ℕℤ

```
m = {
  ab: (m,n,r,min=-10, max=10)=>[...Array(max-min)].flatMap((_,a,list)=>
    list.map((_,b)=>
      [a+min,b+min]
    ).filter(([a,b])=>
      a*m+b*n===r
    ).map(([a,b])=>
      `${a}(${m})+${b}(${n})=${r}`
    )
  ),

  inverse: (modulo, a)=>[...Array(modulo)].map((_,i)=>
    i+1
  ).filter(i=>
    (a*i)%modulo===1
  ),

  gcd: (m_,n)=>m_===0 ?
    n :
    m.gcd(n%m_,m_),

  mod: (n,m)=>n-m*Math.floor(n/m),
};
```

2.3 Manipulation of sums

$$\sum_{k=0}^{n} a + bk = (a + \frac{1}{2}bn)(n + 1)$$

$$\sum_{k=0}^{n} ax^{k} = \frac{a-ax^{n+1}}{1-x}$$

$S_n = \sum_{0 \le k \le n} ax^k$

$S_n + ax^{n+1} = ax^0 + \sum_{0 \le k \le n} ax^{k+1}$

If $S_n = \sum_{0 \le k \le n} k2^k$

$S_n + (n + 1)2^{n+1} = \sum_{0 \le k \le n} (k + 1)2^{k+1}$ // manipulate to replace all sums with S_n

2.4 Multiple Sums

$[1 \le j < k \le n] + [1 \le k < j \le n] = [1 \le j, k \le n] - [1 \le j = k \le n]$

$\sum_{0 \le k < n} H_k = nH_n - n$

2.5 General Methods

1. Look it up
2. Guess and prove by induction
3. Perturbation:

$S_n + a_{n+1} = \sum_{0 \le k \le n} a_{k+1} = ...\ (split\ the\ sum\ apart\ and\ substitute\ the\ sum\ for\ S_n)$

4. Repertoire
5. Replace sums by integrals
6. Expand and contract

$S_n = \sum_{1 \le k \le n} k^2 = \sum_{1 \le j \le k \le n} k = \sum_{1 \le j \le n} \sum_{j \le k \le n} k = ...(replace\ triangular,\ factor\ out\ static)$

2.6 Finite and Infinite Calculus

$\Delta f(x) = f(x + 1) - f(x)$

$x^{\underline{m}} = x(x - 1)...(x - m + 1)\ \ for\, m \ge 0$

$x^{\overline{m}} = x(x + 1)...(x + m - 1)\ \ for\, m \ge 0$

$\Delta x^{\underline{m}} = mx^{\underline{m-1}} = (x + 1)^{\underline{m}} - x^{\underline{m}} = mx(x - 1)...(x - m + 2)$

$g(x) = \Delta f(x)$

$\sum g(x)\delta x = f(x) + C$

$$\sum_a^b g(x)\delta x = \sum_{k=a}^{b-1} g(k) = \sum_{a\le k<b} g(k) = f(x)\Big|_a^b = f(b) - f(a)$$

$$\sum_{0\le k<n} k^{\underline{m}} = \frac{n^{\underline{m}}}{m+1}$$

$f = \Sigma g$	$\Delta f = g$	$f = \Sigma g$	$\Delta f = g$
$x^{\underline{0}} = 1$	0	2^x	2^x
$x^{\underline{1}} = x$	1	c^x	$(c-1)c^x$
$x^{\underline{2}} = x(x-1)$	$2x$	$c^x/(c-1)$	c^x
$x^{\underline{m}}$	$mx^{\underline{m-1}}$	cf	$c\Delta f$
$x^{\underline{m+1}}/(m+1)$	$x^{\underline{m}}$	$f+g$	$\Delta f + \Delta g$
H_x	$x^{\underline{-1}} = 1/(x+1)$	fg	$f\Delta g + \mathrm{E}g\Delta f$

$k^2 = k^{\underline{2}} + k^{\underline{1}}$

$x^{\underline{-m}} = \frac{1}{(x+1)(x+2)...(x+m)}$

$x^{\underline{m+n}} = x^{\underline{m}}(x-m)^{\underline{n}}$

$\sum_a^b x^{\underline{m}}\delta x = \frac{x^{\underline{m+1}}}{m+1}\Big|_a^b \; for\, m \neq -1,\ else := \ H_x\Big|_a^b$

$\sum_{a\le k<b} c^k = \sum_a^b c^x \delta x = \frac{c^x}{c-1}\Big|_a^b = \frac{c^v - c^a}{c-1} \; for\, c \neq 1$

$Ef(x) = f(x+1)$

$\Delta(uv) = u\Delta v + Ev\Delta u$

$\sum u\Delta v = uv - \sum Ev\Delta u$

$g(x) = \Delta f(x) = f(x+1) - f(x) = Ef - f(x)$

3.1 Floors and Ceilings

$\lfloor x \rfloor = max(\{n\colon n \in \mathbb{Z}, n \le x\});\ \ x - 1 < n \le x < n + 1$

$\lceil x \rceil = min(\{n\colon n \in \mathbb{Z}, n \ge x\});\ \ n - 1 < x \le n < x + 1$

$-\lfloor -x \rfloor = \lceil x \rceil$ (same for ceil)

$x - 1 < \lfloor x \rfloor \le x \le \lceil x \rceil < x + 1$

$\lfloor x + n \rfloor = \lfloor x \rfloor + n$

$x < n \iff \lfloor x \rfloor < n$

$n < x \iff n < \lceil x \rceil$

$x \le n \iff \lceil x \rceil \le n$

$n \le x \iff n \le \lfloor x \rfloor$

$\{x\} = x\%1 = x - \lfloor x \rfloor \Leftrightarrow$ x - integer part = fractional part

⌊⌋⌈⌉

3.2 Floor/Ceiling Applications

$\lfloor \frac{x+m}{n} \rfloor = \lfloor \frac{\lfloor x \rfloor + m}{n} \rfloor$ (same for ceil)

$a \backslash b \Leftrightarrow a\%b = 0 \Leftrightarrow m > 0,\ n = mk,\ k \in \mathbb{Z}$

3.4 'MOD': The binary operator

$a\%b = a \bmod b$

$n = qm + r = m\lfloor \frac{n}{m} \rfloor + n\%m = quotient + remainder$

$n\%m = n - m\lfloor \frac{n}{m} \rfloor$

$c(x\%y) = (cx)\%(cy)$

$-1(x\%(-y)) = (-x)\%y$

$0 \le x\%y < y \quad for\ y > 0$

$0 \ge x\%y > y \quad for\ y < 0$

4.1 Divisibility

Greatest Common Divisor = $max\{d : d\%m == 0\ and\ d\%n == 0\}$

$gcd(105, 60) = 15$

Least Common Multiple = $min\{d : d = k_1 m = k_2 m\ for\ some\ k_1, k_2, m \in \mathbb{Z}\}$

$gcd(m, n) = gcd(n\%m, m) \quad for\ 0 \le m < n$

$gcd(0, n) = n$

$m'm + n'n = gcd(m, n) = (\overline{m} - \lceil \frac{n}{m} \rceil \overline{r})m + \overline{r}n$

4.2 Primes

A positive integer is prime if it has exactly 2 divisors (1 and n)

$n = p_1 \ldots p_m = \prod_{k=1}^{m} p_k \quad for\ p_1 \le \ldots \le p_m$

$n = \prod_p p^{n_p} \quad for\ n_p \ge 0$

$k = mn \Leftrightarrow k_p = m_p + n_p \quad for\ all\ p$

$m\%n = 0 \Leftrightarrow m_p \le n_p \quad for\ all\ p$

$k = gcd(m, n) \Leftrightarrow k_p = min(m_p, n_p) \quad for\ all\ p$

$k = lcm(m, n) \Leftrightarrow k_p = max(m_p, n_p) \quad for\ all\ p$

4.3 Prime Examples

~ - asymptotic

$P_n \sim n \ln n \Leftrightarrow \lim_{n\to\infty} \frac{P_n}{n \ln n} = 1$

$\pi(x) \sim \frac{x}{\ln x}$

4.5 Relative Primality

$\frac{m}{gcd(m,n)} \perp \frac{n}{gcd(m,n)}$

$m \perp n \Leftrightarrow m \textit{ and } n \textit{ are integers and } gcd(m,n) = 1 \Leftrightarrow min(m_p, n_p) = 0 \textit{ for all } p \Leftrightarrow m_p n_p = 0 \textit{ for all } p$

$k \perp m \textit{ and } k \perp n \Leftrightarrow k \perp mn$

Reduced fractions consist of relatively prime numbers

$m'n - m'n = 1$

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

$F_N = \{\textit{reduced fractions between } 0 \textit{ and } 1 \textit{ with denominators of } N \textit{ or less}\}$

$M(S) = (\frac{n}{m} \frac{n'}{m'})$

$L = (\frac{1}{0} \frac{1}{1})$

$R = (\frac{1}{1} \frac{0}{1})$

Thus $M(LRRL) = LRRL$

$\frac{m}{n} = f(RS) \Leftrightarrow \frac{m-n}{n} = f(S)$, $\textit{when } m > n$

$\frac{m}{n} = f(LS) \Leftrightarrow \frac{m}{n-m} = f(S)$, $\textit{when } m < n$

4.6 ‘Mod’: the congruence relation

$a \equiv b \% m \Leftrightarrow a\%m = b\%m \Leftrightarrow m\%(a-b) = 0$

$a \equiv b \textit{ and } c \equiv d \Rightarrow a + c \equiv b + d \ \%m$ (same for subtraction)

$a \equiv b \textit{ and } c \equiv d \Rightarrow ac \equiv bd \ \%m \quad \textit{for } b, c \in \mathbb{Z}$

$a \equiv b \Rightarrow a^n \equiv b^n \ \%m \quad \textit{for } a, b \in \mathbb{Z} \textit{ and } n \geq 0$

$ad \equiv bd \Leftrightarrow a \equiv b\%m \quad \textit{for } a, b, d, m \in \mathbb{Z} \textit{ and } d \perp m$

$ad \equiv bd \ \%md \Leftrightarrow a \equiv b\%m \quad \textit{for } d \neq 0$

$ad \equiv bd\%m \Leftrightarrow a \equiv b\%\frac{m}{gcd(d,b)} \quad \textit{for integers } a, b, d, m$

$a \equiv b\%m \textit{ and } a \equiv b\%n \Leftrightarrow a \equiv b\%lcm(m,n) \quad \textit{for integers } m, n > 0$

$a \equiv b\%mn \Leftrightarrow a \equiv b\%m \textit{ and } a \equiv b\%n \quad \textit{if } m \perp n$

$a \equiv b\%m \Leftrightarrow a \equiv b\%p^{m_p}$

Independent residues section

Chinese remainder theorem