Strange Algorithm

Start with $a \in \mathbb{N}$, $a_0 = a$.
If a_0 is even, then $a_1 = a_0/2$
If a_0 is odd, then $a_1 = 3a_0 + 1$

Iterate

$5, 16, 8, 4, 2, 1, 4, 2, 1, 4, 2, 1, \ldots$

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

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

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

$ax + by$; $x, y \in \mathbb{Z}$

What numbers (integers) this way?

If $d \mid a$, $d \mid b$, then

$d \mid ax + by$ for $x, y \in \mathbb{Z}$.

$\gcd(a,b) \mid (ax+by) \quad \forall x, y$

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 $\exists\, x,y \in \mathbb{Z}$ s.t. $g = ax+by$, then g will have to be the smallest positive integer expressed.

$$22x + 60y = \gcd(22,60)$$

First find the gcd:

$$60 = 2 \times (22) + 16$$
$$22 = 1 \times 16 + 6$$
$$16 = 2 \times 6 + 4$$
$$6 = 1 \times 4 + 2 \quad \gcd.$$
$$4 = 2 \times 2 + 0$$

$$\underset{a}{60} = 2 \times \underset{b}{22} + \underset{r_1}{16}, \quad \underset{r_1}{16} = 60 - 2 \times 22$$
$$= a - q_1 b$$
$$= a \cdot \underset{x}{1} - b \cdot \underset{y}{q_1}$$

$$22 = 1 \times 16 + 6$$
$$b = q_2 \times r_1 + r_2$$

$r_2 = b - q_2 \times r_1 = b - q_2(a \cdot 1 - bq_1)$

$= -q_2 a + (1 + q_1 q_2) b$

$r_3 =$

$\vdots$

$r_n = \ ?\,a + ?\,b$

$60 = 2 \times 22 + 16, \quad 16 = a - 2b$

$22 = 1 \times 16 + 6, \quad 6 = 3b - a$

$16 = 2 \times 6 + 4, \quad 4 = 16 - 2 \times 6 = 3a - 8b$

$2 = -4a + 11b.$

$a = q_1 b + r_1$

$b = q_2 r_1 + r_2$

$r_1 = q_3 r_2 + r_3$

$\vdots$

$r_{n-2} = q_n r_{n-1} + r_n$

$r_{n-1} = q_{n+1} r_n$

$a = q_1 b + r_1, \quad r_1 = a - q_1 b$

$b = q_2 r_1 + r_2, \quad r_2 = b - q_2 r_1$

$$= b - q_2(a - q_1 b)$$
$$= -q_2 a + (1 + q_1 q_2) b$$

$r_1 = q_3 r_2 + r_3$, $\quad r_3 = r_1 - q_3 r_2$
$$= (a - q_1 b) - q_3(-q_2 a + (1+q_1 q_2) b)$$
$$= (1 + q_1 q_2)\, a + (-q_1 - q_3 - q_1 q_2 q_3)\, b$$

$\vdots$

<u>QED</u>

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 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 $p \mid a$, 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

$$ax + py = 1 \quad , \text{ for } x, y \in \mathbb{Z}$$

Multiply by b

$$abx + pby = b$$

$p \mid pby$, $p \mid abx$ since $p \mid ab$.

So $p \mid b$.

QED

Theorem If $p \mid (a_1 \cdots a_n)$, 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 $p \nmid a_1$.

$p \mid a_1 a_2 \cdots a_n = a_1 (a_2 \cdots a_n)$

by the lemma it divides $p \mid a_2 \cdots a_n$.

Fundamental Theorem of Arithmetic

Every $n \geq 2$ can be factored into primes

$$n = p_1 \cdots p_k$$

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

$\underline{n=3}$

$\ldots -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, \ldots$

Every integer $a \equiv$ 0, 1 or 2 mod 3

This 0, 1, 2, is the remainder of a after dividing by 3.

$\underline{n=2}$ 0, 1

$\underline{n=4}$ 0, 1, 2, 3 mod 4

Let n be >1.

$\mathbb{Z}/n\mathbb{Z}$ means $\{0,1,2,\dots,n-1\}$
but thought of as the remainders you get on dividing by n.

$\mathbb{Z}/n\mathbb{Z}$

you can add, and multiply

$\mathbb{Z}/2\mathbb{Z}$ $\{0,1\}$

$0+0 \equiv 0 \mod 2$ even+even = even

$0+1 \equiv 1 \mod 2$ even + odd = odd

$1+1 \equiv 0 \mod 2$ odd + odd = even

$0\cdot 0 \equiv 0 \mod 2$ even·even = even

$0\cdot 1 \equiv 0 \mod 2$ even·odd = even

$1\cdot 1 \equiv 1 \mod 2$ odd·odd = odd

$\mathbb{Z}/3\mathbb{Z}$ $(0,1,2)$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\boxed{\mathbb{Z}/4}$

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$

$\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ is a commutative <u>ring</u>, R

- $+$ commutative, associative
- 0, additive inverses
- $\cdot$ commutative, associative
  it distributes over addition
  i.e., $a\cdot(b+c) = ab + a\cdot c$.

If $\forall\, a \in R$, $a \neq 0$, $\exists\, b \in R$ s.t.
$ab = 1$, then R is called a field.