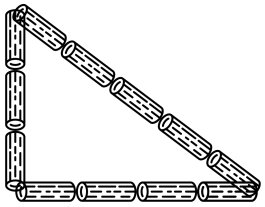
PYTHAGOREAN TRIPLES

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. □

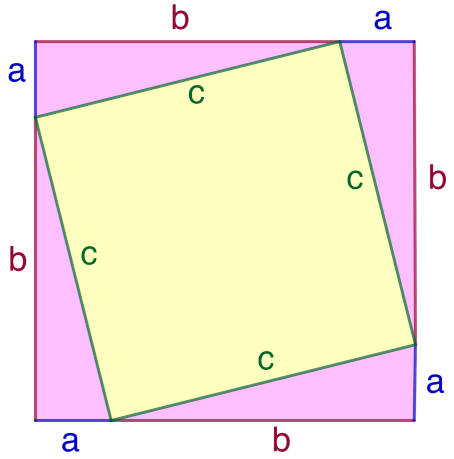
PROPOSITION: Let m, m', n, n' and K be natural numbers. Suppose that

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

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 $a^2 + b^2 = c^2$.



We calculate the area of the big square two ways. First, it is a square with side lengths $a+b$ so the area is

$$(a+b)^2 = a^2 + 2ab + b^2.$$

Second, it consists of a square with side length c and four right triangles with base a and height b, so the area is also

$$c^2 + 4(\frac{1}{2}ab) = c^2 + 2ab.$$

Equating the two and subtracting $2ab$, we get that $a^2 + b^2 = c^2$.

(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.

For (a), we assume that $a^2 + b^2 = c^2$ and test whether the new numbers (da, db, dc) satisfy the equation:

$$(da)^2 + (db)^2 = d^2a^2 + d^2b^2 = d^2(a^2 + b^2) = d^2c^2 = (dc)^2,$$

so they do! Part (b) is similar.

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 $a^2 \equiv 1 \pmod 4$.

First, suppose that a is even, so we can write $a = 2k$ for some integer k. Then $a^2 = (2k)^2 = 4k^2$, and $4k^2 - 0$ is a multiple of 4, so $a^2 \equiv 0 \pmod 4$. Now, suppose that a is odd, so we can write $a = 2k + 1$ for some integer k. Then $a^2 = (2k+1)^2 = 4k^2 + 4k + 1$, and $(4k^2 + 4k + 1) - 1 = 4(k^2 + k)$ is a multiple of 4, so $a^2 \equiv 1 \pmod 4$.

(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.

If a and b are even then $a^2 \equiv 0 \pmod 4$ and $b^2 \equiv 0 \pmod 4$. To obtain a contradiction, suppose that c is odd. Then $c^2 \equiv 1 \pmod 4$, but since $a^2 \equiv 0 \pmod 4$ and $b^2 \equiv 0 \pmod 4$, we know that $a^2 + b^2 \equiv 0 \pmod 4$. The same number can't be equivalent to both 0 and 1 mod 4. This contradicts that $a^2 + b^2 = c^2$.

   (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.

If a and b are odd then $a^2 \equiv 1 \pmod 4$ and $b^2 \equiv 1 \pmod 4$. Then $a^2 + b^2 \equiv 2 \pmod 4$. However, c is either even or odd, so either $c^2 \equiv 0 \pmod 4$ or $c^2 \equiv 1 \pmod 4$. Either way, $a^2 + b^2 \equiv c^2$ is impossible!

(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.

We know that exactly one of a, b is even and the other odd since we ruled out the possibilities. Then c has to be odd, since $a^2 + b^2 \equiv 0 + 1 \equiv 1 \pmod 4$.

(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.

($\Rightarrow$): If n is a perfect square, say that $n = t^2$. Take a prime factorization for t:

$$t = p_1^{\ell_1} \cdots p_k^{\ell_k}.$$

Then

$$n = t^2 = p_1^{2\ell_1} \cdots p_k^{2\ell_k}$$

is a prime factorization of n, and the multiplicities $2\ell_i$ are all even.
($\Leftarrow$): Suppose that the multiplicity of every prime in the prime factorization of n is even. That means we can write

$$n = p_1^{2\ell_1} \cdots p_k^{2\ell_k}$$

for some primes p_i and natural numbers ℓ_i. Then

$$n = (p_1^{\ell_1} \cdots p_k^{\ell_k})^2$$

is a perfect square.

(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.

Take prime factorizations of m and n:

$$m = p_1^{e_1} \cdots p_k^{e_k}, \quad n = q_1^{f_1} \cdots q_s^{f_s};$$

by our assumption, the p's and q's are all different. Then

$$mn = p_1^{e_1} \cdots p_k^{e_k} q_1^{f_1} \cdots q_s^{f_s}$$

is a prime factorization of mn. Since mn is a square, each e_i and f_i is even. But, looking back and m and n, this implies that m and n are 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.

Suppose some prime p divides b and c, then it divides b^2 and c^2, and also $c^2 - b^2$, hence it divides a^2. If a prime p divides a^2, then it divides a. But we've assumed no number divides all three.

(b) Factor $c^2 - b^2$ as $(c-b)(c+b)$. Show that[1] there is no prime factor common to $c-b$ and $c+b$.

Suppose $c-b$ and $c+b$ have a common prime factor p. Then p divides $2c = (c-b)+(c+b)$ and $2b = (c+b)-(c-b)$. We know that b and c have no common prime factors, so the only possibility is $p = 2$. But $c+b$ is odd, so there are no common prime factors.

(c) Show that $c-b$ and $c+b$ are perfect squares.

This follows from (5b) and (6b).

(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.

By (6c), we can write $c + b = s^2$, $c - b = t^2$ for some integers with no common factors. These have to be odd because $c+b$ and $c-b$ are odd, and clearly $s > t$. Then

$$c = \frac{(c+b)+(c-b)}{2} = \frac{s^2+t^2}{2}, \quad b = \frac{(c+b)-(c-b)}{2} = \frac{s^2-t^2}{2},$$
$$\text{and} \quad a = \sqrt{(c+b)(c-b)} = \sqrt{s^2t^2} = st.$$

(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.

To check it is a Pythagorean triple, note first that $s^2 - t^2$ is always even, so these things are integers (which was at risk of failing with the division); then just plug into the formula and chug. To check it is primitive, if a prime p divides $\frac{s^2-t^2}{2}$ and $\frac{s^2+t^2}{2}$, it divides s^2 and t^2, hence s and t, which we assumed to share no factors.

You have proven the following:

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

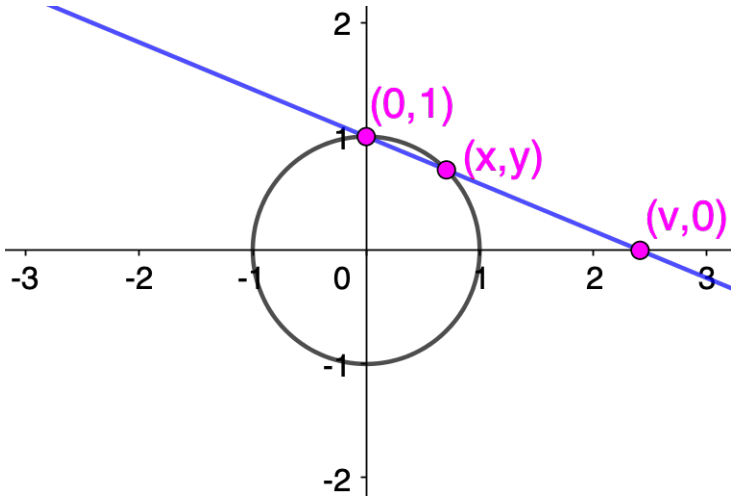
$$a = st, \quad b = \frac{s^2 - t^2}{2}, \quad c = \frac{s^2 + t^2}{2},$$

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

These mysterious formulas have a geometric explanation.

[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.



(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.

$$y = \frac{-1}{v}x + 1$$

(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.

$$x^2 + \left(\frac{-1}{v}x + 1\right)^2 = 1$$
$$\left(1 + \frac{1}{v^2}\right)x^2 + \left(\frac{-2}{v}\right)x = 0$$
$$\left(v^2 + 1\right)x + (-2v) = 0$$
$$x = \frac{2v}{v^2 + 1}$$
$$y = \frac{v^2 - 1}{v^2 + 1}$$

(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.

$$y = \frac{-1}{v}x + 1$$
$$vy = 1 - x$$
$$y = \frac{1 - x}{y}$$

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.

$$(x, y) = \left(\frac{2st}{s^2+t^2}, \frac{s^2-t^2}{s^2+t^2}\right)$$

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

$$(2st)^2 + (s^2-t^2)^2 = (s^2+t^2)^2$$
$$(st)^2 + \left(\frac{s^2-t^2}{2}\right)^2 = \left(\frac{s^2+t^2}{2}\right)^2$$

This is our formula from before.

(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 $x^2 + y^2 = 3$.

We show (a) and leave the rest for you. The point $(1, 1)$ is on this circle. We will use the same trick of taking the line between $(1, 1)$ and a point on the x-axis to parametrize solutions. Following the hint, set $x' = x - 1$ and $y' = y - 1$. If $(v, 0)$ is a point on the x-axis, let's even set $v' = v - 1$. Then the line through $(1, 1)$ and $(0, v)$ in (x, y)-coordinates is the line through $(0, 0)$ and $(v', -1)$ in (x', y')-coordinates, so $y' = -1/v' \cdot x$, and $x' = -v'y'$. Then the equation of the circle is

$$(x'+1)^2 + (y'+1)^2 = 2 \rightsquigarrow x'^2 + 2x' + y'^2 + 2y' = 0$$
$$\rightsquigarrow y'^2(v'^2+1) + 2y'(1-v') = 0 \rightsquigarrow y' = \frac{v'-1}{v'^2+1} \rightsquigarrow x' = -v'\frac{v'-1}{v'^2+1}$$

We need to switch back to (x, y)-coordinates (but it doesn't really matter whether we switch back with v or not, so we won't):

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

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

[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).

(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?

Plug in s/t and clear denominators. For (a), we get the formula

$$(a, b, c) = (t^2 + 2st - s^2, s^2 + 2st - t^2, s^2 + t^2).$$

However, it's not clear whether this accounts for every integer solution: we might have an integer solution that only has a multiple of the form above. This happened when we investigated Pythagorean triples using this method; we have to unexpectedly divide through by 4! I'll leave it to you to investigate if anything is missing here.

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.

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).

(a) The divisors of a are exactly the same as the divisors of $|a|$, and likewise with b. The conclusion is then clear.
(b) Suppose that n divides a/d and b/d. Write $a/d = na'$ and $b/d = nb'$, so $a = nda'$ and $b = ndb'$. If $n > 1$, then $nd > d$ is a common divisor of a/d and b/d, which contradicts the definition of GCD.
(c) For each prime factor p_i of a and b, take the minimum of the multiplicity of p_i in the factorization of a and the multiplicity of p_i in the factorization of b; the product of the p_i's to these powers is the GCD.

(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?

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

$a_0 = 524$, $b_0 = a_1 = 148$, $b_1 = a_2 = 80$, $b_2 = a_3 = 68$, $b_3 = a_4 = 12$, $b_4 = a_5 = 8$, $b_5 = 4$. The GCD is 4.

(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.

$$
\begin{aligned}
80 &= 1 \cdot 524 - 3 \cdot 148 \\
68 &= 1 \cdot 148 - 1 \cdot 80 = 1 \cdot 148 - 1 \cdot (1 \cdot 524 - 3 \cdot 148) \\
&= -1 \cdot 524 + 4 \cdot 148 \\
12 &= 1 \cdot 80 - 1 \cdot 68 = 1 \cdot (1 \cdot 524 - 3 \cdot 148) - 1 \cdot (-1 \cdot 524 + 4 \cdot 148) \\
&= 2 \cdot 524 - 7 \cdot 148 \\
8 &= 1 \cdot 68 - 5 \cdot 12 = 1 \cdot (-1 \cdot 524 + 4 \cdot 148) - 5 \cdot (2 \cdot 524 - 7 \cdot 148) \\
&= -11 \cdot 524 + 39 \cdot 148 \\
4 &= 1 \cdot 12 - 1 \cdot 8 = 1 \cdot (2 \cdot 524 - 7 \cdot 148) - 1 \cdot (-11 \cdot 524 + 39 \cdot 148) \\
&= 13 \cdot 524 - 46 \cdot 148.
\end{aligned}
$$

(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.

$$
\begin{aligned}
184 &= 1 \cdot 99 + 85 \\
99 &= 1 \cdot 85 + 14 \\
85 &= 6 \cdot 14 + 1 \\
14 &= 14 \cdot 1 + 0
\end{aligned}
$$

so the GCD is 1.

$$
\begin{aligned}
85 &= 1 \cdot 184 - 1 \cdot 99 \\
14 &= 1 \cdot 99 - 1 \cdot 85 = 1 \cdot 99 - 1 \cdot (1 \cdot 184 - 1 \cdot 99) = -1 \cdot 184 + 2 \cdot 99 \\
1 &= 1 \cdot 85 - 6 \cdot 14 = 1 \cdot (1 \cdot 184 - 1 \cdot 99) - 6 \cdot (-1 \cdot 184 + 2 \cdot 99) = 7 \cdot 184 - 13 \cdot 85.
\end{aligned}
$$

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.

(a) We can write $a = a'd$ and $b = b'd$. Then $c = ax_0 + by_0 = a'dx_0 + b'dy_0 = d(a'x_0 + b'y_0)$ is a multiple of d.
(b) The Euclidean algorithm!
(c) Take s, t such that $as + bt = d$. Then $a(ms) + b(mt) = md$.
(d) OK!

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

- First we use the Euclidean algorithm to find the GCD of 21 and 56:
$$56 = 2 \cdot 21 + 14$$
$$21 = 1 \cdot 14 + 7$$
$$14 = 2 \cdot 7 + 0$$
it is 7. Since 222 is not a multiple of 7 there is no solution.
- Now that 224 is a multiple of 7, we know that there is a solution. We find a particular solution by running the Euclidean algorithm backwards.
$$14 = 1 \cdot 56 - 2 \cdot 21$$
$$7 = 1 \cdot 21 - 1 \cdot 14 = 1 \cdot 21 - 1 \cdot (1 \cdot 56 - 2 \cdot 21) = -1 \cdot 56 + 3 \cdot 21.$$
Then since $224 = 32 \cdot 7$, we have
$$224 = 32(7) = 32(-1 \cdot 56 + 3 \cdot 21) = -32(56) + 96(21),$$
so $(-32, 96)$ is a particular solution. The general solution is then $(-32 - 8n, 96 + 3n)$ by the formula.

(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?

The system of equations is
$$c + s + p = 100, 20c + 6s + p = 200.$$
Substituting $p = 100 - c - s$ we obtain
$$20c + 6s + 100 - c - s = 200$$
$$19c + 5s = 100.$$
As $\gcd(19, 5) = 1$ this equation will have infinitely many integer solutions. We can find one by the Euclidean Algorithm.
$$19 = 3 \cdot 5 + 4$$
$$5 = 1 \cdot 4 + 1$$
$$4 = 1 \cdot 19 - 3 \cdot 5$$
$$1 = 1 \cdot 5 - 1 \cdot 4 = 1 \cdot 5 - 1 \cdot (1 \cdot 19 - 3 \cdot 5) = -1 \cdot 19 + 4 \cdot 5.$$

[3] Just name the relevant algorithm for now.

Then we multiply through:

$$100 = -100 \cdot 19 + 400 \cdot 5.$$

Hence $c = -100, s = 400$ is one integer solution. By the Theorem, all solutions are of the form

$$c = -100 - 5n, s = 400 + 19n.$$

Since we are looking for nonnegative integer solutions, we see that

$$-100 - 5n \geq 0 \quad \text{and} \quad 400 + 19n \geq 0.$$

This yields $-20 \geq n$ and $-21 \leq n$, hence $n = -21$ and $n = -20$ give the only nonnegative solutions. This yields

$$c = 5, s = 1, p = 94 \qquad \text{and} \qquad c = 0, s = 20, p = 80.$$

(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.

(a) Plug in and check.
(b) Plug in and check.
(c) Recall that a/d and b/d are coprime. Since $a/d(x_0 - x_1) = -b/d(y_0 - y_1)$, by the lemma, a/d divides $y_0 - y_1$; write $y_0 - y_1 = na/d$. Then $a(x_0 - x_1) = -b(y_0 - y_1) = -nab/d$, so $x_0 - x_1 = -nb/d$. Putting things back in place, this gives the formula the statement.

---

(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 $\mathbb{Z}$.

(a) If d is this GCD, then d would divide the LHS but not the RHS.
(b) Take $x_1 = b - a_2x_2 - \cdots - a_nx_n$.
(c) No solution: LHS is even, RHS is odd.
(d) $(x_1, x_2, x_3) = (3 - 7x_2 - 9x_3, x_2, x_3)$ is the general solution.

(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.
   (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 $0 \le r < |a_i|$. 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!

(a)

$$x_1 + 7x_2 + 9x_3 = 3.$$
$$(x_1, x_2, x_3) = (3 - 7x_2 - 9x_3, x_2, x_3)$$

(b) Take the equation:

$$3x + 7y + 8z + 9w = 10.$$
$$3(u - 2y) + 7y + 8z + 9w = 10 \qquad x = u - 2y$$
$$3u + y + 8z + 9w = 10 \qquad x = u - 2y$$
$$(u, y, z, w) = (u, 10 - 3u - 8z - 9w, z, w) \qquad x = u - 2y$$
$$(x, y, z, w) = (u - 2y, 10 - 3u - 8z - 9w, z, w)$$
$$(x, y, z, w) = (u - 2(10 - 3u - 8z - 9w), 10 - 3u - 8z - 9w, z, w)$$
$$(x, y, z, w) = (-20 + 7u + 16z + 18w, 10 - 3u - 8z - 9w, z, w)$$

(c) The coefficient is r, since plugging in we get

$$a_i(x_i' + qx_j) + a_jx_j + \cdots = a_ix_i' + (a_j - qa_i)x_j + \cdots = a_ix_i' + rx_j + \cdots .$$

(d) Take $u = x + 2y$, so we get

$$4u + 3y + 9z = 35.$$

Then take $v = y + u$, so we get

$$u + 3v + 9z = 35.$$

Then v and z are free variables and

$$u = 35 - 3v - 9z,$$

so the general solution, at least in terms of u, v, z, is

$$(u, v, z) = (35 - 3v - 9z, v, z).$$

We need to express y and x in terms of u, v, z (and then v, z) to get the solution. Since $v = y + u$, we have

$$y = v - u = v - (35 - 3v - 9z) = -35 + 4v + 9z.$$

Then, since $u = x + 2y$, $x = u - 2y$, so

$$x = (35 - 3v - 9z) - 2(-35 + 4v + 9z) = 3(35) - 11v - 27z.$$

Thus, the general solution is

$$(x, y, z) = (105 - 11v - 27z, -35 + 4v + 9z, z), \quad v, z \in \mathbb{Z}.$$

(e),(f): Left for you.

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 $\mathbb{Z}_n$.

(a) $13, 18, 23$ (answers may vary).
(b) $13 + 5n$ for $n \in \mathbb{Z}$.
(c) 7, by long division.
(d) True! We just often prefer to call it $[1]$ instead.
(e) $[a] = [b]$.

(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 $\mathbb{Z}_4$).

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

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

(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.

(a) Suppose that $x = a$ is a solution of (†). Then $[a]^2 + 3[a] = [a^2 + 3a] = [6]$ in $\mathbb{Z}_n$, since $a^2 + 3a \equiv 6 \pmod{n}$, so $y = [a]$ is a solution of (‡). Suppose that $y = [a]$ is a solution of (‡). Then $[a^2 + 3a] = [a]^2 + 3[a] = [6]$ in $\mathbb{Z}_n$, so $a^2 + 3a \equiv 6 \pmod{n}$. Thus, a is a solution of (†).
(b) This worked because everything was make out of $+$ and $\times$. If we have any polynomial congruence equation modulo n, then it corresponds to an actual equation in $\mathbb{Z}_n$, and the solution set over $\mathbb{Z}$ is the union of congruence classes corresponding to the solutions in $\mathbb{Z}_n$.

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.

(a) $4 \cdot 16 = 64 \equiv 1 \pmod{21}$, since $21|63$. Also $25, 46$. (Answers may vary.)
(b) As above $ab \equiv 1 \pmod{K}$ if and only if $[a][b] = [1]$ in $\mathbb{Z}_K$.
(c) a is a unit in $\mathbb{Z}_K$ if and only if there is a $b \in \mathbb{Z}$ that is an inverse mod K, if and only if there is a b such that $[b]$ is an inverse to $[a]$ in $\mathbb{Z}_K$, if and only if $[a]$ is a unit in $\mathbb{Z}_K$.
(d) If $[a][b] = [1] = [a][b']$, then $[b] = [b][a][b] = [b][a][b'] = [b']$.

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.

(a) $ax - 1 = bn$ for some b, so $ax - bn = 1$.
(b) We saw last time that this equation has a solution if and only if 1 is a multiple of $\gcd(a, b)$, i.e., a and b are coprime.
(c) We apply the Euclidean algorithm as last time.

$$149 = 6 \cdot 24 + 5$$
$$24 = 4 \cdot 5 + 4$$
$$5 = 1 \cdot 4 + 1$$
$$5 = 1 \cdot 149 - 6 \cdot 24$$
$$4 = 1 \cdot 24 - 4 \cdot 5 = 1 \cdot 24 - 4 \cdot (1 \cdot 149 - 6 \cdot 24) = -4 \cdot 149 + 25 \cdot 24$$
$$1 = 1 \cdot 5 - 1 \cdot 4 = (1 \cdot 149 - 6 \cdot 24) - (-4 \cdot 149 + 25 \cdot 24) = 5 \cdot 149 - 31 \cdot 24.$$

So -31 is 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 $x' \equiv x \pmod{m_1 m_2 \cdots m_k}$.

(a) If p is a common prime factor of m_i and m_i', then p must be a prime factor of one of the m_j with $j \neq i$, since m_i' is the product of these. But this would contradict that m_i and m_j are coprime.
(b) We know that m_i' has an inverse modulo m_i since these are coprime. Then $m_i' m_i^* \equiv 1 \pmod{m_i}$ by definition of inverse, and $m_i' m_i^* \equiv 0 \pmod{m_j}$ since m_j divides m_i'.
(c) Take $x = a_1 m_1' m_1^* + \cdots + a_k m_k' m_k^*$. Taken modulo m_i, this every term but the i-th is zero, and the i-th is congruent to $a_i \cdot 1 = a_i$, so $x \equiv a_i \pmod{m_i}$ for each i.
(d) We can write $x' = x + d m_1 m_2 \cdots m_k$. Then $x' \equiv a_i + d m_1 m_2 \cdots m_k \equiv a_i \pmod{m_i}$ for each i.
(e) Since $x' \equiv a_i \equiv x \pmod{m_i}$, then $m_i \mid (x' - x)$ for each i, and all m_i are coprime, the product divides $x' - x$. This means $x' \equiv x \pmod{m_1 m_2 \cdots m_k}$.

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

(1) We find 2 is an inverse of 17 modulo 11 and 14 is an inverse of 11 modulo 17. So
$$x = 4 \cdot 2 \cdot 17 + 3 \cdot 14 \cdot 11 = 598$$
is a solution, and $598 + 187n$ is the general solution.

(2) We start by finding inverses of 35 modulo 3, 21 modulo 5, and 15 modulo 7; the numbers 2, 1, and 1 work, respectively. Then
$$x = 1 \cdot 2 \cdot 35 + 2 \cdot 1 \cdot 21 + 3 \cdot 1 \cdot 15 = 157$$
works. Since $3 \cdot 5 \cdot 7 = 105$, every solution is of the form $157 + 105n$. The smallest positive solution is 52.

(3) We cannot apply the theorem yet! Let's start by breaking the congruences down. Since $4 \equiv 1 \pmod{3}$ and $4 \equiv 0 \pmod{2}$, we can rewrite the first equation as $x \equiv 0 \pmod{2}$ and $x \equiv 1 \pmod{3}$. Likewise, we can break the second down by writing $13 \equiv 3 \pmod{5}$ and $13 \equiv 1 \pmod{3}$, so $x \equiv 3 \pmod{5}$ and $x \equiv 1 \pmod{3}$. Thus, we can get the system
$$\begin{cases} x \equiv 0 \pmod{2} \\ x \equiv 1 \pmod{3} \\ x \equiv 3 \pmod{5}. \end{cases}$$
Now we can apply the CRT to solve. I got $28 + 30n$.

---

(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 $\mathbb{Z}_5$.

(a) The sum of any two congruence classes in $\mathbb{Z}_n$ is a congruence class in $\mathbb{Z}_n$. Addition is associative since

$$[a] + ([b] + [c]) = [a] + [b + c] = [a + b + c] = [a + b] + [c] = ([a] + [b]) + [c].$$

The element $[0]$ is an identity, since $[0] + [a] = [0 + a] = [a]$ and similarly in the other order. There are inverses, namely $[-a] + [a] = [-a + a] = [0]$.

(b) $[0]$ has order 1; $[1]$ and $[3]$ have order 4; and $[2]$ has order 2.

(c) $[0]$ has order 1; and the rest have order 5.

(d) Yes.

(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 $\mathbb{Z}_8^\times$.

[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.

(a) First the product of units is a unit: if $[a]$ has inverse $[c]$ and $[b]$ has inverse $[d]$, then $[a][b][c][d] = [1]$. Associativity is similar to above. $[1]$ is a unit and is the identity. We have inverses by definition.
(b) $[1]$ has order 1; $[6]$ has order 2; $[2]$ and $[4]$ have order 3; and $[3]$ and $[5]$ have order 6.
(c) $[1]$ has order 1; and $[3]$, $[5]$, and $[7]$ have order 2.
(d) Yes.

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.

(a) Every element of $\mathbb{Z}_p$ except $[0]$ has an inverse, since every number that is not a multiple of p is coprime to p.
(b) Let e be the order of $[a]$, so $[a]^e = [1]$. Then $p-1 = ef$ for some f, so $[a]^{p-1} = [a]^{ef} = ([a]^e)^f = [1]$.
(c) If p does not divide a, then $[a] \neq [0]$ and $[a] \in \mathbb{Z}_p^\times$. Then $[a]^{p-1} = [1]$ implies that $a^{p-1} \equiv 1 \pmod{p}$.

(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) $7^{12} \equiv 1 \pmod{13}$ by FLT.
(2) $7^{96} \equiv (7^{12})^8 \equiv 1 \pmod{13}$
(3) $7^{98} \equiv (7^{12})^8 7^2 \equiv 7^2 \equiv 10 \pmod{13}$
(4) $1505 = 125 \cdot 12 + 5$, so $7^{1505} \equiv 7^5 \equiv 11 \pmod{13}$.

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 the Proposition above to compute the following:
- $\varphi(41) = 40$.
- $\varphi(27) = \varphi(3^3) = 3^2(3-1) = 18$.
- $\varphi(15) = \varphi(3)\varphi(5) = 2 \cdot 4 = 8$.
- $\varphi(100) = \varphi(2^2)\varphi(5^2) = 2(2-1)5(5-1) = 40$.

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

Since $\varphi(100) = 40$, we know $7^{40} \equiv 1 \pmod{100}$. Then

$$7^{2003} = 7^{50 \cdot 40 + 3} \equiv (7^{40})^{50} 7^3 \equiv 7^3 \equiv 343 \equiv 43 \pmod{100},$$

so the last two digits are 43.

(8) 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.

(a) Similar to Lagrange implies FLT.
(b) Every congruence class is represented by nonnegative number less than n. The class of zero is not a unit, so any possible unit is represented by a positive integer less than n. We saw last time that $[a]$ is a unit if and only if a and n are coprime.
(c) a is coprime with p^n if and only if p does not divide n. We count the number of positive integers less than p^n that are not multiples of p, and get the formula above.
(d) Note first that this is a well defined function: if two numbers are congruent modulo mn, they are congruent modulo m and modulo n. CRT says that any pair of residues modulo m and n correspond to a unique congruence class modulo mn; i.e., π is bijective.
(e) For the forward direction, let $[b]$ be an inverse of $[a]$, so $ab \equiv 1 \pmod{mn}$. Then $ab \equiv 1 \pmod{m}$ and $ab \equiv 1 \pmod{n}$, so $[a]$ is a unit in $\mathbb{Z}_m$ and $\mathbb{Z}_n$. For the reverse, let c, d be such that $ac \equiv 1 \pmod{m}$ and $ad \equiv 1 \pmod{n}$. By CRT, there is a b such that $b \equiv c \pmod{m}$ and $b \equiv d \pmod{n}$. Then $ab \equiv ac \equiv 1 \pmod{m}$ and $ab \equiv ad \equiv 1 \pmod{n}$. By the uniqueness part of CRT, $ab \equiv 1 \pmod{mn}$, so a has an inverse mod mn.
(f) By (d) and (e), every unit in $\mathbb{Z}_{mn}$ corresponds to a pair consisting of a unit in $\mathbb{Z}_m$ and a unit in $\mathbb{Z}_n$. Thus, the number of elements of $\mathbb{Z}_{mn}^\times$ is the product of the number of elements in $\mathbb{Z}_m^\times$ and $\mathbb{Z}_n^\times$.

(9) 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.

[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.

(c) If $h_1 \in G \setminus \{1, g, \ldots, g^{e-1}\}$, 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.

(a) If $g^a = g^b$ with $a < b < e$, then $1 = (g^{-1})^a g^a = (g^{-1})^a g^b = g^{b-a}$, which contradicts that e is the smallest exponent with $g^e = 1$.

(b) Because the number of elements of G is the order of g.

(c) If $hg^a = hg^b$ with $a < b < e$, then $g^a = h^{-1}hg^a = h^{-1}hg^b = g^b$, which we saw was impossible. If $g^a = hg^b$, then $g^{a-b} = g^a g^{-b} = hg^b g^{-b} = h$. But $g^{a-b} = g^{e+a-b}$ is on the first list.

(d) Along similar lines, we get an array like this with the rows all distinct. Eventually we must have the whole group, because it is finite. Then the cardinality of G is $(t+1)e$.

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 $\mathbb{Z}_8$.

(a) $\varphi(5) = 4$ so we want order 4. $[2]^1 = [2]$, $[2]^2 = [4]$, $[2]^3 = [3]$, $[2]^4 = [1]$, so the order of $[2]$ is indeed 4.
(b) $\varphi(4) = 2$ so we want order 2. $[3]^1 = [2]$, $[3]^2 = [1]$, so the order of $[3]$ is indeed 2.
(c) $[2]$ doesn't work, since $[2]^3 = [1]$, but $[3]$ is a primitive root.
(d) $[3]^2 = [5]^2 = [7]^2 = [1]$, so nothing has order $4 = \varphi(8)$.

(2) Suppose that $g = [a]$ is a primitive root in $\mathbb{Z}_p$.
   (a) Show that[1] if $0 \le m \le n < p-1$, 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 $0 \le n < p-1$.
   (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 $I : \mathbb{Z}_p^\times \to \mathbb{Z}_{p-1}$.

(a) Let $0 \le m \le n < p-1$ and $x^m = x^n$. Then $[1] = x^{-m}x^m = x^{-m}x^n = x^{n-m}$ and $n - m < p - 1$. Since the order of x is $p-1$, we must have $n - m = 0$, so $n - m$.
(b) From part (1), $\{1, x, x^2, \ldots, x^{p-2}\}$ are distinct elements of $\mathbb{Z}_p^\times$. Since this list has $p-1$ elements and $\mathbb{Z}_p^\times$ does too, each element of $\mathbb{Z}_p^\times$ must occur exactly once.
(c) We need to show that if $y = g^m = g^n$, then $[m] = [n]$ in $\mathbb{Z}_{p-1}$. Say $m \le n$. If $g^m = g^n$, then $1 = g^{n-m}$, so by the lemma, $p - 1 \mid n - m$, and hence $n \equiv m \pmod{p-1}$; i.e., $[m] = [n]$ in $\mathbb{Z}_{p-1}$.

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

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

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

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

Let $x, y \in \mathbb{Z}_p^\times$, and say that $I(x) = [\ell]$ and $I(y) = [m]$. Then $x = [a]^\ell$ and $y = [a]^m$. So, $xy = [a]^\ell[a]^m = [a]^{\ell+m}$, and hence $I(xy) = [\ell + m] = I(x) + I(y)$.
Similarly, since $x^n = [a]^{\ell n}$, $I(x^n) = [\ell n] = [n][\ell] = [n]I(x)$.

(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 $\mathbb{Z}_{11}$.

(a) Compute the powers of $[2]$:

n	0	1	2	3	4	5	6	7	8	9
$[2]^n$	[1]	[2]	[4]	[8]	[5]	[10]	[9]	[7]	[3]	[6]

and $[2]^{10} = [1]$. The index function is just the inverse function:

x	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]
$I(x)$	0	1	8	2	4	9	7	3	6	5

(b) Since $I([3]) = 8$, an element of index 4 would be a square root, so $[5]$ is a square root.

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

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 $\mathbb{Z}_p$.

By FLT, every element of $\mathbb{Z}_p^\times$ is a solution to $x^{p-1} = 1$ in $\mathbb{Z}_p$, so the theorem applies. There are then $\varphi(p-1)$ elements of order $p-1$ in $\mathbb{Z}_p^\times$. Since $\mathbb{Z}_{p-1}^\times$ is nonempty, $\varphi(p-1) > 0$. Thus, there is a primitive root.

(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.

(a) We must show that it is true for $n = 1$ and that if, for each $d < n$, if $x^d = 1$ has d distinct solutions then there are $\varphi(d)$ elements of order d in $\mathbb{Z}_p^\times$, then if $x^n = 1$ has n distinct

solutions then there are $\varphi(n)$ elements of order n in $\mathbb{Z}_p^\times$. Henceforth, we will assume that, for each $d < n$, if $x^d = 1$ has d distinct solutions then there are $\varphi(d)$ elements of order d in $\mathbb{Z}_p^\times$.

(b) The order of x divides n in this case. That is, x is a root of $x^d - 1$.

(c) No, by the first theorem, $x^d - 1$ cannot have more than d roots in $\mathbb{Z}_p$. If $x^n - 1$ has n roots, note that $x^{d(e-1)} + x^{d(e-2)} + \cdots + x^d + 1$ has at most $d(e-1) = n - d$ roots. If $x^d - 1$ had $c < d$ roots, then $x^n - 1$ would have at most $c + (n - d) < d + n - d = n$ roots, contradicting the hypothesis.

(d) The IH applies to every divisor d of n, so for each $d \mid n$, $d < n$, we have $\varphi(d)$ elements of order d.

(e) The total number of solutions to $x^n - 1$ is n. Every such solution either has order n or order d with $d \mid n$ and $d < n$. Adding up all of the latter type gives

$$\sum_{d \mid n, d \neq n} \varphi(d) = \left(\sum_{d \mid n} \varphi(d) \right) - \varphi(n) = n - \varphi(n).$$

Thus, the number of solutions with order n is $\varphi(n)$.

(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.

(a) Every integer between 1 and n occurs in exactly one of the sets on the right hand side.

(b) Following the hint, the integers between 1 and n whose gcd with n is d correspond to integers between 1 and n/d that are coprime with n/d. The phi function counts the latter.

(c) As d ranges through the divisors of n, n/d goes through all of the divisors of n, obtaining each value once. Put together with the previous parts, the formula follows.

(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

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

Since we assumed $[a]$ is a unit, we can rewrite as $x^2 + \frac{[b]}{[a]}x + \frac{[c]}{[a]} = [0]$. Since n is odd, $[2]$ is a unit too, so we can complete the square:

$$\begin{aligned}
[0] &= x^2 + \frac{[b]}{[a]}x + \frac{[c]}{[a]} \\
&= x^2 + [2]\frac{[b]}{[2a]}x + \left(\frac{[b]}{[2a]}\right)^2 - \left(\frac{[b]}{[2a]}\right)^2 + \frac{[c]}{[a]} \\
&= \left(x + \frac{[b]}{[2a]}\right)^2 + \frac{[4ac - b^2]}{[4a^2]},
\end{aligned}$$

so

$$\left(\frac{[2a]x + [b]}{[2a]}\right)^2 = \frac{[b^2 - 4ac]}{[4a^2]}.$$

Thus, x is a solution if and only if $[2a]x + [b]$ is a square root of $[b^2 - 4ac]$. Rearranging slightly gives the form above.

(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, $y' = -y$.

If $y^2 - x = 0$ has a solution, it has at most two since this is a polynomial of degree two over a field. If y is a solution, then $y' = -y$ is too.

(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.

Write $[n] = g^k$, so the index is k. If $k = 2\ell$ is even, then $[n] = g^k = g^{2\ell} = (g^\ell)^2$, so $[n]$ is a quadratic residue. Conversely, if $[n] = [m]^2$, write $[m] = g^\ell$, so $[n] = [m]^2 = g^{2\ell}$, which is even. (Note that even and odd are well-defined in $\mathbb{Z}_{p-1}$ for p odd, since any two representatives differ by a multiple of two.)

[1] Hint: Complete the square!

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

(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 $\mathbb{Z}_{43}$.

(a) $[4] = [2]^2$; $[a^2] = [a]^2$.

(b) We have $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = -1$, so $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = (-1)^2 = 1$.

(c) Using the quadratic formula, we need to determine whether $[12^2 - 4 \cdot 3 \cdot -2] = [168]$ is a square in $\mathbb{Z}_{43}$. By the hint, we have $168 = 4 \cdot 42$, so

$$\left(\frac{168}{43}\right) = \left(\frac{4}{43}\right)\left(\frac{42}{43}\right) = 1\left(\frac{-1}{43}\right) = 1 \cdot -1 = -1.$$

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

We conclude that there are no solutions.

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

Let $g = [a]$ be a primitive root and write $[r] = g^k$ for some k.

If $[r]$ is a residue, then $k = 2\ell$ is even, and $r^{(p-1)/2} \equiv a^{2\ell(p-1)/2} \equiv a^{\ell(p-1)} \equiv 1 \pmod{p}$ by FLT.

If $[r]$ is not a residue, then $k = 2\ell + 1$ is odd, and $r^{(p-1)/2} \equiv a^{(2\ell+1)(p-1)/2} \equiv a^{\ell(p-1)+(p-1)/2} \equiv a^{(p-1)/2} \pmod{p}$ by FLT. We know that $(a^{(p-1)/2})^2 \equiv a^{p-1} \equiv 1 \pmod{p}$ again by FLT, so $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$. But, by definition of primitive root, $a^{(p-1)/2} \not\equiv 1 \pmod{p}$, so $a^{(p-1)/2} \equiv -1 \pmod{p}$.

(6) Prove the proposition above.

We already did part (3). Part (1) is clear since the value of $\left(\frac{a}{p}\right)$ only depends on the congruence class of a modulo p. For (2), take a primitive root $g = [r]$ and write $a \equiv r^k, b \equiv r^\ell$. Then, by Euler's criterion,

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv r^{k\frac{p-1}{2}} r^{\ell\frac{p-1}{2}} \equiv r^{(k+\ell)\frac{p-1}{2}} \equiv \left(\frac{ab}{p}\right) \pmod{p}.$$

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

If $p \equiv 1 \pmod{4}$, write $p = 4k+1$; then $(-1)^{\frac{p-1}{2}} \equiv (-1)^{2k} \equiv 1$, so -1 is a residue by Euler's criterion. If $p \equiv 3 \pmod{4}$, write $p = 4k+3$; then $(-1)^{\frac{p-1}{2}} \equiv (-1)^{2k+1} \equiv -1$, so -1 is not a residue by Euler's criterion.

(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.

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 $\left(\frac{13}{107}\right)$.

(a) $\left(\frac{2}{7}\right) = 1$, $\left(\frac{2}{11}\right) = -1$, and $\left(\frac{2}{101}\right) = -1$.
(b) $\left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1$.
(c) $\left(\frac{13}{107}\right) = \left(\frac{107}{13}\right) = \left(\frac{3}{13}\right) = \left(\frac{13}{3}\right) = \left(\frac{1}{3}\right) = 1$.

(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 $\left(\frac{38}{127}\right)$.

(a) $\left(\frac{10}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{5}{13}\right) = -1 \cdot \left(\frac{13}{5}\right) = -1 \cdot \left(\frac{3}{5}\right) = -1 \cdot \left(\frac{5}{3}\right) = -1 \cdot \left(\frac{2}{3}\right) = -1 \cdot -1 = 1.$
(b) $\left(\frac{38}{127}\right) = \left(\frac{2}{127}\right)\left(\frac{19}{127}\right) = 1 \cdot -1 \cdot \left(\frac{127}{19}\right) = 1 \cdot -1 \cdot \left(\frac{127}{19}\right) = 1 \cdot -1 \cdot \left(\frac{13}{19}\right) = 1 \cdot -1 \cdot \left(\frac{19}{13}\right) = 1 \cdot -1 \cdot \left(\frac{5}{13}\right) = 1 \cdot -1 \cdot \left(\frac{13}{5}\right) = 1 \cdot -1 \cdot \left(\frac{3}{5}\right) = 1 \cdot -1 \cdot -1 = 1.$

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

We compute $[b^2 - 4ac] = [169 - 2 \cdot 4 \cdot 5] = [129] = [26]$. We compute $\left(\frac{26}{103}\right) = \left(\frac{2}{103}\right)\left(\frac{13}{103}\right) = 1 \cdot \left(\frac{103}{13}\right) = 1 \cdot \left(\frac{12}{13}\right) = 1 \cdot \left(\frac{4}{13}\right) \cdot \left(\frac{3}{13}\right) = 1 \cdot 1 \cdot \left(\frac{13}{3}\right) = 1 \cdot 1 \cdot \left(\frac{1}{3}\right) = 1$. So, $[26] \in \mathbb{Z}_{103}$ is a nonzero square, and there are two solutions.

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.

We apply Gauss' Lemma with $a = 2$: we look at the sequence

$$2, 4, 6, \ldots 4\ell, 4\ell + 2, \ldots, 8\ell + 2$$

and compute the list L

$$L = \{2, 4, 6, \ldots 4\ell, -(4\ell + 1), \ldots, -1\}.$$

Thus, the number of positive elements is 2ℓ and the number of negative elements is $p' - 2\ell = 2\ell + 1$, so by Gauss' Lemma,

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

(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.

(a) None are equal, since $ia \equiv ja \pmod{p}$ implies $i \equiv j \pmod{p}$, and none are negative of each other, since $ia \equiv -ja \pmod{p}$ implies $i + j \equiv 0 \pmod{p}$, which can't happen for $0 \leq i < j \leq p'$.
(b) The product of L modulo p is

$$a \cdot 2a \cdot 3a \cdots p'a \equiv (\pm 1) \cdot (\pm 2) \cdot (\pm 3) \cdots (\pm p') \pmod{p},$$

so, if v is the number of negatives, we have

$$a^{p'}(p')! \equiv (-1)^v (p')! \pmod{p}.$$

Since $(p')!$ is a unit mod p, we must have

$$a^{p'} \equiv (-1)^v \pmod{p}.$$

(c) By Euler's criterion,

$$\left(\frac{a}{p}\right) \equiv a^{p'} \equiv (-1)^v \pmod{p}.$$

(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 $\frac{p^2-1}{8} (q-1) = p \sum_{k=1}^{p'} \lfloor kq/p \rfloor + vp - 2 (\sum_{i=1}^{v} b_i)$.
(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.

(a) This sum equals $\frac{p'(p'+1)}{2} = \frac{(p-1)(p+1)}{8} = \frac{p^2-1}{8}$.
(b) Every r_k is either some a_i or $p - b_i$, and each a_i and b_i occurs exactly once.

(c) As in the proof of Gauss' Lemma, each number between 1 and p' occurs exactly once as an a_i or as a b_i. Then use part (a).

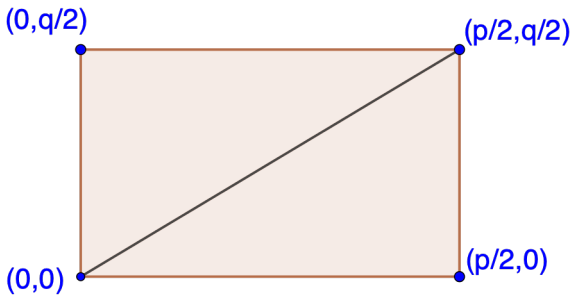
(d)
$$\frac{p^2-1}{8}(q-1) = \sum_{k=1}^{p'} kq = p\sum_{k=1}^{p'} \lfloor kq/p \rfloor + \sum_{k=1}^{p'} r_k$$
$$= p\sum_{k=1}^{p'} \lfloor kq/p \rfloor + \sum_{i=1}^{t} a_i - \sum_{i=1}^{v} b_i + vp.$$

(e) Take (d) minus (c).

(f) Taking (e) modulo 2, since $q-1$ is even and p is odd, we get this congruence. By Gauss' Lemma, $\left(\frac{q}{p}\right) \equiv (-1)^v$, and swapping in for v, we get the statement.

(g) Switching roles,
$$\left(\frac{p}{q}\right) = (-1)^{\sum_{\ell=1}^{q'} \lfloor \ell p/q \rfloor},$$
where $q' = \frac{q-1}{2}$. Plugging into the other Lemma yields
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$
Since $\frac{p-1}{2}$ is even if and only if $p \equiv 1 \pmod 4$ and likewise with q, the exponent above is odd if and only if $p \equiv q \equiv 3 \pmod 4$. The statement of QR follows.

(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.

(a) The integer points inside are exactly the pairs (k, ℓ) with $1 \le k \le \frac{p-1}{2}$ and $1 \le \ell \le \frac{q-1}{2}$.

(b) A point (a, b) on the diagonal would have $qa = pb$, which would imply a is a multiple of p (since p, q coprime), which is impossible.

(c) The possible x values are $1 \leq k \leq \frac{p-1}{2}$ and for any given k, the possible y values are bounded below by 1 and above by kq/p; since these are integers, they range from 1 to $\lfloor \frac{kq}{p} \rfloor$. This yields the sum in the statement.

(d) The first part follows from (c) by switching roles. Since every point in the square is either above or below the diagonal, the equality follows from (a), (c), and (d).

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!)

By way of contradiction, suppose that there are only finitely many primes $p_1, \ldots, p_k$. Consider the number $N = p_1 p_2 \cdots p_k + 1$. This number N is multiple of some prime p. By hypothesis, $p = p_i$ for some i. But $N \equiv 1 \pmod{p_i}$ for each i, so N is not a multiple of p_i, which is a contradiction. We conclude that there must be infinitely many primes.

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

By way of contradiction, suppose that there are only finitely many primes $p_1, \ldots, p_k$ that are congruent to $3 \pmod 4$. Consider the number $N = 4p_1 p_2 \cdots p_k - 1$.

We claim that N is divisible by some prime that is congruent to 3 modulo 4. Since N is odd, it is a product of odd primes; in particular, each prime factor is congruent to 1 or 3 modulo 4. If each factor is congruent to 1, then their product is congruent to 1, but $N \equiv 3 \pmod 4$. Thus, N is divisible by some prime that is congruent to 3 modulo 4.

Thus, N is divisible by p_i for some i. But $N \equiv -1 \pmod{p_i}$, so N is not a multiple of p_i. This is a contradiction. We conclude that there must be infinitely many primes that are congruent to 3 modulo 4.

Alternatively, by way of contradiction, suppose that there are only finitely many primes $p_1, \ldots, p_k$ that are congruent to $3 \pmod 4$. Say that we ordered them so that $p_1 = 3$. Consider the number $N = 4p_2 p_3 \cdots p_k + 3$.

We claim that N is divisible by some prime that is congruent to 3 modulo 4. Since N is odd, it is a product of odd primes; in particular, each prime factor is congruent to 1 or 3 modulo 4. If each factor is congruent to 1, then their product is congruent to 1, but $N \equiv 3 \pmod 4$. Thus, N is divisible by some prime that is congruent to 3 modulo 4.

Thus, N is divisible by p_i for some i. Note that $3 \nmid N$, since $3|3$ but $3 \nmid (4p_2 p_3 \cdots p_k)$. But for $i > 1$, $N \equiv -1 \pmod{p_i}$, so N is not a multiple of p_i either. This is a contradiction. We conclude that there must be infinitely many primes that are congruent to 3 modulo 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.

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

(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?

(a) If we argue as in (2) and create some N that is equivalent to 1 modulo 4, it could be a product of primes that are congruent to 3 modulo 4, as long as the total multiplicity of 3 mod 4 factors is even.

(b) This works for 2 modulo 3. Proceed as in (2) and take $N = 3p_1 \cdots p_k - 1$. The argument works because if a product is $2 \pmod 3$, then one of the factors has to be $2 \pmod 3$. This can't work for 1 modulo 3 since a product of things that all aren't $1 \pmod 3$ can be $1 \pmod 3$.

(c) This can't work for any residue class modulo 5, because no matter what nonzero $[a]$ we take, we can write $[a] = [b_1] \cdots [b_k]$ where all $[b_i] \neq [a]$. For example,

$$[1] = [4][4],\ [2] = [3][4],\ [3] = [2][2][2],\ [4] = [3][3].$$

(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.

By way of contradiction, suppose that there are only finitely many primes $p_1, \ldots, p_k$ that are congruent to $1 \pmod 4$. Consider the number $N = 4(p_1 \cdots p_k)^2 + 1$.

The number N has some prime factor p. Observe that $-1 = 4(p_1 \cdots p_k)^2 - N$, so

$$-1 \equiv (2p_1 \cdots p_k)^2 \pmod p.$$

Thus $\left(\frac{-1}{p}\right) = 1$, which implies that $p \equiv 1 \pmod 4$ by quardatic reciprocity part -1. But then $p = p_i$ for some i, and $N \equiv 1 \pmod{p_i}$, which yields a contradiction. We conclude that there must be infinitely many primes that are congruent to 1 modulo 4.

(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.

By way of contradiction, suppose that there are only finitely many primes $p_1, \ldots, p_k$ that are congruent to $1 \pmod 3$. Consider the number $N = 3(p_1 \cdots p_k)^2 + 1$.

The number N has some prime factor p. Observe that $-1 = 3(p_1 \cdots p_k)^2 - N$, so

$$-1 \equiv 3(p_1 \cdots p_k)^2 \pmod p.$$
$$1/(-3) \equiv (p_1 \cdots p_k)^2 \pmod p.$$

Thus $\left(\frac{-3}{p}\right) = 1$. We compute

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = \begin{cases} 1 \cdot \left(\frac{p}{3}\right) & \text{if } p \equiv 1 \pmod 4 \\ -1 \cdot -\left(\frac{p}{3}\right) & \text{if } p \equiv 3 \pmod 4 \end{cases}$$
$$= \left(\frac{p}{3}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 3 \\ -1 & \text{if } p \equiv 2 \pmod 3. \end{cases}$$

which implies that $p \equiv 1 \pmod 3$. But then $p = p_i$ for some i, and $N \equiv 1 \pmod{p_i}$, which yields a contradiction. We conclude that there must be infinitely many primes that are congruent to 1 modulo 3.

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

Proceeding as above, if not, take $N = 5(p_1 \cdots p_k)^2 - 1$. Note that $5 \nmid N$. Then for a prime p dividing N, we have that $5(p_1 \cdots p_k)^2 \equiv 1 \pmod p$ so

$$1 = \left(\frac{5}{p}\right) = \left(\frac{p}{5}\right),$$

and hence $p \equiv \pm 1 \pmod 5$. But if every prime factor of N is congruent to 1, then $N \equiv 1 \pmod 5$ whereas $N \equiv 4 \pmod 5$. Thus N has a prime factor congruent to 4 mod 5, but this is some p_i leading to a contradiction.

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

Let's start with $p \equiv 7 \pmod 8$, proceed as above and take $N = (4p_1 \cdots p_k)^2 - 2$. Note that N is not a multiple of 4, and must then have an odd prime factor. For $p|N$ odd, we have $2 \equiv (4p_1 \cdots p_k)^2 \pmod p$, so $\left(\frac{2}{p}\right) = 1$, and hence $p \equiv 1, 7 \pmod 8$. But not every prime factor of N is congruent to 1 modulo 8, since this would imply $N \equiv 1, 2, 4 \pmod 8$, but $N \equiv 6 \pmod 8$. So some factor is congruent to 3 modulo 8, hence is some p_i, leading to a contradiction.

Now $p \equiv 3 \pmod 8$. Proceed as above and take $N = (p_1 \cdots p_k)^2 + 2$. Note that each p_i is odd, and $N \equiv 3 \pmod 8$. For $p|N$, we have $-2 \equiv (p_1 \cdots p_k)^2 \pmod p$. We compute

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

so $p \equiv 1, 3 \pmod 8$. But not every prime factor of N is congruent to 1 modulo 8, so some factor is congruent to 3 modulo 8, hence is some p_i, leading to a contradiction.

For $p \equiv 5 \pmod 8$, try your luck with $N = (p_1 \cdots p_k)^2 + 4$.

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

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.

$37 = 1^2 + 6^2$, $41 = 5^2 + 4^2$, $53 = 7^2 + 2^2$

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

$n^2 = n^2 + 0^2$, $2 = 1^2 + 1^2$

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

The squares in $\mathbb{Z}_4$ are $[0]$ and $[1]$, so a number that is a sum of two squares cannot be congruent to 3 modulo 4.

(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 $a^2 + b^2 = p$.

   (a) By QR part -1, we can write $[-1] = [r]^2$ for some $[r] \in \mathbb{Z}_p$, so $r^2 \equiv -1 \pmod p$.
   (b) Note that the source of f has $(k+1)^2$ elements and the target has p elements. Since $k \geq \sqrt{p}$, $k + 1 > \sqrt{p}$, so $(k + 1)^2 > p$. Thus, f cannot be injective, which yields the statement.
   (c) We have $u_1 + rv_1 \equiv u_2 + rv_2 \pmod p$, so $u_1 - u_2 \equiv -r(v_1 - v_2) \pmod p$. Then

$$a^2+b^2 \equiv (u_1-u_2)^2+(v_1-v_2)^2 \equiv (u_1-u_2)^2+r^2(u_1-u_2)^2 \equiv (u_1-u_2)^2-(u_1-u_2)^2 \equiv 0 \pmod p.$$

[1] What did we do in HW#1?
[2] Hint: $k + 1 > \sqrt{p}$.

Also, $a^2 + b^2 \neq 0$, since either $u_1 - u_2 \neq 0$ or $v_1 - v_2 \neq 0$, and $a^2 + b^2 \leq 2k^2 < 2\sqrt{p}^2 = 2p$. We must have $a^2 + b^2 = p$.

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.

   (a) Suppose $n = a^2 + b^2$, $q|n$, and $q \nmid a$. Then $a^2 + b^2 \equiv 0 \pmod q$, and $b^2 \equiv -a^2 \pmod q$, and $[a]^{-1}[b] = [-1]$ in $\mathbb{Z}_p$. This, -1 is a square, so by QR part -1, $q \equiv 1 \pmod 4$. Thus, if $q|n$ and $q \equiv 3 \pmod 4$ then $q|a$. By switching roles, $q|b$ as well. But if $q|a$, then $q^2|a^2$, so $q^2|b^2$, and hence $q^2|(a^2 + b^2)$.
   (b) Read it from left to right.
   (c) Write $n = 2^a p_1^{e_1} \cdots p_k^{e_k} q_1^{f_1} \cdots q_\ell^{f_\ell}$, with $p_i \equiv 1 \pmod 4$ and $q_i \equiv 3 \pmod 4$.
   ($\Leftarrow$) : If each ℓ_i is even, then $q_1^{f_1} \cdots q_\ell^{f_\ell}$ is a square, hence a sum of two squares. Then since $2, p_1, \ldots, p_k$ are sums of two squares, by part (2), n is a sum of two squares.
   ($\Rightarrow$) : Given $n = a^2 + b^2$, we need to show that each ℓ_i is even. We proceed by strong induction on n (with $n = 2$ as a base case). By part (1), we can write $n = q_i^2 n'$ and $n = a^2 + b^2 = (q_i a')^2 + (q_i b')^2$. Thus, $n' = a'^2 + b'^2$. By the induction hypothesis, the multiplicity of q_i in n' is even, say $2w$; then $\ell_i = 2w + 2$ is even. This completes the induction.

[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.

(a) $\frac{56}{27}$.
(b) $\frac{47}{14}$.
(c) A finite continued fraction is made out of integers from addition and division.

(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?

(a) Euclidean algorithm.
(b) Divide the first line by 117 and flip the last fraction.
(c) $\frac{250}{117} = 2 + \cfrac{1}{7 + \cfrac{1}{3 + \frac{1}{5}}}$.
(d) $\frac{7}{5} = 1 + \cfrac{1}{2 + \frac{1}{2}}$.
(e) $\frac{39}{314} = \cfrac{1}{8 + \cfrac{1}{19 + \frac{1}{2}}}$.
(f) The a_i's are just the quotients in 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

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

show that

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

(a) ✓

(b) The formula for q_i is the general formula in the division algorithm (since $u_i/v_i - 1 < \lfloor u_i/v_i \rfloor \leq u_i/v_i$ implies $v_i > u_i - \lfloor u_i/v_i \rfloor v_i \geq 0$.) We then have

$$\frac{u_{i+1}}{v_{i+1}} = \frac{v_i}{r_i} = \frac{v_i}{u_i - \lfloor \frac{u_i}{v_i} \rfloor v_i} = \frac{1}{\frac{u_i}{v_i} - \lfloor \frac{u_i}{v_i} \rfloor}.$$

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?

$\sqrt{2} = [1; 2, 2, 2, \dots]$ and 2's forever, since $\beta_i = \sqrt{2} + 1$ for all $i > 0$, with $C_0, C_1, C_2, C_3 = 1, 3/2, 7/5, 12/5$. $\pi = [3; 7, 15, 1, \dots]$ and a mysterious pattern, with $C_0, C_1, C_2, C_3 = 3, 22/7, 333/106, 355/113$.

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

We have $L = 1 + 1/L$, so $L^2 = L + 1$. This has two roots $\frac{1 \pm \sqrt{5}}{2}$. Since $L > 0$, we must have $L = \frac{1+\sqrt{5}}{2}$, the golden ratio.

(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.

(a) This was the point of problem (3).
(b) If the algorithm terminates, then r has a finite continued fraction, and hence is rational. Conversely, if r is rational, the continued fraction algorithm follows the Euclidean algorithm and after finitely many steps returns a finite continued fraction.

(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.

(a) Set $p = \lfloor r/q \rfloor$.
(b) For the first, we just have C_0, C_1, C_2 along with $\frac{2}{1}$ and $\frac{4}{3}$. For the second, just C_0, C_1, C_2. We are impressed.
(c) This is a good approximation in the sense of Dirichlet Approximation Theroem, since it comes from the continued fraction. $\pi \approx 355/113$ is a very good approximation.

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

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

Then,
(1) $C_k = \dfrac{p_k}{q_k}$ for all $k \geq 0$, and
(2) $p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}$ for all $k \geq 1$.

[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.

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

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

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

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

(d) Use (8a) to show that $\sup\{C_{2k} \,|k \in \mathbb{N}\} = \inf\{C_{2\ell+1} \,|\ell \in \mathbb{N}\}$, 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.

(a)
$$C_k - C_{k-1} = \frac{p_k}{q_k} - p_{k-1}q_{k-1} = \frac{p_k q_{k-1} - p_{k-1}q_k}{q_k q_{k-1}} = \frac{(-1)^{k-1}}{q_k q_{k-1}}$$

(b)
$$C_k - C_{k-2} = C_k - C_{k-1} + C_{k-1} - C_{k-2} = \frac{(-1)^{k-1}}{q_k q_{k-1}} + \frac{(-1)^{k-2}}{q_{k-1}q_{k-2}}$$
$$= (-1)^k \frac{-q_{k-2} + q_k}{q_k q_{k-1} q_{k-2}} = \frac{(-1)^k a_k q_{k-1}}{q_k q_{k-1} q_{k-2}} = \frac{(-1)^k a_k}{q_k q_{k-2}}$$

(c) From (8b), we have $C_k - C_{k-2} > 0$ (so $C_k > C_{k-2}$) if k is even and $C_k - C_{k-2} < 0$ (so $C_k < C_{k-2}$) if k is odd. Thus, the sequence $C_0, C_2, C_4, \ldots$ is increasing and the sequence $C_1, C_3, C_5, \ldots$ is decreasing. By (8a), $C_{2\ell+1} - C_{2\ell} > 0$, so $C_{2\ell+1} > C_{2\ell}$; if $\ell \leq k$, then $C_{2\ell+1} > C_{2\ell} > C_{2k}$; if $\ell \geq k$, then $C_{2\ell+1} > C_{2k+1} > C_{2k}$. Then the sequence $(C_{2k})_{k=1}^{\infty}$ is increasing and bounded above (by, e.g., C_1), and the sequence $(C_{2\ell+1})_{\ell=1}^{\infty}$ decreasing and bounded below (by, e.g., C_0). By the monotone convergence theorem, these sequences converge to their sup and inf, respectively.

(d) Suppose $\sup\{C_{2k}\} < \inf\{C_{2\ell+1}\}$, and left $\delta = \inf\{C_{2\ell+1}\} - \sup\{C_{2k}\}$. Let $2n$ be an even number larger than $1/\delta$. Then
$$C_{2n} < \sup\{C_{2k}\} < \inf\{C_{2\ell+1}\} < C_{2n+1}$$
implies $C_{2n+1} - C_{2n} > 1/(2n)$, but we also have $C_{2n+1} - C_{2n} = 1/(q_{2n}q_{2n-1})$. Since $q_{2n} > 2n$, this is a contradiction. It follows that the sequence of convergents converges.

(e) If n is even, then we have $C_n < \sup\{C_{2k}\} = \beta = \inf\{C_{2\ell+1}\} < C_{n+1}$, and if n is odd, we have $C_{n+1} < \sup\{C_{2k}\} = \beta = \inf\{C_{2\ell+1}\} < C_n$. This shows that $|\beta - C_n| \leq |C_{n+1} - C_n|$. Then from (8a), $|C_{n+1} - C_n| = 1/(q_n q_{n+1}) < 1/q_n^2$.

(9) Prove the Proposition above.

We prove (1) by induction on k. We need two base cases, $k = 0$ and $k = 1$. For those, we have $[a_0;] = a_0/1$, and $[a_0; a_1] = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1}$. Now for the inductive step, suppose this holds for continued fractions of length at most k. Then we can write $C_{k+1} = [a_0; a_1, \ldots, a_k, a_{k+1}] = [a_0; a_1, \ldots, a'_k]$, where $a'_k = a_k + 1/a_{k+1}$. We apply the IH to the latter continued fraction:
$$C_{k+1} = \frac{a'_k p_{k-1} + p_{k-2}}{a'_k q_{k-1} + q_{k-2}} = \frac{(a_k + 1/a_{k+1})p_{k-1} + p_{k-2}}{(a_k + 1/a_{k+1})q_{k-1} + q_{k-2}}$$
$$= \frac{a_{k+1}(a_k p_{k-1} + p_{k-2}) + p_{k-1}}{a_{k+1}(a_k q_{k-1} + q_{k-2}) + q_{k-1}} = \frac{a_{k+1}p_k + p_{k-1}}{a_{k+1}q_k + q_{k-1}} = \frac{p_{k+1}}{q_{k+1}},$$

completing the induction.

We prove (2) by induction too. For $k = 1$, we get

$$p_1 q_0 - p_0 q_1 = (a_0 a_1 + 1) \cdot 1 - a_0 a_1 = 1.$$

Assume the formula holds for k, so

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}.$$

Then

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

completing the inductive step.

(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 $a_0, a_1, a_2, a_3, \ldots$ and $\beta_0, \beta_1, \beta_2, \ldots$ be the sequences arising from the continued fraction algorithm.

(a) Explain why $r = [a_0; a_1, \ldots, a_k, \beta_{k+1}]$. (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) $[a_0; a_1, \ldots, a_k, \beta_{k+1}]$ as in the Proposition above.

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

(a) We argue by induction on k. Since $\beta_0 = r$ and $[a_0;]$ means a_0, the case $k = 0$ holds. If $r = [a_0; a_1, \ldots, a_k, \beta_{k+1}]$, then by definition $\beta_{k+2} = 1/(\beta_{k+1} - a_{k+1})$, so $\beta_{k+1} = a_{k+1} + \frac{1}{\beta_{k+2}}$. Plugging this into the continued fraction setup, $r = [a_0; a_1, \ldots, a_k, a_{k+1}, \beta_{k+2}]$. This completes the induction.

(b) The same proof as the Proposition works.

(c)

$$\begin{aligned} r - C_k &= \frac{\beta_{k+1} p_k + p_{k-1}}{\beta_{k+1} q_k + q_{k-1}} - \frac{p_k}{q_k} \\ &= \frac{\beta_{k+1} p_k q_k + p_{k-1} q_k - p_k \beta_{k+1} q_k - p_k q_{k-1}}{(\beta_{k+1} q_k + q_{k-1}) q_k} \\ &= \frac{p_{k-1} q_k - p_k q_{k-1}}{(\beta_{k+1} q_k + q_{k-1}) q_k} = \frac{(-1)^k}{(\beta_{k+1} q_k + q_{k-1}) q_k} \end{aligned}$$

Since $\beta_{k+1} > a_{k+1}$, we have

$$\beta_{k+1} q_k + q_{k-1} > a_{k+1} q_k + q_{k-1} = q_{k+1}$$

so

$$|r - C_k| < \frac{1}{q_{k+1} q_k} < \frac{1}{q_k^2}.$$

(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.

(a) $9^2 - 5 \cdot 4^2 = 81 - 5 \cdot 16 = 1$✓.
(b) $(\pm x_0)^2 - D(\pm y_0)^2 = x_0^2 - Dy_0^2 = 1$.
(c) $(\pm 1, 0)$.
(d) By throwing in $(\pm 1, 0)$ and taking $\pm$ each coordinate.

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

For $D = 2$ we find $(3, 2)$. For $D = 3$ we find $(2, 1)$, For $D = 5$ we find $(9, 4)$.

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

If $D = d^2$ with $d > 0$, then $x^2 - Dy^2 = (x - dy)(x + dy)$. For any positive integers x, y, we have $x + dy > 1$, and $x - dy \in \mathbb{Z}$, so the product cannot be 1.

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 $a + b\sqrt{D}$.

(a) We check the conditions for a subring: Let $a + b\sqrt{D}, c + d\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$. Then,
- $1 = 1 + 0\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$
- $(a + b\sqrt{D}) - (c + d\sqrt{D}) = (a - c) + (b - d)\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$, and
- $(a + b\sqrt{D})(c + d\sqrt{D}) = (ac + bdD) + (ad + bc)\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$.

(b) If $a + b\sqrt{D} = c + d\sqrt{D}$ and $(a, b) \neq (c, d)$, then $a - c = (d - b)\sqrt{D}$. If $a \neq c$, then we must have $b \neq d$, so either way, $b \neq d$. Then $\sqrt{D} = \frac{a-c}{d-b}$, which contradicts that $\sqrt{D}$ is irrational. Thus, $a + b\sqrt{D} = c + d\sqrt{D}$ implies $(a, b) = (c, d)$.

(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.

(a) Set $\alpha = a + b\sqrt{D}$, $\beta = c + d\sqrt{D}$. Then $\alpha\beta = (ac + bdD) + (ad + bc)\sqrt{D}$ so

$$\begin{aligned} N(\alpha\beta) &= (ac + bdD)^2 - (ad + bc)^2 D \\ &= a^2c^2 + 2abcdD + b^2d^2D^2 - a^2 + d^2D - 2abcdD - b^2c^2D \\ &= a^2c^2 + b^2d^2D^2 - a^2d^2D - b^2c^2D. \end{aligned}$$

On the other hand,

$$N(\alpha)N(\beta) = (a^2 - b^2D)(c^2 - d^2D) = a^2c^2 - a^2d^2D - b^2c^2D + b^2d^2D^2.$$

(b) If α is a unit so $\alpha\beta = 1$ for some β, then

$$1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta),$$

so $N(\alpha)$ is a unit in $\mathbb{Z}$, hence is ± 1. Conversely, if $\alpha = a + b\sqrt{D}$ and $N(\alpha) = \pm 1$, then $(a + b\sqrt{D})(a - b\sqrt{D}) = \pm 1$, so $(a + b\sqrt{D})(\pm(a - b\sqrt{D})) = 1$, and α is a unit.
(c) The product of two elements of norm 1 has norm 1, by the lemma. The element 1 has norm 1, which serves as the identity. By the previous part, an element of norm 1 has an inverse, which must have norm 1 by the lemma.

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.

[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.

(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.

For $D = 2$, the solutions are the coefficients of $(3 + 2\sqrt{2})^k$. The first three solutions are $(3, 2)$, $(17, 12)$, and $(99, 70)$.

For $D = 3$, the solutions are the coefficients of $(2 + \sqrt{3})^k$. The first three solutions are $(2, 1)$, $(7, 4)$, and $(26, 15)$.

For $D = 5$, the solutions are the coefficients of $(9 + 4\sqrt{5})^k$. The first three solutions are $(9, 4)$, $(161, 72)$, and $(2889, 1292)$.

(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.

(a) From the lemma, $N((a + b\sqrt{D})^k) = N(a + b\sqrt{D})^k = 1$ for all k, so all of these are solutions.
(b) We have

$$N(e + f\sqrt{D}) = N(c + d\sqrt{D})N(a - b\sqrt{D}) = N(c + d\sqrt{D})N(a + b\sqrt{D}) = 1,$$

so it is a solution.
(c) From $a^2 - b^2D = 1 > 0$, we find that $a > b\sqrt{D}$, and similarly $c > d\sqrt{D}$. Then $ac > bdD$ so $e = ac - bdD > 0$. Since $0 < a < c$, we have

$$a^2d^2D = a^2(c^2 - 1) = a^2c^2 - a^2 > a^2c^2 - c^2 = (a^2 - 1)c^2 = b^2c^2D,$$

so $ad > bc$, and $f = ad - bc > 0$. Finally, we have

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

so $c = ae + bfD > e$.
(d) If not, let $c+d\sqrt{D}$ be the smallest positive solution not of this form. Then $e+f\sqrt{D} := (c+d\sqrt{D})(a-b\sqrt{D})$ is also not a power of $a+b\sqrt{D}$, since if $e+f\sqrt{D} = (a+b\sqrt{D})^k$, then $c + d\sqrt{D} = (e + f\sqrt{D})(a + b\sqrt{D}) = (a + b\sqrt{D})^{k+1}$, a contradiction. But by the previous part, $e + f\sqrt{D}$ is a smaller positive solution; a contradiction.

[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 $a + b\sqrt{D}$.

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

[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 $D = 21$.

(a) Compute the continued fraction for $\sqrt{D}$, and test whether $p_k^2 - Dq_k^2 = 1$ for the sequence of convergents $C_k = \frac{p_k}{q_k}$. The first one that works is the smallest positive solution of Pell's equation.
(b) For $D = 2$, the convergent $C_1 = \frac{3}{2}$ yields the smallest solution $(3, 2)$.
For $D = 3$, the convergent $C_1 = \frac{2}{1}$ yields the solution $(2, 1)$.
For $D = 10$, the convergent $C_1 = \frac{19}{6}$ yields the solution $(19, 6)$.
For $D = 21$, the convergent $C_5 = \frac{55}{12}$ yields the solution $(55, 12)$.
(c) For $D = 10$, the positive solutions $(x_k, y_k)$are given by the coefficients of $x_k + y_k\sqrt{10} = (19 + 6\sqrt{10})^k$.
For $D = 21$, the positive solutions $(x_k, y_k)$are given by the coefficients of $x_k + y_k\sqrt{21} = (55 + 12\sqrt{21})^k$.

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

Suppose that (a, b) is a positive solution to the Pell's equation, so $a^2 - Db^2 = 1$. Dividing through by b^2,

$$\left|\left(\frac{a}{b}\right)^2 - D\right| < \frac{1}{b^2}.$$

Factoring the left-hand side, we get

$$\left|\frac{a}{b} - \sqrt{D}\right| \left|\frac{a}{b} + \sqrt{D}\right| < \frac{1}{b^2}, \quad \text{so} \quad \left|\frac{a}{b} - \sqrt{D}\right| < \frac{1}{b^2\left|\frac{a}{b} + \sqrt{D}\right|}.$$

We claim that $\frac{a}{b} + \sqrt{D} > 2$ for any solution to Pell's equation. Indeed, $D \geq 2$ implies $\sqrt{D} > 1$ and $a > b$ implies $\frac{a}{b} > 1$ as well. Thus, from the equations above, we have

$$\left|\frac{a}{b} - \sqrt{D}\right| < \frac{1}{2b^2}.$$

By the Theorem (Good approximations are convergents), $\frac{a}{b}$ must be a convergent of $\sqrt{D}$.

(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.

(a) By Dirichlet's approximation theorem, there are infinitely many p/q such that

$$\left|\frac{p}{q} - \sqrt{D}\right| < \frac{1}{q^2},$$

given by the convergents of the continued fraction of $\sqrt{D}$. Then

$$\left|\left(\frac{p}{q}\right)^2 - D\right| = \left|\frac{p}{q} - \sqrt{D}\right| \left|\frac{p}{q} + \sqrt{D}\right| < \frac{\left|\frac{p}{q} + \sqrt{D}\right|}{q^2},$$

so

$$|p^2 - Dq^2| < \frac{p}{q} + \sqrt{D}.$$

Since $q \geq 1$, we have that $\frac{p}{q} - \sqrt{D} \leq 1$ by Dirichlet, so $\frac{p}{q} + \sqrt{D} < 2\sqrt{D} + 1$. (Note that equality is impossible since $\sqrt{D}$ is irrational.)
For p/q as above, taking $x_i = p$, $y_i = q$, we get infinitely many pairs of integers with $|x_i^2 - Dy_i^2| < 2\sqrt{D} + 1$.

(b) There are finitely many integers m such that $|m| < 2\sqrt{D} + 1$, so by the pigeonhole principle, there must be some m such that there are infinitely many (x_i, y_i) with $x_i^2 - Dy_i^2 = m$.

(c) Take m as in the previous part; this m is nonzero since $\sqrt{D}$ is irrational. For each element in the sequence obtained in the previous part, it corresponds to one element of $\mathbb{Z}_{|m|} \times \mathbb{Z}_{|m|}$ by taking the congruences

$$\begin{cases} x_i \equiv a \pmod{|m|} \\ y_i \equiv b \pmod{|m|} \end{cases}.$$

Since $\mathbb{Z}_{|m|} \times \mathbb{Z}_{|m|}$ is finite, by the pigeonhole principle, there must be some element of $\mathbb{Z}_{|m|} \times \mathbb{Z}_{|m|}$ corresponding to infinitely many elements of the sequence. This gives the statement.

(d) Given $i \neq j$ and x_i, x_j, y_i, y_j as in the previous part, note that

$$N(x_j + y_j\sqrt{D}) = N(x_i + y_i\sqrt{D}) = m.$$

We can write

$$\frac{x_j + y_j\sqrt{D}}{x_i + y_i\sqrt{D}} = \frac{1}{m}(x_j + y_j\sqrt{D})(x_i - y_i\sqrt{D}) = \frac{1}{m}((x_ix_j - y_iy_jD) + (x_jy_i - x_iy_j)\sqrt{D}).$$

We claim that

$$x_ix_j - y_iy_jD \equiv x_jy_i - x_iy_j \equiv 0 \pmod{|m|}.$$

Indeed,

$$\begin{aligned} x_ix_j - y_iy_jD &\equiv a^2 - b^2D \equiv m \equiv 0 \pmod{|m|} \\ x_jy_i - x_iy_j &\equiv ab - ab \equiv 0 \pmod{|m|}. \end{aligned}$$

This implies that the coefficients of $(x_ix_j - y_iy_jD) + (x_jy_i - x_iy_j)\sqrt{D}$ are divisible by m, so the number above is an element of $\mathbb{Z}[\sqrt{D}]$.

(e) In the previous part, we have found an element $\alpha \in \mathbb{Z}[\sqrt{D}]$ such that $\alpha(x_i + y_i\sqrt{D}) = x_j + y_j\sqrt{D}$ and

$$N(x_j + y_j\sqrt{D}) = N(x_i + y_i\sqrt{D}) = m \neq 0.$$

Thus, by the lemma, we much have $N(\alpha) = 1$. This yields the solution we seek.

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

Suppose that p/q is not a convergent of r. If $q = q_k$ for some k but $p \neq p_k$, then

$$\left|r - \frac{p}{q_k}\right| \geq \left|\left|\frac{p}{q_k} - \frac{p_k}{q_k}\right| - \left|r - \frac{p_k}{q_k}\right|\right|.$$

Since $\left|\frac{p}{q_k} - \frac{p_k}{q_k}\right| \geq \frac{1}{q_k}$ and $\left|r - \frac{p_k}{q_k}\right| < \frac{1}{q_k^2}$ by Dirichlet approximation Theorem, the difference above is at least $\frac{q_k - 1}{q_k^2} > \frac{1}{2q_k^2}$, contradicting the hypotheses. Thus, we must have $q \neq q_k$ for any k, so $q_{k-1} < q < q_k$ for some k.

By hypothesis,

$$\left|r - \frac{p}{q}\right| < \frac{1}{2q^2} < \frac{1}{2qq_{k-1}}.$$

Following the proof of Problem set #5 problem #4, by replacing k by $k-1$ in steps (a)–(d), we see that

$$|q_{k-1}r - p_{k-1}| \leq |qr - p|.$$

Since $|qr - p| < 1/2q$, by hypothesis, we get

$$\left|r - \frac{p_{k-1}}{q_{k-1}}\right| \leq \frac{1}{2qq_{k-1}}.$$

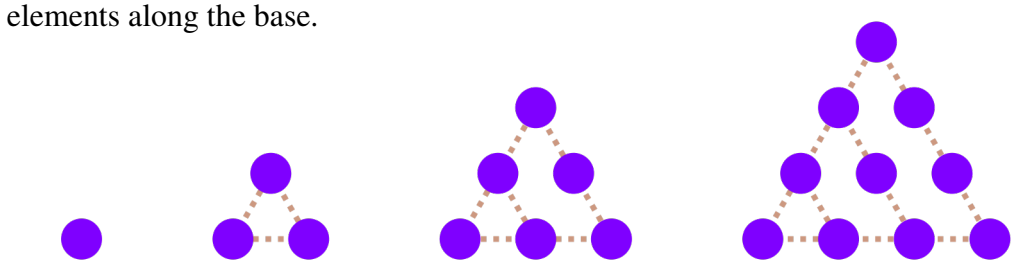
[1]Hint: If not, we can assume $q_{k-1} < q < q_k$ for some k. In Problem set #5 problem #4, the same proof with $k-1$ in place of k in parts (a)–(d) shows that, under the same hypotheses, $|qr - p| \geq |q_{k-1}r - p_{k-1}|$. Then show that $|\frac{p}{q} - \frac{p_{k-1}}{q_{k-1}}| < \frac{1}{qq_{k-1}}$.

Then, by the triangle inequality,

$$\left|\frac{p}{q}-\frac{p_{k-1}}{q_{k-1}}\right| \leq \left|r-\frac{p}{q}\right| + \left|r-\frac{p_{k-1}}{q_{k-1}}\right| < \frac{1}{2qq_{k-1}} + \frac{1}{2qq_{k-1}} = \frac{1}{qq_{k-1}}.$$

Clearing denominators, this forces $\left|\frac{p}{q}-\frac{p_{k-1}}{q_{k-1}}\right| = 0$. This contradicts the assumption that p/q is not a convergent of r.

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.

Going from T_n to T_{n+1}, we add one row of $n+1$ elements, so $T_{n+1} = T_n + (n+1)$, and the formula $T_n = 1 + 2 + \cdots + n$ is then clear. For the second, we can write

$$\begin{aligned} T_n + T_n &= (1 + 2 + \cdots + n) + (n + (n-1) + \cdots + 1) \\ &= (n+1) + \cdots + (n+1) = n(n+1), \end{aligned}$$

so $T_n = \dfrac{n(n+1)}{2}$.

(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.

(a) We have $\dfrac{m(m+1)}{2} = n^2$, so $m^2 + m = 2n^2$. Completing the square on the left gives

$$(m + \frac{1}{2})^2 - \frac{1}{4} = 2n^2,$$

and clearing denominators,

$$(2m+1)^2 - 1 = 8n^2.$$

Setting $x = 2m+1$ and $y = 2n$, we get the equation

$$x^2 - 2y^2 = 1,$$

a Pell's equation.

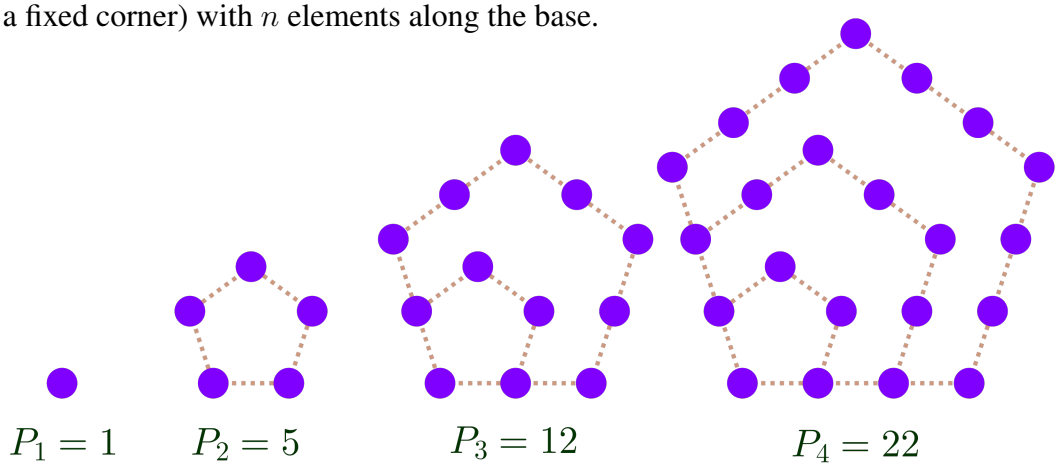
(b) The solutions (x, y) of $x^2 - 2y^2 = 1$ come from coefficients of $x + y\sqrt{2} = (3 + 2\sqrt{2})^k$ for $k \in \mathbb{N}$. Thus, if $T_m = n^2$ is a square-triangular number, $(2m+1, 2n) = (x, y)$ comes from the coefficients of $(3 + 2\sqrt{2})^k$ for $k \in \mathbb{N}$.
Conversely, given (x, y) such that $x + y\sqrt{2} = (3+2\sqrt{2})^k$, we can write $(x, y) = (2m+1, 2n)$ for some integers $m = \frac{x-1}{2}$, $n = \frac{y}{2}$ since x is odd and y is even: we can see this by induction,

[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.

since if x is odd and y is even, then $(x+y\sqrt{2})(3+2\sqrt{2}) = (3x+4y)+(3y+2x)\sqrt{2}$ has $3x+4y$ odd and $3y+2x$ even.

(c) The first four solutions of the Pell's equation above are $(3,2)$, $(17,12)$, $(99,70)$, $(577,408)$. We then have $n = y/2$, and the actual number is $n^2 = y^2/4$. We get the numbers: $1, 36, 1225, 41616$.

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.

(a) $P_m - P_{m-1}$ corresponds to two sides of length m and one side of length $m-2$, so $3m-2$. Then we get

$$P_m = 3(1+2+\cdots+m) - 2m = 3\frac{m(m+1)}{2} - 2m = \frac{3m^2-m}{2}.$$

(b) We start with $\frac{3m^2-m}{2} = n^2$, so $m^2 - \frac{m}{3} = \frac{2n^2}{3}$. Completing the square gives

$$(m-\frac{1}{6})^2 - \frac{1}{36} = \frac{2n^2}{3}$$

and clearing denominators yields

$$(6m-1)^2 - 1 = 24n^2.$$

Set $x = 6m-1$ and $y = 2n$ to get

$$x^2 - 6y^2 = 1,$$

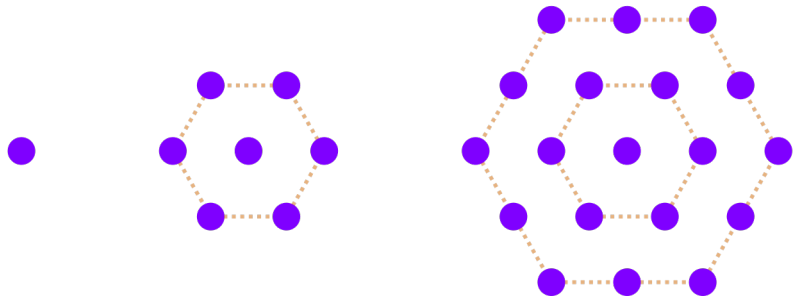
a Pell's equation.

(c) We find $(x,y) = (5,2)$ as the smallest positive solution to the Pell's equation above, so the solutions (x,y) of $x^2-6y^2=1$ come from coefficients of $x+y\sqrt{6} = (5+2\sqrt{6})^k$ for $k \in \mathbb{N}$.

Thus, if $P_m = n^2$ is a square-pentagonal number, $(6m-1, 2n) = (x, y)$ comes from the coefficients of $(5+2\sqrt{6})^k$ for $k \in \mathbb{N}$.
To determine which values of k yield an x with $x \equiv 5 \pmod 6$, and y even we compute that $(x+y\sqrt{6})(5+2\sqrt{6}) = (5x+12y)+(2x+5y)\sqrt{6}$. Since for $k=1$, y is even, by induction, we see that y is even for all k. Furthermore, if (x_k, y_k) is the kth solution, then $x_{k+1} \equiv 5x_k \pmod 6$. Since $x_1 \equiv 5 \pmod 6$, we determine that $x_k \equiv 5 \pmod 6$ exactly when k is *odd*.

(d) We compute the odd-indexed solutions to the Pell's equation $5+2\sqrt{6}$, $(5+2\sqrt{6})^3 = 485+198\sqrt{6}$, $(5+2\sqrt{6})^5 = 47525+19402\sqrt{6}$. Then we find that $n = y/2$, and the actual number we seek is n^2, so we get $1, 9801, 94109401$ as the square-pentagonal numbers.

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.

We have $H_m - H_{m-1}$ is given by six sides with $m-1$ elements, so is $6(m-1)$. Using the formula from (1) we get that the mth centered hexagonal number is $3m^2-3m+1$. Now we set $3m^2-3m+1 = n^2$, and complete the square:

$$m^2 - m + \frac{1}{3} = \frac{n^2}{3}$$
$$(m-\frac{1}{2})^2 - \frac{1}{4} + \frac{1}{3} = \frac{n^2}{3}$$
$$3(2m-1)^2 + 1 = 4n^2,$$

so setting $x = 2n$, $y = 2m-1$, we get the Pell's equation $x^2 - 3y^2 = 1$.

The solutions (x, y) to this Pell's equation are given by $x_k + y_k\sqrt{3} = (2+\sqrt{3})^k$. However, we only obtain integer solutions $(m, n) = (\frac{y+1}{2}, \frac{x}{2})$ to the original equation when x is even and y is odd. Multiplying out, we see that $x_{k+1} = 2x_k + 3y_k \equiv y_k \pmod 2$ and $y_{k+1} = x_k + 2y_k \equiv x_k \pmod 2$. Since x_1 is even and y_1 is odd, we have x_k even and y_k odd exactly when k is odd.

Then we take $n^2 = (x_k/2)^2$ for $k = 1, 3, 5$ to get $1, 169, 32761$.

(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.

Given m, n like so, we have

$$\frac{m(m-1)}{2} = \frac{n(n+1)}{2} - \frac{m(m+1)}{2}$$
$$2m^2 = n^2 + n$$
$$2m^2 = \left(n + \frac{1}{2}\right)^2 - \frac{1}{4}$$
$$2(2m)^2 = (2n+1)^2 - 1$$

so setting $x = 2n+1$ and $y = 2m$, we get solutions to Pell's equation $x^2 - 2y^2 = 1$. As above, we see that a solution (x, y) must have x odd and y even, so any solution to Pell's equation yields a solution (m, n) of the original; in particular,

$$K = \frac{\frac{y}{2}(\frac{y}{2}-1)}{2} = \frac{y(y-2)}{8}.$$

From $y = 12, 70, 408$, we get $K = 15, 595, 20706$.

(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:

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

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

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

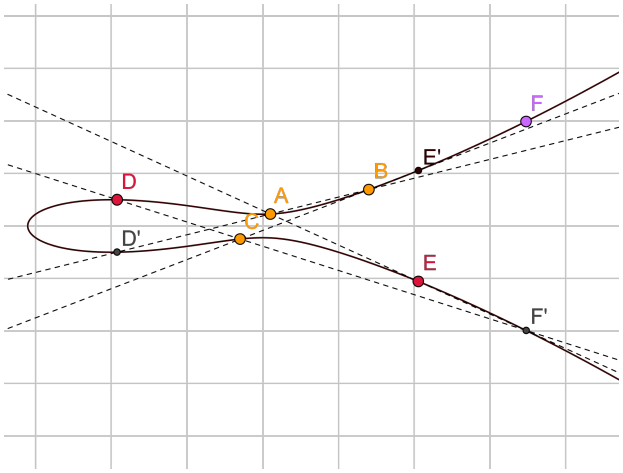
(1) Drawing the operations $\star$ and $-^\vee$:
   (a) For each of the curves given, see if you can find labeled points P, Q, R such that $P \star Q = R$. Can you find all such triples?
   (b) For each of the curves given, mark your own points and see if you can compute the operation $\star$.

Answers vary for different placemats and selected points.

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

The line between P and Q is the same as the line between Q and 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?



$A \star B = D$, and $D \star C = F$, while $B \star C = E$ and $A \star E = F$. Thus, $(A \star B) \star C = F = A \star (B \star C)$. This corresponds to the associativity of the operation.

(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 $S = Q \star R$.

For (a), plug in the values to check. For (b), we compute R by taking the line between P and Q, which is $y = x + 2$, and plugging this into the equation to get $(x+2)^2 = x^3 + 2x + 4$. This yields $0 = x^3 - x^2 + 2x = x(x-2)(x+1)$. The roots $x = 0$ and $x = -1$ correspond to P and Q, so the third point corresponds to $x = 2$. Then $(2, 4)$ is the third point on the line. We reflect to get $R = (2, -4)$.

We repeat the process with Q, R, to get $S = (7, 19)$.

(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.

(a) If $P = (x_0, y_0) \in E$, so that $y_0^2 = x_0^3 + ax_0 + b$, then $(-y_0)^2 = x_0^3 + ax_0 + b$, so that $P^\vee = (x_0, -y_0) \in E$.
(b) Points on the x-axis.
(c) Reflection over the x-axis reflects the tangent line as well. If the tangent line had nonzero slope m, then its reflection would have slope $-m \neq m$. The case of a horizontal tangent on the x-axis is also impossible, though it takes a little longer to argue geometrically, and we'll skip it for now.

(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 $4P$.

(a) The line approaches the tangent line to E at P.
(b) $2P := P \star P$ should be the reflection of the point Q that is on intersection of the tangent line at P and E.
(c) Answers vary.
(d) To compute $2P$ we compute the tangent line to E at P. From calculus, this line is $y = x + 1$. Plugging this into the original equation, we get $(x+1)^2 = x^3 + 2x + 1$, so $0 = x^3 - x^2 = x^2(x-1)$. The double root $x = 0$ corresponds to the point P, so the other point is with $x = 1$, namely $(1, 2)$. Thus $2P = (1, -2)$. Continuing $3P = (8, 23)$, and $4P = \left(\frac{-7}{16}, \frac{13}{64}\right)$.

(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?

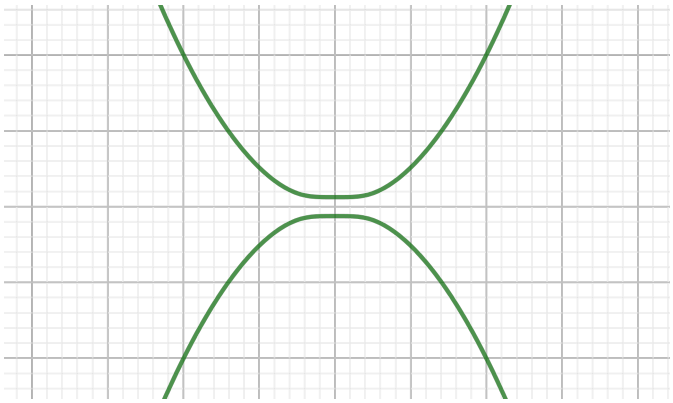
(a) To compute $P \star \infty$, we may be inclined to take the vertical line through P, and take the other intersection point, which is $P^\vee$, then reflect, to get P.
(b) If $P \star Q = \infty$, then Q is the point on the line between P and $\infty^\vee = \infty$, which is $P^\vee$.
(c) Yes.

(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.

(a) Points on the x-axis.
(b) Points whose tangent line meets a point in E on the x-axis.
(c) An inflection point corresponds to a triple intersection with the tangent line, so morally, the third point on the line between P and P is P, so $P \star P = P^\vee$, and then $P \star P \star P = P^\vee \star P = \infty$.
(d) OK
(e) Points whose tangent line meets an inflection point in E.

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 $E_{\mathbb{Q}}$.

[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) 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).

> The line between two rational points has a rational slope and rational intersection. Plugging this into the equation for E gives a rational degree three polynomial in x. Two of the roots we already know (from the two points, or a double root in the case of a tangent line) and are rational; then by long division, the third root is rational. Thus the x-coordinate is rational, and the y-coordinate is rational too; still rational after reflecting.

(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.

> We have $P^\vee = (-2, -3)$ as well. We also get $2P = (8, -23)$, $2P^\vee = (8, 23)$, etc.

(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.

> We find that P$\star P = \infty$, $P \star Q = R^\vee$, $P \star R = Q^\vee$, , $Q \star Q = Q^\vee$ (since Q is an inflection point), $Q \star R = P$, and $R \star R = Q$. Similar things happen with $Q^\vee$ and $R^\vee$. The upshot is that these five points plus ∞ form a finite subgroup of $\overline{E}_{\mathbb{Q}}$ so there are not more solutions that can be generated from these.

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.

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

(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 $\overline{E}_5$.

   (a) $\overline{E}_5 = \{(0,2), (0,3), (1,0), (3,1), (3,4), \infty\}$.
   (b) $\overline{E}_5$ is a group with 6 elements. By Lagrange's Theorem, the order of an element divides the order of the group.
   (c) To compute $2P$, we find the tangent line through P. By implicit differentiation, we get $[2]y\frac{dy}{dx} = [3]x^2$, so the slope of the tangent line at P is $\frac{[3]\cdot[3]^2}{[2]\cdot[1]} = \frac{[27]}{[2]} = \frac{[2]}{[2]} = [1]$. The tangent line is then $y = x + [3]$. Plugging this into the original equation and solving (or just testing the other points in E) we get that the other point of intersection is $([0], [3])$, so $2P = ([0], [-3]) = ([0], [2])$. To compute $3P$,we take the line between P and $2P$. The slope is $\frac{[1]-[2]}{[3]-[0]} = \frac{[4]}{[3]} = [4][2] = [3]$, so the line is $y = [3]x + [2]$. The third point of intersection (by substitution or trial and error) is $([1], [0])$, which is its own inverse, so $3P = ([1], [0])$.
   (d) Since we ruled out 2 and 3, we know that P has order exactly 6. Then $3(2P) = \infty$ but $2(2P) \neq \infty$, so $2P$ has order 3, and $3P$ has order 2. The remaining points are $([0], [3]) = (2P)^\vee = 4P$ which has order 3 and $([3], [4]) = P^\vee = 5P$ which has order 6.

(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 $8P = \infty$.

   (a) $\overline{E}_5 = \{(0,1), (0,4), (1,1), (1,4), (3,0), (4,1), (4,4), \infty\}$.
   (b) The order of $\overline{E}_5$ is 8, so by Lagrange, every element has order dividing 8, which implies even (whenever the order isn't 1).
   (c) If the order of P is d and $d|8$, write $8 = de$; then $8P = deP = e(dP) = e\infty = \infty$.

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 $d = e^{-1} \pmod{\phi(n)}$.

(a) $n = 47 \cdot 59 = 2773$. By the proposition, $\phi(2773) = \phi(47) \cdot \phi(59) = (47-1)(59-1) = 2668$.
(b) 17 has an inverse modulo $\phi(n)$ if and only if $\gcd(17, \phi(n)) = 1$. 17 is prime, and 17 does not divide 2668, so 17 has an inverse.
(c) We apply the Euclidean Algorithm to find the inverse of 17:

$$2668 = 17 \cdot 156 + 16$$
$$17 = 16 \cdot 1 + 1$$

Thus we find after algebra that $1 = 17 \cdot 157 + 2668(-1)$, and so $d = 157$.

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

[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 $041507 = 41507$.

(a) $H = 08$ and $I = 09$, so our integer is 809.
(b) $809^{17} \equiv 522 \pmod{2773}$. If we wish to do this by hand, we could first calculate $809^2 \pmod{2773}$, then 809^4, 809^8, 809^{16}, and finally 809^{17}.

(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 $x \neq m$.

(a) We can use the Chinese Remainder Theorem to solve the system of congruences:

$$x \equiv 522^{157} \pmod{47}$$
$$x \equiv 522^{157} \pmod{59}$$

(since this forms a unique congruence class modulo n.) We can reduce 522 modulo 47 and 59 to 5 and 50 respectively; we also know that $\phi(47) = 46$ and $\phi(59) = 58$, and that $5^{46} \equiv 1 \pmod{46}$ and $50^{58} \equiv 1 \pmod{59}$. Thus we can instead solve:

$$x \equiv 5^{19} \pmod{47}$$
$$x \equiv 50^{41} \pmod{59}$$

We can solve this system of congruences using techniques from class and find $x = 809$.
(b) This decodes into the original "HI".
(c) Since $ed \equiv 1 \pmod{\phi(n)}$, $ed = \phi(n) \cdot k + 1$ for some integer k. Recall by Euler's Theorem that $a^{\phi(n)} \equiv 1 \pmod{n}$, so we have $m^{ed} \equiv m^{\phi(n)\cdot k+1} \equiv m^{\phi(n)\cdot k} \cdot m \equiv 1^k \cdot m \equiv m \pmod{n}$.
(d) The result is 88. Actually, $x \equiv m \pmod{n}$, but since $m \geq n$, $m \neq x$.

(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 $d = e^{-1} \pmod{\phi(n)}$.

Results depend on choice of primes p and q and public key e.

(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?

Results depend on choice of primes p and q, public key e, and message m.
For (5c), we need to find p and q in order to determine the private key d; the specific result will vary.

[3] HINT: Try using the Chinese Remainder Theorem to work with smaller numbers.
[4] If at any point you're waiting, work ahead on future problems!

(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.

(a) The factors are 31 and 53.

(b) Based on prime approximations, we would expect to test roughly 10^{306} primes. If we could test 1,000,000 primes per second, it would still take 10^{293} years!

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 $\left(\frac{n}{q_i}\right) = 1$.

(b) Check[7] that each element in the factor base is not a prime factor of n.

(c) Find the first[8] 5 convergents $C_k = \frac{p_k}{q_k}$ 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.

(a) The primes in range are 2, 3, 5, and 7. Of these, 3053 is a square modulo 2 and 7, thus the factor base is $\{2, 7\}$.

(b) We can see that 2 does not divide 3053, and by the Euclidean Algorithm $3057 = 7 \cdot 436 + 1$ and is not a divisor.

(c) Apply the Continued Fraction Algorithm:

k	β_k	α_k
0	$\sqrt{3053}$	55
1	≈ 3.93	3
2	≈ 1.06	1
3	≈ 15.03	15

k	β_k	α_k
4	$\cdots$	27
5	$\cdots$	1
6	$\cdots$	1

[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 $-b_k = (-1)p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$.

We then evaluate the fractions:

$$C_0 = \frac{55}{1} \qquad C_1 = \frac{166}{3} \qquad C_2 = \frac{221}{4}$$
$$C_3 = \frac{3481}{63} \qquad C_4 = \frac{94208}{1705} \qquad C_5 = \frac{97889}{1768}$$

We then have:

k	p_k	a_k	b_k
0	55	55	-28
1	166	166	79
2	221	221	-7
3	3481	428	4
4	94208	2618	-61
5	97889	3046	49

(d) b_1 and b_4 cannot be written as a product of primes in the factor base, so we will not consider them. Of the remainder, we have:

$$b_0 = (-1)\cdot 2^2 \cdot 7 \qquad b_2 = (-1)\cdot 7^1 \qquad b_3 = 2^2 \qquad b_5 = 7^2$$

Any of the following can form trivial squares work:

i. $\{ \big(55,\ (-1\cdot 2^2\cdot 7)\big),\ \big(221,\ (-1\cdot 7)\big) \}$

ii. $\{ (428,\ 2^2) \}$

- $\{ (3046,\ 7^2) \}$: Since $3046 \equiv \pm 7 \pmod{3053}$, we discard this one.

iii. $\{ (428,\ 2^2)\ (3046,\ 7^2) \}$

- $\{ \big(55,\ (-1\cdot 2^2\cdot 7)\big),\ \big(221,\ (-1\cdot 7)\big),\ (428,\ 2^2) \}$: $28 \equiv \pm 28$, so we discard.
- $\{ \big(55,\ (-1\cdot 2^2\cdot 7)\big),\ \big(221,\ (-1\cdot 7)\big),\ (428,\ 2^2),\ (3046,\ 7^2) \}$: $2857 \equiv \pm 196$, discard.

Further solutions will consider (i), but all of them will work.

(e) With (i), we find $A \equiv 2996$, $B \equiv 14$. We confirm that $A^2 \equiv 196 \equiv B^2 \pmod{3053}$.

(f) The Theorem tells us that we will get nontrivial factors of 3053 by calculating $\gcd(A+B, 3053) = \gcd(3010, 3053)$ and $\gcd(A-B, 3053) = \gcd(2982, 3053)$. Applying the Euclidean Algorithm:

$$3053 = 3010\cdot 1 + 43 \qquad 3053 = 2982\cdot 1 + 71$$
$$3010 = 43\cdot 70 \qquad 2982 = 71\cdot 42$$

A quick check reveals that $43\cdot 71 = 3053$!