the best way to count

bonus: magic sequences

Lucilla

definition floor, fract

the *floor function* $x \mapsto \lfloor x \rfloor$ is defined as the largest integer less than or equal to x.
it satisfies $\lfloor x \rfloor = x$ for integer x and $x - 1 < \lfloor x \rfloor < x$ otherwise.
this function is idempotent: $\lfloor \lfloor x \rfloor \rfloor = \lfloor x \rfloor$.

the *fractional part function* $x \mapsto \{x\}$ is defined as $x - \lfloor x \rfloor$.
it satisfies $\{x\} = 0$ for integer x and $0 < \{x\} < 1$ otherwise.
this function is idempotent: $\{\{x\}\} = \{x\}$.
it is also periodic with period 1; if n is an integer, then $\{x + n\} = \{x\}$.

definition div, mod

the *Euclidean division functions* div and mod are defined as follows:

- $a \,\mathsf{div}\, b = \lfloor a/b \rfloor$;
- $a \,\mathsf{mod}\, b = b \cdot \{a/b\}$.

div and mod satisfy the *Euclidean division theorem*:
for any integer a and natural number b with $b \neq 0$, there exist integers q and r such that $0 \leq r < b$ and $a = q \cdot b + r$, namely $q = a \,\mathsf{div}\, b$ and $r = a \,\mathsf{mod}\, b$.

the simultaneous application of div and mod is denoted divmod; the statement $a \,\mathsf{divmod}\, b = (q, r)$ is to be read as $a \,\mathsf{div}\, b = q \ \wedge \ a \,\mathsf{mod}\, b = r$.

definition magic sequence

let b be a natural number (the *base*); $b > 1$.
let n be a natural number, $n > 1$.
let s be a natural number, $1 \leq s < n$.

the *magic sequence* for n in *base* b with *offset* s (usually $s = 1$) is an infinite sequence of integers mag_i $(i \geq 0)$ defined recursively as:

- $\mathsf{mag}_0 = s$;
- $\mathsf{mag}_{i+1} = (b \cdot \mathsf{mag}_i) \,\mathsf{mod}\, n$.

the corresponding *quotient sequence* is the sequence div_i $(i \geq 1)$ defined as
$\mathsf{div}_{i+1} = (b \cdot \mathsf{mag}_i) \,\mathsf{div}\, n$.

example of a magic sequence with $b = 6, n = 11, s = 1$:

- $\mathsf{mag}_0 = 1$;
- $(1 \cdot 6) \,\mathsf{divmod}\, 11 = (0, 6) \ \Rightarrow \ \mathsf{div}_1 = 0,\ \mathsf{mag}_1 = 6$;
- $(6 \cdot 6) \,\mathsf{divmod}\, 11 = (3, 3) \ \Rightarrow \ \mathsf{div}_2 = 3,\ \mathsf{mag}_2 = 3$;
- $(3 \cdot 6) \,\mathsf{divmod}\, 11 = (1, 7) \ \Rightarrow \ \mathsf{div}_3 = 1,\ \mathsf{mag}_3 = 7$;
- $(7 \cdot 6) \,\mathsf{divmod}\, 11 = (3, 9) \ \Rightarrow \ \mathsf{div}_4 = 3,\ \mathsf{mag}_4 = 9$;
- ...

magic sequence divisibility test

lemma

let u, v be integers, and let n be a natural number, $n > 1$. then:

- $(u + v) \bmod n = ((u \bmod n) + (v \bmod n)) \bmod n$;
- $(u \cdot v) \bmod n = ((u \bmod n) \cdot (v \bmod n)) \bmod n$.

proof: the first statement is equivalent to

$$\{x + y\} = \{\{x\} + \{y\}\}$$

by setting $x := \frac{u}{n}$, $y := \frac{v}{n}$; observe that

$$\{\{x\} + \{y\}\} = \{x - \lfloor x \rfloor + y - \lfloor y \rfloor\} = \{x + y - (\lfloor x \rfloor + \lfloor y \rfloor)\};$$

noting that $(\lfloor x \rfloor + \lfloor y \rfloor)$ is an integer completes the equality.

the second statement is equivalent to

$$\left\{\frac{u}{n} \cdot \frac{v}{n} \cdot n\right\} = \left\{\left\{\frac{u}{n}\right\} \cdot \left\{\frac{v}{n}\right\} \cdot n\right\}$$

where the right-hand side can be expanded as

$$\begin{aligned}
\left\{\left\{\frac{u}{n}\right\} \cdot \left\{\frac{v}{n}\right\} \cdot n\right\} &= \left\{\left(\frac{u}{n} - \left\lfloor\frac{u}{n}\right\rfloor\right) \cdot \left(\frac{v}{n} - \left\lfloor\frac{v}{n}\right\rfloor\right) \cdot n\right\} \\
&= \left\{\left(\frac{u}{n} \cdot \frac{v}{n} - \frac{u}{n} \cdot \left\lfloor\frac{v}{n}\right\rfloor - \left\lfloor\frac{u}{n}\right\rfloor \cdot \frac{v}{n} + \left\lfloor\frac{u}{n}\right\rfloor \cdot \left\lfloor\frac{v}{n}\right\rfloor\right) \cdot n\right\} \\
&= \left\{\frac{u}{n} \cdot \frac{v}{n} \cdot n + \left(\left\lfloor\frac{u}{n}\right\rfloor \cdot \left\lfloor\frac{v}{n}\right\rfloor \cdot n - u \cdot \left\lfloor\frac{v}{n}\right\rfloor - v \cdot \left\lfloor\frac{u}{n}\right\rfloor\right)\right\}
\end{aligned}$$

and again noting that

$$\left(\left\lfloor\frac{u}{n}\right\rfloor \cdot \left\lfloor\frac{v}{n}\right\rfloor \cdot n - u \cdot \left\lfloor\frac{v}{n}\right\rfloor - v \cdot \left\lfloor\frac{u}{n}\right\rfloor\right)$$

is an integer. ■

corollary

variants where only one variable has had mod applied to it, namely

$$(u + v) \bmod n = (u + (v \bmod n)) \bmod n$$
$$(u \cdot v) \bmod n = (u \cdot (v \bmod n)) \bmod n$$

follow with a similar proof. alternatively, they can be derived by applying the normal variant twice, then using the idempotence of mod (which follows from the idempotence of the fractional part function) on one of the variables, then applying the normal variant backwards.

lemma

let mag_i be the magic sequence of n in base b with offset s. then

$$(s \cdot b^i) \mathbin{\mathsf{mod}} n = \mathsf{mag}_i$$

for all $i \geq 0$.

proof: induction for i.

let $i = 0$, then we have $s \mathbin{\mathsf{mod}} n = s$, which is true because $1 \leq s < n$.

suppose the statement is true for some i, then

$$\begin{aligned}
\mathsf{mag}_{i+1} &= (b \cdot \mathsf{mag}_i) \mathbin{\mathsf{mod}} n \\
&= (b \cdot (s \cdot b^i) \mathbin{\mathsf{mod}} n) \mathbin{\mathsf{mod}} n \\
&= (b \cdot s \cdot b^i) \mathbin{\mathsf{mod}} n \\
&= (s \cdot b^{i+1}) \mathbin{\mathsf{mod}} n,
\end{aligned}$$

thus the statement is true for $i + 1$, and hence for all $i \geq 0$. ∎

definition base-b representation

let b be a natural number (the *base*); $b > 1$.
let num be a natural number, $\mathsf{num} \geq 0$.

the *base-b representation* of num is a sequence d_i $(i \geq 0)$ which satisfies $0 \leq d_i < b$ for all i, only finitely many d_i are nonzero, and

$$\sum_i b^i \cdot d_i = \mathsf{num}.$$

the sequence d_i exists and is unique. d_i are called the *digits* of num in base b.

theorem magic sequence divisibility test

let mag_i be the magic sequence of n in base b with offset $s = 1$.
let num be a natural number, and let d_i be its digits in base b.
then

$$\mathsf{num} \mathbin{\mathsf{mod}} n = \left(\sum_i \mathsf{mag}_i \cdot d_i \right) \mathbin{\mathsf{mod}} n.$$

proof:

$$\begin{aligned}
\mathsf{num} \mathbin{\mathsf{mod}} n = \left(\sum_i b^i \cdot d_i \right) \mathbin{\mathsf{mod}} n &= \sum_i \big((b^i \cdot d_i) \mathbin{\mathsf{mod}} n \big) \mathbin{\mathsf{mod}} n \\
&= \sum_i \big(((b^i \mathbin{\mathsf{mod}} n) \cdot d_i) \mathbin{\mathsf{mod}} n \big) \mathbin{\mathsf{mod}} n \\
&= \sum_i \big((\mathsf{mag}_i \cdot d_i) \mathbin{\mathsf{mod}} n \big) \mathbin{\mathsf{mod}} n \\
&= \left(\sum_i \mathsf{mag}_i \cdot d_i \right) \mathbin{\mathsf{mod}} n.
\end{aligned}$$

∎

magic sequence fractions

lemma

let mag_i be the magic sequence of n in base b with offset s, and let div_i be the corresponding quotient sequence. then

$$\frac{s \cdot b^i}{n} - b^{i-1} \cdot \mathsf{div}_1 - b^{i-2} \cdot \mathsf{div}_2 - \ldots - \mathsf{div}_i = \frac{\mathsf{mag}_i}{n}$$

for all $i \geq 0$.

proof: induction for i.

let $i = 0$, then we have

$$\frac{s \cdot b^0}{n} = \frac{s}{n} = \frac{\mathsf{mag}_0}{n}.$$

suppose the statement is true for some i, then

$$\begin{aligned}
&\frac{s \cdot b^{i+1}}{n} - b^i \cdot \mathsf{div}_1 - b^{i-1} \cdot \mathsf{div}_2 - \ldots - b \cdot \mathsf{div}_i - \mathsf{div}_{i+1} \\
&= b \cdot \left(\frac{s \cdot b^i}{n} - b^{i-1} \cdot \mathsf{div}_1 - b^{i-2} \cdot \mathsf{div}_2 - \ldots - \mathsf{div}_i \right) - \mathsf{div}_{i+1} \\
&= \frac{b \cdot \mathsf{mag}_i}{n} - \mathsf{div}_{i+1} \\
&= \frac{b \cdot \mathsf{mag}_i}{n} - (b \cdot \mathsf{mag}_i) \;\mathsf{div}\; n \\
&= \frac{b \cdot \mathsf{mag}_i}{n} - \left\lfloor \frac{b \cdot \mathsf{mag}_i}{n} \right\rfloor = \left\{ \frac{b \cdot \mathsf{mag}_i}{n} \right\} \\
&= \frac{(b \cdot \mathsf{mag}_i) \;\mathsf{mod}\; n}{n} = \frac{\mathsf{mag}_{i+1}}{n},
\end{aligned}$$

thus the statement is true for $i + 1$ and hence for all $i \geq 0$. ■

definition base-b fractional expansion

let b be a natural number (the *base*); $b > 1$.
let ratio be a real number, $0 \leq \mathsf{ratio} < 1$.

the *base-b fractional expansion* of ratio is a sequence r_i $(i \geq 1)$ which satisfies $0 \leq r_i < b$ for all i and

$$\mathsf{ratio} - \frac{1}{b^k} < \sum_{i \leq k} \frac{r_i}{b^i} \leq \mathsf{ratio}$$

for all $k \geq 1$.

the sequence r_i exists and is unique. r_i are called the *digits* of ratio in base b, and it holds that

$$\sum_i^{\infty} \frac{r_i}{b^i} = \mathsf{ratio}.$$

(the second condition is necessary for uniqueness. without it, some real numbers have two different fractional expansions, e.g. $\frac{1}{5} = 0.1999\ldots = 0.2000\ldots$ in base ten. with this definition, only $0.2000\ldots$ is a valid fractional expansion.)

theorem magic sequence fractions

let mag_i be the magic sequence of n in base b with offset s,
and let div_i be the corresponding quotient sequence.
let r_i be the digits of s/n in base b.
then $\mathsf{div}_i = r_i$ for all $i \geq 1$.

proof: induction for i.

first let $i = 1$. suppose $\frac{s}{n} = \frac{r_1}{b}$ exactly. then $r_1 = \frac{s \cdot b}{n}$. but r_1 must be an integer, so take

$$\left\lfloor \frac{s \cdot b}{n} \right\rfloor = (s \cdot b) \ \mathsf{div}\ n = (b \cdot \mathsf{mag}_0) \ \mathsf{div}\ n = \mathsf{div}_1$$

instead. the inequality $x - 1 < \lfloor x \rfloor \leq x$ for the floor function then implies the inequality

$$\frac{s}{n} - \frac{1}{b} < \frac{r_1}{b} \leq \frac{s}{n}.$$

now suppose $\mathsf{div}_j = r_j$ for all $j \leq i$. suppose

$$\frac{s}{n} = \frac{r_1}{b} + \frac{r_2}{b^2} + \ldots + \frac{r_i}{b^i} + \frac{r_{i+1}}{b^{i+1}}$$

exactly; this implies

$$\frac{s}{n} - \frac{\mathsf{div}_1}{b} - \frac{\mathsf{div}_2}{b^2} - \ldots - \frac{\mathsf{div}_i}{b^i} = \frac{r_{i+1}}{b^{i+1}}.$$

in that case

$$r_{i+1} = b \cdot \left(\frac{s \cdot b^i}{n} - b^{i-1} \cdot \mathsf{div}_1 - b^{i-2} \cdot \mathsf{div}_2 - \ldots - \mathsf{div}_i \right),$$

which by the lemma above is equal to $b \cdot \frac{\mathsf{mag}_{i+1}}{n}$. but r_{i+1} must be an integer, so take

$$\left\lfloor \frac{b \cdot \mathsf{mag}_{i+1}}{n} \right\rfloor = (b \cdot \mathsf{mag}_{i+1}) \ \mathsf{div}\ n = \mathsf{div}_{i+1}$$

instead; and again the floor function inequality implies

$$\frac{s}{n} - \frac{1}{b^{i+1}} < \sum_{j \leq i+1} \frac{r_j}{b^j} \leq \frac{s}{n}.$$

■