8) Let a, b, n be integers, with $n > 0$.

(a) When does the equation $[a]x = [b]$ have a solution in $\mathbb{Z}_n$? Give an answer in terms of properties of the integers a, b, and n that we have discussed in class.

(b) How many solutions does the equation $[a]x = [b]$ have a solution in $\mathbb{Z}_n$? Give an answer in terms of properties of the integers a, b, and n that we have discussed in class.

Key Points:

- Definition of congruence classes and $\mathbb{Z}_n$.
- Relationship between solving congruences and solving equations in $\mathbb{Z}_n$.
- A number is a unit modulo n if and only if a and n are coprime.
- How to find inverses modulo n.
- Using CRT to solve multiple congruences.

[2] Real problem from Master Sun's Mathematical Manual (fourth century AD)!

THE UNIT GROUP, FERMAT'S LITTLE THEOREM, AND EULER'S THEOREM

DEFINITION: A **group** is a set G equipped with a product operation

$$G \times G \to G \qquad (g, h) \mapsto gh$$

and an **identity** element $1 \in G$ such that

- the product is associative: $(gh)k = g(hk)$ for all $g, h, k \in G$,
- $g1 = 1g = g$ for all $g \in G$, and
- for every $g \in G$, there is an inverse element $g^{-1} \in G$ such that $gg^{-1} = g^{-1}g = 1$.

A group is **abelian** if the product is commutative: $gh = hg$ for all $g, h \in G$. A **finite group** is a group G that is a finite set.

DEFINITION: Let G be a group and $g \in G$. The **order** of g is the smallest positive integer n such that $g^n = e$, if some such n exists, and ∞ if no such integer exists.

LAGRANGE'S THEOREM: Let G be a finite group and $g \in G$. Then the order of g is finite and divides the cardinality of the group G.

(1) The additive group $\mathbb{Z}_n$: Let n be a positive integer.
   (a) Show[1] that the set $\mathbb{Z}_n$ with the addition operation and identity element $[0]$ is a group. We will write $\mathbb{Z}_n$ to denote this group with this operation in general.
   (b) Find the order of each element in $\mathbb{Z}_4$.
   (c) Find the order of each element in $\mathbb{Z}_5$.
   (d) Check that Lagrange's theorem holds for $\mathbb{Z}_4$ and $\mathbb{Z}_5$.

(2) The group $\mathbb{Z}_n^\times$: Let n be a positive integer.
   (a) Show that the set

$$\mathbb{Z}_n^\times := \{a \in \mathbb{Z}_n \mid a \text{ is a unit in } \mathbb{Z}_n\}$$

   with the multiplication operation and identity element $[1]$ is a group. We will write $\mathbb{Z}_n^\times$ to denote this group with this operation in general.
   (b) Find the order of each element in $\mathbb{Z}_7^\times$.
   (c) Find the order of each element in $\mathbb{Z}_8^\times$.
   (d) Check that Lagrange's theorem holds for $\mathbb{Z}_7^\times$ and $\mathbb{Z}_8^\times$.

FERMAT'S LITTLE THEOREM: Let p be a prime number and a an integer. If p does not divide a, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

(3) Lagrange's Theorem implies Fermat's Little Theorem:
   (a) Show that $\mathbb{Z}_p^\times$ has exactly $p - 1$ elements.
   (b) Use Lagrange's theorem to show that if $[a] \in \mathbb{Z}_p^\times$, then $[a]^{p-1} = [1]$ in $\mathbb{Z}_p$.
   (c) Deduce Fermat's Little Theorem.

(4) Use Fermat's Little Theorem to find the smallest nonnegative integer congruent to each of the following: (a) $7^{12} \pmod{13}$, (b) $7^{96} \pmod{13}$, (c) $7^{98} \pmod{13}$, (d) $7^{1505} \pmod{13}$.

[1] Even though we are saying "product" operation, write gh for the typical group operation, and 1 for the typical identity element, we can take $(g, h) \mapsto g + h$ here. We just need to check the three rules above.

DEFINITION: Let n be a positive integer. We define $\varphi(n)$ to be the number of elements of $\mathbb{Z}_n^\times$. We call this **Euler's phi function**.

PROPOSITION: Euler's phi function satisfies the following properties.

(1) If p is a prime and n is a positive integer, then $\varphi(p^n) = p^{n-1}(p-1)$.
(2) If m, n are coprime positive integers, then $\varphi(mn) = \varphi(m)\varphi(n)$.

EULER'S THEOREM: Let a, n be coprime integers, with n positive. Then

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

(5) Use the Proposition above to compute the following:
- $\varphi(41)$
- $\varphi(27)$
- $\varphi(15)$
- $\varphi(100)$.

(6) Use Euler's Theorem to compute the last two digits of 7^{2003}.

(7) Euler's phi function and Euler's Theorem.
(a) Explain why Lagrange's Theorem implies Euler's Theorem.
(b) Explain why $\varphi(n)$ is equal to the number of positive integers less than n that are coprime to n.
(c) Prove the first part of the Proposition above.
(d) Use CRT to explain why the map

$$\begin{aligned} \mathbb{Z}_{mn} &\xrightarrow{\pi} \mathbb{Z}_m \times \mathbb{Z}_n \\ [a]_{mn} &\mapsto ([a]_m, [a]_n) \end{aligned}$$

is bijective.
(e) Show[2] that $[a]_{mn}$ is a unit in $\mathbb{Z}_{mn}$ if and only if $[a]_m$ is a unit in $\mathbb{Z}_m$ and $[a]_n$ is a unit in $\mathbb{Z}_n$.
(f) Conclude the proof of the second part of the Proposition above.

(8) Proof of Lagrange's Theorem: Let G be a finite group and $g \in G$. Let e be the order of g.
(a) Consider the list $1, g, \ldots, g^{e-1}$. Explain why these elements are all distinct.
(b) If $G = \{1, g, \ldots, g^{e-1}\}$, explain why Lagrange's Theorem holds.
(c) If $h_1 \in G \smallsetminus \{1, g, \ldots, g^{e-1}\}$, explain why the list of elements $h_1, h_1 g, \ldots, h_1 g^{e-1}$ are all distinct. Then explain why $\{1, g, \ldots, g^{e-1}\}$ and $\{h_1, h_1 g, \ldots, h_1 g^{e-1}\}$ are disjoint.
(d) Continue this process to form a table

$$\begin{array}{cccc} 1 & g & \ldots & g^{e-1} \\ h_1 & h_1 g & \ldots & h_1 g^{e-1} \\ \vdots & \vdots & \ddots & \vdots \\ h_t & h_t g & \ldots & h_t g^{e-1} \end{array}$$

Conclude the proof of the theorem.

[2]For the forward direction, take an inverse $[b]_{mn}$ for $[a]_{mn}$ is a unit in $\mathbb{Z}_{mn}$ and consider $[b]_m$ and $[b]_n$. For the reverse, take inverses $[c]_m$ and $[d]_n$ for $[a]_m$ and $[a]_n$ respectively, and apply CRT.

PRIMITIVE ROOTS AND DISCRETE LOGARITHMS

PROPOSITION: Let p be a prime. Let $p(x)$ be a polynomial of degree d with coefficients in $\mathbb{Z}_p$. Then $p(x)$ has at most d roots in $\mathbb{Z}_p$. □

LEMMA (FROM HW): If G is a group, $g \in G$, and n a positive integer such that $g^n = 1$, then the order of g divides n.

DEFINITION: Let n be a positive integer. An element $g \in \mathbb{Z}_n^\times$ is a **primitive root** if the order of g in $\mathbb{Z}_n^\times$ equals $\phi(n)$ (the cardinality of $\mathbb{Z}_n^\times$).

THEOREM: Let p be a prime number. Then there exists a primitive root in $\mathbb{Z}_p^\times$.

(1) Warmup with primitive roots:
   (a) Check that $[2]$ is a primitive root in $\mathbb{Z}_5$.
   (b) Check that $[3]$ is a primitive root in $\mathbb{Z}_4$.
   (c) Find a primitive root in $\mathbb{Z}_7$.
   (d) Show that there is no primitive root in $\mathbb{Z}_8$.

(2) Suppose that $g = [a]$ is a primitive root in $\mathbb{Z}_p$.
   (a) Show that[1] if $0 \leq m \leq n < p-1$, and $g^m = g^n$, then $m = n$.
   (b) Show that every element of $\mathbb{Z}_p^\times$ can be written as g^n for a unique integer n with $0 \leq n < p-1$.
   (c) Show that the relation $y \in \mathbb{Z}_p^\times \rightsquigarrow [m] \in \mathbb{Z}_{p-1}$ if $y = g^m$ is a well-defined function $I : \mathbb{Z}_p^\times \to \mathbb{Z}_{p-1}$.

DEFINITION: If $[a]$ is a primitive root in $\mathbb{Z}_p$, the function

$$\mathbb{Z}_p^\times \to \mathbb{Z}_{p-1} \quad [b] \mapsto [m] \text{ such that } [b] = [a]^m$$

is called the **discrete logarithm** or **index** of $\mathbb{Z}_p^\times$ with base $[a]$.

(3) Let p be a prime and $[a]$ a primitive root in $\mathbb{Z}_p$. Show that the corresponding discrete logarithm function $I : \mathbb{Z}_p^\times \to \mathbb{Z}_{p-1}$ satisfies the property

$$I(xy) = I(x) + I(y) \quad \text{and} \quad I(x^n) = [n]I(x)$$

for $x, y \in \mathbb{Z}_p^\times$ and $n \in \mathbb{N}$.

(4) (a) Verify that $[2]$ is a primitive root in $\mathbb{Z}_{11}$ and compute the corresponding discrete logarithm.
   (b) Use this function to find a square root of $[3]$ in $\mathbb{Z}_{11}$.

PROPOSITION: Let n be a positive integer. Then $\displaystyle\sum_{d \,|\, n} \varphi(d) = n$.

THEOREM: Let p be a prime. Suppose that there are n distinct solutions to $x^n = 1$ in $\mathbb{Z}_p$. Then $\mathbb{Z}_p^\times$ has exactly $\varphi(n)$ elements of order n.

(5) Explain how the theorem above implies that there exists a primitive root in $\mathbb{Z}_p$.

[1] Hint: x^m has an inverse.

(6) Proof of Theorem (using the Proposition): Fix a prime number p.
   (a) We proceed by strong induction on n. What does that mean concretely here? Complete the case $n = 1$.
   (b) Suppose that $x^n = 1$ but the order of x in $\mathbb{Z}_p^\times$ is not n. What does the Lemma say about the order of x? Rephrase this in terms of x satisfying an equation.
   (c) Suppose that d is a divisor of n, and write $n = de$. Note that
   $$x^n - 1 = (x^d - 1)(x^{d(e-1)} + x^{d(e-2)} + \cdots + x^d + 1).$$
   In particular, every solution of $x^n - 1$ is a root of $x^d - 1$ or of $x^{d(e-1)} + x^{d(e-2)} + \cdots + x^d + 1$. Can $x^d - 1$ have more than d roots in $\mathbb{Z}_p$? Can $x^d - 1$ have less than d roots in $\mathbb{Z}_p$ if $x^n - 1$ has n roots?
   (d) Apply the induction hypothesis to show that the number of solutions to $x^n = 1$ of order *less than* n is $\sum_{d \mid n, d \neq n} \varphi(d)$.
   (e) Apply the Proposition to conclude the proof of the Theorem.

(7) Proof of Proposition:
   (a) Explain the following formula:
   $$n = \sum_{d \mid n} \#\{a \mid 1 \leq a \leq n \text{ and } \gcd(a, n) = d\}.$$
   (b) Explain[2] why
   $$\#\{a \mid 1 \leq a \leq n \text{ and } \gcd(a, n) = d\} = \varphi(n/d).$$
   (c) Finally, explain[3] why
   $$\sum_{d \mid n} \varphi(n/d) = \sum_{d \mid n} \varphi(d)$$
   and complete the proof.

(8) Let p, q be distinct odd primes. Show that there is no primitive root of $\mathbb{Z}_{pq}$: i.e., there is no element of order $\varphi(pq)$ in $\mathbb{Z}_{pq}^\times$.

[2]Hint: You proved that if $\gcd(a, n) = d$, then $\gcd(a/d, n/d) = 1$; also, if $\gcd(b, n/d) = 1$, then $\gcd(bd, n) = d$.

[3]Hint: As d ranges through all the divisors of n, so does n/d.

QUADRATIC RESIDUES

DEFINITION: We say that an element $x \in \mathbb{Z}_n$ is a **square** or a **quadratic residue** if there is some $y \in \mathbb{Z}_n$ such that $y^2 = x$, and in this case, we call y a **square root** of x.

(1) Let n be an odd positive integer. Suppose that $[a]$ is a unit in $\mathbb{Z}_n$. Show that[1] the solutions x to the equation $[a]x^2 + [b]x + [c] = [0]$ in $\mathbb{Z}_n$ are exactly the elements of the form

$$x = \frac{-[b] + u}{[2a]} \quad \text{such that } u \text{ is a square root of } [b^2 - 4ac].$$

(2) Let p be an odd prime and $x \in \mathbb{Z}_p^\times$. Show that if x is a quadratic residue, then x has exactly two square roots $y \neq y'$, and for these roots, $y' = -y$.

(3) Let p be a prime number and g be a primitive root of $\mathbb{Z}_p$. Show that $[n] \in \mathbb{Z}_p^\times$ is a quadratic residue if and only if the index of $[n]$ with respect to g is even.

DEFINITION: Let p be an odd prime. For $r \in \mathbb{Z}$ not a multiple of p we define the **Legendre symbol** of r with respect to p as

$$\left(\frac{r}{p}\right) = \begin{cases} 1 & \text{if } [r] \text{ is a square in } \mathbb{Z}_p, \\ -1 & \text{if } [r] \text{ is a not square in } \mathbb{Z}_p. \end{cases}$$

THEOREM (EULER'S CRITERION): For p an odd prime and $r \in \mathbb{Z}$ not a multiple of p, we have

$$\left(\frac{r}{p}\right) \equiv r^{(p-1)/2} \pmod{p}.$$

THEOREM (QUADRATIC RECIPROCITY PART -1): If p is odd, then

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}.$$

PROPOSITION: Let p be an odd prime and a, b integers not divisible by p. Then

(1) $a \equiv b \pmod p$ implies that $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

(3) $\left(\frac{a^2}{p}\right) = 1$.

[1] Hint: Complete the square!

(4) (a) Without using the Proposition above, explain why $\left(\frac{4}{p}\right) = 1$ for p an odd prime. Now explain why part (3) of the Proposition above is true in general.

(b) Use the Proposition above to explain the following: If a, b are not squares modulo p, then ab is a square modulo p.

(c) Use[2] the Proposition and Corollary above to determine how many solutions x to

$$[3]x^2 + [12]x - [2] = [0]$$

there are in $\mathbb{Z}_{43}$.

(5) Use problem #3 to prove Euler's criterion.

(6) Prove the proposition above.

(7) Use Euler's criterion to prove QR part -1 above.

(8) When n is not a prime...

(a) Does the conclusion of #4(b) hold if n is replaced by a general positive integer n instead of a prime p?

(b) Suppose that $n = pq$ for primes $p \neq q$. Show that a is a quadratic residue modulo n if and only if a is a quadratic residue modulo p and a quadratic residue modulo q.

[2] You might find it convenient to write $168 = 4 \cdot 42$.

QUADRATIC RECIPROCITY

From last time:

DEFINITION: Let p be an odd prime. For $r \in \mathbb{Z}$ not a multiple of p we define the **Legendre symbol** of r with respect to p as

$$\left(\frac{r}{p}\right) = \begin{cases} 1 & \text{if } [r] \text{ is a square in } \mathbb{Z}_p, \\ -1 & \text{if } [r] \text{ is a not square in } \mathbb{Z}_p. \end{cases}$$

PROPOSITION: Let p be an odd prime and a, b integers not divisible by p. Then

(1) $a \equiv b \pmod{p}$ implies that $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

(3) $\left(\frac{a^2}{p}\right) = 1$. □

THEOREM (QUADRATIC RECIPROCITY): Let p and q be distinct odd primes. Then

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \qquad \text{if either } p \equiv 1 \pmod{4} \text{ or } q \equiv 1 \pmod{4},$$
$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right) \qquad \text{if both } p \equiv 3 \pmod{4} \text{ and } q \equiv 3 \pmod{4}.$$

THEOREM (QUADRATIC RECIPROCITY PART 2): Let p be an odd prime. Then

$$\left(\frac{2}{p}\right) = 1 \qquad \text{if } p \equiv \pm 1 \pmod{8},$$
$$\left(\frac{2}{p}\right) = -1 \qquad \text{if } p \equiv \pm 3 \pmod{8}.$$

(1) Computing quadratic residues with QR & QR part 2:
   (a) Compute $\left(\frac{2}{7}\right)$, $\left(\frac{2}{11}\right)$, and $\left(\frac{2}{101}\right)$.
   (b) What does QR say about $\left(\frac{3}{7}\right)$? Simplify the new Legendre symbol and evaluate.
   (c) Apply the same strategy as the previous part to compute $\left(\frac{13}{107}\right)$.

(2) Computing quadratic residues QR, QR part 2, and the proposition:
   (a) Compute $\left(\frac{10}{13}\right)$ by starting with Proposition part (2), then continuing as in the previous problem.
   (b) Compute $\left(\frac{38}{127}\right)$.

(3) How many solutions does the equation $[4]x^2 - [13]x + [5] = 0$ have in $\mathbb{Z}_{103}$?

GAUSS' LEMMA: Let p be an odd prime and set $p' = \frac{p-1}{2}$. Note that every integer coprime to p is congruent modulo p to a unique integer in the set $S = \{\pm 1, \pm 2, \cdots, \pm p'\}$.

Let a be an integer coprime to p. Consider the sequence

$$a, 2a, 3a, \ldots, p'a$$

and replace each element in the sequence with element of S that is congruent with modulo p to get a list L of p'-many elements of S.

Then $\left(\frac{a}{p}\right) = (-1)^{\nu}$, where ν is the number of negative integers in L.

LEMMA: Let p and q be two coprime odd positive integers. Then

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor + \sum_{\ell=1}^{\frac{q-1}{2}} \left\lfloor \frac{\ell p}{q} \right\rfloor = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

(4) (Partial) proof of QR part 2 using Gauss' Lemma: Let's just deal with $p \equiv 3 \pmod 8$. Write $p = 8\ell + 3$, so $p' = 4\ell + 1$. Compute L explicitly and deduce the result.

(5) Proof of Gauss' Lemma:
   (a) Show that none of the elements of L equal each other, nor are $\pm$ each other. Conclude that L is, in some order, $\pm 1, \pm 2, \ldots, \pm p'$, with each of $1, 2, \ldots, p'$ occurring once with a definite sign.
   (b) Compute the product of L modulo p two different ways and simplify.
   (c) Apply Euler's criterion, and conclude the proof.

(6) Proof of QR using Gauss' Lemma and other lemma: Take p, q distinct odd primes. For each $k \in \{1, 2, \ldots, p'\}$, write $kq = \lfloor kq/p \rfloor p + r_k$ with $1 \leq r_k \leq p-1$. Write

$$\{[q], [2q], \ldots, [p'q]\} = \{[r_1], [r_2], \ldots, [r_{p'}]\} = \{[a_1], \ldots, [a_u]\} \cup \{[-b_1], \ldots, [-b_v]\}$$

with $0 < a_i < p'$ and $0 < b_i < p'$, as in the statement of Gauss' Lemma.
   (a) Explain why $\sum_{k=1}^{p'} k = \frac{p^2-1}{8}$.
   (b) Explain why $\sum_{k=1}^{p'} r_k = \sum_{i=1}^{t} a_i - \sum_{i=1}^{v} b_i + vp$.
   (c) Explain why $\sum_{i=1}^{t} a_i + \sum_{i=1}^{v} b_i = \frac{p^2-1}{8}$.
   (d) Explain why $\frac{p^2-1}{8}\, q = p \sum_{k=1}^{p'} \lfloor kq/p \rfloor + \sum_{i=1}^{t} a_i - \sum_{i=1}^{v} b_i + vp$.
   (e) Explain why $\frac{p^2-1}{8}\,(q-1) = p \sum_{k=1}^{p'} \lfloor kq/p \rfloor + vp - 2\left(\sum_{i=1}^{v} b_i\right)$.
   (f) Explain why $v \equiv \sum_{k=1}^{p'} \lfloor kq/p \rfloor \pmod 2$, and apply Gauss' Lemma to deduce

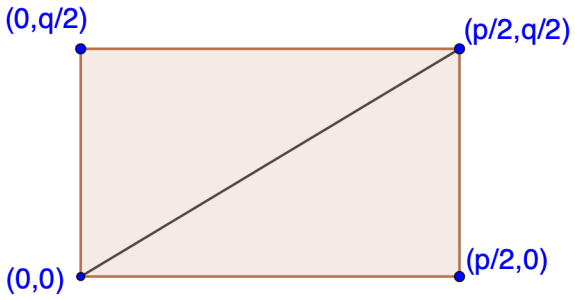
$$\left(\frac{q}{p}\right) = (-1)^{\sum_{k=1}^{p'} \lfloor kq/p \rfloor}.$$

   (g) Switch the roles of p and q, and plug the result into the other Lemma to show that

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

   Deduce the theorem.

(7) Proof of other lemma: Consider the rectangle below.



(a) Show that the number of integer points inside the rectangle (excluding the edges) is $\frac{p-1}{2} \cdot \frac{q-1}{2}$.

(b) Show that there are no integer points on the diagonal.

(c) Show that the number of integer points below the diagonal is $\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor$.

(d) Show that the number of integer points above the diagonal is $\sum_{\ell=1}^{\frac{q-1}{2}} \left\lfloor \frac{\ell p}{q} \right\rfloor$. Conclude the proof.

PRIMES IN ARITHMETIC PROGRESSIONS

THEOREM (EUCLID): There are infinitely many primes.

(1) Prove Euclid's Theorem as follows:
By way of contradiction, suppose that there are only finitely many primes $p_1, \ldots, p_k$. Consider the number $N = p_1 p_2 \cdots p_k + 1$ and derive a contradiction. (Warning: the contradiction is *not* that N must be prime!)

(2) Modify[1] Euclid's argument to show that there are infinitely many primes p such that $p \equiv 3 \pmod 4$.

(3) Extending your argument from (2):
   (a) Explain why your method from (2) cannot be used in the same way to show that there are infinitely many primes p such that $p \equiv 1 \pmod 4$.
   (b) For which classes $[a] \in \mathbb{Z}_3^\times$ can your argument from (2) be modified to show that there are infinitely many primes congruent to a modulo 3? Complete these cases.
   (c) For which classes $[a] \in \mathbb{Z}_5^\times$ can your argument from (2) be used in the same way to show that there are infinitely many primes congruent to a modulo 5?

(4) In this problem we will show that there are infinitely many primes congruent to 1 modulo 4:
If there are only finitely many $p_1, \ldots, p_k$, consider $N = 4(p_1 \cdots p_k)^2 + 1$. Show that if q is a prime factor of N then -1 is a quadratic residue modulo N, and conclude the proof.

(5) Show that there are infinitely many primes congruent to 1 modulo 3.
Hint: Consider $N = 3(p_1 \cdots p_k)^2 + 1$, and note that $[a]^{-1}$ is a square if and only if $[a]$ is a square.

(6) Show that there are infinitely many primes congruent to 4 modulo 5.

(7) Show that there are infinitely many primes congruent modulo 8 to 7, to 5, and to 3.

THEOREM* (DIRICHLET): If a and n are coprime integers, with $n > 0$, then there are infinitely many primes p such that $p \equiv a \pmod n$.

[1] Hint: Use a different formula for N that returns a number congruent to 3 modulo 4.

SUMS OF SQUARES

Recall:
THEOREM (QR PART -1): For p an odd prime, -1 is a square in $\mathbb{Z}_p$ if and only if $p \equiv 1 \pmod 4$.

THEOREM: An odd prime is a sum of two squares if and only if it is congruent to 1 modulo 4.

(1) Express $37, 41$, and 53 as sums of two squares.

(2) Show that every square and that every even prime is a sum of two squares.

(3) Show[1] the "only if" direction in the theorem above.

(4) Proof of "if" direction:
   (a) Explain why there is some natural number r with $r^2 \equiv -1 \pmod p$.
   (b) Let $k = \lfloor \sqrt{p} \rfloor$ and $S = \{0, 1, \ldots, k\}$. Explain why the function
   $$f : S \times S \to \mathbb{Z}_p$$
   $$(u, v) \mapsto [u + rv]$$
   must[2] admit two input pairs $(u_1, v_1) \neq (u_2, v_2)$ such that $f(u_1, v_1) = f(u_2, v_2)$.
   (c) Show that $a = u_1 - u_2$ and $b = v_1 - v_2$ satisfy $a^2 + b^2 = p$.

SUMS OF TWO SQUARES THEOREM: A positive integer n is a sum of two squares if and only if: for every prime p such that $p \equiv 3 \pmod 4$ and p divides n, the multiplicity of p in the prime factorization of n is even.

(5) Proof of Sums of Two Squares Theorem:
   (a) Show[3] that if $q \equiv 3 \pmod 4$ is prime and divides $n = a^2 + b^2$, then q divides a and q divides b. Conclude that q^2 divides n in this case.
   (b) Use the formula $(a^2+b^2)(c^2+d^2) = (ac-bd)^2+(ad+bc)^2$ to explain why any product of numbers that are sums of two squares is itself a sum of two squares.
   (c) Complete the proof of the Theorem.

---

[1] What did we do in HW#1?
[2] Hint: $k + 1 > \sqrt{p}$.
[3] If $q \not| a$, show that $[b]/[a]$ is a square root of -1.

SUMS OF FOUR SQUARES THEOREM: Every positive integer n is a sum of four squares.

(5) Proof of Sums of Four Squares Theorem:

(a) Use the formula

$$(a^2+b^2+c^2+d^2)(e^2+f^2+g^2+h^2) = (ae+bf+cg+dh)^2 + (af-be+ch-dg)^2 + (ag-bh-ce+df)^2 + (ah+bg-cf-de)^2$$

to conclude that a product of sums of four squares is a sum of four squares. In particular, it suffices to show that every prime is a sum of four squares.

(b) Show[4] that if p is an odd prime, then there are integers x and y such that $x^2+y^2 \equiv -1 \pmod{p}$ and $0 \leq x, y < p/2$. Deduce that for some $k < p$ we can write kp as a sum of three (and hence four) squares.

(c) Let p be an odd prime. Suppose that the smallest $p > 0$ such that kp is a sum of four squares is greater than one. First, if k is even and $kp = a^2+b^2+c^2+d^2$, explain why we can rearrange so that $a \equiv b \pmod{2}$ and $c \equiv d \pmod{2}$. Then show that

$$\frac{k}{2}p = \left(\frac{a-b}{2}\right)^2 + \left(\frac{a+b}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2 + \left(\frac{c+d}{2}\right)^2$$

and deduce that k is odd.

(d) Continuing the case where p is odd, $kp = a^2+b^2+c^2+d^2$ with k minimal and odd, suppose that $k > 1$. Take a', b', c', d' such that $a' \equiv a \pmod{k}$ and $-m/2 < a' < m/2$, and likewise with the others. Explain why $a'^2+b'^2+c'^2+d'^2 = kr$ for some $r < k$.

(e) Continuing the previous part, use the identity from part (a) to write $(kp)(kr)$ as a sum of four squares, and show that each of numbers whose squares appear is a multiple of k. Deduce that pr is a sum of four squares, contradicting the hypothesis that $k > 1$. This concludes the proof.

[4]Hint: Show that for the sets $S = \{0^2 1^2, \ldots, (\frac{p-1}{2})^2\}$ and $T = \{-1-0^2, -1-1^2, \ldots, -1-(\frac{p-1}{2})^2\}$ there are $s \in S$ and $t \in T$ that are congruent modulo p.

CONTINUED FRACTIONS

DEFINITION: A **finite continued fraction** is an expression of the form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}}$$

for some integers $a_0 \in \mathbb{Z}, a_1, \ldots, a_n \in \mathbb{Z}_{>0}$.
We write $[a_0; a_1, \ldots, a_n]$ as shorthand for this.

An **infinite continued fraction** is an expression of the form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}}$$

for some integers $a_0 \in \mathbb{Z}, a_1, a_2, a_3, \ldots \in \mathbb{Z}_{>0}$.
We write $[a_0; a_1, a_2, \ldots]$ as shorthand for this.

By a **continued fraction** we mean either an infinite or finite continued fraction. We call the numbers a_i the **partial quotients** in the continued fraction.

(1) Evaluating finite continued fractions:
   (a) Evaluate $2 + \cfrac{1}{13 + \frac{1}{2}}$.
   (b) Evaluate $[3; 2, 1, 4]$
   (c) Explain why every finite continued fraction evaluates to a rational number.

(2) Using the Euclidean algorithm to compute finite continued fractions:
   (a) What type of computation is the computation below?

$$\begin{aligned} 250 &= 2 \cdot 117 + 16 \\ 117 &= 7 \cdot 16 + 5 \\ 16 &= 3 \cdot 5 + 1 \\ 5 &= 5 \cdot 1 \end{aligned}$$

   (b) How does one obtain $\dfrac{250}{117} = 2 + \cfrac{1}{\frac{117}{16}}$ from the computation above?
   (c) Repeat (b) to obtain a finite continued fraction expansion for $\frac{250}{117}$.
   (d) Use the steps above to obtain a finite continued fraction expansion for $\frac{7}{5}$.
   (e) Use the steps above to obtain a finite continued fraction expansion for $\frac{39}{314}$.
   (f) What is the general formula for the continued fraction $[a_0; a_1, \ldots, a_n]$ for m/n in terms of the Euclidean algorithm?

(3) Euclidean algorithm and continued fraction algorithm:
   (a) In the computation from (2a) above, check that

$$2 = \left\lfloor \frac{250}{117} \right\rfloor \text{ and that } \frac{117}{16} = \left(\frac{250}{117} - \left\lfloor \frac{250}{117} \right\rfloor \right)^{-1}.$$

   (b) More generally, in the Euclidean algorithm

$$\begin{aligned} &\vdots \quad \vdots \quad \vdots \quad \vdots \\ u_i &= q_i \cdot v_i + r_i && (u_{i+1} = v_i) \\ u_{i+1} &= q_{i+1} \cdot v_{i+1} + r_{i+1} && (v_{i+1} = r_i) \\ &\vdots \quad \vdots \quad \vdots \quad \vdots \end{aligned}$$

   show that

$$q_i = \left\lfloor \frac{u_i}{v_i} \right\rfloor \text{ and } \frac{u_{i+1}}{v_{i+1}} = \left(\frac{u_i}{v_i} - \left\lfloor \frac{u_i}{v_i} \right\rfloor \right)^{-1}.$$

DEFINITION: Given an infinite continued fraction $[a_0; a_1, a_2, \dots]$, the k-th **convergent** of the continued fraction is the value C_k of the finite continued fraction $[a_0; a_1, \dots, a_k]$.

THEOREM (CONVERGENCE OF CONTINUED FRACTIONS): Every infinite continued fraction converges to a real number; i.e., for any $[a_0; a_1, a_2, a_3, \dots]$ with $a_0 \in \mathbb{Z}$ and $a_1, a_2, \dots \in \mathbb{Z}_{>0}$, the sequence of convergents $C_1, C_2, C_3, \dots$ converges. We call this limit the value of the infinite continued fraction.

CONTINUED FRACTION ALGORITHM: Given a real number r,

(I) Start with $\beta_0 := r$ and $n := 0$.
(II) Set $a_n := \lfloor \beta_n \rfloor$.
(III) If $a_n = \beta_n$, STOP; the continued fraction is $[a_0; a_1, \dots, a_n]$.
Else, set $\beta_{n+1} := (\beta_n - a_n)^{-1}$, and return to Step (II).

If the algorithm does not terminate, the continued fraction is $[a_0; a_1, a_2, \dots]$.

THEOREM (CORRECTNESS OF CONTINUED FRACTION ALGORITHM): For any real number r, the continued fraction obtained from the Continued Fraction Algorithm with input r converges to r.

PROPOSITION: Let r be a real number. The Continued Fraction Algorithm with input r terminates in finitely many steps if and only if r is rational.

DIRICHLET APPROXIMATION THEOREM: Let $r = [a_0; a_1, a_2, a_3, \dots]$ be a real number. Then for every convergent $C_k = \dfrac{p_k}{q_k}$ (in lowest terms), we have $\left| r - \dfrac{p_k}{q_k} \right| < \dfrac{1}{q_k^2}$.

In particular, if r is irrational, there are infinitely many rational numbers $\dfrac{p}{q}$ such that $\left| r - \dfrac{p}{q} \right| < \dfrac{1}{q^2}$.

(4) Use the continued fraction algorithm to find the first four ($n \leq 3$) partial quotients and convergents for $\sqrt{2}$, and π. Can you find the whole continued fraction for either of these?

(5) Find[1] the value of the continued fraction $1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{\ddots}}}$.

(6) Continued fraction algorithm and rational numbers.
   (a) Explain why the continued fraction algorithm just creates a continued fraction in the same way the Euclidean algorithm does as we did in problem (2).
   (b) Explain why the Proposition above is true.

(7) Dirichlet Approximation Theorem.
   (a) Let r be any real number. Explain why for *any* positive integer q, there is some integer p such that $|r - \frac{p}{q}| < \frac{1}{q}$. Conclude that $|r - \frac{p}{q}| < \frac{1}{q}$ is "not very impressive".
   (b) For $r = \sqrt{2}$, find all rational numbers p/q with $|r - \frac{p}{q}| < \frac{1}{q^2}$ with $q \leq 6$ and compare to the list of convergents C_0, C_1, C_2. What about $|r - \frac{p}{q}| < \frac{1}{2q^2}$? Conclude that $|r - \frac{p}{q}| < \frac{1}{q^2}$ is "pretty impressive".
   (c) Discuss $\pi \approx \frac{22}{7}$ in the context of the results above. Give a better approximation.

[1] Hint: This limit has a value L. Find an equation that L satisfies by recognizing L as a smaller piece of this continued fraction.

PROPOSITION: Let $[a_0; a_1, a_2, \dots]$ be a continued fraction. Set

$$p_0 := a_0, \quad p_1 := a_0a_1 + 1, \quad p_k := a_kp_{k-1} + p_{k-2}$$
$$q_0 := 1, \quad q_1 := a_1, \quad q_k := a_kq_{k-1} + q_{k-2}.$$

Then,

(1) $C_k = \dfrac{p_k}{q_k}$ for all $k \geq 0$, and

(2) $p_kq_{k-1} - p_{k-1}q_k = (-1)^{k-1}$ for all $k \geq 1$.

(8) Proof of convergence Theorem and Dirichlet Approximation Theorem.

(a) Use the Proposition above to show that $C_k - C_{k-1} = \dfrac{(-1)^{k-1}}{q_kq_{k-1}}$ for all $k \geq 1$.

(b) Use the Proposition above to show that $C_k - C_{k-2} = \dfrac{(-1)^k a_k}{q_kq_{k-2}}$ for all $k \geq 2$.

(c) Use (8b) to show that the sequence $C_0, C_2, C_4, \dots$ is increasing, that the sequence $C_1, C_3, C_5, \dots$ is decreasing; use (8a) to show that $C_{2k} < C_{2\ell+1}$ for all k, ℓ. Deduce that $\lim_{k\to\infty} C_{2k} = \sup\{C_{2k} \mid k \in \mathbb{N}\}$ and $\lim_{\ell\to\infty} C_{2\ell+1} = \inf\{C_{2\ell+1} \mid \ell \in \mathbb{N}\}$ both exist.

(d) Use (8a) to show that $\sup\{C_{2k} \mid k \in \mathbb{N}\} = \inf\{C_{2\ell+1} \mid \ell \in \mathbb{N}\}$, and hence that $\lim_{n\to\infty} C_n$ exists and is equal to both of these values. Thus, every continued fraction converges.

(e) Suppose that β is the value of our continued fraction. Use (8d) to show that $|\beta - C_n| \leq |C_{n+1} - C_n|$, and use (8a) to deduce Dirichlet's Approximation.

(9) Prove the Proposition above.

(10) Proof of Correctness of Continued Fraction Algorithm:

If r is rational, the algorithm terminates and returns r, so we can assume that r is irrational and that the algorithm does not terminate. Given r, let $a_0, a_1, a_2, a_3, \dots$ and $\beta_0, \beta_1, \beta_2, \dots$ be the sequences arising from the continued fraction algorithm.

(a) Explain why $r = [a_0; a_1, \dots, a_k, \beta_{k+1}]$. (Note, β_{k+1} is not an integer, but we can plug it into a finite continued fraction anyway.)

(b) Explain why $r = \dfrac{\beta_{k+1}p_k + p_{k-1}}{\beta_{k+1}q_k + q_{k-1}}$ where p_k, q_k, where p_k, q_k are the numbers coming from the continued fraction (with an irrational number snuck in) $[a_0; a_1, \dots, a_k, \beta_{k+1}]$ as in the Proposition above.

(c) Show that $|r - C_k| < \dfrac{1}{q_kq_{k+1}}$ for all $k \geq 1$ and deduce the result.

(11) Prove the following theorem, which basically says that the convergents are the *best* approximations of a rational number.

THEOREM: Let r be a real number, $C_k = \frac{p_k}{q_k}$ be the k-th convergent of r, and $\frac{p}{q} \neq r$ be a rational number. If $q \leq q_k$, then $\left|r - \dfrac{p}{q}\right| \geq \left|r - \dfrac{p_k}{q_k}\right|$.

PELL'S EQUATION AND UNITS IN $\mathbb{Z}[\sqrt{D}]$

DEFINITION: The equation $x^2 - Dy^2 = 1$ for some fixed positive integer D that is not a perfect square, where the variables x, y range through integers is called a **Pell's equation**. We say that a solution (x_0, y_0) is a **positive solution** if x_0, y_0 are both positive integers. We say that one positive solution (x_0, y_0) is **smaller** than another positive solution (x_1, y_1) if $x_0 < x_1$; equivalently, $y_0 < y_1$.

(1) Warmup with Pell's equation:
   (a) Verify that $(9, 4)$ is a solution to Pell's equation with $D = 5$.
   (b) Fix some D. Show that if (x_0, y_0) is a solution to Pell's equation, then $(\pm x_0, \pm y_0)$ are solutions to Pell's equation with the same D.
   (c) What two trivial solutions does every Pell's equation have?
   (d) Explain how to recover all solutions from just the positive solutions.

(2) By trial and error find the smallest positive solutions to Pell's equation with $D = 2$, $D = 3$, and $D = 5$.

(3) Suppose that D is a perfect square. Show that the equation $x^2 - Dy^2 = 1$ has no positive solutions.

DEFINITION: Let D be a positive integer that is not a perfect square. We define the **quadratic ring** of D to be

$$\mathbb{Z}[\sqrt{D}] := \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{R}.$$

DEFINITION: For the quadratic ring $\mathbb{Z}[\sqrt{D}]$ we define the **norm** function

$$N : \mathbb{Z}[\sqrt{D}] \to \mathbb{Z} \qquad N(a + b\sqrt{D}) = a^2 - b^2 D.$$

Note that $N(a + b\sqrt{D}) = (a + b\sqrt{D})(a - b\sqrt{D})$.

LEMMA: For the quadratic ring $\mathbb{Z}[\sqrt{D}]$ the norm function satisfies the multiplicative property $N(\alpha\beta) = N(\alpha)N(\beta)$.

(4) Warmup with $\mathbb{Z}[\sqrt{D}]$:
   (a) Show[1] that $\mathbb{Z}[\sqrt{D}]$ is a ring.
   (b) Show that every element in $\mathbb{Z}[\sqrt{D}]$ has a unique expression in the form $a + b\sqrt{D}$.

(5) Norms, units, and Pell's equation:
   (a) Prove the Lemma above.
   (b) Show that an element of $\mathbb{Z}[\sqrt{D}]$ is a unit (has a multiplicative inverse) if and only if its norm is ± 1.
   (c) Show that the set of units of $\mathbb{Z}[\sqrt{D}]$ forms a group under multiplication.
   (d) Show that the set of elements $a + b\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$ such that (a, b) is a solution to the Pell's equation $x^2 - Dy^2 = 1$ forms a group under multiplication.

[1] Recall: to check that a subset of a ring is a subring, it suffices to show that it contains the multiplicative identity and is closed under subtraction and multiplication.

THEOREM: Let D be a positive integer that is not a perfect square. Consider the Pell's equation $x^2 - Dy^2 = 1$. Let (a, b) be the smallest positive solution (assuming that some positive solution exists). Then every positive solution (c, d) can be obtained by the rule

$$c + d\sqrt{D} = (a + b\sqrt{D})^k$$

for some positive integer k.

(7) Use the Theorem above and your work from (2) to give a formula for all solutions to each of the Pell's equations
- $x^2 - 2y^2 = 1$
- $x^2 - 3y^2 = 1$
- $x^2 - 5y^2 = 1$

Then, for each of these, find the smallest three solutions.

(8) Proof of Theorem: Assume that (a, b) is the smallest positive solution to the Pell's equation $x^2 - Dy^2 = 1$.
(a) Show that pair of the form (c, d) where $c + d\sqrt{D} = (a + b\sqrt{D})^k$ is a positive solution to the same Pell's equation.
(b) Suppose that $(c, d) \neq (a, b)$ is a positive solution to Pell's equation. Show that if

$$e + f\sqrt{D} := (c + d\sqrt{D})(a - b\sqrt{D}),$$

then (e, f) is a solution to Pell's equation.
(c) Show[2] that, for e, f as in the previous part, $e, f > 0$ and $e < c$.
(d) Complete the proof of the Theorem.

(9) Use[3] your work from (7) to give a closed formula for all solutions to the same particular Pell's equations.

[2]For $e > 0$, note that $a > b\sqrt{D}$ and $c > d\sqrt{D}$. For $f > 0$, you might start with $a^2(c^2 - 1) > (a^2 - 1)c^2$. For $e < c$, multiply the equation above by $a + b\sqrt{D}$.

[3]Hint: The coefficients of $(m + n\sqrt{2})(3 + 2\sqrt{2})$ are the entries of $\begin{bmatrix} 3 & 4 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} m \\ n \end{bmatrix}$.

PELL'S EQUATION AND CONTINUED FRACTIONS

THEOREM (EXISTENCE OF SOLUTIONS TO PELL'S EQUATION): Let D be a positive integer that is not a perfect square. Then the Pell's equation $x^2 - Dy^2 = 1$ has a positive solution.

THEOREM (SOLUTIONS TO PELL'S EQUATION ARE CONVERGENTS): Let D be a positive integer that is not a perfect square. For every positive solution (a, b) to the Pell's equation $x^2 - Dy^2 = 1$, there is some $k \in \mathbb{Z}_{\geq 0}$ such that the ratio $\frac{a}{b}$ is a convergent C_k of the continued fraction of $\sqrt{D}$.

THEOREM (GOOD APPROXIMATIONS ARE CONVERGENTS): Let r be an irrational real number. If p, q are integers with $q > 0$ such that $|r - \frac{p}{q}| < \frac{1}{2q^2}$, then there is some $k \in \mathbb{Z}_{\geq 0}$ such that $\frac{p}{q}$ is a convergent C_k of the continued fraction of r.

(1) Solving Pell's equation completely:
   (a) Given the theorems above, devise a method to find the smallest positive solution to the Pell's equation $x^2 - Dy^2 = 1$.
   (b) Apply your method for $D = 2$, $D = 3$, $D = 10$, and $D = 21$. Compare your results for $D = 2$ and $D = 3$ to what you found last time by trial and error.
   (c) Give a formula for all positive solutions to Pell's equation for $D = 10$ and $D = 21$.

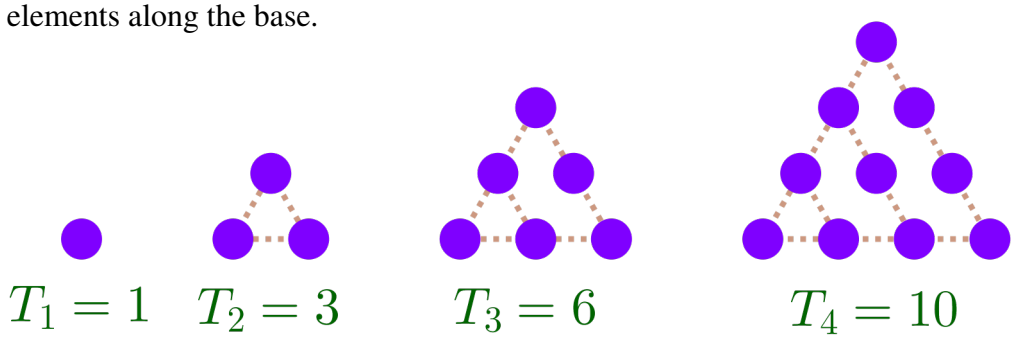
(2) Prove the Theorem (Solutions to Pell's equation are convergents) using the Theorem (Good approximations are convergents).

(3) Proof of Theorem (Existence of solutions to Pell's equation):
   (a) Use Dirichlet's approximation theorem to show that there are infinitely many pairs of integers (x_i, y_i) such that $|x_i^2 - Dy_i^2| < 2\sqrt{D} + 1$.
   (b) Show that there is some integer m with $0 < |m| < 2\sqrt{D} + 1$ such that there are infinitely many pairs of integers (x_i, y_i) with $x_i^2 - Dy_i^2 = m$.
   (c) Show that there is some integer m with $|m| < 2\sqrt{D} + 1$ and $a, b \in \mathbb{Z}$ such that there are infinitely many pairs of integers (x_i, y_i) with
   $$\begin{cases} x_i^2 - Dy_i^2 = m \\ x_i \equiv a \pmod{|m|} \\ y_i \equiv b \pmod{|m|} \end{cases}.$$
   (d) Given $i \neq j$ and x_i, x_j, y_i, y_j as in the previous part, show that $\frac{x_j + y_j\sqrt{D}}{x_i + y_i\sqrt{D}}$ is an element of $\mathbb{Z}[\sqrt{D}]$.
   (e) Complete the proof of the Theorem.

(4) Prove[1] Theorem (Good approximations are convergents).

[1]Hint: If not, we can assume $q_{k-1} < q < q_k$ for some k. In Problem set #5 problem #4, the same proof with $k-1$ in place of k in parts (a)–(d) shows that, under the same hypotheses, $|qr - p| \geq |q_{k-1}r - p_{k-1}|$. Then show that $|\frac{p}{q} - \frac{p_{k-1}}{q_{k-1}}| < \frac{1}{qq_{k-1}}$.

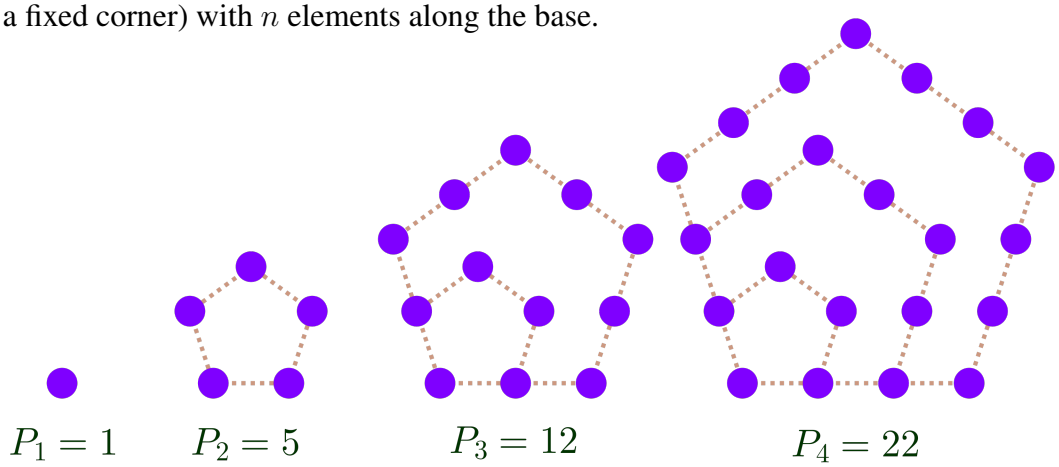
DEFINITION: A **triangular number** is a natural number T_n that counts the number of dots in a triangular array with n elements along the base.



(1) Explain why $T_n = 1+2+\cdots+n$. Then find[1] and prove a closed formula for the nth triangular number.

(2) In this problem we will classify all square-triangular numbers: numbers that are simultaneously triangular numbers and squares.
   (a) Set $T_m = n^2$. Complete the square on the left-hand side, and clear denominators. Write x and y for the squares[2] appearing in the equation. What sort of equation in x and y do you get?
   (b) Solve the equation in x and y. How is the integer solution set in the original equation in m and n related to the x and y equation?
   (c) Use your work to write down the first four square-triangular numbers.

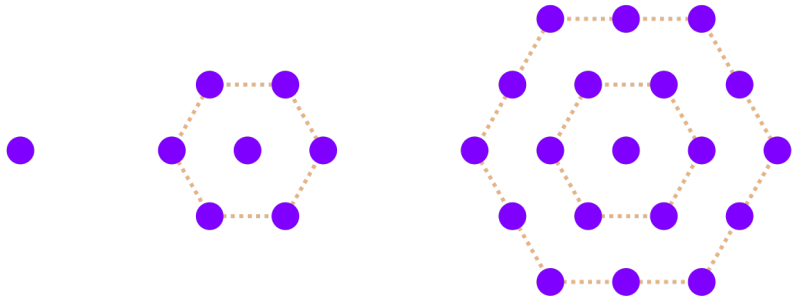
DEFINITION: A **pentagonal number** is a natural number P_n that counts the number of dots in a pentagonal array (with a fixed corner) with n elements along the base.



(3) In this problem we will classify all square-pentagonal numbers: numbers that are simultaneously triangular numbers and squares.
   (a) Find a formula for $P_m - P_{m-1}$. Use this and Problem (1) to give a closed formula for P_m.
   (b) Set $P_m = n^2$. Complete the square on the left-hand side, and clear denominators. Write x and y for the squares appearing in the equation. What sort of equation in x and y do you get?
   (c) Solve the equation in x and y. How is the integer solution set in the original equation in m and n related to the x and y equation? (Warning: This is more subtle than in the triangular case!)
   (d) Use your work to write down the first three square-pentagonal numbers.

[1]Hint: Write $T_n + T_n = (1 + 2 + \cdots + n) + (n + (n-1) + \cdots + 1)$.
[2]Suggestion: Write $8 = 2 \cdot 2^2$ and include the 2 from 2^2 in y.

DEFINITION: A **centered hexagonal number** is a number of the form is a natural number H_n that counts the number of dots in a hexagonal array (with a fixed center) with n elements along the base.



$H_1 = 1$ $H_2 = 7$ $H_3 = 19$

(4) Give a formula for all centered hexagonal numbers. Then give a formula for all square-(centered) hexagonal numbers, and list the first three of these.

(5) Find all numbers K that can be written in in the form

$$K = 1 + 2 + \cdots + (m-1) = (m+1) + (m+2) + \cdots + n$$

for some $m, n \in \mathbb{N}$. For example, the smallest such K is

$$15 = 1 + 2 + \cdots + 5 = 7 + 8.$$

In particular, find the first three such numbers.

(6) Find all numbers K that can be written in in the form

$$K = 1 + 2 + \cdots + m = (m+1) + (m+2) + \cdots + n$$

for some $m, n \in \mathbb{N}$. For example, the two smallest such K are

$$3 = 1 + 2 = 3 \quad \text{and} \quad 105 = 1 + 2 + \cdots + 14 = 15 + 16 + \cdots + 20.$$

ELLIPTIC CURVES

DEFINITION: A (real) **elliptic curve** is the solution set E in $\mathbb{R}^2$ to an equation of the form $y^2 = x^3 + ax + b$ for real constants $a, b \in \mathbb{R}$ that satisfy the technical assumption that $4a^3 + 27b^2 \neq 0$. For an elliptic curve E we define $\overline{E} = E \cup \{\infty\}$, where ∞ is a formal symbol.

Intuitively, we think of ∞ as a point infinitely far up or down in the y-direction.

We write $f_E(x, y) = y^2 - (x^3 + ax + b)$ for the elliptic curve E as above, so

$$E = \{(x, y) \in \mathbb{R}^2 \mid f_E(x, y) = 0\}.$$

DEFINITION (OPERATION ON AN ELLIPTIC CURVE): For an elliptic curve E, and points $P, Q \in E$ with $P \neq Q$, we set:

$$P^\vee := \text{the reflection of } P \text{ over the } x\text{-axis}$$

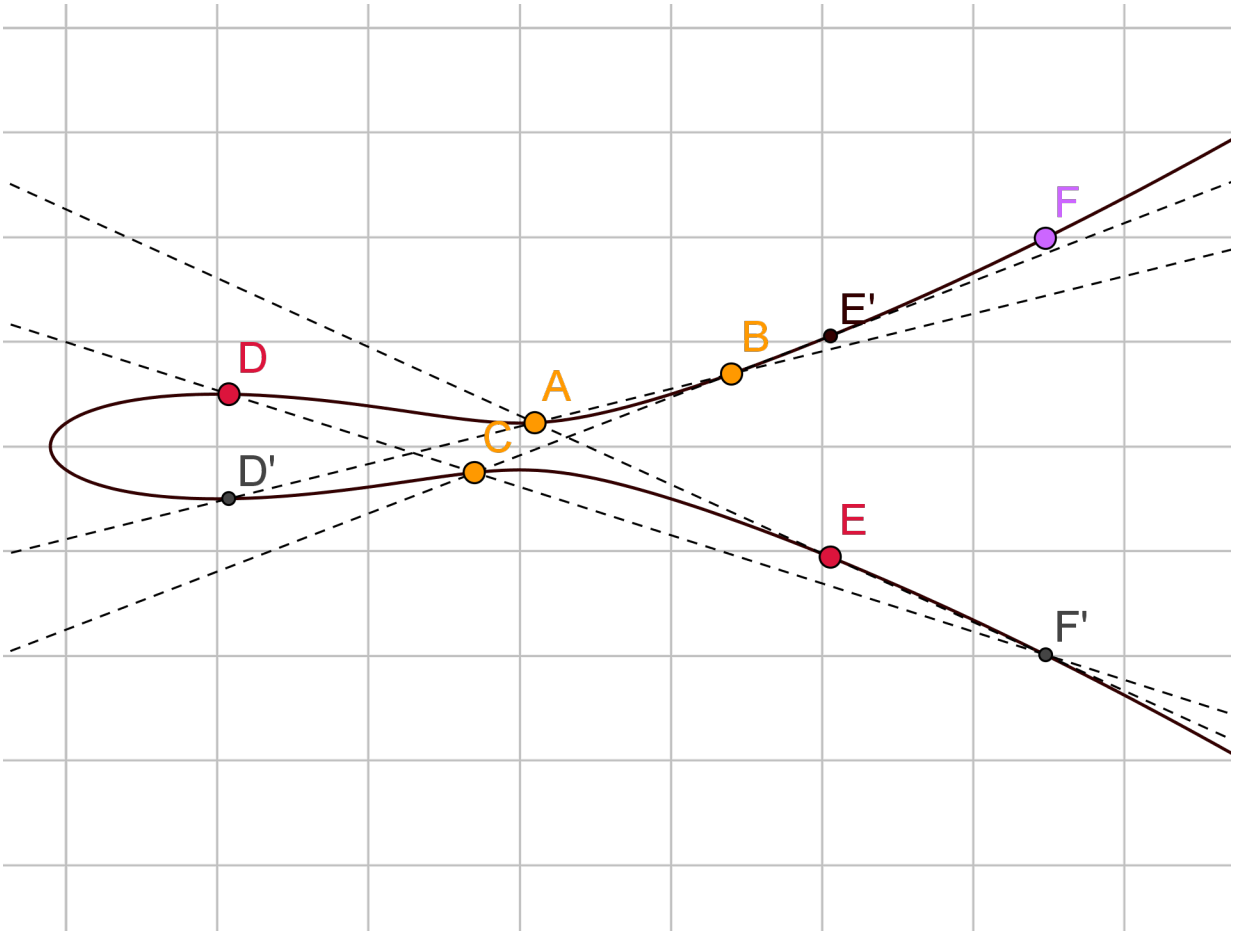
$$P \star Q := R^\vee, \text{ where } R \text{ is the third}^{1} \text{ point of intersection of the line between } P \text{ and } Q \text{ and } E.$$

THEOREM: There is a group structure on $\overline{E}$ with operation $\star$, identity element ∞, and inverse $-^\vee$.

(1) Drawing the operations $\star$ and $-^\vee$:
   (a) For each of the curves given, see if you can find labeled points P, Q, R such that $P \star Q = R$. Can you find all such triples?
   (b) For each of the curves given, mark your own points and see if you can compute the operation $\star$.

(2) Explain why $P \star Q = Q \star P$.

(3) Compute $(A \star B) \star C$ and $A \star (B \star C)$ in the example below. How is this related to the Theorem above?



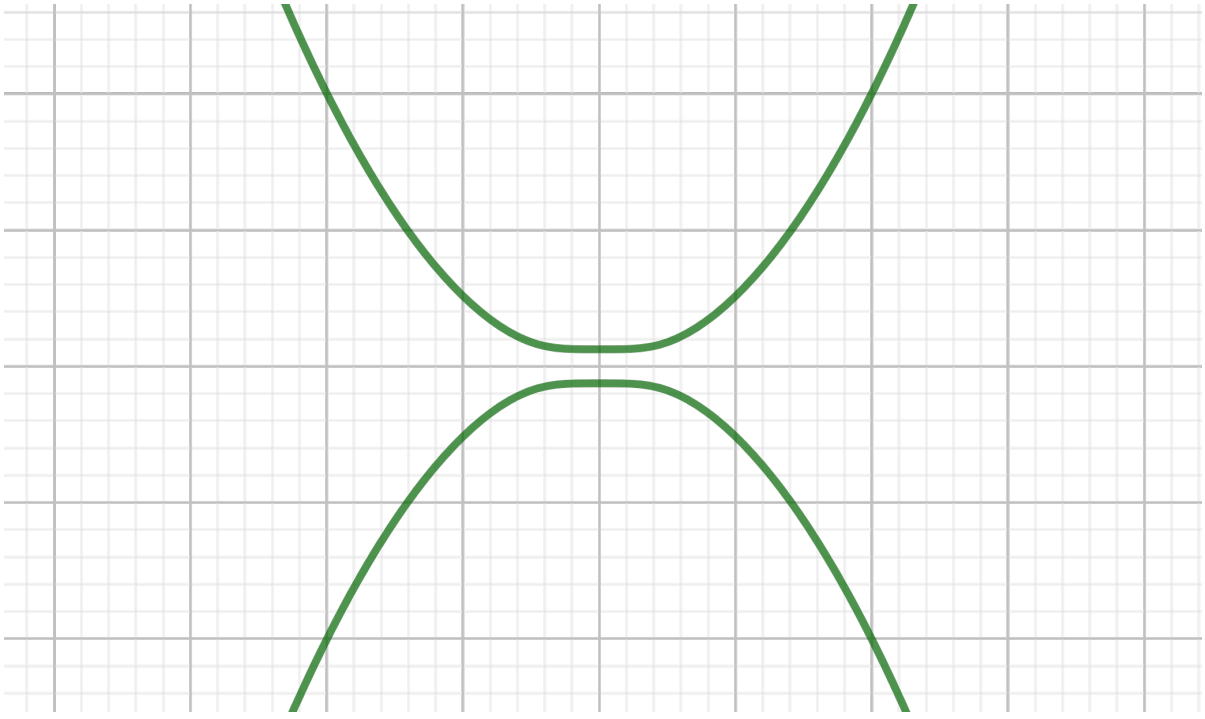
(4) Let E be the elliptic curve given by the equation $y^2 = x^3 + 2x + 4$.
   (a) Verify that $P = (-1, 1)$ and $Q = (0, 2)$ are points in E.
   (b) Compute $R = P \star Q$ and $S = Q \star R$.

(5) The operation $-^\vee$:
   (a) Explain algebraically why $P \in E$ implies $P^\vee \in E$, so $-^\vee$ is a valid operation on E.
   (b) For which points is $P = P^\vee$?
   (c) Explain geometrically why $P = P^\vee$ implies the tangent line to E at P is vertical.

(6) The doubling operation on an elliptic curve:
   (a) Let E be an elliptic curve and $P, Q \in E$. What happens to the line between P and Q if P stays fixed and Q approaches P?
   (b) Use the previous part to come up with a definition for $2P := P \star P$.
   (c) For each of the curves given, choose some points P and find $2P$ geometrically.
   (d) Let E be the elliptic curve given by the equation $y^2 = x^3 + 2x + 1$ and $P = (0, 1)$. Compute $2P$, $3P$, and $4P$.

(7) The group operation and ∞: Let's agree that "the line between P and ∞" is the vertical line through P and that "the reflection of ∞ over the x-axis is ∞."
   (a) With the agreements above, explain why the definition of $\star$ is consistent with $P \star \infty = \infty \star P = P$.
   (b) Given an element P, according to the agreements above, what element Q solves $P \star Q = \infty$?
   (c) Are your answers consistent with the Theorem above?

(8) Well-definedness of $\star$:
   (a) Consider the equation $y^2 = -x^2 + 1$. Note that $-^\vee$ makes sense on this curve. Take two points P, Q on this curve, and attempt the operation $\star$. What goes wrong?
   (b) Consider the equation $y^2 = \frac{1}{4}(x^4 + 1)$, depicted below. Take various combinations of points P, Q on this curve, and attempt the operation $\star$. What goes wrong?
   (c) Draw a random squiggle that is symmetric over the x-axis. Take various combinations of points P, Q on this squiggle, and attempt the operation $\star$. What goes wrong?



(9) Well-definedness of $\star$ continued:

(a) Let E be an elliptic curve, and $L = \{(x, y) \mid y = mx + b\}$ be a nonvertical line. Show that the x-coordinates of points in $L \cap E$ are exactly the zeros of $g_{E,L}(x) := f_E(x, mx + b)$.

(b) Show that $L \cap E$ has at most three points. Thus, for $P \neq Q \in E$, there is at most one other point on E and on the line between P and Q.

(c) Show that if $|L \cap E| \geq 2$, then either $g_{E,L}$ has three distinct roots, or else it has two roots, one of which has multiplicity two.

LEMMA: The condition $4a^3 + 27b^2 \neq 0$ guarantees that every point on E has a tangent line; i.e., implicit differentiation specifies a well-defined value (or infinity) for $\frac{dy}{dx}$ at each point.

LEMMA: If $P = (x_0, y_0) \in E$ and L a (nonvertical) line through P, then $g_{E,L}(x)$ has a double root at x_0 if and only if L is the tangent line to E at P.

(d) Use the Lemmas above to show that if $P \neq Q$ and L is the lime between P and Q, exactly one of the following happens:

- L intersects E in a third point (and no more).
- L is the tangent line to E at P and does not intersect E anywhere else.
- L is the tangent line to E at Q and does not intersect E anywhere else.

What should the value of $P \star Q$ be in each case?

(e) Prove the Lemmas above.

ELLIPTIC CURVES OVER $\mathbb{Q}$ AND $\mathbb{Z}_p$

From last time:

DEFINITION: A (real) **elliptic curve** is the solution set E in $\mathbb{R}^2$ to an equation of the form $y^2 = x^3 + ax + b$ for real constants $a, b \in \mathbb{R}$ that satisfy the technical assumption that $4a^3 + 27b^2 \neq 0$. For an elliptic curve E we define $\overline{E} = E \cup \{\infty\}$, where ∞ is a formal symbol.

Intuitively, we think of ∞ as a point infinitely far up or down in the y-direction.

DEFINITION (OPERATION ON AN ELLIPTIC CURVE): For an elliptic curve E, and points $P, Q \in E$ with $P \neq Q$, we set:

$P^\vee :=$ the reflection of P over the x-axis

$P \star Q := R^\vee,$ where R is the third point of intersection of the line between P and Q and E

$P \star P := S^\vee,$ where S is the other point of intersection of the tangent line to E at P and E.

THEOREM: There is a group structure on $\overline{E}$ with operation $\star$, identity element ∞, and inverse $-^\vee$.

(1) Points of low order[1]. Let $\overline{E} = E \cup \{\infty\}$ be a real elliptic curve the group law above.
   (a) How can you identify the points of order 2 on $\overline{E}$ geometrically? Mark them on each of your placemats. Note: They may not be labelled points.
   (b) How can you identify the points of order 4 on $\overline{E}$ geometrically? Mark them on each of your placemats. Note: They may not be labelled points.
   (c) Points of order 3 on $\overline{E}$ correspond to a special particular case of the group operation $\star$ that we haven't discussed yet: if $3P = \infty$ if and only if P is an inflection point. Discuss whether this rule is "morally consistent" with the rules above or if it is "totally out of left field".
   (d) Mark the points of order 3 on each of your placemats. Note: They may not be labelled points.
   (e) How can you identify the points of order 6 on $\overline{E}$ geometrically? Mark them on each of your placemats. Note: They may not be labelled points.

THEOREM: If E is a real elliptic curve given by the equation $y^2 = x^3 + ax + b$ for rational numbers $a, b \in \mathbb{Q}$, then the set of rational points on E (along with the infinity point "∞") form a group with operation $\star$, identity element ∞, and inverse $-^\vee$. We denote this group by $E_{\mathbb{Q}}$.

(2) Explain how[2] the theorem about the group structure on $\overline{E}_{\mathbb{Q}}$ above follows from the theorem about the group structure on $\overline{E}$ (real elliptic curves).

(3) The equation $y^2 = x^3 + 17$ has a rational solution $(-2, 3)$. Use this solution and the group structure on $\overline{E}_{\mathbb{Q}}$ to come up with at least five more rational solutions.

(4) The equation $y^2 = x^3 + 1$ has at least five easy rational solutions: $P = (-1, 0)$, $Q = (0, 1)$, $Q^\vee = (0, -1)$, $R = (2, 3)$, $R^\vee = (2, -3)$. Use the group structure on $\overline{E}_{\mathbb{Q}}$ to try to come up with more rational solutions.

[1] Recall: The order of an element g in a group G with identity 1 is the smallest integer n such that $g^n = 1$, if such an n exists, and infinite otherwise.

[2] Hint: How do you compute $P \star Q$ algebraically?

DEFINITION: Let $p \geq 5$ be a prime. An **elliptic curve** over $\mathbb{Z}_p$ is the solution set E_p in $\mathbb{Z}_p \times \mathbb{Z}_p$ to an equation of the form $y^2 = x^3 + [a]x + [b]$ for real constants $[a], [b] \in \mathbb{Z}_p$ that satisfy the technical assumption that $[4][a]^3 + [27][b]^2 \neq 0$. For an elliptic curve E_p we define $\overline{E}_p = E_p \cup \{\infty\}$, where ∞ is a formal symbol.

THEOREM: There is a group structure on $\overline{E}_p$ with operation $\star$, identity element ∞, and inverse $-^\vee$ given by the same geometric rules as in the real case.

(5) The elliptic curve $\overline{E}_5 : y^2 = x^3 - x + [1]$.
   (a) Use trial and error to compute all of the points in $\overline{E}_5$.
   (b) For $P = (0, 1)$ and $Q = (1, 1)$, compute $P \star Q$ and $2P$.

---

(6) In this problem, we will prove that the elliptic curve $E : y^2 = x^3 + 7$ has no integer solutions.
   (a) Suppose that (a, b) is an integer solution. Show that a must be odd.
   (b) Show that $b^2 + 1 = (a + 2)((a - 1)^2 + 3)$.
   (c) Show that there exists a prime $q \equiv 3 \pmod 4$ that divides the integer in (b), and obtain a contradiction.

(7) Let $a, b \in \mathbb{R}$ be real numbers. Show that every solution point $P = (x, y)$ of the equation $y^2 = x^3 + ax + b$ has a well-defined tangent line (i.e., implicit differentiation yields a well-defined real or infinite "value" of $\frac{dy}{dx}$ at every point) if and only if $4a^3 + 27b^2 \neq 0$.

(8) Use geometric and calculus considerations to give upper bounds on the number of points of
   - order 2
   - order 3
   - order 4

   on any real or rational elliptic curve.

ELLIPTIC CURVES OVER FINITE FIELDS

DEFINITION: Let $p \geq 5$ be a prime. An **elliptic curve** over $\mathbb{Z}_p$ is the solution set E_p in $\mathbb{Z}_p \times \mathbb{Z}_p$ to an equation of the form $y^2 = x^3 + [a]x + [b]$ for real constants $[a], [b] \in \mathbb{Z}_p$ that satisfy the technical assumption that $[4][a]^3 + [27][b]^2 \neq 0$. For an elliptic curve E_p we define $\overline{E}_p = E_p \cup \{\infty\}$, where ∞ is a formal symbol.

THEOREM: There is a group structure on $\overline{E}_p$ with operation $\star$, identity element ∞, and inverse $-^\vee$ given by the same geometric rules as in the real case.

(1) Consider the elliptic curve $\overline{E}_5 : y^2 = x^3 - [1]$ over $\mathbb{Z}_5$.
   (a) Use trial and error to compute all of the points in $\overline{E}_5$.
   (b) Without any computation, explain why each element of E_5 (not including ∞) has order $2, 3$, or 6.
   (c) For $P = ([3], [1])$, compute $2P$ and $3P$.
   (d) Without any further computation of $\star$ with lines and whatnot, determine the order of each point in $\overline{E}_5$.

(2) Consider the elliptic curve $\overline{E}_5 : y^2 = x^3 - x + [1]$ over $\mathbb{Z}_5$.
   (a) Use trial and error to compute all of the points in $\overline{E}_5$.
   (b) Explain why there are no points in E_5 (not including ∞) with odd order.
   (c) Explain why every point $P \in \overline{E}_5$ has $8P = \infty$.

RSA Encryption and Prime Factorization

People have needed to communicate information secretly for almost as long as we've been around. We can easily see how this can benefit finance or military, but it's even used in our day-to-day as computers communicate with each other. The earliest form of cryptography used what are known as **symmetric-key ciphers**, where two parties had access to a secret key that could both encrypt and decrypt messages. Of course, this requires the parties to have a way to communicate secretly in the first place. As technology advanced, the need for more sophisticated methods became necessary.

The RSA Cryptosystem—named after Ron Rivest, Adi Shamir, and Len Adleman, the first to publish[1] this method—is what is known as a **asymmetric-key cipher**, where everyone is allowed to encrypt with the public key, but only the holder of the private key can decrypt, making it great for one-way communications! While relatively new, it is built on notions, theorems, and work that has long existed in mathematics (we've covered most of it in class!).

RECALL: The **unit group** of n is the set $\mathbb{Z}_n^\times := \{a \in \mathbb{Z}_n \mid a \text{ is a unit in } \mathbb{Z}_n\}$.

RECALL: Euler's phi function satisfies the following properties:

(1) If p is prime and n is a positive integer, then $\phi(p^n) = p^{(n-1)}(p-1)$.
(2) If m, n are positive coprime integers, then $\phi(mn) = \phi(m)\phi(n)$.

(1) Generating an RSA Key:
   (a) Let $p = 47$ and $q = 59$. Calculate $n = pq$ and find $\phi(n)$.
   (b) Let $e = 17$. Explain why e has an inverse modulo $\phi(n)$.
   (c) Find $d = e^{-1} \pmod{\phi(n)}$.

(2) Encoding and Encrypting:
   (a) Encode the message "HI" into an integer m by converting the letters into numbers according to the table below and concatenating them in order.[2]

	A	B	C	D	E	F	G	H
00	01	02	03	04	05	06	07	08
I	J	K	L	M	N	O	P	Q
09	10	11	12	13	14	15	16	17
R	S	T	U	V	W	X	Y	Z
18	19	20	21	22	23	24	25	26

   (b) Find $y \equiv m^e \pmod{n}$.

(3) Decoding and Decrypting:
   (a) Find $x \equiv y^d \pmod{n}$ using any techniques[3] from class.
   (b) Decode x into a message by reversing the encoding in (2a).
   (c) Explain why $m^{ed} \equiv m \pmod{n}$.
   (d) Encode the message "CAT" as an integer m, then find and compare $y \equiv m^{17} \pmod{2773}$ and $x \equiv y^{157} \pmod{2773}$. Explain why $x \neq m$.

(4) Creating your own key-pair:
   (a) Choose two large primes and compute $n = p \cdot q$ and $\phi(n)$.
   (b) Choose any $0 < e < \phi(n)$ in $\mathbb{Z}_n^\times$.
   (c) Write your n and e on the board; these make up your public key.
   (d) Find $d = e^{-1} \pmod{\phi(n)}$.

[1] Clifford Cocks, an English mathematician, had actually developed a version of this four years prior, but he didn't think it was worth publishing!

[2] For example, "DOG" becomes $041507 = 41507$.

[3] HINT: Try using the Chinese Remainder Theorem to work with smaller numbers.

(5) Sending messages[4]:
   (a) Find another group to exchange messages with. Come up with a message m and encrypt it using that group's n and e. Write your encrypted message on the board.
   (b) Once the other group has written their encrypted message for you on the board, decrypt it and see what they sent.
   (c) Pick any group's message on the board and see if you can decrypt it, using any techniques. What do you need to know before you can decrypt the message?

FACTORING METHODS

(6) Factoring by **Trial Division**:
   (a) Let $n = 1643$ be the product of two primes. Factor n by brute force, i.e., attempt to divide by each[5] prime up to n.
   (b) There is a $200,000 cash reward for factoring a 617-digit product of two primes. Explain why this is unreasonable to do by Trial Division.

> THEOREM: If $a^2 \equiv b^2 \pmod{n}$, then $\gcd(a+b,n)\cdot\gcd(a-b,n) = n$. Furthermore, if $a \not\equiv \pm b \pmod{n}$, then $\gcd(a+b,n)$ and $\gcd(a-b,n)$ are non-trivial factors of n.

(7) Factoring by the **Continued Fraction Algorithm**:
   (a) Let $n = 3053$ be the product of two primes. Find the **factor base** of n: the set of positive primes[6] $q_i \leq 7$ where $\left(\dfrac{n}{q_i}\right) = 1$.
   (b) Check[7] that each element in the factor base is not a prime factor of n.
   (c) Find the first[8] 5 convergents $C_k = \dfrac{p_k}{q_k}$ of $\sqrt{n}$. For each of these, compute $a_k \equiv p_k \pmod{n}$ and $b_k \equiv p_k^2 \pmod{n}$.
   (d) Write each b_k as a product of primes in the factor base, if possible[9]. Find a nonempty set of pairs $(a_i, b_i), \ldots, (a_j, b_j)$ such that $b_i \cdots b_j$ is trivially a square modulo n and
$$a_i \cdots a_j \not\equiv \pm\sqrt{b_i \cdots b_j} \pmod{n}$$
.
   (e) Let $A \equiv a_i \cdots a_j \pmod{n}$ and $B \equiv \sqrt{b_i \cdots b_j} \pmod{n}$. Calculate and compare $A^2 \pmod{n}$ and $B^2 \pmod{n}$.
   (f) Apply the Theorem, and use the Euclidean Algorithm to find the prime factors of n.

---

[4] If at any point you're waiting, work ahead on future problems!

[5] HINT: Start by determining a reasonable upper bound for the smallest prime factor of n, and then divide and conquer.

[6] The upper bound of 7 was not arbitrary; $7 = \lfloor e^{\frac{1}{2}\sqrt{\ln(n)\ln(\ln(n))}} \rfloor$.

[7] If an element were to be a factor of n, then we can reduce n by that factor and try again.

[8] This choice was arbitrary. If we wish to do this in general, we'll take one convergent at a time until we find a solution.

[9] If b_k isn't possible, try $-b_k = (-1)p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$.

(Some) Primes between 1000 and 9999

8539	5801	3251	7487	3083	8269	5749	4127	3823	1871	1567	1777	5711
7817	3529	2239	2797	6691	6247	2579	1307	2749	5813	6091	5651	1499
4337	7589	6143	8741	9283	1321	8011	2657	7043	8369	7219	2311	7681
8629	8039	1097	5021	7561	1237	2161	8849	9467	6571	2741	4549	4421
9533	9391	7793	9007	5849	9479	3643	6053	8171	9209	2069	2459	7193
7159	5501	7841	7573	9859	2647	6679	3163	7649	6173	5011	7541	1291
6277	1789	2609	8573	5303	5657	5179	9649	6131	1753	4597	5953	9551
8761	3881	3407	2699	4493	8677	4657	1481	4457	9629	8599	8147	7549
4591	9067	5479	4229	8819	6287	3637	5927	7247	1217	6421	8093	6427
1439	5557	7451	6529	6491	8287	5323	7753	9103	1033	1609	3187	3023
6911	1973	7457	7499	1913	8123	1901	5851	7879	2693	1259	1123	8467
8689	9161	6737	9239	2969	4729	6899	2131	7919	9419	3391	9511	2113
3931	2753	1487	9967	1367	7703	3079	1069	6121	4157	1549	6043	9371
9721	8821	9199	9491	1627	3607	4139	1427	1399	9187	7949	9397	6373
9203	2383	5861	6547	4651	8543	5189	5683	6833	1999	1453	5413	6823
5449	3709	6971	5669	6977	7591	1301	8753	6197	2269	8389	6367	7547
1153	8867	3793	2557	6151	8537	3181	9803	5807	3049	4751	9949	9403
8209	1733	1741	3923	7019	3119	4639	8647	5113	3697	2879	7907	5923
5233	3889	9781	4523	5023	7993	8087	9539	4793	2437	9839	8641	3329
1669	2251	4801	3659	4049	9767	1093	2617	5417	8191	4261	3581	3673
5903	4783	6983	7013	8713	9349	6079	6599	3037	7621	6857	9241	2777
7243	9973	7207	6959	1229	7351	5641	6569	7433	5387	9311	5527	9689
3121	2399	3547	1091	6553	1279	1721	2273	7607	8951	7529	6073	7727
7901	1759	2423	3539	4831	2333	3089	7321	7669	6163	4759	4691	4969
8513	9857	3911	1289	1201	3853	5843	5647	7109	3677	3217	4519	1277
3767	3833	7757	5689	1979	1483	8837	3313	9787	9337	3449	4663	5653
1879	8563	9437	2153	5779	2347	8923	5279	4211	8419	6067	5419	9227
1621	9011	9619	6709	4703	5167	8971	9041	4463	3671	5347	8803	8429
3727	8069	1543	3533	3739	7507	2591	1559	6761	8831	1447	4093	6961
3469	9473	7489	1787	3343	4363	7829	8317	4679	4051	6359	7349	4021
7309	8297	5879	2099	9059	6011	7537	6449	4243	9431	4909	9341	6829
7213	2417	1187	8719	6997	4153	7297	9377	9293	9631	6089	2441	4253
1423	1451	4111	9091	1723	5273	6217	1009	2917	2897	1303	9661	8293
2677	6133	1061	1213	7883	5003	7723	7517	7691	1571	5443	5581	7307
3613	8969	4973	8929	3323	1063	2137	2833	4273	3433	2857	4129	1373
5399	4957	2539	2287	3701	5981	2887	7027	4583	4231	1747	4567	2039
1019	1021	2521	3557	4007	9871	3299	1049	5039	9497	1163	2473	2927
4507	7477	9221	8053	8807	4219	8081	3221	7417	2711	3373	8623	3851
7717	3821	7577	2063	1231	4861	7393	8009	7699	5087	3389	6113	9181
7069	6221	6451	9109	7559	6703	4817	9851	2551	2341	4721	2861	3907
2203	4391	3011	8747	3623	7283	6871	3359	8311	9749	7411	2351	4951
3361	3919	2027	8219	6361	9613	4919	2281	5821	8443	6803	1429	6299
8839	4517	6661	2801	8447	5147	6397	5531	1867	5119	1583	3041	9739
1601	4649	6389	4073	7867	1693	6883	3541	8779	9043	8017	3467	2339
8461	5297	9343	2357	1531	6791	9929	3691	6733	8933	2971	9817	8273
4079	1129	8699	6203	1523	4673	6907	5869	2803	3229	2707	5659	7369
4483	8179	8893	6779	6563	8731	2659	3929	3559	3527	2687	3779	4877
9461	8861	4177	4003	1283	4733	1223	8291	7103	1667	7853	5227	4993