Chapter 4

Number Theory

This all about the "counting numbers" how hard could it be?

Divisibility (pretty much everything is in $\mathbb{Z}$)

$m \mid n \iff m \neq 0$ &
$n = mk$ for some $k \in \mathbb{Z}$

"m divides n"

$m \nmid n$ "m does not divide n"

Often we say "n is a multiple of m"
$\Longrightarrow$ $n = mk$ but m need not be positive

Thus $\exists$ only one multiple of 0 and nothing is divisible by 0. Every integer is a multiple of -1 but none are divisible by -1!

Can extend multiple/divisibility to any numbers, but we will mostly deal with integers.

$\gcd(m,n) = \max\{k \mid k \backslash m \text{ and } k \backslash n\}$

e.g. $\gcd(12,18) = 6$ (used in fraction simplification calcs.)

Note: if $n > 0$, $\gcd(0,n) = n$, also $\gcd(0,0)$ is undefined. (why?)

$\operatorname{lcm}(m,n) = \min\{k \mid k > 0, m \backslash n \backslash k\}$
(used in common denomenator calcs.)

It is common to study gcd over lcm because of it's nice properties:

with $0 \le m < n$

$\gcd(0,n) = n$;

$\gcd(m,n) = \gcd(n \bmod m, m)$ $m > 0$

$\gcd(12,18) = \gcd(6,12) = \gcd(0,6) = 6$

this forms the basis for Euclid's algorithm

the second statement is true because:

if $a \backslash n$ and m then $a \backslash n \bmod m = n - \left\lfloor \frac{n}{m} \right\rfloor m$

We also get integers m' and n' s.t.

$mm' + nn' = \gcd(m,n)$

Why? $m=0$ choose $m'=0, n'=1$.
let $r = n \bmod m$ & continue via Euclid computing $\bar{r}, \bar{m} \Rightarrow$

$$\bar{r}r + \bar{m}m = \gcd(r, m)$$

$$r = n \bmod m = n - \lfloor \tfrac{n}{m} \rfloor m \qquad \gcd(r,m) = \gcd(m,n)$$

$$\Rightarrow \quad \bar{r}\underbrace{\left(n - \lfloor \tfrac{n}{m} \rfloor m\right)}_{r} + \bar{m}m = \gcd(r,m) = \gcd(m,n)$$

or

$$(\bar{m} - \lfloor \tfrac{n}{m} \rfloor \bar{r})m + \bar{r}n = \gcd(m,n), \text{ thus}$$

choose

$$m' = \bar{m} - \lfloor \tfrac{n}{m} \rfloor \bar{r} \quad , \quad n' = \bar{r}$$

$\gcd(12, 18)$: $6 = 0 \cdot 0 + 1 \cdot 6 = 1 \cdot 6 + 0 \cdot 12$
$= (-1)\,12 + 1 \cdot 18$

d, m', n' together help prove that the result is correct.

Assume that d is not the $\gcd(m,n) = D$

but $D \mid m'm + n'n = d$ so $D \leq d$!

the (m', n', d) are a "self-certifying" proof of gcd correctness

If $k \backslash m$, $k \backslash n \iff k \backslash \gcd(m,n)$

$= m'm + n'n = m'k m_k + n'k n_k = k(m'm_k + n'n_k)$

"$\Leftarrow$" $k \backslash \gcd(m,n) = d$ but $d \backslash m$ and n so

$k \backslash m$ and $k \backslash n$. Any common divisor of m and n is also a divisor of d.

Handy Rule:

$$\sum_{m \backslash n} a_m = \sum_{m \backslash n} a_{n/m} \qquad n \in \mathbb{Z}^+ \quad \circledast$$

e.g. $n = 12$ $\quad a_1 + a_2 + a_3 + a_4 + a_6 + a_{12}$

$=$

$a_{12} + a_6 + a_4 + a_3 + a_2 + a_1$.

more generally

$$\sum_{m \backslash n} a_m = \sum_{k} \sum_{m > 0} a_m [n = mk]$$

for $n > 0$ r.h.s. is $\sum_{k \backslash n} a_{n/k} \Rightarrow \circledast$, and also

this works for negative.

A double sum:

$$\sum_{m \backslash n} \sum_{k \backslash m} a_{k,m} = \sum_{k \backslash n} \sum_{l \backslash (n/k)} a_{k, kl}$$

writing $m = kl$ for $l \backslash \left(\frac{n}{k}\right)$

Consider this when $n = 12$

$$a_{1,1} + (a_{1,2} + a_{2,2}) + (a_{1,3} + a_{3,3}) +$$
$$(a_{1,4} + a_{3,4} + a_{4,4}) + (a_{1,6} + a_{2,6} + a_{3,6} + a_{6,6}) + (a_{1,12} + a_{2,12} +$$
$$+ a_{3,12} + a_{4,12} + a_{6,12} + a_{12,12}) = (a_{1,1} + a_{1,2} + a_{1,3} + a_{1,4} + a_{1,6} + a_{1,12})$$
$$+ (a_{2,2} + a_{2,4} + a_{2,6} + a_{2,12}) + (a_{3,3} + a_{3,6} + a_{3,12}) + (a_{4,4} + a_{4,12})$$
$$+ (a_{6,6} + a_{6,12}) + a_{12,12}$$

To prove this equality we rewrite as:

(n fixed)

$$\sum_{j,l} \sum_{k,m>0} a_{k,m} [n = jm][m = kl] = \text{l.h.s.}$$

$$= \sum_{j} \sum_{k,l>0} a_{k,kl} [n = jlk] \quad \text{and} \quad \text{r.h.s.} =$$

$$\sum_{j,m} \sum_{k,l>0} a_{k,kl} [n = jk][n/k = ml] = \sum_{m} \sum_{k,l>0} a_{k,kl} [n = mlk]$$

Primes: $p \in \mathbb{Z}^+$ is prime if it has only 2 divisors: 1 is not a prime by convention

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, ...

numbers that are not prime are composite

Primes are the "units" of integers via multiplication. Let $n \in \mathbb{Z}^+$ then

$$n = p_1 \cdots p_m = \prod_{k=1}^{m} p_k \quad \circledast \qquad p_1 \le p_2 \le \cdots \le p_m$$

Why? $n > 1$ if not prime has $n_1 \setminus n$ & $n_1 \in n$

so $n = n_1 \cdot n_2$ and we induce on n_1 & n_2.

The prime expansion is unique: the "Fundamental Theorem of Arithmetic."

Consider $x = m + n\sqrt{10}$ $\quad m, n \in \mathbb{Z}$

the set of such x's is closed under mult. Can define a "prime" here for x's that cannot be nontrivially factored:

$6 = 2 \cdot 3 = (4+\sqrt{10})(4-\sqrt{10})$ is not "prime," but

$2, 3, 4+\sqrt{10}, 4-\sqrt{10}$ are prime, so no unique factorization here!

Proof of unique prime factorization in $\mathbb{Z}^+$:

For $n = 1$ there is only one factorization, the empty product in $\circledast$.

$n > 1$: $n = p_1 \cdots p_m = q_1 \cdots q_k \quad p_1 \le \cdots \le p_m, \; q_1 \le \cdots \le q_k$

assume the p's & q's are prime. Will prove $p_1 = q_1$, if not $p_1 \neq q_1$ WLOG & $p_1 < q_i$ $i = 1, \dots, k$

$\gcd(p_1, q_1) = 1 = ap_1 + bq_1 \Rightarrow ap_1(q_2 \cdots q_m) + bq_1(q_2 \cdots q_m) = q_2 q_3 \cdots q_k$

$= ap_1(q_2 \cdots q_m) + bn$ so $p_1 \mid (q_2 \cdots q_m)$ so

$q_2 \cdots q_k$ has a prime factorization including p_1,

but $q_2 \cdots q_k < n$ so it has a unique factorization

and we get a contradiction $\Rightarrow p_1 = q_1$. Other factors work the same way. □

Often see FTA $n = \prod_p p^{n_p}$, all $n_p \geq 0$

$\langle n_2, n_3, n_5, \dots \rangle$ uniquely describes n, so it can be thought of as a number system

$12 \sim \langle 2, 1, 0, 0, \dots \rangle$ $18 \sim \langle 1, 2, 0, 0, \dots \rangle$

$k = mn \iff k_p = m_p + n_p \quad \forall p$

$m \mid n \iff m_p \leq n_p \quad \forall p$

$k = \gcd(m, n) \iff k_p = \min(m_p, n_p) \quad \forall p$

$k = \operatorname{lcm}(m, n) \iff k_p = \max(m_p, n_p) \quad \forall p$

e.g. $\gcd(12, 18) = 2^{\min(2,1)} \cdot 3^{\min(1,2)} = 2 \cdot 3 = 6$

$\operatorname{lcm}(12, 18) = 2^{\max(2,1)} \cdot 3^{\max(1,2)} = 2^2 \cdot 3^2 = 36$

If $p \mid mn$ then $p \mid m$ and/or $p \mid n$

but if $c \mid mn$ it may not divide either.
e.g. $4 \mid 60$ but $4 \nmid 6$ and $4 \nmid 10$!

How many primes are there? Euclid knew there were infinitely many: suppose not, then there are $2, 3, 5, \ldots, P_k$ consider $M = 2 \cdot 3 \cdot 5 \cdots P_k + 1$

$p_i \nmid M$ $i = 1, \ldots, k$ thus either M is prime or $\exists\ p_j > P_k \Rightarrow p_j \mid M \Longrightarrow$ there is no largest prime, infinitely many.

Can define Euclid number $e_n = e_1 e_2 \cdots e_{n-1} + 1$, $n \geq 1$
(empty product)

$e_1 = 1 + 1$

$e_2 = 2 + 1$, $e_3 = 2 \cdot 3 + 1 = 7$, $e_4 = 2 \cdot 3 \cdot 7 + 1 = 43$

they are all prime, but $e_5 = 1807 = 13 \cdot 139$, e_6 is prime, $e_7 = 547 \cdot 607 \cdot 1033 \cdot 31051$

$e_8 = 29881 \cdot 67003 \cdot 9119521 \cdot 6212157481$

$e_9, \ldots, e_{17}$ are composite. However:

$$\gcd(e_m, e_n) = 1, \quad \text{when } m \neq n$$
(like primes)

$e_n \bmod e_m = 1$ when $n > m$, so

$\gcd(e_m, e_n) = \gcd(1, e_m) = \gcd(0, 1) = 1$

Let g_j be the smallest factor (prime) of e_j, then $g_1, g_2, g_3, \ldots$ are all different, and thus this sequence contains ∞-many primes.

The recurrence for e_n is: $n > 0$

$$e_n = e_1 e_2 \cdots e_{n-1} + 1 = (e_{n-1} - 1) e_{n-1} + 1 = e_{n-1}^2 - e_{n-1} + 1$$

Thus e_n has about twice as many digits as e_{n-1}

Can prove that ← rounding

$$e_n = \left\lfloor E^{2^n} + \frac{1}{2} \right\rfloor, \; E \approx 1.264 \ldots, \text{ also}$$

$$p_n = \lfloor P^{3^n} \rfloor \text{ for some } P \text{ constant}$$

has p_n prime $\forall n$. In both cases E, P are "computed" from e_n, p_n.

Nobody knows a formula that gives only primes!

a number of the form $2^p - 1$ with p, prime is a Mersenne number, when prime it is called a Mersenne prime. The largest known prime is

$$2^{13466917} - 1 = (111\ldots1)_2$$

has 4,053,946 decimal digits $\sim$ 5000 pages of text.

Mersenne primes are the 5 largest known primes because testing a Mersenne number for primality is easy with the Lucas-Lehmer test.

Mersenne exponents that are prime are 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, ...

Why must p be prime for 2^p-1 to be prime?

$2^{mk}-1 = (2^m-1)(2^{m(k-1)}+2^{m(k-2)}+\cdots+2^m+1)$

(proof by contradiction).

However 2^p-1 is not always prime $2^{11}-1 = 2047 = 23 \cdot 89$

Note something akin to Lucas-Lehmer works for integers of the form $2^n k+1$ for small k. Perhaps one could find bigger primes this way.

How many primes are there? ∞

Are there more evens or perfect squares?

n^{th} $2n$ n^2 ↺ n^{th} even occurs quicker than n^{th} square

up to x $\lfloor \frac{x}{2} \rfloor$ even integers ← bigger

$\lfloor \sqrt{x} \rfloor$ perfect squares

$P_n \sim n \ln n$ (n^{th} prime)

"asyptotic to" $\lim_{n\to\infty} P_n / n\ln n = 1$

$\pi(x) = \#\{p \mid p \le x\} \sim \frac{x}{\ln x}$

$2n < P_n < n^2$ (evens → P_n ← squares; P_n: primes)

more exactly

$\ln x - \frac{3}{2} < \frac{x}{\pi(x)} < \ln x - \frac{1}{2} \quad x \ge 67$

$n(\ln n + \ln\ln n - \frac{3}{2}) < P_n < n(\ln n + \ln\ln n - \frac{1}{2}) \quad n \ge 20$

If n is a random integer $\ln n^{-1}$ is the chance it will be prime.

e.g. $n = 10^{16}$ $16 \ln 10 \approx 36.8$

between $10^{16} - 370 \cdot 10^{16} - 1$ there are 10 primes!

However, prime distribution has irregularities: all numbers are composite in the interval:

$(p_1 p_2 \cdots p_n + 2,\ p_1 p_2 \cdots p_n p_{n+1} - 1)$

There are also twin primes $(p, p+2)$

$(5,7)$; $(11,13)$; $(17,19)$; $(29,31)$; ...

are there infinitely many?

Have all seen Sieve of Eratosthenes to calc. all $\pi(x)$ primes less than x.

② 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ ... x

every other, every third, ... circled numbers are primes.

Factorial Factors:

$$n! = 1 \cdot 2 \cdot 3 \cdot \ldots n = \prod_{k=1}^{n} k, \quad n \in \mathbb{Z} \geq 0$$

$$0! = 1 \quad \text{(empty product)}$$

$n! = n \cdot (n-1)!$ number of distict permutations of n things "arises frequently in combinatorics"

n	0	1	2	3	4	5	6	7	8	9	10
$n!$	1	1	2	6	24	120	720	5040	40320	362880	3628800

$10! \sim 3.5 \times 10^6$ # of digit in $n!$ n when $n \geq 25$.

$$(n!)^2 = (1 \cdot 2 \cdot \cdots \cdot n)(n \cdot n-1 \cdot \cdots \cdot 2 \cdot 1) = \prod_{k=1}^{n} k(n+1-k)$$

$$n \leq k(n+1-k) \leq \left(\frac{n+1}{2}\right)^2$$

$$\prod_{k=1}^{n} n \leq (n!)^2 \leq \prod_{k=1}^{n} \left(\frac{n+1}{2}\right)^2$$

$$n^{n/2} \leq n! \leq \left(\frac{n+1}{2}\right)^n$$

Stirling: $n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$

$\sqrt{2\pi 10}\left(\frac{10}{e}\right)^{10}$ is $\frac{1}{120}$ too small to 10!

What is the largest power of p that divides $n!$?

$\varepsilon_p(n!)$	1	2	3	4	5	6	7	8	9	10	Power of 2
divisible by 2		x		x		x		x		x	$5 = \lfloor 10/2 \rfloor$
" " 4				x				x			$2 = \lfloor 10/4 \rfloor$
" " 8								x			$1 = \lfloor 10/8 \rfloor$

columns form $\rho(k)$ ruler function; $\varepsilon_2(10!) = 8$.

$$\varepsilon_2(n!) = \left\lfloor \frac{n}{2} \right\rfloor + \left\lfloor \frac{n}{4} \right\rfloor + \cdots = \sum_{k \geq 1} \left\lfloor \frac{n}{2^k} \right\rfloor$$

(sum is finite)

$\varepsilon_2(100!) = 50 + 25 + 12 + 6 + 3 + 1 = 97$

recall: $\left\lfloor \frac{n}{2^{k+1}} \right\rfloor = \left\lfloor \left\lfloor \frac{n}{2^k} \right\rfloor / 2 \right\rfloor$, let's look in binary

$$\begin{aligned}
100 &= (1100100)_2 = 100 \\
\lfloor 100/2 \rfloor &= (110010)_2 = 50 \\
\lfloor 100/4 \rfloor &= (11001)_2 = 25 \\
\lfloor 100/8 \rfloor &= (1100)_2 = 12 \\
\lfloor 100/16 \rfloor &= (110)_2 = 6 \\
\lfloor 100/32 \rfloor &= (11)_2 = 3 \\
\lfloor 100/64 \rfloor &= (1)_2 = 1
\end{aligned}$$

thus each term is just the right-shift (with truncation) of the previous term.

Note: each 1 in the binary rep. of n contributes 2^n to n and $2^{n-1}|$ to $\varepsilon_2(n!)$. Thus sum up all the 1's to get n and you have $\nu_2(n)$ of them:

$$\varepsilon_2(n!) = n - \nu_2(n)$$

In general $\varepsilon_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor$,

how big is $\varepsilon_p(n!)$?

$$\varepsilon_p(n!) < \frac{n}{p} + \frac{n}{p^2} + \cdots = \frac{n}{p}\left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right)$$

$$= \frac{n}{p}\left(\frac{p}{p-1}\right) = \frac{n}{p-1}$$

$p = 2$, $n = 100$ $\quad 97 < 100$

$n - \nu_2(n) \sim n$ as $\nu_2(n) \leq \lceil \lg n \rceil \ll n$

p's contribution to $n!$ is $p^{\varepsilon_p(n!)}$,

$$\varepsilon_p(n!) \quad p^{\varepsilon_p(n!)} < p^{n/(p-1)}$$

also $p \leq 2^{p-1}$: $p^{n/p-1} \leq \left(2^{(p-1)}\right)^{n/p-1} = 2^n$, use this for another proof that there are ∞ primes.

Assume not : $2, 3, \ldots, p_k \leftarrow$ largest

$$n! < (2^n)^k = 2^{nk} \quad \forall n$$

Choose $n = 2^{2k}$: $n! < 2^{nk} = 2^{2^{2k} k} = n^{n/2}$

but we proved $n! \geq n^{n/2}$, a contradiction!

Also: $n! < 2^{n\pi(n)}$, using Stirling

$$\sqrt{2\pi n}\left(\frac{n}{e}\right)^n < n! < 2^{n\pi(n)}$$

$$\tfrac{1}{2}\lg(2\pi n) + n\lg(n/e) < n\pi(n)$$

$$\lg\left(\frac{n}{e}\right) \leq \pi(n) \quad \text{weak lower bd.}$$

Relative Primality $\gcd(m,n) = 1$ "relatively prime"

new notation $m \perp n \iff m, n \in \mathbb{Z}$ & $\gcd(m,n) = 1$

$\frac{m}{n}$ is in lowest terms $\iff m \perp n$

$\frac{m}{d} \perp \frac{n}{d}$, $d = \gcd(m,n)$ follows from $\gcd(km, kn) = k\gcd(m,n)$. More facts

$$m \perp n \iff \min(m_p, n_p) = 0 \quad \forall p$$
$$\text{"} \iff m_p n_p = 0 \quad \forall p$$

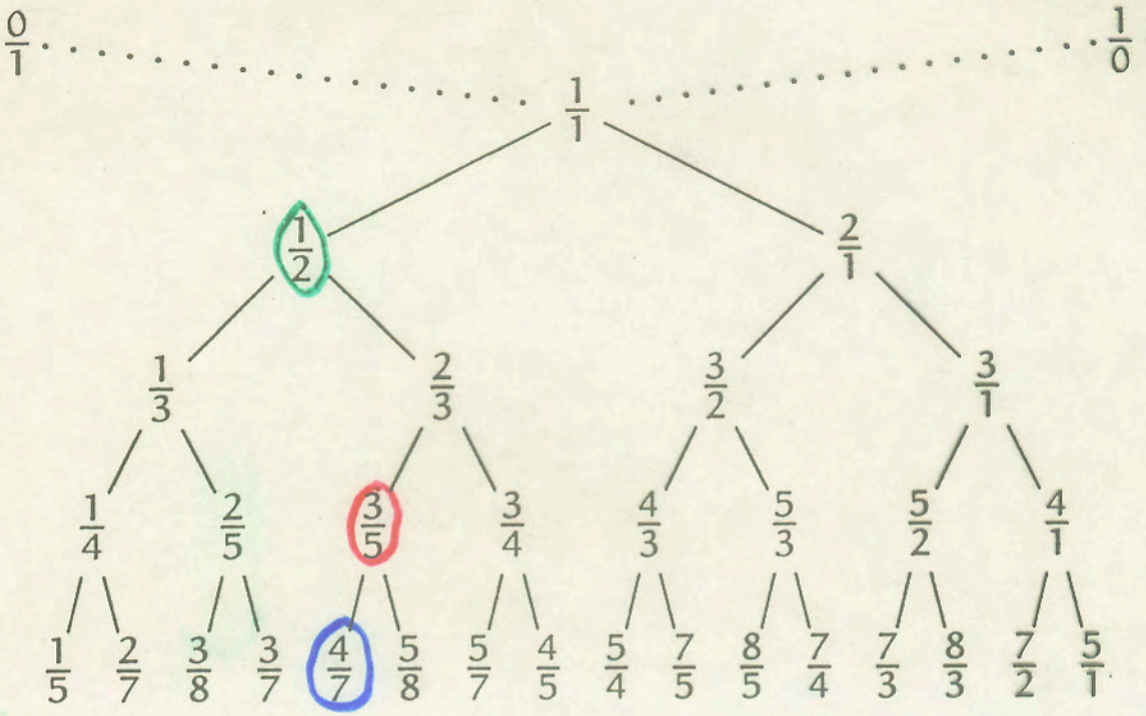
$$k \perp m \text{ & } k \perp n \iff k \perp mn$$
$$\iff k_p m_p > 0 \text{ & } k_p n_p = 0 \iff k_p(m_p + n_p) = 0 \; \forall p$$

Stern-Brocot Tree: all non-neg. $\frac{m}{n}$ with $m \perp n$

↑ German mathematician ↖ French clock maker

Idea: begin with $(\frac{0}{1}, \frac{1}{0})$, repeat as desired

insert $\frac{m+m'}{n+n'}$ between $\frac{m}{n}$ & $\frac{m'}{n'}$, adjacent

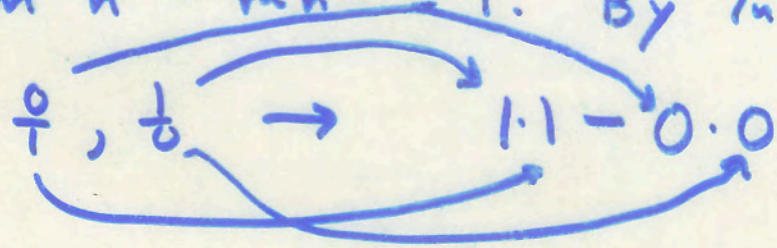


e.g. $\frac{1}{2} = \frac{m}{n}$ $\frac{3}{5} = \frac{m'}{n'}$, $\frac{m+m'}{n+n'} = \frac{4}{7}$

↑ nearest up & left ↑ nearest up & right

Why does $\frac{m+m'}{n+n'}$ always end up in lowest term?

If $\frac{m}{n}$ & $\frac{m'}{n'}$ are consecutive in the construction then: $m'n - mn' = 1$. By induction



when we insert $\frac{m+m'}{n+n'}$ it becomes consecutive to either $\frac{m}{n}$ or $\frac{m'}{n'}$, two cases:

1: $(m+m')n - m(n+n') = mn + m'n - mn - mn' = 1$

2: $m'(n+n') - (m+m')n' = m'n + m'n' - mn' - m'n' = 1$ □

Thus if $\frac{m}{n} < \frac{m'}{n'} \Rightarrow \frac{m}{n} < \frac{m+m'}{n+n'} < \frac{m'}{n'}$ ← ↖ ↑ mediant of

simple excercise to prove it.

If $\frac{a}{b}$ with $a \perp b$, does it appear somewhere in the list? Yes!

parentheses ⇒ not yet seen

$$\frac{m}{n} = \frac{0}{1} < \left(\frac{a}{b}\right) < \frac{1}{0} = \frac{m'}{n'}$$

at some stage $\frac{m}{n} < \left(\frac{a}{b}\right) < \frac{m'}{n'} \rightarrow \frac{m+m'}{n+n'}$ is inserted next. Either: $\frac{m+m'}{n+n'}$ = Med.

1. Med $= \frac{a}{b}$ (we win) or
2. Med $< \frac{a}{b}$
3. Med $> \frac{a}{b}$, this cannot go on forever

$\frac{a}{b} - \frac{m}{n} > 0 \Rightarrow an - bm \geq 1$

$\frac{m'}{n'} - \frac{a}{b} > 0 \Rightarrow bm' - an' \geq 1$, thus

$$(m'+n')(an-bm) + (m+n)(bm'-an') \geq (m'+n') + (m+n)$$

$$a m'n + \underline{ann'} - \underline{bm'm} - bmn' + \underline{bm'm} + bm'n - an'm - \underline{ann'} =$$

$$a(m'n - n'm) + b(m'n - mn') = a+b$$

↑ ← $= 1$

$a+b \geq m'+n'+m+n$, at each step

either $m'+n'$ or $m+n$ increases, so in at most $a+b$ step $\frac{a}{b}$ appears.

The Farey Series of order N:

$$\left\{ \frac{m}{n} \mid m \perp n,\ m \le n,\ n \le N \right\}$$
arranged in increasing order

$$\mathcal{F}_6 = \left\{ \frac{0}{1}, \frac{1}{6}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{5}{6}, \frac{1}{1} \right\}$$

Start with $\mathcal{F}_1 = \frac{0}{1}, \frac{1}{1}$, can proceed by inserting mediants with appropriate denominator

Note: Stern-Brocot tree never produces a denominator $\le N$ from denom. $> N$, so

$\mathcal{F}_N$ is a subtree of S-B with pruning, also if

$\frac{m}{n}, \frac{m'}{n'}$ are consecutive in $\mathcal{F}_N$

$\Rightarrow m'n - mn' = 1$ (see above in $\mathcal{F}_6$)

Can build up $\mathcal{F}_N$ from $\mathcal{F}_{N-1}$ as follows.

$\mathcal{F}_{N-1}$ lacks $\frac{1}{N}, \frac{2}{N}, \cdots \frac{N-1}{N}$, where to insert them?

$\frac{m+m'}{N}$ is put between $\frac{m}{n}$ & $\frac{m'}{n'}$, $N = n+n'$

$$\mathcal{F}_7 = \frac{0}{1}, \frac{1}{7}, \frac{1}{6}, \frac{1}{5}, \frac{1}{4}, \frac{2}{7}, \frac{1}{3}, \frac{2}{5}, \frac{3}{7}, \frac{1}{2}, \frac{4}{7}, \frac{3}{5}, \frac{2}{3}, \frac{5}{7}, \frac{3}{4}, \frac{4}{5}, \frac{5}{6}, \frac{6}{7}, \frac{1}{1}$$

Not entirely true: if N prime $\mathcal{F}_N$ has $N-1$ more terms than $\mathcal{F}_{N-1}$.

When $m \perp n$ ($\gcd(m,n)$) $\exists\ a, b \Rightarrow ma - nb = 1$, let (*)

$\frac{a}{b}$ precede $\frac{m}{n}$ in $\mathcal{F}_n$, the above follows.

e.g. $3a - 7b = 1$ has $a = 5, b = 2$: $\frac{2}{5}, \frac{3}{7}$ in $\mathcal{F}_7$

So we can always solve (*) with
$0 \le b < a < n$ if $0 < m < n$ or
if $0 < n < m$ or $m \perp n$ can solve (*) with $0 < a < b < m$
by letting $\frac{a}{b}$ follow $\frac{n}{m}$ in $\mathcal{F}_m$.

Can regard Stern-Brocot as a number system.
Each $\frac{m}{n}$ reduced occurs once in S-B.

L → go left down the tree
R → go right down the tree

LRRL $\quad \frac{1}{1} \to \frac{1}{2} \to \frac{2}{3} \to \frac{3}{4} \to \frac{5}{7}$

how to get $\frac{1}{1}$, the root $\frac{1}{1} = I$, identity

1. Given m, n; $m \perp n$ what is string?
2. Given string of L's & R's what is $\frac{m}{n}$?

↑ S = string, what is $f(S)$ ← fraction

right or left requires knowing $\frac{m}{n}$ & $\frac{m'}{n'}$

Keep $M(S) = \begin{pmatrix} n & n' \\ m & m' \end{pmatrix}$, $M(I) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

is a good starting point.

L: $n' \leftarrow n+n'$; $m' \leftarrow m+m'$

$$M(SL) = \begin{pmatrix} n & n+n' \\ m & m+m' \end{pmatrix} = \begin{pmatrix} n & n' \\ m & m' \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$ ← L

R: $n \leftarrow n+n'$; $m \leftarrow m+m'$

$$M(SR) = \begin{pmatrix} n+n' & n' \\ m+m' & m' \end{pmatrix} = \begin{pmatrix} n & n' \\ m & m' \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$ ← R

So $M(LRRL) = LRRL = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

$= \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}$

$\frac{3}{3} = \frac{m}{n}$, $\frac{3}{4} = \frac{m'}{n'}$ are ancestral to $\frac{m+m'}{n+n'} = \frac{5}{7}$.

Question 1: $R \rightarrow$ gets bigger
$L \rightarrow$ gets smaller, binary search

$S := I$;
while $\frac{m}{n} \neq f(S)$ do
(too big) if $\frac{m}{n} < f(S)$ then (output(L); $S := SL$)
(too small) else (output(R); $S := SR$)

What if we want to operate on m, n instead of maintaining strings of L's, R's?

$$S = \begin{pmatrix} n & n' \\ m & m' \end{pmatrix} \qquad RS = \begin{pmatrix} n & n' \\ m+n & m'+n' \end{pmatrix}$$

So, $f(S) = \frac{m+m'}{n+n'}$ $f(RS) = \frac{(m+m')+(m'+n')}{n+n'}$

1st step of algor. with $m>n$ will be R,

and $f(RS) = f(S)+1$

if we had begun with $\frac{m-n}{n}$ instead of $\frac{m}{n}$.
Similar behavior when analyzing L first, in summary

$$\frac{m}{n} = f(RS) \iff \frac{m-n}{n} = f(S) \qquad m>n$$

$$\frac{m}{n} = f(LS) \iff \frac{m}{n-m} = f(S) \qquad m<n$$

```
while m ≠ n do
    if m < n  then (output(L); n := n-m)
              else (output(R); m := m-n)
```

e.g. $\frac{5}{7} = \frac{m}{n}$

m =	5	5	3	1	1
n =	7	2	2	2	1
output	L	R	R	L	

Irrationals do not appear in the S-B tree, but using the 1st algorithm we can "approximate"

$$e = RL^0RLR^2LRL^4RLR^6LRL^8RLR^{10}LRL^{12}RL\cdots$$

$$\overset{R}{\tfrac{1}{1}}, \overset{R}{\tfrac{2}{1}}, \overset{L}{\tfrac{3}{1}}, \overset{R}{\tfrac{5}{2}}, \overset{R}{\tfrac{8}{3}}, \overset{L}{\tfrac{11}{4}}, \overset{R}{\tfrac{19}{7}}, \overset{L}{\tfrac{30}{11}}, \overset{L}{\tfrac{49}{18}}, \overset{L}{\tfrac{68}{25}}, \overset{L}{\tfrac{87}{32}}, \overset{R}{\tfrac{106}{39}}, \overset{L}{\tfrac{193}{71}}, \overset{R}{\tfrac{299}{110}}, \ldots$$

these are the "simplest" rational upper/lower bounds to e in order of closeness.

$\frac{878}{323} \approx 2.718266 \approx .999994e$ with 16 letters
about 16 bits accuracy in e!

For α, irrational, we modify the matrix-free

if $\alpha < 1$ then (output(L); $\alpha := \alpha/(1-\alpha)$)
else (output(R); $\alpha = \alpha - 1$).

if α is rational we get ordinary answer but with RL^{ω} appended.

$\alpha = 1$ R ($\alpha = 0$) LLL ...

$\frac{1}{1}, \frac{2}{1}, \frac{3}{2}, \frac{4}{3}, \frac{5}{4}, \rightarrow 1$ in the limit

like $1 = 0.999\overline{9}$. In binary every number has a unique representation not ending in all 1's. In S-B every number has a unique representation not ending in all R's.

In binary is true for $[0,1)$ in S-B $[0,\infty)$

$0 \leftrightarrow L$; $1 \leftrightarrow R$

get a one-to-one order preserving correspondence between $[0,1)$ and $[0,\infty)$!

Given $\alpha = \frac{m}{n}$ we get $\left\lfloor \frac{m}{n} \right\rfloor$ R's then

$\left\lfloor \frac{n}{m \bmod n} \right\rfloor$ L's, then $\left\lfloor \frac{m \bmod n}{n \bmod (m \bmod n)} \right\rfloor$ R's ...

these are just the numbers in Euclid's algorithm!

MOD as a Congruence Relation

$$a \equiv b \pmod m \iff a \bmod m = b \bmod m$$

"a is congruent to b modulo m", similarly

$$a \equiv b \pmod m \iff a - b = km,$$

Proof: $\Rightarrow$

$$a = a \bmod m + km, \quad b = b \bmod m + lm$$

$$a - b = a \bmod m + km - b \bmod m - lm = (k-l)m$$

$\Leftarrow$ $a - b = km$, $a = b$ if $m = 0$, otherwise

$$a \bmod m = a - \left\lfloor \frac{a}{m} \right\rfloor m = (b + km) - \left\lfloor \frac{(b+km)}{m} \right\rfloor m$$

$$= b - \left\lfloor \frac{b}{m} \right\rfloor m = b \bmod m. \quad \square$$

$8 \equiv 23 \pmod 5$, $8 - 23 = -15$ is a mult. of 5 ✓

"$\equiv$" is an equivalence relation & is

reflexive	$a \equiv a$		
symmetric	$a \equiv b$	$\Rightarrow$	$b \equiv a$
transitive	$a \equiv b \equiv c$	$\Rightarrow$	$a \equiv c$

In our case $a \equiv b \iff f(a) = f(b)$; $f(x) = x \bmod m$

$$a \equiv b \;\&\; c \equiv d \;\Rightarrow\; \begin{cases} a + c \equiv b + d \pmod m \\ a - c \equiv b - d \pmod m \end{cases}$$

note, if m is known + const., $\pmod m$ is not necessary

$a \equiv b$ + $c \equiv d \Rightarrow ac \equiv bd \pmod m$

multiples of m

Proof: $ac - bd = (a-b)c + b(c-d)$ □

and so if $a \equiv b \Rightarrow a^n \equiv b^n$, $a,b \in \mathbb{Z}$ $n \geq 0$

e.g. $2 \equiv -1 \pmod 3 \Rightarrow 2^n \equiv (-1)^n \pmod 3$
so $2^n - 1 \equiv 0 \pmod 3$ when n is even.

Caveat, division doesn't behave the same under $\equiv$:

$$ad \equiv bd \pmod m \Rightarrow a \equiv b \pmod m$$

$6 = 3 \cdot 2 \equiv 10 = 5 \cdot 2 \pmod 4$ but $3 \not\equiv 5 \pmod 4$

But $ad \equiv bd \iff a \equiv b \pmod m$, $a,b,d,m \in \mathbb{Z}$, $d \perp m$ then

$15 = 3 \cdot 5 \equiv 35 = 7 \cdot 5 \pmod m$
$3 \equiv 7 \pmod m$ unless $m = k5$

Proof: since $\gcd(d,m) = 1$ $\exists\ m', d' \in \mathbb{Z}$

$dd' + mm' = 1$ so $dd' \equiv 1 \pmod m$

$ad \equiv bd \iff add' \equiv bdd'$

$a \cdot 1 \equiv b \cdot 1 \pmod m$ d' is like $\frac{1}{d} \pmod m$

d' is the "multiplicative inverse of d modulo m"

Note: $ad \equiv bd \pmod{md} \iff a \equiv b \pmod{m}$ for $d \neq 0$

Proof is true for $a, b, d, m \in \mathbb{R}$: $(a \bmod md)d = ad \bmod md$

The last two together give

$$ad \equiv bd \pmod{m} \iff a \equiv b \left(\bmod \frac{m}{\gcd(d,m)}\right), a, b, d, m \in \mathbb{Z}$$

note $dd' + mm' = \gcd(d,m)$, so $add' \equiv bdd' \pmod{m}$

$$a(\gcd(d,m)) \equiv b(\gcd(d,m)) \pmod{m} \iff$$

$$a \equiv b \pmod{\frac{m}{\gcd(d,m)}} \quad \square$$

If $a \equiv b \pmod{100}$ then $a \equiv b \pmod{10}$ or modulo any divisor of 100. $a - b = k100$ is stronger than saying $a - b = k10$. Generally

$$a \equiv b \pmod{md} \Rightarrow a \equiv b \pmod{m}, d \in \mathbb{Z}$$

$$a - b = kmd = lm \text{ with } l = kd$$

Also: $a \equiv b \pmod{m}$ & $a \equiv b \pmod{n} \iff$
$a \equiv b \pmod{\text{lcm}(m,n)}$, $m, n \in \mathbb{Z}^+$

$a - b = k_m m$ & $a - b = k_n n$, so

$k_m m = k_n n$ must equal at least $\text{lcm}(m,n)$

e.g. if $a \equiv b$ modulo $12 \cdot 18$ $a \equiv b \pmod{36}$

note if $m \perp n$ then $\text{lcm}(m,n) = mn$, so

$$a \equiv b \pmod{mn} \iff \begin{matrix} a \equiv b \pmod{m} \\ a \equiv b \pmod{n} \end{matrix} \quad \text{if } m \perp n$$

e.g. $a \equiv b \pmod{100} \iff a \equiv b \pmod{25} \cdot \pmod{4}$

this is a special case of the Chinese Remainder Thm

If $m = \prod p^{m_p}$ (prime factorization), then

$$a \equiv b \pmod{m} \iff a \equiv b \pmod{p^{m_p}} \ \forall p.$$

Independent Residues

The CRT above implies a "residue number system"

$$\text{Res}(x) = (x \bmod m_1, \dots, x \bmod m_r) \text{ with}$$
$$m_j \perp m_k \text{ for } 1 \le j < k \le r.$$

Knowing $x \bmod m_j \ \forall j$ allows to compute $x \bmod m$, $m = \prod_{j=1}^{r} m_j$ (usually big)

$x \bmod 15$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$x \bmod 3$	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2
$x \bmod 5$	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4

$\text{Res}(8) = (2,3)$ & is unique modulo 15.

An advantage is that we can perform addition, subtraction, and multiplication componentwise in the residue system.

$7 \cdot 13 \pmod{15}$: $7 = (1,2)$; $13 = (1,3)$

$1 \cdot 1 \bmod 3 = 1$; $2 \cdot 3 \bmod 5 = 1$

answer is $(1,1) = 1 = 7 \cdot 13 \pmod{15}$

The independence of components is great for computing. E.g. have m_k primes near 2^{31}, then can do arithmetic modulo $m \approx 2^{31 \cdot k}$ without multiprecision software (no carries!)

Division? Suppose we have to compute an integer as a quotient of two large numbers.

Can do this modulo several large p_k's. We can do division modulo p_k unless the divisor is a multiple of p_k, then change p_k.

Given $(x \bmod m_1, \ldots, x \bmod m_k)$ how do we get $x \bmod m$? We do it with linear superposition. Consider $(x \bmod 3, x \bmod 5)$, first solve $(1,0)$, $(0,1)$

$(1,0) = a(10)$ + $(0,1) = b(6)$ so

$(x,y) = (ax + by) \bmod 15$

If $m \perp n$ how do we find $a, b \ni$

$a \bmod m = 1 \quad a \bmod n = 0$
$b \bmod m = 0 \quad b \bmod n = 1$ all hold.

With Euclid we find $m'm + n'n = 1$

$a = n'n \quad + \quad b = m'm$ (reduce mod mn as desired)

Problem: How many solutions to

$$x^2 \equiv 1 \pmod{m}$$

first consider $m = p^k$, $k > 0$ (prime power)

$$(x-1)(x+1) \equiv 0 \pmod{p^k}$$

so $p \backslash (x-1)$ or $p \backslash (x+1)$ (if it divides both $p = 2$)

with $p > 2$ $p^k \backslash (x+1)$ or $p^k \backslash (x-1)$, so

$x \equiv 1$ & $x \equiv -1 \pmod{p^k}$ are the slns.

If $p = 2$ if $2^k \backslash (x-1)(x+1) \Rightarrow x-1$ or $x+1$ is divisible by 2 but not 4 & the other by 2^{k-1}.

$$x \equiv \pm 1 \quad , \quad x \equiv 2^{k-1} \pm 1$$

$x^2 \equiv 1 \pmod{2^3}$ $x = 1, 3, 5, 7$; thus the sequence of any odd integer has the form $8n+1$.

$x^2 \equiv 1 \pmod{m} \Leftrightarrow x^2 \equiv 1 \pmod{p^{m_p}}$ $\forall p \backslash m$

for each $p \neq 2$ there are two solutions. Thus with r prime factors (not 2) there are 2^r solutions. In general there are

$$2^{r + [8\backslash m] + [4\backslash m] - [2\backslash m]}$$

Additional Applications

Recall that the last results derived in Chapter 3 used the assertion:

$$i \text{ in mod } m \qquad i = 0, 1, \cdots, m-1$$

consist of precisely d copies of the m/d numbers

$$0, d, 2d, \cdots, m-d \quad (m-d \equiv -d \pmod m)$$

in some (fixed) order with $d = \gcd(m, n)$

e.g. $m = 12, n = 8 \Rightarrow d = 4$

$0, 8, 4, 0, 8, 4, 0, 8, 4, 0, 8, 4.$ — 4 copies

one set $\qquad m/d = 3$

We now prove these results.

"d copies": $i n \equiv k n \pmod m \iff$

$$i\left(\tfrac{n}{d}\right) \equiv k\left(\tfrac{n}{d}\right) \pmod{m/d}$$

thus the $0 \le k < \frac{n}{d}$ we get d times. □

"k's are $\{0, d, 2d, \ldots, m-d\}$":

$m = m'd$, $n = n'd$ so

$$kn \bmod m = kn'd \bmod m'd = d(kn' \bmod m')$$

$0 \le kn' \bmod m' < m'$ ⊛ are the numbers

when $k = 0, 1, \ldots, m'-1$. Also $m' \perp n'$, so

WLOG can consider $d = 1$, and so by pigeon hole ⊛ are just $\{0, 1, 2, \ldots, m'-1\}$ in some order, since

$$jn' \equiv kn' \pmod{m'} \iff j \equiv k \pmod{m'}$$
$$\text{if } m' \perp n'$$

thus we get m' distinct numbers in ⊛ □.

A direct argument: $m \perp n$ and $j \in [0 \ldots m)$ is given we want to compute k s.t.

$$kn \equiv j \pmod{m}.$$

$$kn n' \equiv jn' \pmod{m} \quad \text{but } n'n + m'n = 1$$

so $nn' \equiv 1 \pmod{m}$ and

$k \equiv j n' \pmod{m}$

Fermat's Little Theorem:

$$n^{p-1} \equiv 1 \pmod{p}, \text{ if } n \perp p$$

Proof: With p prime $n \perp p \Rightarrow n \neq kp$. From above we know

$in \bmod p$, $i = 1, 2, \ldots, p-1$ are a permutation of $\{1, 2, \ldots, p-1\}$, so

$$n \cdot 2n \cdot 3n \cdot \ldots \cdot ((p-1)n) \equiv (p-1)! \pmod{p}$$

$$n^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$$

can divide out $(p-1)!$ since $(p-1)! \perp p$. □

Alternatively $n^p \equiv n \pmod{p}$, $n \in \mathbb{Z}$

Proof: Case $n \perp p \Rightarrow n^{p-1} \equiv 1 \pmod{p}$ and we multiply by n □.

Case $n \not\perp p$, i.e. $p \mid n$, thus $n = kp$

$$n^p \equiv k^p p^p \equiv k p^p \pmod{p}$$

But $p^p \bmod p = 0 = p$ so

$$n^p \equiv np \pmod{p}$$
$$\equiv n$$

□

Fermat also noted that $f_n = 2^{2^n}+1$ was prime for $n = 0, 1, 2, 3, 4$. He suspected this was always prime:

$f_0 = 2^{2^0}+1 = 2^1+1 = 3$, $f_1 = 2^{2^1}+1 = 2^2+1 = 5$

$f_2 = 2^{2^2}+1 = 2^4+1 = 17$, $f_3 = 2^{2^3}+1 = 2^8+1 = 257$

$f_4 = 2^{2^4}+1 = 2^{16}+1 = 65537$ all prime.

f_i is the i^{th} Fermat number, when prime it is called a "Fermat prime."

$f_5 = 2^{2^5}+1 = 2^{32}+1 = 4294967297$ is not prime.
(in binary $100\cdots01$, with $\underbrace{00\cdots0}_{2^5-1}$)

Fermat could have used his own result to prove $2^{32}+1$ is not prime. Using Fermat's little theorem

$$3^{2^{32}} \equiv 1 \pmod{2^{32}+1}$$ if is prime

This is the basis of Miller-Rabin probabilistic primality testing.

We can compute $3^{2^{32}} \bmod 2^{32}+1$ with 32 squarings modulo $2^{32}+1$ starting with 3:

$$3^{2^{32}} \equiv 3029026160 \pmod{2^{32}+1}$$

this <u>proves</u> fs is <u>not</u> prime. However, if it turned out to be 1, it would <u>not</u> prove fs to be prime.

When proving FLT we cancelled $(p-1)!$
Turns out that $(p-1)! \equiv -1 \pmod p$, and more generally we have Wilson's theorem:

$$(n-1)! \equiv -1 \pmod n \iff n \text{ is prime}$$

Proof: if $n>1$ is <u>not</u> prime $\exists\, p^{n>1}_{<n}$ s.t. $p \mid n$ and $p \mid (n-1)!$

If $(n-1)! \equiv -1 \pmod n \Rightarrow (n-1)! \equiv -1 \pmod p$, why? But $(n-1)! \equiv 0 \pmod p$ $\square$.

Now let p be prime and we prove

$$(p-1)! \equiv -1 \pmod{p}.$$

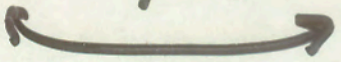
If $n \perp p$ then $\exists\, n' \ni n'n \equiv 1 \pmod{p}$

Now pair up inverses in $[1 \ldots p-1]$, there are $\frac{p-1}{2}$ such pairs so

$$(p-1)! \equiv (1)^{\frac{p-1}{2}} \pmod{p}$$

Wait! Case $p=5$ $\quad 4! = 24 \equiv -1 \pmod{5}$

$1'=1,\ 2'=3,\ 3'=2,\ 4'=4$



pair up

$$4! \equiv 1 \cdot 2 \cdot 3 \cdot 4 = 1 \cdot 4 \equiv -1 \pmod{5}$$

must find numbers that are their own inverses, i.e. x's $\rightarrow$

$$x^2 \equiv 1 \pmod{p}$$

There are two roots for $p>2$: 1 & $p-1$,
when $p=2$: $(2-1)! = 1 \equiv -1 \pmod{2}$ is clear

$$(p-1)! = 1 \cdot (\text{pairs}) \cdot (p-1) \equiv p-1 \equiv -1 \pmod{p}$$

Wilson theorem doesn't help prove primality like FLT

Phi and Mu

How many integers less than m are relatively prime to m?

Answer: $\varphi(m)$ Euler's Totient function

Simple cases: $\varphi(1) = 1$, $\varphi(p) = p-1$

$\varphi(m) < m-1$ if m composite

Note: Fermat's Little Theorem can be recast as

$$n^{\varphi(m)} \equiv 1 \pmod{m}, \quad n \perp m$$

Let $m = p^k$, now $n \perp p^k \Leftrightarrow p \nmid n$,

the mults. of p in $\{0, 1, \ldots, p^k - 1\}$ are $\{0, p, 2p, \ldots, p^k - p\}$, there are p^{k-1} of them

so $$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$$
$$= p^k\left(1 - \frac{1}{p}\right)$$

Also, when $k=1 \rightarrow \varphi(p) = p-1$.

when $m > 1$ is composite but not a prime power, $m = m_1 m_2$ with $m_1 \perp m_2$, then $\mathbb{Z}_m$ can be written as $(n \bmod m_1, n \bmod m_2)$ & $n \perp m \iff n \bmod m_1 \perp m_1$ & $n \bmod m_2 \perp m_2$

Thus $\varphi(m) = \varphi(m_1)\varphi(m_2)$ as there are $\varphi(m_1)$ "1st" components & $\varphi(m_2)$ "2nd" components

Thus $\varphi(m)$ is multiplicative:

f is mult. if $f(1)=1$ & $f(m_1 m_2) = f(m_1) f(m_2)$, $m_1 \perp m_2$.

$\varphi(12) = \varphi(4)\cdot\varphi(3) = 4(1-\frac{1}{2})\cdot 2$

$= 2\cdot 2 = 4$

A multiplicative function is defined by its

on the primes! Thus

$$\varphi(m) = \prod_{p \setminus m} \left(p^{m_p} - p^{m_p - 1} \right) = m \prod_{p \setminus m} \left(1 - \frac{1}{p}\right)$$

Application: $\frac{m}{n}$ is basic if $0 \le m < n$, so $\varphi(n)$ is the # reduced basic fractions with denominator n. Recall $\mathcal{F}_n$ = all reduced basic fraction with denom $\le n$ plus $\frac{1}{1}$

$$\frac{0}{12}\ \frac{1}{12}\ \frac{2}{12}\ \frac{3}{12}\ \frac{4}{12}\ \frac{5}{12}\ \frac{6}{12}\ \frac{7}{12}\ \frac{8}{12}\ \frac{9}{12}\ \frac{10}{12}\ \frac{11}{12}$$

↑ not basic

↓ reduction

$$\frac{0}{1}\ \frac{1}{12}\ \frac{1}{6}\ \frac{1}{4}\ \frac{1}{3}\ \frac{5}{12}\ \frac{1}{2}\ \frac{7}{12}\ \frac{2}{3}\ \frac{3}{4}\ \frac{5}{6}\ \frac{11}{12}$$

↓ by denominator

$$\frac{0}{1};\ \frac{1}{2};\ \frac{1}{3}, \frac{2}{3};\ \frac{1}{4}, \frac{3}{4};\ \frac{1}{6}, \frac{5}{6};\ \frac{1}{12}, \frac{5}{12}, \frac{7}{12}, \frac{11}{12}$$

Note: Every divisor, d, of 12 is a denom. with $\varphi(d)$ different numerators, thus

$$\varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) = 12$$

This holds $\forall m$: $\sum_{d \mid m} \varphi(d) = m$

Many problems in number theory require sums over the divisors of numbers. Let f be such that

$$g(m) = \sum_{d \mid m} f(d) \quad \text{is multiplicative,}$$

then f must be multiplicative too.
(note $g(m) = m$ is another reason $\varphi(m)$ is mult.)

Proof: (induction on m)

$f(1) = g(1) = 1$; Let $m > 1$ and assume

$f(m_1 m_2) = f(m_1) f(m_2)$ when $m_1 \perp m_2$, $m_1 m_2 < m$.

Assume $m = m_1 m_2$, $m_1 \perp m_2$

$$g(m_1 m_2) = \sum_{d \mid m_1 m_2} f(d) = \sum_{d_1 \mid m_1} \sum_{d_2 \mid m_2} f(d_1 d_2)$$

note $d_1 \perp d_2$, $f(d_1 d_2) = f(d_1) f(d_2)$, except

when $d_1 = m_1$ & $d_2 = m_2$:

$$\left(\sum_{d_1 \backslash m_1} f(d_1) \sum_{d_2 \backslash m_2} f(d_2)\right) - f(m_1) f(m_2) + f(m_1, m_2)$$

$$= g(m_1) g(m_2) - f(m_1) f(m_2) + f(m_1, m_2)$$

$$= g(m_1, m_2)$$

but $g(m_1, m_2) = g(m_1) g(m_2)$ so

$$f(m_1, m_2) = f(m_1) f(m_2). \quad \square$$

$\Leftarrow$ is trivial.

Möbius Function:

$$\forall\, m \geq 1 \qquad \sum_{d \backslash m} \mu(d) = [m = 1]$$

Thus $m = 1$: $\sum_{d \backslash 1} \mu(d) = \mu(1) = 1$

$m = 2$: $\sum_{d \backslash 2} \mu(d) = \mu(1) + \mu(2) = 0$

$$\Rightarrow \mu(2) = -1$$

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

Dedekind & Liouville notice the "Möbius" inversion formula/principle:

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

important for multiplicative functions!

<u>Proof</u>: $\Rightarrow$ Assume $g(m) = \sum_{d \mid m} f(d)$

$$\sum_{d \mid m} \mu(d)\, g\left(\tfrac{m}{d}\right) = \sum_{d \mid m} \mu\left(\tfrac{m}{d}\right) g(d)$$

$$= \sum_{d \mid m} \mu\left(\tfrac{m}{d}\right) \sum_{k \mid d} f(k) = \sum_{k \mid m} \sum_{d \mid \frac{m}{k}} \mu\left(\tfrac{m}{kd}\right) f(k)$$

$$= \sum_{k \mid m} \sum_{d \mid \frac{m}{k}} \mu(d)\, f(k) = f(m) \qquad \square.$$

$$= [m/k = 1]$$

$g(m) = [m=1] = \sum_{d \backslash m} \mu(d)$ is multiplicative so $\mu(d)$ is as well. Thus we can compute $\mu(m)$ without the recurrence by studying its values on prime powers:

$m = p^k$

$$\sum_{d \backslash m} \mu(d) = \mu(1) + \mu(p) + \cdots + \mu(p^k) = 0$$

so $\mu(p) = -1$ and $\mu(p^k) = 0$ for $k > 1$:

$$\mu(m) = \prod_{p \backslash m} \mu(p^{v_p(m)}) = \begin{cases} (-1)^r & \text{if } m = p_1 \cdots p_r \\ 0 & \text{if } p^2 \backslash m \text{ for some prime } p \end{cases}$$

$\mu(m) \neq 0$ if m is "square-free"

Applying inversion to $\sum_{d \backslash m} \varphi(d) = m$ we get: $\varphi(m) = \sum_{d \backslash m} \mu(d) \frac{m}{d}$

E.g. $\varphi(12) = \mu(1)\cdot 12 + \mu(2)\cdot 6 + \mu(3)\cdot 4$
$+ \mu(4)\cdot 3 + \mu(6)\cdot 2 + \mu(12)\cdot 1$

$= 1\cdot 12 + (-1)\cdot 6 + (-1)\cdot 4 + 0\cdot 3 + 1\cdot 2 + 0\cdot 12 = 4$

If m is divisible by $p_1, \dots, p_r$, the sum has only 2^r terms. Recall $\varphi(m) = m\prod(1-\frac{1}{p_i})$, if we multiply this out we get 2^r terms, like in inclusion/exclusion.

Example: How many fractions in $\mathcal{F}_n$:

$$\Phi(x) = \sum_{1 \le m \le x} \varphi(m)$$

We will derive a formula with the help of:

$$\sum_{d \ge 1} \Phi\left(\frac{x}{d}\right) = \frac{1}{2}\lfloor x \rfloor \lfloor 1+x \rfloor \quad \forall\, x \in \mathbb{R}$$

there are $\frac{1}{2}\lfloor x \rfloor \lfloor 1+x \rfloor$ $\frac{m}{n}$ with $0 \le m \le n \le x$

and those with $\gcd(m,n) = d$ are $\Phi\left(\frac{x}{d}\right)$

$\frac{m}{n}$: $0 \le m \le \frac{x}{d}$

n	0	1	2	3	4	5	6	7	8	9	10	11	12
$\varphi(n)$	-	1	1	2	2	4	2	6	4	6	4	10	4
$\Phi(n)$	0	1	2	4	6	10	12	18	22	28	32	42	46

Check $x = 12$:

$$\Phi(12) + \Phi(6) + \Phi(4) + \Phi(3) + \Phi(2) + 6\cdot\Phi(1) =$$

$$46 + 12 + 6 + 4 + 2 + 6 = 78 = \tfrac{1}{2}\,12\cdot 13$$

An alternative Möbius is:

$$g(x) = \sum_{d\geq 1} f\left(\frac{x}{d}\right) \iff f(x) = \sum_{d\geq 1} \mu(d)\, g\left(\frac{x}{d}\right)$$

Proof: Assume $\Rightarrow$

$$= \sum_{d\geq 1} \mu(d) \sum_{k\geq 1} f\left(\frac{x}{kd}\right)$$

$$= \sum_{m\geq 1} f\left(\frac{x}{m}\right) \sum_{d,k\geq 1} \mu(d)\,[m = kd] = \sum_{m\geq 1} f\left(\frac{x}{m}\right) \sum_{d\mid m} \mu(d) =$$

$$\sum_{m\geq 1} f\left(\frac{x}{m}\right)[m = 1] = f(x)$$

So: $\Phi(x) = \frac{1}{2} \sum_{d \geq 1} \mu(d) \left\lfloor \frac{x}{d} \right\rfloor \left\lfloor 1 + \frac{x}{d} \right\rfloor$

2. $\Phi(12) = 1 \cdot 12 \cdot 13 + (-1) \cdot 6 \cdot 7 + -1 \cdot 4 \cdot 5 + 0 \cdot 3 \cdot 4 +$
$(-1) \cdot 2 \cdot 3 + 1 \cdot 2 \cdot 3 + (-1) \cdot 1 \cdot 2 + 1 \cdot 2 - 1 \cdot 2)$

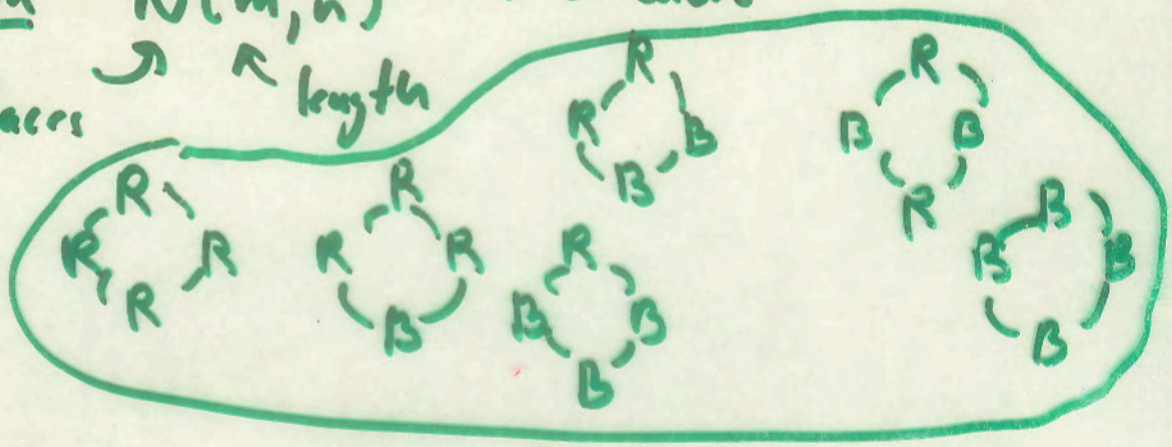
$= 92 \implies \Phi(12) = 46$

and can show $\Phi(x) = \frac{3}{\pi^2} x^2 + O(x \log x)$

An application $N(m,n)$ ← # of colors, ↖ length

# of necklaces

$N(4,2) = 6$ with rotational symmetry



Note: Reflections count!

$\neq$

No obvious recurrence, so let's break them into strings

$m = 4, n = 2$:

RRRR	RRRR	RRRR	RRRR	(no B's)
RRBR	RRRB	BRRR	RBRR	(1 B)
RBBR	RRBB	BRRB	RBRR	(2 B's)
RBRB	BRBR	RBRB	BRBR	(2 B's)
RBBB	BRBB	BBRB	BBBR	(3 B's)
BBBB	BBBB	BBBB	BBBB	(All B's)

Each of the n^m possible strings appears above in the $m\,N(m,n)$ strings, with repeated patterns.

How many times does $a_0 \cdots a_{m-1}$ appear?

Answer: # of cyclic shifts that give the same pattern.

$$m\,N(m,n) = \sum_{a_0,\ldots a_{m-1} \in S_n} \sum_{0 \le k < m} [a_0 \cdots a_{m-1} = a_k \cdots a_{m-1} a_0 \cdots a_{k-1}]$$

S_n is the set of n colors

$$= \sum_{0 \le k < m} \sum_{a_0 \cdots a_{m-1} \in S_n} [a_0 \cdots a_{m-1} = a_k \cdots a_{m-1} a_0 \cdots a_{k-1}]$$

For $m=12$, $k=8$ we want to count # of solns. to:

$$a_0 a_1 a_2 \cdots a_{11} = a_8 a_9 a_{10} a_{11} a_0 \cdots a_7, \text{ or}$$

$a_0 = a_8 = a_4$; $a_1 = a_9 = a_5$; $a_2 = a_{10} = a_6$; $a_3 = a_{11} = a_7$

each can be chosen independently: n^4 ways, we have

$$a_j = a_{(j+k) \bmod m} \quad 0 \le j < m,$$

we get equivalence classes with indices:

$$j \text{ with } l(j+kl) \bmod m \quad l = 1, 2, \ldots$$

Recall that multiples of k mod m are $\{0, d, 2d, \ldots, m-d\}$ with $d = \gcd(k, m)$, so choose $a_0, \ldots, a_{d-1}$ independently and set $a_j = a_{j-d}$ $d \le j < m$, with n^d solutions.

We have proved that

$$m\,N(m,n) = \sum_{0 \le k < m} n^{\gcd(k,m)},$$

so

$$N(m,n) = \frac{1}{m} \sum_{d \mid m} n^d \sum_{0 \le k < m} [d = \gcd(k,m)] =$$

$$= \frac{1}{m} \sum_{d \mid m} n^d \sum_{0 \le k < m} \left[k/d \perp m/d \right] = \frac{1}{m} \sum_{d \mid m} n^d \sum_{\substack{0 \le k < m \\ k \perp m/d}} \left[k \perp \frac{m}{d} \right]$$

note: $\sum_{0 \le k < \frac{m}{d}} \left[k \perp \frac{m}{d} \right] = \varphi(m/d)$, so

$$N(m,n) = \frac{1}{m} \sum_{d \mid m} n^d \varphi\left(\frac{m}{d}\right) = \frac{1}{m} \sum_{d \mid m} n^{d/m} \varphi(d)$$

check: $N(4,2) = \frac{1}{4} \sum_{d \mid 4} \varphi(d)\, 2^{4/d} =$

$$\frac{1}{4}\left(\varphi(1) \cdot 2^{4/1} + \varphi(2) \cdot 2^{4/2} + \varphi(4) \cdot 2^{4/4} \right) =$$

$$\frac{1}{4}\left(1 \cdot 2^4 + 1 \cdot 2^2 + 2 \cdot 2^1 \right) = \frac{1}{4}\left(16 + 4 + 4\right) = \frac{24}{4} = 6 \checkmark$$

We will prove that (we divide by m!)

$$\sum_{d \mid m} \varphi(d)\, n^{m/d} \equiv 0 \pmod{m} \quad (*)$$

$m = p$: $\varphi(1) \cdot n^p + \varphi(m) \cdot n \Rightarrow n^p + (p-1)n \equiv 0 \pmod{m}$

FLT!

So (*) is a different generalization of FLT.

$m=4$ is the smallest prime power:

$$n^4 + n^2 + 2n \equiv 0 \pmod 4$$

n = even all terms are $0 \pmod 4$, why?

n = odd $n^4 \equiv n^2 \equiv 1 \pmod 4$ but $2n$ is $2 \pmod 4$ so they add up to $0 \pmod 4$.

$m=12$ might be tricky:

$$n^{12} + n^6 + 2n^4 + 2n^3 + 2n^2 + 4n \equiv 0 \pmod{12}$$

Try to prove $\pmod 3$, $\pmod 4$, by CRT

this suffices; $\pmod 3$: $n^3 + 2n \equiv 0 \pmod 3$

$$n^{12} + n^6 + 2n^4 + 2n^3 + 2n^2 + 4n = (n^{12} + \underbrace{2n^4}_{n^4}) + (n^6 + 2n^2) + 2(n^3 + 2n)$$

$$= 0 + 0 + 2 \cdot 0 \pmod 3$$

$\pmod 4$: $n^4 + n^2 + 2n \equiv 0 \pmod 4$

$$n^{12} + n^6 + 2n^4 + 2n^3 + 2n^2 + 4n \equiv$$

$$(n^{12} + n^6 + 2n^3) + 2(n^4 + n^2 + 2n) \equiv 0 + 2 \cdot 0 \pmod 4$$

↑ eval. at n^3 □

Prime powers: $m = p^3$

$$n^{p^3} + \varphi(p)\, n^{p^2} + \varphi(p^2)\, n^p + \varphi(p^3)\, n \equiv$$

$$n^{p^3} + (p-1)\, n^{p^2} + (p^2-p)\, n^p + (p^3-p^2)\, n \equiv$$

$$(n^{p^3} - n^{p^2}) + p(n^{p^2} - n^p) + p^2(n^p - n) + p^3 n$$

↑ divisible by p^3 ↑ p^3 ↑ p FLT, twice

so $n^p \equiv n + p \cdot g$; $(n^p)^p = n^{p^2} \equiv (n + p \cdot g)^p$

$$\equiv n^p + (pg)^1 n^{p-1}\binom{p}{1} + (pg)^2 n^{p-2}\binom{p}{2} + \cdots$$

$$\equiv n^p + p^2 Q \quad \text{(why?)} \qquad \text{so } n^{p^2} - n^p \equiv p^2 Q \equiv 0 \pmod{p^2}$$

$$n^{p^3} = (n^{p^2})^p \equiv (n^p + p^2 Q)^p \equiv$$

$$= n^{p^2} + (p^2Q)^1 n^{p(p-1)}\binom{p}{1} + (p^2Q)^2 n^{p(p-2)}\binom{p}{2} + \dots$$

$$= n^{p^2} + p^3 Q \qquad \text{so } n^{p^3} - n^{p^2} = p^3 Q \equiv 0 \pmod{p^3}$$

This proves for p^3, but we can prove, by induction that

$$n^{p^k} = n^{p^{k-1}} + p^k \cdot \mathcal{L} \quad \text{so}$$

$$n^{p^k} - n^{p^{k-1}} \equiv 0 \pmod{p^k}, \; k > 0,$$

which proves for $m = p^k$, $k > 0$.

When $m = m_1 m_2$, $m_1 \perp m_2$ with the result true for m_1 & m_2

$$\sum_{d \mid m} \varphi(d)\, n^{m/d} = \sum_{d_1 \mid m_1,\, d_2 \mid m_2} \varphi(d_1 d_2)\, n^{m_1 m_2 / d_1 d_2} =$$

$$\sum_{d_1 \mid m_1} \varphi(d_1) \left(\sum_{d_2 \mid m_2} \varphi(d_2) \underbrace{\left(n^{m_1/d_1}\right)^{m_2/d_2}}_{\equiv 0 \pmod{m_2}} \right), \text{ by}$$

switching sums can get $\equiv 0 \pmod{m_1}$