Solving Linear Congruences

How many solutions does $ax \equiv b \pmod{m}$ have, for $0 \le x \le m-1$? The answer depends upon a, b, m.

Case 1: $a \perp m$

We have seen $ax \pmod{m}$ defines a permutation for $0 \le x \le m-1$. Thus exactly one of them must be b!

Case 2: $g = GCD(a,m) > 1$ $\boxed{ax \equiv b}$

For any solution x, $m \mid (ax-b)$. Since $g \mid m$, $g \mid ax-b$. But since $g \mid ax$ and $g \mid b \Rightarrow g \mid ax-b$. Thus there can be no solutions!

ex: $2x \equiv 1 \pmod{4}$ has no solutions

Case 3: $g = GCD(a,m) > 1$ $\boxed{g \mid b}$

Since this is the case we can divide all terms by g. $ax \equiv b \pmod m \iff \frac{a}{g}x \equiv \frac{b}{g} \pmod{\frac{m}{g}}$.

why? $m \mid ax - b \Rightarrow \frac{m}{g} \mid \frac{(ax-b)}{g}$ and

$\frac{m}{g} \mid \frac{(ax-b)}{g} \Rightarrow g\left(\frac{m}{g}\right) \mid \frac{g(ax-b)}{g}$

But now $\frac{a}{g} \perp \frac{m}{g}$, so this second congruence has exactly one solution $0 \le x' < \frac{m}{g}$. Any multiple of $\frac{m}{g}$ $+x'$ is a solution of the second congruence, and there are g distinct k such that $0 \le x' + k\frac{m}{g} \le m-1$

So there are g distinct solutions!

Ex: $12x \equiv 18 \pmod{30} \Rightarrow 2x' \equiv 3 \pmod 5$

$2(4) \equiv 3 \pmod 5$

$X = \{4, 9, 14, 19, 24, 29\}$

But how do we find the solution?

We know how to count the number of solutions, and reduce our problem to a congruence with exactly one solution - but how do we solve that?

$$863x \equiv 880 \pmod{2151}$$

We can reduce the problem to one with a smaller modulus, as follows

$$ax \equiv b \pmod{m} \text{ or } my \equiv -b \pmod{a}$$

Since a can be reduced mod m, the new modulus is strictly smaller than m. Further, if y solves the second congruence, $x = (my+b)/a$ solves the first!

Why? $my \equiv -b \pmod{a} \Rightarrow a \mid my+b \Rightarrow$

$xa = my+b$ for some integer $x = \frac{my+b}{a}$

This x solves the first congruence!

$$a\left(\frac{my+b}{a}\right) = \boxed{my+b \equiv b \pmod{m}}$$

This gives us an algorithm to solve any linear congruence → keep reducing the modulus until we can solve it, then work backwards.

Ex: $863x \equiv 880 \pmod{2151}$

$my \equiv -b \bmod a$

$x = \frac{my+b}{a}$

$\Rightarrow 2151y \equiv -880 \pmod{863}$

$425y \equiv 846 \pmod{863}$

$\Rightarrow 863z \equiv -846 \pmod{425}$

$13z \equiv 4 \pmod{425}$

$\Rightarrow 425w \equiv -4 \pmod{13}$

$9w \equiv 9 \pmod{13}$

$w \equiv 1 \pmod{13}$

$z = (425 \cdot 1 + 4)/13 = 33$

$y = (33 \cdot 863 + 846)/425 = 69$

$x = (2151 \cdot 69 + 880)/863 = \boxed{173}$

$863 \cdot 173 \equiv 880 \pmod{2151}$

$69 \cdot 2151 = 863 \cdot 173 - 880$

Systems of Congruences

Sometimes we are confronted with a series of congruences, and it is asked whether there is an integer which satisfies all of them.

$x \equiv 1 \pmod 5$ $\quad x = \{1, 6, \ldots\}$

$x \equiv 0 \pmod 2$ $\quad x = \{0, 2, 4, 6, 8\}$

YES, $x = 6$

$x \equiv 1 \pmod 4$ $\quad x = \{1, 5, 9, 13, 17, 21, \ldots\}$

$x \equiv 2 \pmod 6$ $\quad x = \{2, 8, 14, 20, 26 \ldots\}$

No - evens + odds

Sun Tsŭ solved the problem around 350 AD with the Chinese Remainder Theorem

The Chinese Remainder Theorem

Let $M = m_1 m_2 \cdots m_r$ and $m_i \perp m_j$ $i \neq j$.
Any system of congruences $x \equiv a_i \pmod{m_i}$ $1 \leq i \leq r$
has exactly one solution $\pmod{M}$

Proof: It is clear $\frac{M}{m_j}$ must be an integer
for any m_j, and $m_j \perp \frac{M}{m_j}$.

Thus $\exists$ integer b_j such that $\left(M/m_j\right) b_j \equiv 1 \pmod{m_j}$

Further, $\left(M/m_j\right) b_j \equiv 0 \pmod{m_i}$ if $i \neq j$.

Let $x_0 = \sum_{j=1}^{r} \frac{M}{m_j} b_j a_j$.

x_0 satisfies each congruence since

$$x_0 \equiv \sum_{j=1}^{r} \frac{M}{m_j} b_j a_j \equiv \frac{M}{m_i} b_i a_i \equiv a_i \pmod{m_i}$$

■

Ex: $x \equiv 3 \pmod 4$ $x \equiv 4 \pmod 5$ $x \equiv 3 \pmod 7$

$M = 4 \cdot 5 \cdot 7 = 140$

$\frac{140}{4}(b_1) \equiv 1 \pmod 4$ $\quad b_1 = -1$

$\frac{140}{5}(b_2) \equiv 1 \pmod 5$ $\quad b_2 = 2$

$\frac{140}{7}(b_3) \equiv 1 \pmod 7$ $\quad b_3 = -1$

$X_0 = \frac{140}{4}(-1)(3) + \frac{140}{5}(2)(4) + \frac{140}{7}(-1)(3)$

$= -105 + 224 + -60 = \boxed{59}$

$59 \bmod 4 = -1 = 3$ ✓

$59 \bmod 5 = -1 = 4$ ✓

$59 \bmod 7 = 3$ ✓

Note that the Chinese Remainder Theorem also gives another way to solve linear congruences if we can factor the modulus, since

$$ax \equiv b \pmod{m_1 m_2 \cdots m_r} \iff \begin{cases} ax \equiv b \pmod{m_1} \\ ax \equiv b \pmod{m_2} \\ \vdots \\ ax \equiv b \pmod{m_r} \end{cases}$$

Proof:

$m_1 m_2 \cdots m_r \mid (ax-b) \rightarrow m_1 \mid (ax-b)$

$m_1 \mid (ax-b) \text{ and } m_2 \mid (ax-b) \rightarrow \operatorname{LCM}(m_1, m_2) \mid (ax-b)$

$\operatorname{LCM}(m_1, m_2) = m_1 \cdot m_2$ if $m_1 \perp m_2$

Ex: $19x \equiv 1 \pmod{140} \iff$

$19x \equiv 1 \pmod{4}$ ↓ $x \equiv 3 \pmod{4}$

$19x \equiv 1 \pmod{5}$ ↓ $x \equiv 4 \pmod{5}$

$19x \equiv 1 \pmod{7}$ ↓ $x \equiv 3 \pmod{7}$

Since these are the system of the previous example $x = 59$

The Euler ϕ - Function

$\phi(N)$ is the number of integers less than N which are relatively prime to N, from 0 to $N-1$

$\phi(1) = 1$

$\phi(p) = p-1$, if p is prime:

N	1	2	3	4	5	6	7	8	9	10	11	12
$\phi(N)$	1	1	2	2	4	2	6	4	6	4	10	4

This is true because 1 is relatively prime to everything.

Computing $\phi(N)$ is clearly no easier than testing primality

Sylvester - the first Jewish professor in America, and who fled UVA when he shot at a student called $\phi(N)$ the totient function.

A function is multiplicative when
$f(ab) = f(a)\,f(b)$ whenever $a \perp b$.

$f(x) = x$ is multiplicative

$f(x) = x^a$ is multiplicative

$\phi(x)$ is multiplicative

Proof:

$\phi(p^k) = \underbrace{p^k}_{N} - \underbrace{p^{k-1}}_{\{0,\ p,\ 2p,\ 3p \cdots (p^{k-1})\}}$ if p is prime:

If not, $M = M_1 M_2$, $M_1 \perp M_2$

$N \perp M \iff N \bmod M_1 \perp M_1$ and $N \bmod M_2 \perp M_2$ } from GCD algorithm

Each N, $0 \le N < M$ is determined by its residues MOD M_1 & M_2

Thus the pairs of residues which define the integers relatively prime to m are made up of integers relatively prime to M_1, M_2,

So $\phi(M_1 M_2) = \phi(M_1)\,\phi(M_2)$ ∎

The Farey Sequence

If we construct mediants in order of increasing denominators, we get the Farey Sequence

1	$\frac{0}{1}$								$\frac{1}{1}$
2	$\frac{0}{1}$			$\frac{1}{2}$					$\frac{1}{1}$
3	$\frac{0}{1}$		$\frac{1}{3}$	$\frac{1}{2}$		$\frac{2}{3}$			$\frac{1}{1}$
4	$\frac{0}{1}$	$\frac{1}{4}$	$\frac{1}{3}$	$\frac{1}{2}$		$\frac{2}{3}$	$\frac{3}{4}$		$\frac{1}{1}$

The mediant of $\frac{a}{b}, \frac{c}{d}$ is $\frac{a+c}{b+d}$

How many fractions are there in the sequence up to N?

$$\sum_{i=1}^{N} \sum_{J} (J \perp i) = \sum_{i=1}^{N} \phi(i)$$

} Eulers ϕ-function or the totient function

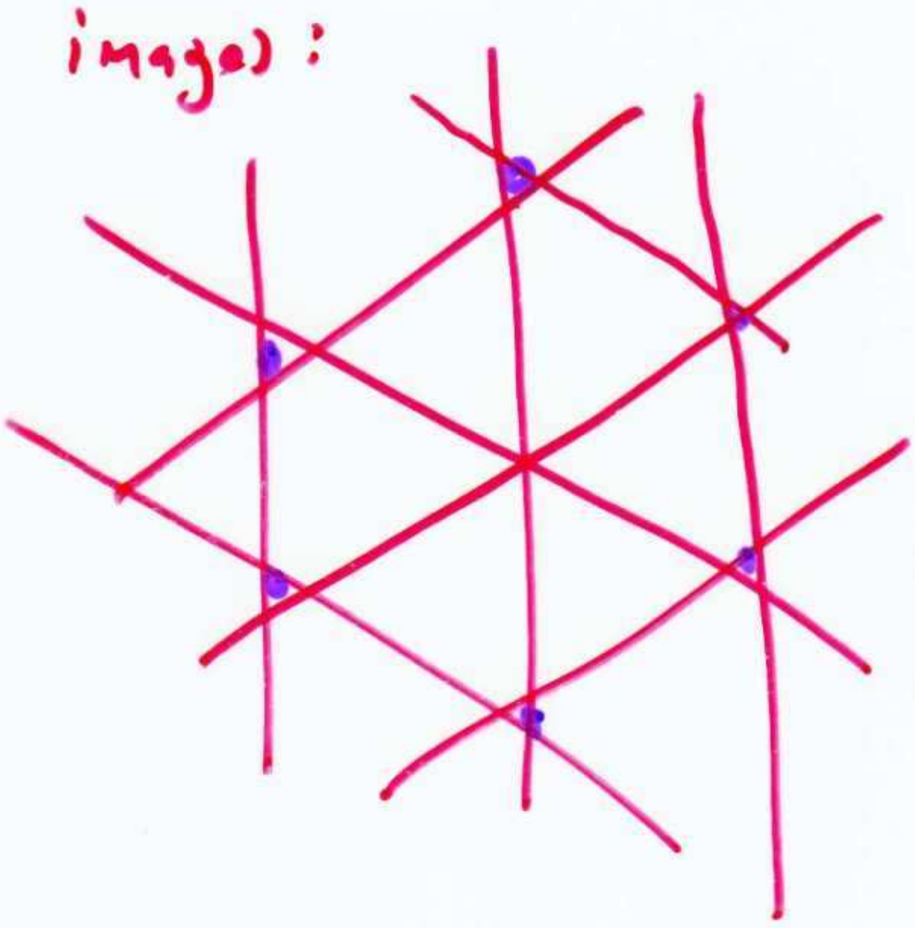
This comes up in asking how many slopes are defined in an NxN lattice?

Independent of reflection ($-m$) and inversion ($1/m$) the Farey sequence describes all slopes in the lattice.

Since $\sum_{i=1}^{N} \phi(i) \sim 3N^2/\pi^2 + O(N \log N)$, there are a quadratic number of slopes.

Counting k-projections of a Point Set

For an arrangment of N points, a k-projection is a direction whose perpendicular defines $\leq k$ point images:

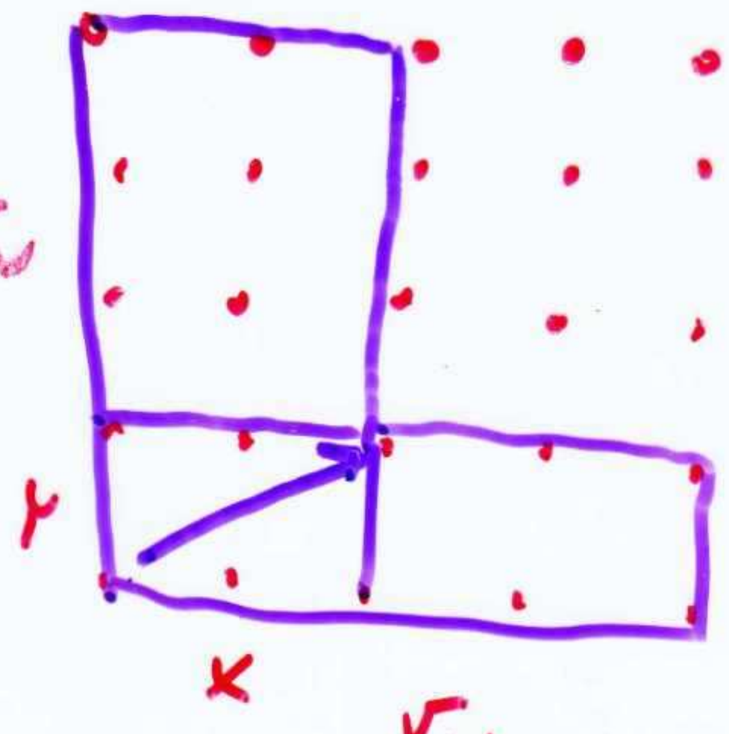


A regular 2N-gon contains N N-Projections, so $V_k(N)$, the maximum number of k projections on N-points, $V_N(2N) \geq N$

In my thesis, I prove "tight" bounds on $V_k(N)$ for all k, N.

In general, how can we make a lot of k-projections for a wide-range of k?

Try an integer lattice:



The size of the projection defined by slope X/y is the number of points in the L-shaped region: $\sqrt{N}(x+y) - xy$

Thus we know a $N^q \times N^q$ portion of the grid, $0 \le q \le N^{1/2}$ defines $\Theta(N^{2q})$ slopes from the Farey Sequence analysis.

For each direction $x < y \le N^q$, so the maximum size of any of these k-projections is $N^{1/2}(2N^q) \approx N^{\frac{2q+1}{2}}$

So there are $\Theta(N^{2q})$ $N^{\frac{2q+1}{2}}$ k-projections which simplify to:

$$V_k(N) \ge \Omega(k^2/N)$$

There is a matching lower bound, so

$$V_k(N) = \Theta(k^2/N), \quad ck \le N \le k^2/c.$$

Solving a congruence

Just like we can solve an equation or an inequality, given a congruence we can determine which values it holds for.

Ex: How many solutions to $X^2 \equiv 1 \pmod{m}$, $0 \leq x < m$?

These are the "square roots of 1 mod n".

Clearly $x > 0$, $x = 1$ is a solution.

One tool we can use is breaking m into its prime factorization $m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$

$a \equiv b \pmod{m}$ and $a \equiv b \pmod{n} \Leftrightarrow$

$a \equiv b \pmod{\text{lcm}(m,n)}$

since $a - b = km = ln$, $p_1^{e_1} p_2^{e_2} \cdots \mid a-b$

$\underbrace{\qquad\qquad}_{n}$

any subset of the union of these two prime factorizations divides $a-b$.

$p_1^{e_1} \cdots \mid a-b$

$\underbrace{\qquad\qquad}_{m}$

Extending this argument, since M is the product of prime factors $M = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$

$a \equiv b \pmod{p_i^{e_i}}$ for $i = 1, \ldots, k$ $\iff$ $a \equiv b \pmod{M}$

Thus if $(X+1)(X-1) \equiv 0 \pmod{M}$

it must be true for each prime factor of M.

$(X+1)(X-1) \equiv 0 \pmod{p_i^{e_i}}$

If $p_i \neq 2$, no prime divides both $X+1$ or $X-1$, thus

$p_i^{e_i} \mid (X+1)$ or $p_i^{e_i} \mid (X-1)$

So there are two solutions, $X = \pm 1$

If $p_i = 2$, 4 cannot divide both $(X+1)$ & $(X-1)$,

so if $4 \mid (X+1) \Rightarrow p_i^{e_i - 1} \mid (X-1)$

if $4 \mid (X-1) \rightarrow p_i^{e_i - 1} \mid (X+1)$

So there are 4 solutions to $(X+1)(X-1) \equiv 0 \pmod{2^k}$

$X = \pm 1$

$X = 2^{k-1} \pm 1$

when $e_i \geq 3$.

Since any integer x mod n is uniquely determined by the residue values for each prime factors of n, and since we have specified the number of residues per prime factor which satisfy the equation, any choice per prime gives a solution.

So the number of solutions is 2^k if n is odd.

Relative Primality

When $\gcd(m,n)=1$, m and n are relatively prime.

$m \perp n \iff m, n$ are integers s.t. $\gcd(m,n)=1$

$k \perp n$ and $k \perp m \iff k \perp mn$

Any reduced fraction m/n has $m \perp n$.

There are two systematic procedures to construct all reduced proper fractions, the second a variant of the first:

To construct a fraction between $\frac{m}{n} + \frac{m'}{n'}$, we can use the mediant $\frac{m+m'}{n+n'}$.

The mediant is $> \frac{m}{n}$ if $m, n, m', n' > 0$, and $\frac{m}{n} < \frac{m'}{n'}$

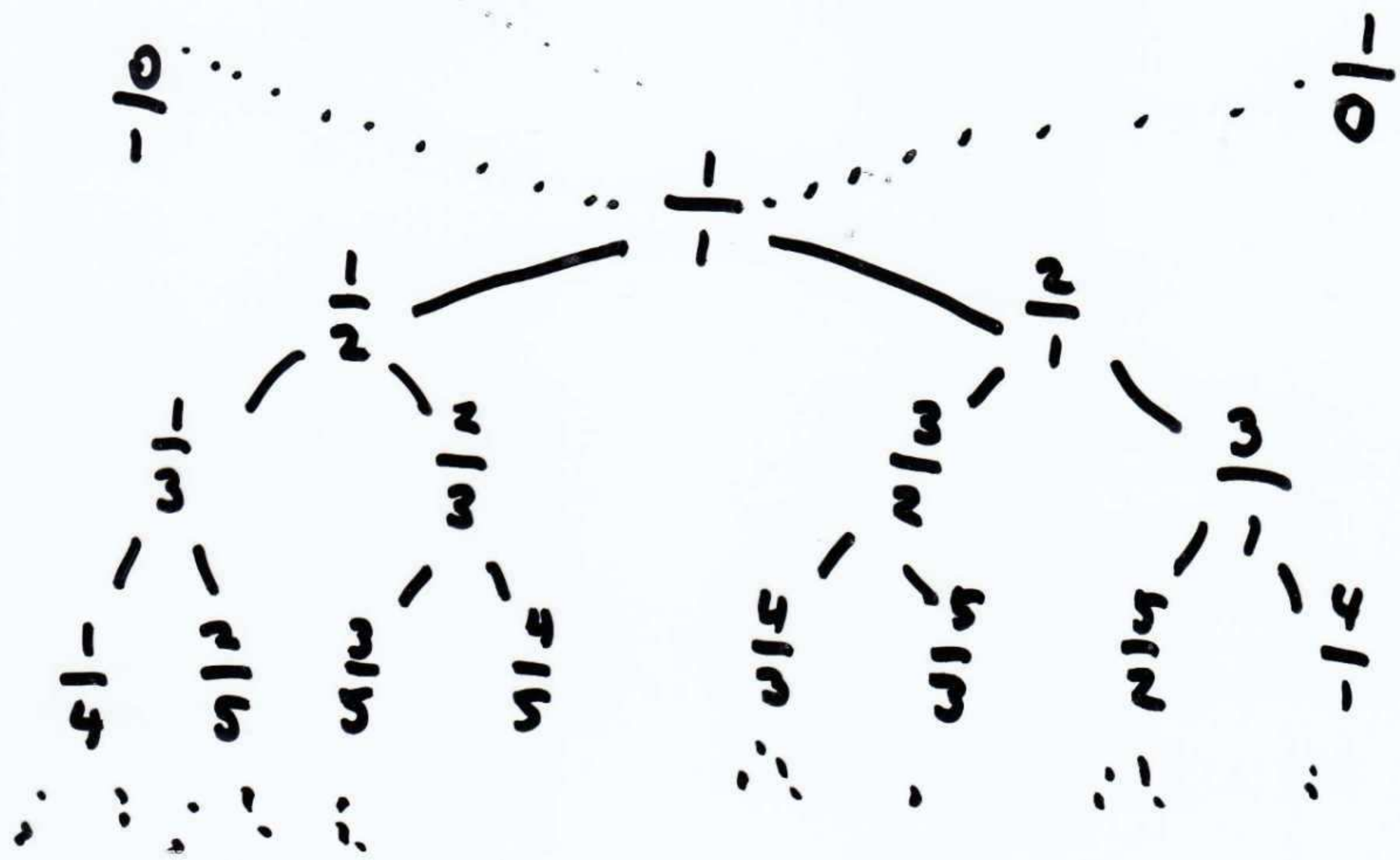
$$\frac{m+m'}{n+n'} - \frac{m}{n} = \frac{n(m+m')-m(n+n')}{n(n+n')} \geq 0$$

$$= nm' \geq mn'$$

$$= \frac{m'}{n'} \geq \frac{m}{n}$$

so the mediant is indeed between the fractions.

If we do this from $0/1$ + $1/0$, we get a tree of fractions:



This infinite tree eventually generates all reduced fractions! By our previous analysis, the new fractions fit between the old.

Between any two adjacent fractions $\frac{m}{n}$, $\frac{m'}{n'}$ in the tree, $mn' - nm' = 1$, since it is true for $\frac{0}{1}$, $\frac{1}{0}$ and

$$\frac{m}{n} < \frac{m+m'}{n+n'} < \frac{m'}{n'}$$

$$n(m+m') - m(n+n')$$
$$= nm' - nm$$

$$(n+n')(m') - (m+m')n' = nm' - nm$$

But how do we know that no fraction is skipped?

By traversing down the tree, the intervals between fractions keeps getting smaller.

$$\frac{m}{n} < \left(\frac{a}{b}\right) < \frac{m'}{n'}$$

At each stage, either $\frac{a}{b}$ is the median, or to the left or right of it.

But at each step, at least 1 is added to either the numerator/denominator of one of the bounds, so it must stop within $a+b$ iterations.

Since this construction gets all the fractions, it gives us a system for representing fractions as strings to L, R: for left and right transitions down the tree.

This gives a binary search algorithm for finding rational approximations to real numbers.

$$e = RL^0RLR^2LRL^4RL^6\ldots$$

Formula for the N^{th} Prime

Jones, Canad. Math. Bull. 18, (1975) pp. 433 gives the following useless but interesting way to calculate the N^{th} prime number.

Wilson's Theorem stated that $(j-1)! \equiv -1 \pmod{j}$ if and only if j is prime.

If j is composite, $(j-1)! \equiv 0 \bmod j$ except $j = 4$, $6 \equiv 2 \bmod 4$. Thus:

$$\left(\left[(j-1)! \right]^2 \bmod j \right) = \begin{cases} (J \text{ is prime}) \end{cases}$$

in Iversonian Notation.

Thus the number of primes less than i, $\pi(i)$,

$$\pi(i) = \sum_{j=1}^{i} \left[(j-1)! \right]^2 \bmod j$$

And since

$$p_i = \sum_{j=0}^{\infty} \left(\pi(j) < i \right)$$

This gives an iversonian formula for the i^{th} prime.

Plugging it in gives

$$P_i = \sum_{k=1}^{\infty}\left(\left(\sum_{j=1}^{i}[(j-1)!]^2 \bmod j\right) < i\right)$$

The sum does not have to go ∞, just greater than the k^{th} prime

Further, since $\underbrace{(q < n)}_{\text{inversion}} = 1 \dot{-} ((1+q) \dot{-} n)$

where $x \dot{-} y = x - y \;,\; x > y$
$x \dot{-} y = 0 \;,\; y \geq x$
} proper subtraction

Thus:

$$P_N = \sum_{i=0}^{N^2}\left(1 \dot{-} \left(\left(\sum_{j=0}^{i}(j-1)!^2 \bmod j\right) \dot{-} N\right)\right)$$

This is not useful for computation but is weird and interesting.

Inversion Formulae

In certain circumstances, it is possible to determine a function if we know the sum of the function:

Ex: $$G(x) = \sum_{i=1}^{x} F(i)$$

Then we know

$$F(x) = G(x) - G(x-1)$$

Thus if it is ever easier to work with the running sum of something, we can do that and convert back later.

The Möbius inversion formula lets us do the same thing over sums taken over divisors:

$$g(n) = \sum_{d \mid n} f(d) \iff f(n) = \sum_{d \mid n} \mu(d)\, g\left(\frac{n}{d}\right)$$

The Mobius Function $\mu(N)$

$$\sum_{d \backslash m} \mu(d) = (m=1)$$ } Iversonian notation

Thus: $\mu(1) = 1$

Further, this sum must equal 0 whenever else.

Thus $\mu(p) = -1$, since $1 + p$ are the only divisors.

what whe $\mu(p^2)$? $\mu(1) + \mu(p) + \mu(p^2) = 0$,

so $\mu(p^k) = 0$, $k > 1$

Since the mobius function is multiplicative, any number N which is divisible by a square, $\mu(N) = 0$.

If N is the product of r distinct prime factors, $\mu(N) = (-1)^r$.

N	1	2	3	4	5	6	7	8	9	10	11	12
$\mu(N)$	1	-1	-1	0	-1	1	-1	0	0	1	-1	0

$$\mu(N) = \begin{cases} (-1)^r & \text{if } n = p_1 p_2 \cdots p_r \\ 0 & \text{if } n \text{ is divisible by some } p^2 \end{cases}$$

Using the Mobius Inversion Formula

Observe $\sum_{d \backslash m} \phi(d) = m$

Clearly true when m is prime: $\phi(1) + \phi(p) = 1 + m - 1$

If $m = p^e$,

$$\sum_{d \backslash m} \phi(d) = \phi(1) + \phi(p) + \phi(p^2) \cdots + \phi(p^e)$$
$$= 1 + p - 1 + p(p-1) \cdots + p^{e-1}(p-1)$$
$$= p^e \quad \text{(telescoping sum)}$$

Now assume true for any m which is the product of as most $\underline{k}$ distinct prime factors:

Suppose $N = p^e m$, $p^e \perp m$

$$\sum_{d \backslash N} \phi(d) = \sum_{d \backslash m} \phi(d) + \sum_{d \backslash m} \phi(pd) + \cdots + \sum_{d \backslash m} \phi(p^e d)$$

$$= \underbrace{\sum_{d \backslash m}}_{\text{induction}} \phi(d) \underbrace{\sum_{i=1}^{e} \phi(p^i)}_{\text{prime pow}} \quad \text{since } \phi \text{ is multiplicative}$$

$$= m \cdot p^e = N$$

∎

So $\sum_{d \mid n} \phi(d) = n$.

We have the sum of $\phi(n)$ over its divisors equalling something reasonable.

Mobius Inversion Formula:

$$g(n) = \sum_{d \mid n} f(d) \iff f(n) = \sum_{d \mid n} \mu(d)\, g\left(\frac{n}{d}\right).$$

Setting $g(n) = n$, $f(n) = \phi(n)$ gives

$$\boxed{\phi(n) = \sum_{d \mid n} n/d\, \mu(d)}$$

Proof of (Möbius Inversion Theorem)

If $g(n) = \sum_{d \mid n} f(d)$, then

$$\sum_{d \mid n} \mu(d)\, g\left(\frac{n}{d}\right) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) g(d)$$ change order of summation.

$$= \sum_{d \mid n} \mu\left(\frac{n}{d}\right) \sum_{k \mid d} f(k)$$ substitution

$$= \sum_{k \mid n} \sum_{d \mid (n/k)} \mu\left(\frac{n}{kd}\right) f(k)$$ interchange order of summation

$$= \sum_{k \mid n} \sum_{d \mid (n/k)} \mu(d)\, f(k)$$ $k \mid d \mid n$ verify substitution by case analysis

$$= \sum_{k \mid n} (n/k = 1)\, f(k)$$ original definition of $\mu(d)$.

$$= f(n)$$ only true of $k = n$.