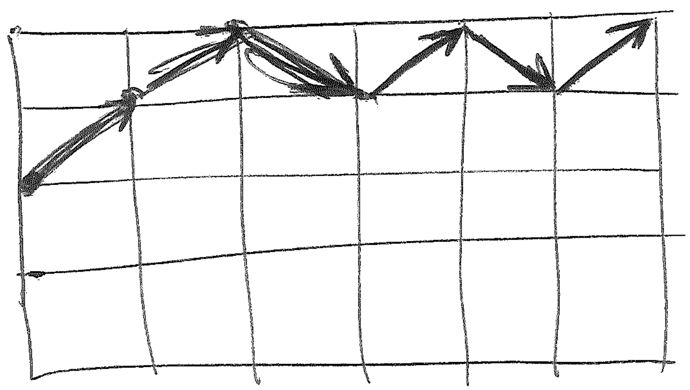
6.5. Dyck paths

Def: An up-down path is (informally) a path in $\mathbb{Z}^2$ that uses only the following two types of steps:

- "positive steps" (i.e., steps $(a, b) \mapsto (a+1, b+1)$);
- "negative steps" (i.e., steps $(a, b) \mapsto (a+1, b-1)$).

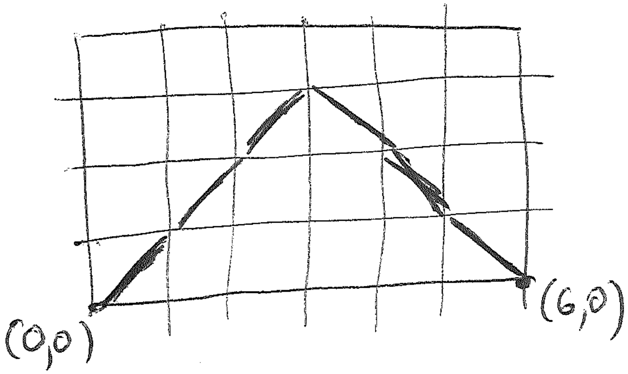
[Ex:

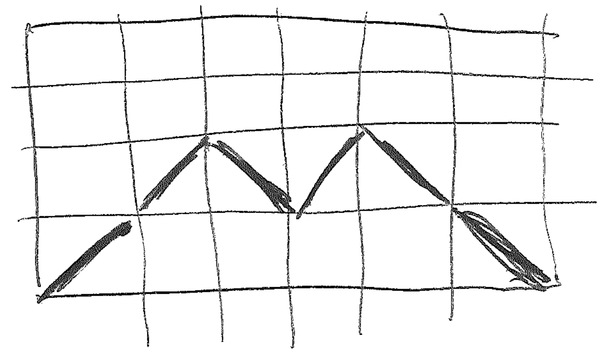


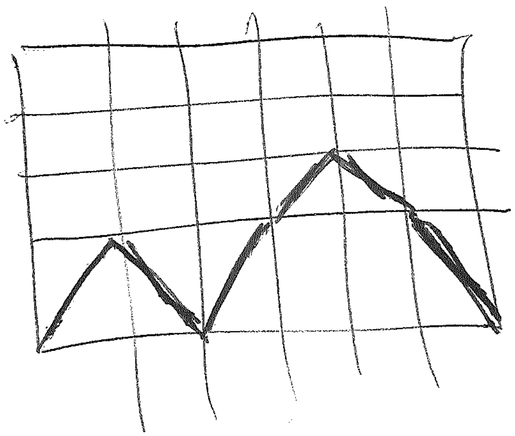
]

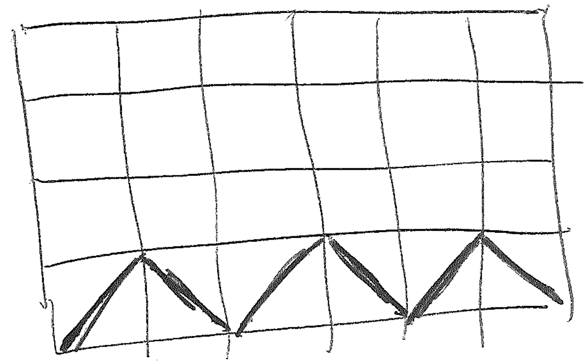
A Dyck path is an up-down path that never falls below the x-axis (i.e., each point (x, y) on the path satisfies $y \geq 0$).

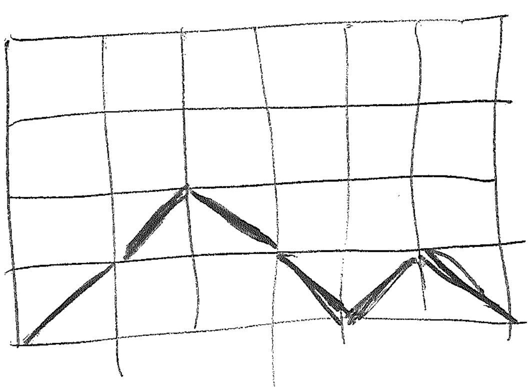
Ex: The Dyck paths from $(0,0)$ to $(6,0)$ are











There are $5 = C_3$ of them.

Prop. 6.8. Let $n \in \mathbb{N}$. Then,

$$(\#\text{ of Dyck paths from } (0,0) \text{ to } (2n,0)) = C_n.$$

Proof. The map

$$\{\text{Dyck paths from } (0,0) \text{ to } (2n,0)\} \to \{\text{legal paths from } (0,0) \text{ to } (n,n)\},$$

which replaces each point (x,y) on the Dyck path by $\left(\frac{x+y}{2}, \frac{x-y}{2}\right)$ is a bijection. Thus, it follows from

$$(\#\text{of legal paths}) = C_n.$$

$\square$

6.6. Super-Catalan numbers

Def. Let $n, m \in \mathbb{N}$. Set $T(m,n) = \dfrac{(2m)!\,(2n)!}{m!\,n!\,(m+n)!}$

Thm. 6.9. (a) $T(m,n)$ is a positive integer $\forall m,n \in \mathbb{N}$, and is even when $m+n>0$.

(b) $T(m,n) = \binom{2m}{m}\binom{2n}{n} \Big/ \binom{m+n}{m}$ $\forall m,n \in \mathbb{N}$.

(c) $T(m,0) = \binom{2m}{m}$ $\forall m \in \mathbb{N}$,

(d) $T(m,1) = 2C_m$ $\forall m \in \mathbb{N}$.

(e) $4T(m,n) = T(m+1,n) + T(m,n+1)$ $\forall m,n \in \mathbb{N}$,

(f) $T(m,n) = T(n,m)$ $\forall m,n \in \mathbb{N}$.

(g) $T(m,n) = \sum_{k=-p}^{p} (-1)^k \binom{2m}{m+k}\binom{2n}{n-k}$, where $p = \min\{m,n\}$.

Proofs. See [detnotes, Exercise 3.24] and/or google for "super-Catalan numbers". No one knows what $T(m,n)$ counts. $\square$

7. Necklaces

7.1. ϕ & μ

Def. Let $\mathbb{P}$ be the set $\{1,2,3,\ldots\}$ (as opposed to $\mathbb{N} = \{0,1,2,3,\ldots\}$).

Recall: Euler's totient function is the function
$\phi : \mathbb{P} \to \mathbb{N}$ ~~def~~ sending each n to
(# of all $m \in [n]$ coprime to n).

Prop. 7.1. Let $n \in \mathbb{P}$. Let $p_1, p_2, \ldots, p_k$ be the distinct prime divisors of n. Then, $\phi(n) = n \prod_{i \in [k]} \left(1 - \frac{1}{p_i}\right)$.

Proof. This is Thm 2.30 with new notations. $\square$

Thm. 7.2. Let $n \in \mathbb{P}$. Then, $\sum_{d \mid n} \phi(d) = n$.

Here and in the following,
"$\sum_{d \mid n}$" means "$\sum_{d \in \mathbb{P};\ d \mid n}$".

Proof of Thm. 7.2. We have

$$(63) \qquad n = \sum_{i \in [n]} 1 = \sum_{d \mid n} \sum_{\substack{i \in [n]; \\ \gcd(i,n) = d}} 1$$

(recall: gcd (a, b) is the greatest common divisor of a and b; it is divisible by each other divisor of a and b).

But fix a positive divisor d of n.
Then, the map

$$\{i \in [n] \mid \gcd(i,n) = d\} \to \{m \in [\tfrac{n}{d}] \mid m \text{ is coprime to } \tfrac{n}{d}\},$$

$$i \mapsto i/d$$

is well-defined & bijective. Thus,

(# of $i \in [n]$ such that $\gcd(i,n) = d$)
= (# of $m \in [\frac{n}{d}]$ such that m is coprime to $\frac{n}{d}$)
$= \phi(\frac{n}{d})$ (by the definition of ϕ).

~~Summing~~ In other words,

$$\sum_{\substack{i \in [n]; \\ \gcd(i,n) = d}} 1 = \phi\left(\frac{n}{d}\right).$$

Summing up this equality over all positive divisors d of n, we get

$$\sum_{d \mid n} \sum_{\substack{i \in [n]; \\ \gcd(i,n)=d}} 1 = \sum_{d \mid n} \phi\left(\frac{n}{d}\right) = \sum_{d \mid n} \phi(d)$$

(here, we substituted d for n/d, since the map $\{\text{positive divisors of } n\} \to \{\text{positive divisors of } n\}$,

$$d \mapsto \frac{n}{d}$$

is bijective).

$\square$

Thus, (63) becomes $n = \sum_{d \mid n} \phi(d)$.

<u>Rmk.</u> Alternative way to explain this proof:
Double-count the n fractions $\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \ldots, \frac{n}{n}$.
After cancelling, their denominators will be divisors of n, with each positive divisor d occurring exactly $\phi(d)$ times.

Def. An $n \in \mathbb{P}$ is said to be <u>squarefree</u> if no $\underbrace{\text{square}}_{=\text{perfect square}} > 1$ divides n.

In other words, n is squarefree if each prime appears at most once in its factorization.

For example, 15 is squarefree (since $15 = 3 \cdot 5$) but 12 is not (since $2^2 \mid 12$ or since $12 = 2^2 \cdot 3$).

Def. The <u>(number-theoretical) Möbius function</u> is the function $\mu : \mathbb{P} \to \mathbb{Z}$ sending each n to

$$\begin{cases} (-1)^{(\#\text{ of prime factors of } n)}, & \text{if } n \text{ is squarefree;} \\ 0, & \text{otherwise.} \end{cases}$$

Ex:

n	1	2	3	4	5	6	7	8	9	10	11	12	13
$\mu(n)$	1	-1	-1	0	-1	1	-1	0	0	1	-1	0	-1

Thm. 7.3. Let $n \in \mathbb{P}$. Then, $\sum_{d \mid n} \mu(d) = [n=1]$.

Proof. Let $p_1, p_2, \ldots, p_k$ be the distinct prime factors of n.

Then, $n=1$ is equivalent to $k=0$.

Thus, $[n=1] = [k=0]$.

Now, the divisors of n all have the form $p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ with $a_1, a_2, \ldots, a_k \geq 0$. Among these, the squarefree divisors are the ones where $a_1, a_2, \ldots, a_k \leq 1$.

Thus, the squarefree divisors of n are precisely the numbers $\prod_{i \in I} p_i$ for $I \subseteq [k]$. More precisely, the map

$$\{\text{subsets of } [k]\} \to \{\text{squarefree divisors of } [n]\},$$
$$I \mapsto \prod_{i \in I} p_i$$

is a bijection (by the Fundamental Theorem of Arithmetic).

Hence,
$$\sum_{\substack{d \mid n; \\ d \text{ is squarefree}}} \mu(d) = \sum_{I \subseteq [k]} \underbrace{\mu\left(\prod_{i \in I} p_i\right)}_{=(-1)^{|I|}}$$

$$= \sum_{I \subseteq [k]} (-1)^{|I|} = [[k] = \varnothing] \quad (\text{by Thm. 2.24})$$

$$= [k = 0] = [n = 1].$$

Now,

$$\sum_{d \mid n} \mu(d) = \underbrace{\sum_{\substack{d \mid n; \\ d \text{ is squarefree}}} \mu(d)}_{= [n=1]} + \sum_{\substack{d \mid n; \\ d \text{ is not} \\ \text{squarefree}}} \underbrace{\mu(d)}_{\substack{=0 \\ (\text{by the} \\ \text{definition} \\ \text{of } \mu)}}$$

$$= [n = 1].$$

$\square$

~~Cor~~ **Thm. 7.4** (number-theoretical Möbius inversion I).

Let $(a_1, a_2, a_3, \ldots)$ and $(b_1, b_2, b_3, \ldots)$ be two sequences of numbers. Assume that

$$a_n = \sum_{d \mid n} b_d \quad \text{for all } n \in \mathbb{P}. \tag{64}$$

Then,

(65) $$b_n = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) a_d \quad \text{for all } n \in \mathbb{P}.$$

Ex: In the situation of Thm. 7.4, we have

$$b_8 = a_8 - a_4 \quad \text{(by (65) for } n=8\text{)}$$

and $$b_{12} = a_{12} - a_6 - a_4 + a_2 \quad \text{(by (65) to } n=12\text{)}.$$

Check: $$a_8 - a_4 = (b_8 + b_4 + b_2 + b_1) - (b_4 + b_2 + b_1) = b_8;$$

$$\begin{aligned} a_{12} - a_6 - a_4 + a_2 = &\ (b_{12} + b_6 + b_4 + b_3 + b_2 + b_1) \\ - &\ (b_6 + b_3 + b_2 + b_1) \\ - &\ (b_4 + b_2 + b_1) \\ + &\ (b_2 + b_1) \\ = &\ b_{12}. \end{aligned}$$

Proof of Thm. 7.4. ~~We have~~ Fix $n \in \mathbb{P}$. Then,

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) a_d$$

$$= \sum_{e|n} \mu\left(\frac{n}{e}\right) \underbrace{a_e}_{\substack{=\sum_{d|e} b_d \\ \text{(by (64))}}} = \sum_{e|n} \mu\left(\frac{n}{e}\right) \sum_{d|e} b_d$$

$$= \underbrace{\sum_{e|n} \sum_{d|e}}_{=\sum_{d|n} \sum_{\substack{e|n; \\ d|e}}} \mu\left(\frac{n}{e}\right) b_d = \sum_{d|n} \underbrace{\sum_{\substack{e|n; \\ d|e}} \mu\left(\frac{n}{e}\right)}_{=\sum_{f|\frac{n}{d}} \mu(f)} b_d$$

(here, we substituted f for $\frac{n}{e}$, since the map

$\{\text{divisors } e \text{ of } n \text{ that satisfy } d|e\} \to \{\text{divisors of } \frac{n}{d}\}$,

$e \mapsto \frac{n}{e}$ is a bijection)

$$= \sum_{d \mid n} \underbrace{\sum_{f \mid \frac{n}{d}} \mu(f)}_{\substack{= \left[\frac{n}{d} = 1\right] \\ \text{(by Thm. 7.3, applied to } \frac{n}{d} \\ \text{instead of } n)}} b_d$$

$$= \sum_{d \mid n} \underbrace{\left[\frac{n}{d} = 1\right]}_{= [d = n]} b_d = \sum_{d \mid n} [d = n] b_d = b_n. \quad \square$$

<u>Rmk.</u> The converse also holds: (65) $\Longrightarrow$ (64).

<u>Prop. 7.5.</u> Let $n \in \mathbb{P}$. Then, $\sum_{d \mid n} \frac{n}{d} \mu(d) = \phi(n)$.

<u>1st proof.</u> Thm. 7.2 says $n = \sum_{d \mid n} \phi(d)$, for all $n \in \mathbb{P}$.

Thus, Thm. 7.4 (applied to $a_i = i$ and $b_i = \phi(i)$) yields

$$\phi(n) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) d = \sum_{d \mid n} \mu(d) \frac{n}{d}$$

(here, we have substituted $\frac{n}{d}$ for d in the sum, as before). $\square$

<u>2nd proof (idea).</u> Let $p_1, p_2, \ldots, p_k$ be the distinct prime divisors of n. Then, Prop. 7.1 yields

$$\phi(n) = n \prod_{i \in [k]} \left(1 - \frac{1}{p_i}\right)$$

$$\underset{\text{Prop. 2.29(b)}}{=} n \sum_{I \subseteq [k]} (-1)^{|I|} \prod_{i \in I} \frac{1}{p_i}$$

$$= n \sum_{\substack{d \mid n; \\ d \text{ is squarefree}}} \mu(d) \frac{1}{d} \qquad \left(\begin{array}{c}\text{by the same reasoning} \\ \text{as in the proof of} \\ \text{Thm. 7.3}\end{array}\right)$$

$$= n \sum_{d \mid n} \mu(d) \frac{1}{d} \qquad \left(\begin{array}{c}\text{since } \mu(d) = 0 \\ \text{when } d \text{ is not squarefree}\end{array}\right)$$

$$= \sum_{d \mid n} \mu(d) \frac{n}{d}.$$ $\square$

See number theory texts for more about ϕ, μ and similar functions (e.g. [Niven / Zuckerman / Montgomery]).

7.2. A simple lemma

Prop. 7.6. Let X be a finite set. Let ρ be a permutation of X. Let n be a positive integer such that $\rho^n = \mathrm{id}$. Then, ~~ρ has a disjoint every~~ the size of any cycle of ρ divides n.

Proof. Let C be a cycle of ρ. We must show $|C| \mid n$. Let $x \in C$. Let k be the smallest positive integer such that $\rho^k(x) = x$. Now, if $p \in \mathbb{N}$ is arbitrary, then

$$\rho^p(x) = \rho^{p \% k}(x),$$

where $p \% k$ means "remainder of p modulo k".

(Proof of (66): Induction on p, using $\rho^k(x) = x$.)

~~Now,~~ Also, $\rho^0(x), \rho^1(x), \ldots, \rho^{k-1}(x)$ are distinct, since otherwise there would be $0 \leq a < b < k$ such that $\rho^a(x) = \rho^b(x) \implies x = \rho^{b-a}(x)$, which would contradict the minimality of k.

Thus, $C = \underbrace{\{\rho^0(x), \rho^1(x), \ldots, \rho^{k-1}(x)\}}_{k \text{ distinct elements}}$, so that $|C| = k$.

Now, (66) yields $\rho^n(x) = \rho^{n \% k}(x)$. Hence

$$\rho^{n\%k}(x) = \underbrace{\rho^n}_{=id}(x) = x = \rho^0(x)$$

$$\implies \quad n \% k = 0 \quad \text{(since } \rho^0(1), \rho^1(x), \ldots, \rho^{k-1}(x) \text{ are distinct)}$$

$$\implies \quad k \mid n \quad \implies \quad |C| = k \mid n.$$

□

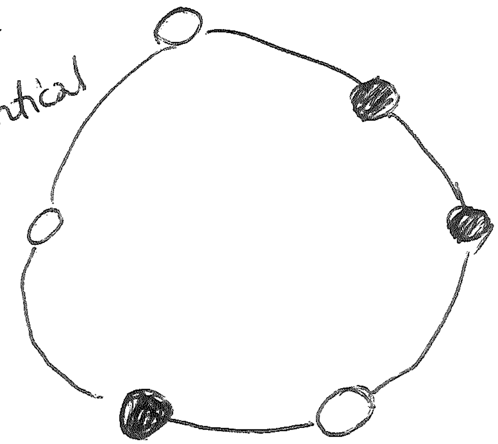
(We have used Prop. 7.6 already when we were discussing shift-equivalence.)

7.3. Necklaces

Idea:

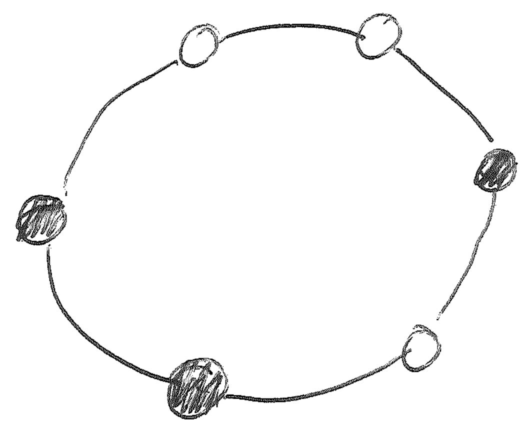
Consider rotated versions to be identical

=



but reflected versions are not (unless you can also get them by rotation)

≠



Def: Let Q be a set. Let n be a positive integer.

(a) The map

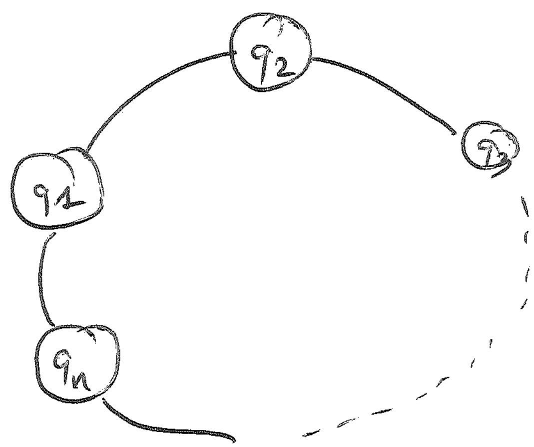
$$\rho : Q^n \to Q^n,$$
$$(q_1, q_2, \ldots, q_n) \mapsto (q_2, q_3, \ldots, q_n, q_1)$$

is called rotation.

This ρ is a permutation of Q^n, and satisfies $\rho^n = \mathrm{id}$.

(b) The cycles of ρ are called necklaces with n beads and colors from Q.

(Idea: the necklace containing $(q_1, q_2, \ldots, q_n)$ is



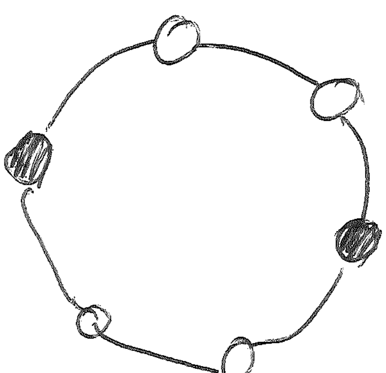
)

If $(q_1, q_2, \dots, q_n) \in Q^n$, then $[(q_1, q_2, \dots, q_n)]$ shall mean the necklace (= cycle of ρ) that contains it,

(c) The set of all necklaces with n beads and colors from Q is denoted by Q^n_{neck}.

(d) The cardinality of a necklace (i.e., the # of n-tuples $\vec{q} \in Q^n$ that belong to this necklace) is called its <u>period</u>.

[<u>Ex:</u> The necklace $[(2,1,1,2,1,1)]$
$= \{(2,1,1,2,1,1),$
$(1,1,2,1,1,2),$
$(1,2,1,1,2,1)\}$



$(2 \hat{=} \bullet$ and $1 \hat{=} \circ)$

has period 3.]

(e) The set of all necklaces with n beads and colors from Q having period k is denoted by $Q^n_{\text{neck},k}$.

<u>Question:</u> How many necklaces are there in Q^n_{neck}, when n and $|Q|$ are given?

<u>Cor. 7.7.</u> The period of any necklace in Q^n_{neck} is a positive divisor of n.

<u>Proof.</u> It is the size of a cycle of ρ, thus divides n (by Prop. 7.6). $\square$

<u>Lem. 7.8.</u> Let Q and n be as before. Let k be a positive divisor of n. Then,

$$|Q^n_{\text{neck},k}| = |Q^k_{\text{neck},k}|.$$

Thm. 7.9. Let Q and n be as before. Let $q = |Q|$.

(a) We have $$|Q^n_{\text{neck},n}| = \frac{1}{n}\sum_{d \mid n} \mu\left(\frac{n}{d}\right) q^d = \frac{1}{n}\sum_{d \mid n} \mu(d)\, q^{n/d}.$$

(b) We have $$|Q^n_{\text{neck}}| = \frac{1}{n}\sum_{d \mid n} \phi\left(\frac{n}{d}\right) q^d = \frac{1}{n}\sum_{d \mid n} \phi(d)\, q^{n/d}.$$

(c) Let $Q = [q]$, and let $a_1, a_2, \ldots, a_q \in \mathbb{N}$. Then,

(# of necklaces with n beads and colors from Q, where color i appears a_i many times $\forall i$)

$$= \frac{1}{n}\sum_{d \mid n} \phi\left(\frac{n}{d}\right) \underbrace{\binom{d}{a_1\frac{d}{n}, a_2\frac{d}{n}, \ldots, a_q\frac{d}{n}}}_{\substack{\text{This is understood to be} \\ 0 \text{ unless all the } a_i\frac{d}{n} \in \mathbb{N} \\ \text{and } \sum_i a_i = n}}.$$