**Strange Algorithm**

Start with $a \in \mathbb{N}$, $a_0 = a$.

- If $a_0$ is even, then $a_i = \frac{a_i}{2}$
- If $a_0$ is odd, then $a_i = 3a_0 + 1$

**Collatz Conjecture**

Starting with any $a$, do you get down to 1 eventually?

5, 16, 8, 4, 2, 1, 4, 2, 1, 4, 2, ...

6, 3, 10, 5, 16, 8, 4, 2, 1

Start with $a, b \in \mathbb{N}$.

$a|x+b$, $x, y \in \mathbb{Z}$

What numbers (integers) this way?

If $d | a$, $d | b$, then $d | ax + by$ for $x, y \in \mathbb{Z}$.

$gcd(a, b) | (ax + by)$ for $x, y \in \mathbb{Z}$.
Proposition: The smallest positive number you express as \( ax + by \), \( x, y \in \mathbb{Z} \) is \( \gcd(a, b) = g \).

Proof: \( g \mid ax + by \).

If we can show \( \exists x, y \in \mathbb{Z} \) st. \( g = ax + by \), then \( g \) will have to be the smallest positive integer expressed.

\[
22x + 60y = \gcd(22, 60)
\]

First find the \( \gcd \):

\[
60 = 2 \times (22) + 16
\]
\[
22 = 1 \times 16 + 6
\]
\[
16 = 2 \times 6 + 4
\]
\[
4 = 1 \times 4 + 0
\]

\( \gcd = 4 \).

\[
60 = 2 \times 22 + 16, \quad 16 = 60 - 2 \times 22
\]
\[
22 = 1 \times 16 + 6
\]
\[
b = q_1 \times r_1 + r_2 = a \cdot 1 - b \cdot 0
\]
\[ r_2 = b - q_2 r_1 = b - \frac{q_1}{q_2} (a_1 - b_2) \]
\[ = -q_2 a + (1 + q_1 q_2) b \]

\[ r_3 = \quad \]

\[ r_n = \ ? a + \ ? b. \]

\[ 60 = 2 \times 22 + 16, \quad 16 = a - 2b \]
\[ 22 = 1 \times 16 + 6, \quad 6 = 3b - a \]
\[ 16 = 2 \times 6 + 4, \quad 4 = 16 - 2 \times 6 = 3a - 8b \]
\[ 2 = -4a + 11b. \]

\[ \]
\[ a = q_1 b + r_1 \]
\[ b = q_2 r_1 + r_2 \]
\[ r_1 = q_3 r_2 + r_3 \]
\[ \]
\[ r_{n+2} = q_n r_{n+1} + r_n \]
\[ r_{n+1} = q_n r_n \]

\[ a = q_1 b + r_1, \quad r_1 = a - 2b \]
\[ b = q_2 r_1 + r_2, \quad r_2 = b - q_2 r_1 \]
\[ r_1 = r_3 r_2 + r_5, \quad r_5 = r_1 - q_3 r_2 \]
\[ = (a - q_2 b) - q_3 (-q_2 a + q_2 b) \]
\[ = (1 + q_3 q_2) a + (-1 - q_2 q_3) b \]

\[ \text{QED} \]

If \( \gcd(a, b) = 1 \), we say they're relatively prime.

If \( \gcd(a, b) = 1 \),

\[ ax + by = 1 \]
has a soln \( x, y \in \mathbb{Z} \).

So, we can hit any integer, \( n \).

\[ ax + by = 1, \quad a(nx) + b(ny) = n \]

More generally,

\[ ax + by = n \] has soln \( \iff \)

\[ n = a \text{ multiple of } \gcd(a, b) \].
Prime factorization

Lemma: Let \( p \) be a prime. And \( p \mid ab \). Then \( p \mid a \) or \( p \mid b \).

Proof: If \( p \nmid a \), we're done.
So assume \( p \nmid a \). Then
\[
\gcd(p,a)\mid p, \quad \gcd(p,a)\mid a
\]
So \( \gcd(p,a) = p \) or \( 1 \). If \( p \), then \( p \mid a \)
which we assume is not the case.
We can solve
\[
a x + p y = 1, \quad \text{for } x, y \in \mathbb{Z}
\]
Multiply by \( b \)
\[
ab x + pb y = b
\]
\( p \mid pb y \), \( p \mid ab x \) since \( p \mid ab \).
So \( p \mid b \). QED
Theorem If \( p \mid (a_1, \ldots, a_n) \), \( p \) prime then \( p \mid a_1 \), or \( p \mid a_2 \) or \( \ldots \) or \( p \mid a_n \).

Proof If \( p \mid a_1 \), we're done.

So assume \( p \nmid a_1 \).

\[ p \mid a_1 a_2 \ldots a_n = a_1 (a_2 \ldots a_n) \]

by the lemma it divides \( p \mid a_2 \ldots a_n \).

\[ \text{Fundamental Theorem of Arithmetic} \]

Every \( n \geq 2 \) can be factored into primes

\[ n = p_1 \ldots p_k \]

in exactly (up to rearranging the order of the primes)
Modular Arithmetic

Let \( n \in \mathbb{N} \), \( n > 1 \).
We say \( a, b \in \mathbb{Z} \)
\( a \equiv b \mod n \) if \( n \mid (a - b) \)

Examples

\[ n = 3 \]
\[ \ldots -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, \ldots \]

Every integer \( a \equiv 0 \mod 3 \)
or \( 1 \)

Thus \( 0, 1, 2 \) is the remainder of \( a \) after dividing by 3.

\[ n = 2 \]
\[ 0, 1 \]

\[ n = 4 \]
\[ 0, 1, 2, 3 \mod 4 \]
Let \( n \) be \( \geq 1 \).

The set \( \mathbb{Z} / n \mathbb{Z} \) means \( \{0, 1, 2, \ldots, n-1\} \) but thought of as the remainders you get in dividing by \( n \).

That you can add, and multiply.

\[
\begin{align*}
0+0 & \equiv 0 \mod 2 & \text{even} + \text{even} &= \text{even} \\
0+1 & \equiv 1 \mod 2 & \text{even} + \text{odd} &= \text{odd} \\
1+1 & \equiv 0 \mod 2 & \text{odd} + \text{odd} &= \text{even}
\end{align*}
\]

\[
\begin{align*}
0 \cdot 0 & \equiv 0 \mod 2 & \text{even} \cdot \text{even} &= \text{even} \\
0 \cdot 1 & \equiv 0 \mod 2 & \text{even} \cdot \text{odd} &= \text{even} \\
1 \cdot 1 & \equiv 1 \mod 2 & \text{odd} \cdot \text{odd} &= \text{odd}
\end{align*}
\]

\[
\begin{pmatrix}
0 & 1 & 2 \\
1 & 2 & 0 \\
2 & 0 & 1
\end{pmatrix}
\]
\[ \begin{array}{cccc} 
0 & 1 & 2 & 3 \\
0 & 0 & 1 & 2 \\
1 & 2 & 3 & 0 \\
2 & 3 & 0 & 1 \\
3 & 0 & 1 & 2 \\
\end{array} \]

\[ \begin{array}{cccc} 
0 & 1 & 2 & 3 \\
0 & 0 & 0 & 0 \\
1 & 0 & 1 & 2 \\
2 & 0 & 2 & 0 \\
3 & 0 & 3 & 2 \\
\end{array} \]

Q, R, C

2) \( \mathbb{Z} / n \mathbb{Z} \) is a ring, \( R \)

- commutative, associative
- additive inverses
- commutative, associative

\[ \text{It distributes over addition} \]

\[ \text{ie, } a \cdot (b + c) = ab + ac. \]

If \( \forall a \in R, \ a \neq 0 \), \( \exists b \in R \) s.t. 

\[ ab = 1, \text{ then } R \text{ is called a field.} \]