Exercises from Section 1.2.4

Tord M. Johnson

March 9, 2014

1. [*00*] What are $\lfloor 1.1 \rfloor$, $\lfloor -1.1 \rfloor$, $\lceil -1.1 \rceil$, $\lfloor 0.99999 \rfloor$, and $\lfloor \lg 35 \rfloor$?

We have:

$$\begin{aligned} \lfloor 1.1 \rfloor &= 1 && 1 \le 1.1 < 2 \\ \lfloor -1.1 \rfloor &= -2 && -2 \le -1.1 < -1 \\ \lceil -1.1 \rceil &= -1 && -2 < -1.1 \le -1 \\ \lfloor 0.99999 \rfloor &= 0 && 0 \le 0.99999 < 1 \\ \lfloor \lg 35 \rfloor &= 5 && 5 = \lg 32 \le \lg 35 < \lg 64 = 6 \end{aligned}$$

▶ **2.** [*01*] What is $\lceil \lfloor x \rfloor \rceil$?

$\lceil \lfloor x \rfloor \rceil = \lfloor x \rfloor$ since $\lfloor x \rfloor$ is an integer and $\lfloor x \rfloor - 1 < \lfloor x \rfloor \le \lfloor x \rfloor$.

3. [*M10*] Let n be an integer, and let x be a real number. Prove that a) $\lfloor x \rfloor < n$ if and only if $x < n$; b) $n \le \lfloor x \rfloor$ if and only if $n \le x$; c) $\lceil x \rceil \le n$ if and only if $x \le n$; d) $n < \lceil x \rceil$ if and only if $n < x$; e) $\lfloor x \rfloor = n$ if and only if $x - 1 < n \le x$, and if and only if $n \le x < n + 1$; f) $\lceil x \rceil = n$ if and only if $x \le n < x + 1$, and if and only if $n - 1 < x \le n$.

[*These formulas are the most important tools for proving facts about* $\lfloor x \rfloor$ *and* $\lceil x \rceil$.]

We may prove the various propositions.

Proposition (A)**.** *$\lfloor x \rfloor < n$ if and only if $x < n$ for all integers n, real numbers x.*

Proof. Let n be an integer and x a real number. We must show that $\lfloor x \rfloor < n$ if and only if $x < n$.

If $\lfloor x \rfloor < n$:

$$\begin{aligned} & \lfloor x \rfloor \le x < \lfloor x \rfloor + 1 \\ & \lfloor x \rfloor < n \implies \lfloor x \rfloor + 1 \le n \\ \therefore \quad & x < n \end{aligned}$$

If $x < n$:

$$\begin{aligned} & \lfloor x \rfloor \le x < \lfloor x \rfloor + 1 \\ & x < n \\ \therefore \quad & \lfloor x \rfloor < n \end{aligned}$$

Therefore, $\lfloor x \rfloor < n$ if and only if $x < n$. □

Proposition (B)**.** *$n \le \lfloor x \rfloor$ if and only if $n \le x$ for all integers n, real numbers x.*

Proof. Let n be an integer and x a real number. We must show that $n \leq \lfloor x \rfloor$ if and only if $n \leq x$.

If $n \leq \lfloor x \rfloor$:

$$\begin{aligned} & \lfloor x \rfloor \leq x < \lfloor x \rfloor + 1 \\ & n \leq \lfloor x \rfloor \\ \therefore \quad & n \leq x \end{aligned}$$

If $n \leq x$:

$$\begin{aligned} & \lfloor x \rfloor \leq x < \lfloor x \rfloor + 1 \quad \Longrightarrow \quad \lfloor x \rfloor - 1 \leq x - 1 < \lfloor x \rfloor \\ & n \leq x \\ \therefore \quad & n < \lfloor x \rfloor + 1 \quad \Longrightarrow \quad n \leq \lfloor x \rfloor \end{aligned}$$

Therefore, $n \leq \lfloor x \rfloor$ if and only if $n \leq x$. □

Proposition (C)**.** *$\lceil x \rceil \leq n$ if and only if $x \leq n$ for all integers n, real numbers x.*

Proof. Let n be an integer and x a real number. We must show that $\lceil x \rceil \leq n$ if and only if $x \leq n$.

If $\lceil x \rceil \leq n$:

$$\begin{aligned} & \lceil x \rceil - 1 < x \leq \lceil x \rceil \\ & \lceil x \rceil \leq n \\ \therefore \quad & x \leq n \end{aligned}$$

If $x \leq n$:

$$\begin{aligned} & \lceil x \rceil - 1 < x \leq \lceil x \rceil \\ & x \leq n \\ \therefore \quad & \lceil x \rceil - 1 < n \quad \Longrightarrow \quad \lceil x \rceil \leq n \end{aligned}$$

Therefore, $\lceil x \rceil \leq n$ if and only if $x \leq n$. □

Proposition (D)**.** *$n < \lceil x \rceil$ if and only if $n < x$ for all integers n, real numbers x.*

Proof. Let n be an integer and x a real number. We must show that $n < \lceil x \rceil$ if and only if $n < x$.

If $n < \lceil x \rceil$:

$$\begin{aligned} & \lceil x \rceil - 1 < x \leq \lceil x \rceil \\ & n < \lceil x \rceil \quad \Longrightarrow \quad n \leq \lceil x \rceil - 1 \\ \therefore \quad & n < x \end{aligned}$$

If $n < x$:

$$\begin{aligned} & \lceil x \rceil - 1 < x \leq \lceil x \rceil \\ & n < x \\ \therefore \quad & n < \lceil x \rceil \end{aligned}$$

Therefore, $n < \lceil x \rceil$ if and only if $n < x$. □

Proposition (E)**.** *$\lfloor x \rfloor = n$ if and only if $x-1 < n \leq x$, and if and only if $n \leq x < n+1$ for all integers n, real numbers x.*

Proof. Let n be an integer and x a real number. We must show that $\lfloor x \rfloor = n$ if and only if $x - 1 < n \leq x$, and if and only if $n \leq x < n + 1$.

If $\lfloor x \rfloor = n$:

$$\begin{aligned} & \lfloor x \rfloor = n \implies n \leq \lfloor x \rfloor \implies n \leq x && \text{from (b)} \\ & \lfloor x \rfloor = n \implies \lfloor x \rfloor \leq n \implies \lfloor x \rfloor < n+1 \implies x < n+1 \equiv x-1 < n && \text{from (a)} \\ \therefore \quad & x - 1 < n \leq x \wedge n \leq x < n + 1 \end{aligned}$$

If $x - 1 < n \leq x$:

$$\begin{aligned} & x - 1 < n \leq x \implies n \leq \lfloor x \rfloor && \text{from (b)} \\ & x - 1 < n \leq x \implies x < n+1 \implies \lfloor x \rfloor < n+1 \implies \lfloor x \rfloor \leq n && \text{from (a)} \\ \therefore \quad & n \leq \lfloor x \rfloor \wedge \lfloor x \rfloor \leq n \implies \lfloor x \rfloor = n \end{aligned}$$

If $n \leq x < n + 1$:

$$\begin{aligned} & n \leq x < n+1 \implies n \leq \lfloor x \rfloor && \text{from (b)} \\ & n \leq x < n+1 \implies x < n+1 \implies \lfloor x \rfloor < n+1 \implies \lfloor x \rfloor \leq n && \text{from (a)} \\ \therefore \quad & n \leq \lfloor x \rfloor \wedge \lfloor x \rfloor \leq n \implies \lfloor x \rfloor = n \end{aligned}$$

Therefore, $\lfloor x \rfloor = n$ if and only if $x - 1 < n \leq x$, and if and only if $n \leq x < n + 1$. □

Proposition (F)**.** *$\lceil x \rceil = n$ if and only if $x \leq n < x+1$, and if and only if $n-1 < x \leq n$ for all integers n, real numbers x.*

Proof. Let n be an integer and x a real number. We must show that $\lceil x \rceil = n$ if and only if $x \leq n < x + 1$, and if and only if $n - 1 < x \leq n$.

If $\lceil x \rceil = n$:

$$\begin{aligned} & \lceil x \rceil = n \implies \lceil x \rceil \leq n \implies x \leq n && \text{from (c)} \\ & \lceil x \rceil = n \implies n \leq \lceil x \rceil \implies n-1 < \lceil x \rceil \implies n-1 < x \equiv n < x+1 && \text{from (d)} \\ \therefore \quad & x \leq n < x + 1 \wedge n - 1 < x \leq n \end{aligned}$$

If $x \le n < x+1$:

$$\begin{array}{lllll} x \le n < x+1 & \implies & x \le n & \implies & \lceil x \rceil \le n & & \text{from (c)} \\ x \le n < x+1 & \implies & n-1 < x & \implies & n-1 < \lceil x \rceil \implies n \le \lceil x \rceil & & \text{from (d)} \\ \therefore \quad \lceil x \rceil \le n \wedge n \le \lceil x \rceil & \implies & \lceil x \rceil = n & & & & \end{array}$$

If $n-1 < x \le n$:

$$\begin{array}{lllll} n-1 < x \le n & \implies & x \le n & \implies & \lceil x \rceil \le n & & \text{from (c)} \\ n-1 < x \le n & \implies & n-1 < x & \implies & n-1 < \lceil x \rceil \implies n \le \lceil x \rceil & & \text{from (d)} \\ \therefore \quad \lceil x \rceil \le n \wedge n \le \lceil x \rceil & \implies & \lceil x \rceil = n & & & & \end{array}$$

Therefore, $\lceil x \rceil = n$ if and only if $x \le n < x+1$, and if and only if $n-1 < x \le n$. □

► **4.** [*M10*] Using the previous exercise, prove that $\lfloor -x \rfloor = -\lceil x \rceil$.

Proposition. $\lfloor -x \rfloor = -\lceil x \rceil$ *for any real number* x.

Proof. Let x be an arbitrary real number. We must show that $\lfloor -x \rfloor = -\lceil x \rceil$.

Given

$$\begin{array}{lll} \lceil x \rceil - 1 < x \le \lceil x \rceil & \implies & -\lceil x \rceil + 1 > -x \ge -\lceil x \rceil \\ & \implies & -\lceil x \rceil \le -x < -\lceil x \rceil + 1 \end{array}$$

and

$$\begin{array}{lll} \lceil x \rceil - 1 < x \le \lceil x \rceil & \implies & x \le \lceil x \rceil < x+1 \\ & \implies & -x \ge -\lceil x \rceil > -x-1 \\ & \implies & -x-1 < -\lceil x \rceil \le -x, \end{array}$$

by the previous exercise, we have

$$\lfloor -x \rfloor = -\lceil x \rceil$$

as we needed to show. □

5. [*16*] Given that x is a positive real number, state a simple formula that expresses x *rounded to the nearest integer*. The desired rounding rule is to produce $\lfloor x \rfloor$ when $x \bmod 1 < \frac{1}{2}$, and to produce $\lceil x \rceil$ when $x \bmod 1 \ge \frac{1}{2}$. Your answer should be a single formula that covers both cases. Discuss the rounding that would be obtained by your formula when x is negative.

A simple formula to express x *rounded to the nearest integer* could be given as

$$\text{round}(x) = \left\lfloor x + \frac{1}{2} \right\rfloor.$$

Note that it satisfies the requirements, as

$$\begin{aligned}
\operatorname{round}(x) &= \left\lfloor x + \frac{1}{2} \right\rfloor \\
&= \left\lfloor x + \frac{1}{2} + \lfloor x \rfloor - \lfloor x \rfloor \right\rfloor \\
&= \left\lfloor \lfloor x \rfloor + x - \lfloor x \rfloor + \frac{1}{2} \right\rfloor \\
&= \left\lfloor \lfloor x \rfloor + x \bmod 1 + \frac{1}{2} \right\rfloor \\
&= \lfloor x \rfloor + \left\lfloor x \bmod 1 + \frac{1}{2} \right\rfloor \\
&= \begin{cases} \lfloor x \rfloor + 0 = \lfloor x \rfloor & \text{if } x \bmod 1 < \frac{1}{2} \\ \lfloor x \rfloor + 1 = \lceil x \rceil & \text{if } x \bmod 1 \geq \frac{1}{2}. \end{cases}
\end{aligned}$$

(Note that $x \bmod 1 \geq \frac{1}{2}$ implies x is not an integer, otherwise $x \bmod 1 = 0$.)

For negative values of x, we find that (in general), $\operatorname{round}(-x) = -\operatorname{round}(x)$ *except* when $x \bmod 1 = \frac{1}{2}$, in which case x is rounded *away from zero* if positive, *towards zero* if negative.

► **6.** [*20*] Which of the following equations are true for all positive real numbers x? (a) $\left\lfloor \sqrt{\lfloor x \rfloor} \right\rfloor = \lfloor \sqrt{x} \rfloor$; (b) $\left\lceil \sqrt{\lceil x \rceil} \right\rceil = \lceil \sqrt{x} \rceil$; (c) $\left\lceil \sqrt{\lfloor x \rfloor} \right\rceil = \lceil \sqrt{x} \rceil$.

Some, but not all, of the equations are true.

(a) $\left\lfloor \sqrt{\lfloor x \rfloor} \right\rfloor = \lfloor \sqrt{x} \rfloor$ is true, since for an arbitrary integer n,

$$\begin{aligned}
\lfloor \sqrt{x} \rfloor = n \implies & \quad n \leq \sqrt{x} < n+1 \\
\implies & \quad n^2 \leq x < (n+1)^2 \\
\implies & \quad n^2 \leq \lfloor x \rfloor < (n+1)^2 \\
\implies & \quad n \leq \sqrt{\lfloor x \rfloor} < n+1 \\
\implies & \quad \left\lfloor \sqrt{\lfloor x \rfloor} \right\rfloor = n.
\end{aligned}$$

(b) $\left\lceil \sqrt{\lceil x \rceil} \right\rceil = \lceil \sqrt{x} \rceil$ is true, since for an arbitrary integer n,

$$\begin{aligned}
\lceil \sqrt{x} \rceil = n \implies & \quad n < \sqrt{x} \leq n+1 \\
\implies & \quad n^2 < x \leq (n+1)^2 \\
\implies & \quad n^2 < \lceil x \rceil \leq (n+1)^2 \\
\implies & \quad n \leq \sqrt{\lceil x \rceil} < n+1 \\
\implies & \quad \left\lceil \sqrt{\lceil x \rceil} \right\rceil = n.
\end{aligned}$$

(c) $\left\lceil \sqrt{\lfloor x \rfloor} \right\rceil = \lceil \sqrt{x} \rceil$ is not true, as can be demonstrated by counterexample. Consider $x = \frac{9}{4}$. Then

$$\left\lceil \sqrt{\left\lfloor \frac{9}{4} \right\rfloor} \right\rceil = \left\lceil \sqrt{1} \right\rceil = \lceil 1 \rceil = 1$$

but

$$\left\lceil \sqrt{\frac{9}{4}} \right\rceil = \left\lceil \frac{3}{2} \right\rceil = 2.$$

7. [*M15*] Show that $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x+y \rfloor$ and that equality holds if and only if $x \bmod 1 + y \bmod 1 < 1$. Does a smiliar formula hold for ceilings?

We may prove the proposition.

Proposition. $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x+y \rfloor$ *and equality holds if and only if* $x \bmod 1 + y \bmod 1 < 1$.

Proof. Let x and y be arbitrary real numbers. We must show that

$$\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor$$

and that equality holds if and only if $x \bmod 1 + y \bmod 1 < 1$.

But

$$\begin{aligned} \lfloor x+y \rfloor &= \lfloor \lfloor x \rfloor + x \bmod 1 + \lfloor y \rfloor + y \bmod 1 \rfloor \\ &= \lfloor x \rfloor + \lfloor y \rfloor + \lfloor x \bmod 1 + y \bmod 1 \rfloor \\ &= \begin{cases} \lfloor x \rfloor + \lfloor y \rfloor & \text{if } x \bmod 1 + y \bmod 1 < 1 \\ \lfloor x \rfloor + \lfloor y \rfloor + 1 & \text{otherwise.} \end{cases} \end{aligned}$$

That is, $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor$ and equality holds if and only if $x \bmod 1 + y \bmod 1 < 1$, as we needed to show. □

A similar formula holds for ceilings. In particular

$$\lceil x + y \rceil \leq \lceil x \rceil + \lceil y \rceil$$

with equality if and only if $(-x) \bmod 1 + (-y) \bmod 1 < 1$ since

$$\begin{aligned} \lceil x+y \rceil &= -\lfloor -x - y \rfloor \\ &= -\lfloor \lfloor -x \rfloor + (-x) \bmod 1 + \lfloor -y \rfloor + (-y) \bmod 1 \rfloor \\ &= -\lfloor -x \rfloor - \lfloor -y \rfloor - \lfloor (-x) \bmod 1 + (-y) \bmod 1 \rfloor \\ &= \begin{cases} \lceil x \rceil + \lceil y \rceil & \text{if } (-x) \bmod 1 + (-y) \bmod 1 < 1 \\ \lceil x \rceil + \lceil y \rceil - 1 & \text{otherwise.} \end{cases} \end{aligned}$$

Note that if x and y are not integers,

$$\begin{aligned} (-x) \bmod 1 + (-y) \bmod 1 < 1 \quad &\iff \quad -x - \lfloor -x \rfloor + -y - \lfloor -y \rfloor < 1 \\ &\iff \quad -x + \lceil x \rceil + -y + \lceil y \rceil < 1 \\ &\iff \quad -x + \lfloor x \rfloor + 1 + -y + \lfloor y \rfloor + 1 < 1 \\ &\iff \quad x + -\lfloor x \rfloor - 1 + y - \lfloor y \rfloor - 1 > -1 \\ &\iff \quad x \bmod 1 + y \bmod 1 - 2 > -1 \\ &\iff \quad x \bmod 1 + y \bmod 1 > 1. \end{aligned}$$

8. [*00*] What are $100 \bmod 3$, $100 \bmod 7$, $-100 \bmod 7$, $-100 \bmod 0$?

We have:

$$\begin{aligned} 100 \bmod 3 &= 1 && \text{since } 1 = 100 - 33(3) \\ 100 \bmod 7 &= 2 && \text{since } 2 = 100 - 14(7) \\ -100 \bmod 7 &= 5 && \text{since } 5 = -100 - 7\lfloor -100/7 \rfloor = -100 + 7(15) \\ -100 \bmod 0 &= -100. \end{aligned}$$

9. [*05*] What are 5 mod −3, 18 mod −3, −2 mod −3?

We have:

$$\begin{aligned} 5 \bmod -3 &= -1 && \text{since } -1 = 5 - (-3)\lfloor -5/3 \rfloor = 5 - 3(2) \\ 18 \bmod -3 &= 0 && \text{since } 0 = 18 - (-3)\lfloor -18/3 \rfloor = 18 - 3(6) \\ -2 \bmod -3 &= -2 && \text{since } -2 = -2 - (-3)\lfloor 2/3 \rfloor = -2 + 3(0). \end{aligned}$$

► **10.** [*10*] What are 1.1 mod 1, 0.11 mod .1, 0.11 mod −.1?

We have:

$$\begin{aligned} 1.1 \bmod 1 &= 0.1 && \text{since } 0.1 = 1.1 - 1\lfloor 1.1/1 \rfloor \\ 0.11 \bmod 0.1 &= 0.01 && \text{since } 0.01 = 0.11 - 0.1\lfloor 0.11/0.1 \rfloor \\ 0.11 \bmod -0.1 &= -0.09 && \text{since } 0.09 = 0.11 + 0.1\lfloor -0.11/0.1 \rfloor = 0.11 - 0.1(2). \end{aligned}$$

11. [*00*] What does "$x \equiv y$ (modulo 0)" mean by our conventions?

"$x \equiv y \pmod 0$" means $x = y$, since $x \equiv y \pmod 0$ is equivalent to asserting $x \bmod 0 = x = y = y \bmod 0$.

12. [*00*] What integers are relatively prime to 1?

All integers are relatively prime to 1 since for any integer n, $\gcd(n, 1) = 1$.

13. [*M00*] By convention, we say that the greatest common divisor of 0 and n is $|n|$. What integers are relatively prime to 0?

Given that $\gcd(0, n) = |n|$ for any integer n, then only -1 and 1 are relatively prime to 0.

► **14.** [*12*] If $x \bmod 3 = 2$ and $x \bmod 5 = 3$, what is $x \bmod 15$?

We have:

$$\begin{aligned} & x \equiv 2 \pmod 3 \quad \wedge \quad x \equiv 3 \pmod 5 \\ \iff & \quad 5x \equiv 10 \pmod{15} \quad \wedge \quad 3x \equiv 9 \pmod{15} && \text{by Law C} \\ \iff & \quad (5-3)x \equiv (10-9) \pmod{15} && \text{by Law A} \\ \iff & \quad (3-2)x \equiv (9-1) \pmod{15} && \text{by Law A} \\ \iff & \quad x \equiv 8 \pmod{15}. \end{aligned}$$

15. [*10*] Prove that $z(x \bmod y) = (zx) \bmod (zy)$. [Law C is an immediate consequence of this distributive law.]

Proposition. $z(x \bmod y) = (zx) \bmod (zy)$, $z \neq 0$.

Proof. Let x, y, and z be arbitrary real numbers, $z \neq 0$. We must show that

$$z(x \bmod y) = (zx) \bmod (zy).$$

But

$$x \bmod y = x - y \left\lfloor \frac{x}{y} \right\rfloor$$

if and only if

$$\begin{aligned} z(x \bmod y) &= z\left(x - y\left\lfloor \frac{x}{y} \right\rfloor\right) \\ &= zx - zy\left\lfloor \frac{x}{y} \right\rfloor \\ &= zx - zy\left\lfloor \frac{zx}{zy} \right\rfloor \\ &= (zx) \bmod (zy) \end{aligned}$$

as we needed to show. □

16. [*M10*] Assume that $y > 0$. Show that if $(x-z)/y$ is an integer and if $0 \le z < y$, then $z = x \bmod y$.

Proposition. *if* $y|(x-z)$ *and* $0 \le z < y$, *then* $z = x \bmod y$.

Proof. Let x, y, and z be arbitrary integers such that $y|(x-z)$ and $0 \le z < y$. We must show that $z = x \bmod y$.

But

$$\begin{aligned} x \bmod y &= x - y\left\lfloor \frac{x}{y} \right\rfloor \\ &= x - y\left\lfloor \frac{x+z-z}{y} \right\rfloor \\ &= x - y\left\lfloor \frac{x-z}{y} + \frac{z}{y} \right\rfloor \\ &= x - y\left(\frac{x-z}{y} + \left\lfloor \frac{z}{y} \right\rfloor\right) && \text{since } y|(x-z) \\ &= x - y\left(\frac{x-z}{y} + 0\right) && \text{since } 0 \le z < y \\ &= x - y\frac{x-z}{y} \\ &= x - x + z \\ &= z \end{aligned}$$

as we needed to show. □

17. [*M15*] Prove Law A directly from the definition of congruence, and also prove half of Law D: If $a \equiv b$ (modulo rs), then $a \equiv b$ (modulo r) and $a \equiv b$ (modulo s). (Here r and s are arbitrary integers.)

We may prove Law A.

Proposition. *If* $a \equiv b$ *and* $x \equiv y$, *then* $a \pm x \equiv b \pm y$ *and* $ax \equiv by \pmod m$.

Proof. Let a, b, x, y, and m be arbitrary integers so that $a \equiv b$ and $x \equiv y$. We must show that $a \pm x \equiv b \pm y$ and $ax \equiv by \pmod m$.

For some integer r and s, we have

$$a = b + mr \quad \wedge \quad x = y + ms.$$

In the case of addition, $a + x \equiv b + y \pmod m$ since

$$\begin{aligned} a + x &= b + mr + y + ms \\ &= b + y + m(r+s) \end{aligned}$$

for some integer $r + s$.

Similarly, in the case of subtraction, $a - x \equiv b - y \pmod{m}$ since

$$\begin{aligned} a - x &= b + mr - y - ms \\ &= b - y + m(r - s) \end{aligned}$$

for some integer $r - s$.

In the case of multiplication, $ax \equiv by \pmod{m}$ since

$$\begin{aligned} ax &= (b + mr)(y - ms) \\ &= by + ymr - bms - m^2rs \\ &= by + m(yr - bs - mrs) \end{aligned}$$

for some integer $yr - bs - mrs$.

Therefore, if $a \equiv b$ and $x \equiv y$, then $a \pm x \equiv b \pm y$ and $ax \equiv by \pmod{m}$ as we needed to show. □

We may also prove half of Law D, which doesn't require the assumption that $r \perp s$.

Proposition. *If $a \equiv b \pmod{rs}$, then $a \equiv b \pmod{r}$ and $a \equiv b \pmod{s}$.*

Proof. Let a, b, r, and s be arbitrary integers so that $a \equiv b \pmod{rs}$. We must show that $a \equiv b \pmod{r}$ and $a \equiv b \pmod{s}$.

But

$$a = b + rst$$

for some integer t, in which case we have that $a = b + ru$ and $a = b + sv$ for integers $u = st$ and $v = rt$.

Therefore, if $a \equiv b \pmod{rs}$, then $a \equiv b \pmod{r}$ and $a \equiv b \pmod{s}$. □

18. [*M15*] Using Law B, prove the other half of Law D: If $a \equiv b$ (modulo r) and $a \equiv b$ (modulo s), then $a \equiv b$ (modulo rs), provided that $r \perp s$.

Proposition. *If $a \equiv b \pmod{r}$ and $a \equiv b \pmod{s}$, then $a \equiv b \pmod{rs}$, provided $r \perp s$.*

Proof. Let a, b, r, and s be arbitrary integers so that $a \equiv b \pmod{r}$ and $a \equiv b \pmod{s}$, with $r \perp s$. We must show that $a \equiv b \pmod{rs}$.

But

$$a \equiv b \pmod{r},$$

or equivalently, $a = b + ru$ for some integer u. We also necessarily have that $ru = sv = 0 + sv$ for some integer v, or equivalently, that

$$ru \equiv 0 \pmod{s}$$

since

$$\begin{aligned} a = b + ru \quad \wedge \quad a = b + sv \quad &\iff \quad a - a = (b + ru) - (b - sv) \\ &\iff \quad 0 = ru - sv \\ &\iff \quad ru = sv. \end{aligned}$$

By Law B, since $r \perp s$,

$$u \equiv 0 \pmod{s},$$

or equivalently, $u = 0 + sv' = sv'$ for some integer v'. Substituting sv' for u gives us that $a = b + rsv'$, or equivalently, that

$$a \equiv b \pmod{rs}.$$

Therefore, if $a \equiv b \pmod{r}$ and $a \equiv b \pmod{s}$, then $a \equiv b \pmod{rs}$, provided $r \perp s$. □

► **19.** [*M10*] (*Law of inverses.*) If $n \perp m$, there is an integer n' such that $nn' \equiv 1$ (modulo m). Prove this, using the extension of Euclid's algorithm (Algorithm 1.2.1E).

Proposition. *If $n \perp m$, there is an integer n' such that $nn' \equiv 1 \pmod{m}$.*

Proof. Let n and m be arbitrary integers such that $n \perp m$. We must show that there exists an integer n' such that $nn' \equiv 1 \pmod{m}$.

Let d be the greatest common divisor of m and n as computed by Algorithm 1.2.1E. Then there exists two other integers m' and n' such that

$$m'm + n'n = d.$$

Since $n \perp m$, we must have that $d = 1$, and so, $nn' = 1 + m(-m')$, or equivalently,

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

as we needed to show. □

20. [*M15*] Use the law of inverses and Law A to prove Law B.

Proposition. *If $ax \equiv by$ and $a \equiv b$, and if $a \perp m$, then $x \equiv y \pmod{m}$.*

Proof. Let a, b, x, y, and m be arbitrary integers such that $ax \equiv by$, $a \equiv b$, and $a \perp m \pmod{m}$. We must show that $x \equiv y \pmod{m}$.

Since $a \perp m$, by the law of inverses we know there exists an integer a' such that

$$aa' \equiv 1 \pmod{m}.$$

Since $a \equiv b$, from Law A

$$aa' \equiv ba' \equiv 1 \pmod{m}.$$

Finally, since $ax \equiv by \pmod{m}$, by Law A again, multiplying the congrunce by a' yields

$$a'ax \equiv a'by \quad \Longrightarrow \quad x \equiv y \pmod{m}$$

as we needed to show. □

21. [*M22*] (*Fundamental theorem of arithmetic.*) Use Law B and exercise 1.2.1-5 to prove that every integer $n > 1$ has a *unique* representation as a product of primes (except for the order of the factors). In other words, show that there is exactly one way to write $n = p_1 p_2 \dots p_k$ where each p_j is prime and $p_1 \le p_2 \le \cdots \le p_k$.

Proposition. *Every integer $n > 1$ has a* unique *representation as a product of primes (except for the order of the factors).*

Proof. Let n be an arbitrary integer such that $n > 1$. We must show that n has a unique representation as a product of primes (except for the order of the factors).

By exercise 1.2.1-5, we have that $n = \prod_{1 \le i \le r} p_i$ for some arbitrary set of primes p_i, $1 \le i \le r$. We must show that if $n = \prod_{1 \le j \le s} q_j$ for some other arbitrary set of primes q_j, $1 \le j \le s$, that in fact, $r = s$ and $p_i = q_{\sigma(i)}$ for some permutation $\sigma(i) = j$.

Let us assume, however, they are not. That is, let us assume that for all $1 \le j \le s$, $q_j \neq p_1$. Since $\prod_{1 \le i \le r} p_i = \prod_{1 \le j \le s} q_j$, we have that

$$\prod_{1 \le i \le r} p_i \equiv 0 \pmod{p_1} \iff \prod_{1 \le j \le s} q_j \equiv 0 \pmod{p_1}.$$

As all p_i and q_j are each a set of primes and $q_j \neq p_1$, we have that $q_j \perp p_1$, allowing us to apply Law B (since $q_j \equiv q_j \pmod{p_1}$) successively until we obtain

$$1 \equiv 0 \pmod{p_1}.$$

But this requires $p_1 = 1$, and since p_1 is a prime, a condradiction. Hence, there exists a $q_{j'}$ such that $q_{j'} = p_1$. We may factor this prime out of our equation as

$$n/p_1 = \prod_{2 \le i \le r} p_i = \prod_{\substack{1 \le j \le s \\ j \neq j'}} q_j = \frac{\prod_{1 \le j \le s} q_j}{p_1}.$$

If n was prime, then clearly $n = p_1$ and we have proven there is a unique representation for this trivial case $r = s = 1$. Otherwise, we may prove by induction on $k = r = s$ that this is so. That is, if we assume that

$$n_k = \prod_{1 \le i \le k} p_i = \prod_{1 \le i \le k} q_{\sigma(i)}$$

is a unique factorization, we must show that

$$n_{k+1} = \prod_{1 \le i \le k+1} p_i = \prod_{1 \le j \le s'} q_j = \prod_{1 \le i \le k+1} q_{\sigma'(i)}$$

is too for some integer $s' = k + 1$. But we can make a similar proof by contradiction, assuming that for all $1 \le j \le s$, $q_j \neq p_{k+1}$. Since $\prod_{1 \le i \le r} p_i = \prod_{1 \le j \le s} q_j$, we have that

$$\prod_{1 \le i \le r} p_i \equiv 0 \pmod{p_{k+1}} \iff \prod_{1 \le j \le s} q_j \equiv 0 \pmod{p_{k+1}}.$$

As all p_i and q_j are each a set of primes and $q_j \neq p_{k+1}$, we have that $q_j \perp p_{k+1}$, allowing us to apply Law B (since $q_j \equiv q_j \pmod{p_{k+1}}$) successively until we obtain

$$1 \equiv 0 \pmod{p_{k+1}}.$$

But this requires $p_{k+1} = 1$, and since p_{k+1} is a prime, a condradiction. Hence, there exists a $q_{j'}$ such that $q_{j'} = p_{k+1}$. Then

$$\begin{aligned} n_{k+1} &= \prod_{1 \le i \le k+1} p_i \\ &= p_{k+1} \prod_{1 \le i \le k} p_i \\ &= p_{k+1} \prod_{1 \le i \le k} q_{\sigma(i)} \\ &= q_{j'} \prod_{1 \le i \le k} q_{\sigma(i)} \\ &= \prod_{1 \le i \le k+1} q_{\sigma'(i)}. \end{aligned}$$

for

$$\sigma'(i) = \begin{cases} \sigma(i) & \text{if } 1 \le i \le k \\ j' & \text{if } i = k+1. \end{cases}$$

We necessarily have $s' = k+1$, as both p_{k+1} and q'_j are primes and may not be further factored (leading to the inequalities $s' < k+1$ and $s' > k+1$, respectively, if they were not). Hence the result as we needed to show. □

► **22.** [*M10*] Give an example to show that Law B is not always true if a is not relatively prime to m.

An example to show that Law B is not always true if a is not relatively prime to m is for $a = 2$, $b = 0$, $x = 1$, $y = 0$, and $m = 2$ so that $a = 2 \not\perp 2 = m$. Then

$$\begin{aligned} 2(1) &\equiv 0(0) \pmod 2, \\ 2 &\equiv 0 \pmod 2 \end{aligned}$$

but

$$1 \not\equiv 0 \pmod 2.$$

23. [*M10*] Give an example to show that Law D is not always true if r is not relatively prime to s.

An example to show that Law D is not always true if r is not relatively prime to s is for $a = r = s = 2$ and $b = 0$ so that $r = 2 \not\perp 2 = s$. Then

$$\begin{aligned} 2 &\equiv 0 \pmod 2, \\ 2 &\equiv 0 \pmod 2 \end{aligned}$$

but

$$2 \not\equiv 0 \pmod{2(2)}.$$

► **24.** [*M20*] To what extent can Laws A, B, C, and D be generalized to apply to arbitrary real numbers instead of integers?

We have that Law A for addition and subtraction hold, as well as Law C.

We may prove Law A.

Proposition. *If $a \equiv b$ and $x \equiv y$, then $a \pm x \equiv b \pm y$ and $ax \equiv by \pmod m$.*

Proof. Let a, b, x, y, and m be arbitrary real numbers so that $a \equiv b$ and $x \equiv y$. We must show that $a \pm x \equiv b \pm y$.

For some integer r and s, we have

$$a = b + mr \quad \wedge \quad x = y + ms.$$

In the case of addition, $a + x \equiv b + y \pmod m$ since

$$\begin{aligned} a + x &= b + mr + y + ms \\ &= b + y + m(r + s) \end{aligned}$$

for some integer $r + s$.

Similarly, in the case of subtraction, $a - x \equiv b - y \pmod m$ since

$$\begin{aligned} a - x &= b + mr - y - ms \\ &= b - y + m(r - s) \end{aligned}$$

for some integer $r - s$.

Therefore, if $a \equiv b$ and $x \equiv y$, then $a \pm x \equiv b \pm y$ and $ax \equiv by \pmod m$ as we needed to show. □

To see why Law A for multiplication does not hold for the real numbers, consider as an example $a = \frac{2}{3}$, $b = -\frac{1}{3}$, $x = \frac{3}{5}$, $y = -\frac{2}{5}$, and $m = 1$. Then

$$\begin{aligned} \frac{2}{3} &\equiv -\frac{1}{3} \pmod 1, \\ \frac{3}{5} &\equiv -\frac{2}{5} \pmod 1 \end{aligned}$$

but

$$\frac{2}{5} \not\equiv \frac{2}{15} \pmod 1.$$

To see why Law B does not hold for the real numbers, consider as an example $a = \frac{2}{3}$, $b = -\frac{1}{3}$, $x = \frac{3}{5}$, $y = \frac{9}{5}$, and $m = 1$. Then

$$\begin{aligned} \frac{6}{15} &\equiv -\frac{9}{15} \pmod 1, \\ \frac{2}{3} &\equiv -\frac{1}{3} \pmod 1 \end{aligned}$$

but

$$\frac{3}{5} \not\equiv \frac{9}{5} \pmod 1.$$

(Note that even the more general relation $x \equiv y \pmod{\frac{m}{\gcd(a,m)}} \iff \frac{3}{5} \equiv \frac{9}{5} \pmod 3$ doesn't hold, assuming Thomae's function so that $\gcd(\frac{2}{3}, 1) = \frac{1}{3}$.)

We may prove Law C.

Proposition. *$a \equiv b \pmod m$ if and only if $an \equiv bn \pmod{mn}$, when $n \neq 0$.*

Proof. Let a, b, m, and n be arbitrary real numbers such that $n \neq 0$. We must show that $a \equiv b \pmod m$ if and only if $an \equiv bn \pmod{mn}$.

By exercise 15, we have that

$$\begin{aligned} a \equiv b \pmod m &\iff a \bmod m = b \bmod m \\ &\iff n(a \bmod m) = n(b \bmod m) \\ &\iff an \bmod mn = bn \bmod mn \\ &\iff an \equiv bn \pmod{mn} \end{aligned}$$

as we needed to show. □

To see why Law D does not hold for the real numbers, consider as an example $a = \frac{1}{2}$, $b = -1$, and $r = s = \frac{3}{2}$. Then

$$\begin{aligned} \frac{1}{2} &\equiv -1 \pmod{\frac{3}{2}}, \\ \frac{1}{2} &\equiv -1 \pmod{\frac{3}{2}} \end{aligned}$$

but

$$\frac{1}{2} \not\equiv -1 \pmod{\frac{9}{4}}.$$

25. [*M02*] Show that, according to Theorem F, $a^{p-1} \bmod p = [a \text{ is not a multiple of } p]$, whenever p is a prime number.

Proposition. *$a^{p-1} \bmod p = [a \perp p]$ whenever p is a prime number.*

Proof. Let a and p be arbitrary integers such that p is prime. We must show that $a^{p-1} \bmod p = [a \perp p]$.

By Theorem F, we have that $a^p \equiv a \pmod{p}$. In the case $a \perp p$, we may apply Law B to deduce that $a^{p-1} \equiv 1 \pmod{p}$, or equivalently, that

$$a^{p-1} \bmod p = 1 \bmod p = 1 = [a \perp p]$$

since $p > 1$.

In the case that $a \not\perp p$, $a \mid p$, and since $p > 1$, we have that

$$a^{p-1} \bmod p = 0 = 0 \bmod p = [a \perp p].$$

Therefore, in either case,

$$a^{p-1} \bmod p = [a \perp p]$$

as we needed to show. □

26. [*M15*] Let p be an odd prime number, let a be any integer, and let $b = a^{(p-1)/2}$. Show that $b \bmod p$ is either 0 or 1 or $p - 1$. [*Hint:* Consider $(b + 1)(b - 1)$.]

Proposition. *$a^{(p-1)/2} \bmod p$ is either 0, 1, or $p - 1$.*

Proof. Let a and p be arbitrary integers such that p is prime and let $b = a^{(p-1)/2}$. We must show that $b \bmod p$ is either 0, 1, or $p - 1$.
If $b \not\perp p$, then clearly $b \bmod p = 0$. Otherwise, we need only examine the case $b \perp p$. By Theorem F, we have that $a^p \equiv a \pmod{p}$. We may apply Law B to deduce that $a^{p-1} \equiv 1 \pmod{p}$, or equivalently by Law A, that

$$a^{p-1} - 1 \equiv 0 \pmod{p}.$$

But

$$\begin{aligned} a^{p-1} - 1 &= b^2 - 1 \\ &= (b + 1)(b - 1) \end{aligned}$$

so that

$$(b + 1)(b - 1) \equiv 0 \pmod{p}.$$

By canceling out each factor, we obtain

$$\begin{aligned} b + 1 \equiv 0 \pmod{p} &\iff b \equiv -1 \pmod{p} \\ &\iff b \equiv p - 1 \pmod{p} \end{aligned}$$

and

$$b - 1 \equiv 0 \pmod{p} \iff b \equiv 1 \pmod{p}.$$

Therefore, $b \bmod p$ is either 0, 1, or $p - 1$ as we needed to show. □

27. [*M15*] Given that n is a positive integer, let $\varphi(n)$ be the number of values among $\{0, 1, \ldots, n - 1\}$ that are relatively prime to n. Thus $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, etc. Show that $\varphi(p) = p - 1$ if p is a prime number; and evaluate $\varphi(p^e)$ when e is a positive integer.

We may prove a propery of Euler's totient function, defined as

$$\varphi(n) = |\{k : 1 \le k \le n \wedge k \perp n\}|.$$

Proposition. $\varphi(p) = p - 1$ *if* p *is a prime number.*

Proof. Let p be an arbitrary prime number. We must show that $\varphi(p) = p - 1$.

Since p is a prime number, its only divisors are 1 and p. That is, $k \perp p$ for $1 \leq k < p$ but not for $k = p$. And so

$$\begin{aligned}\varphi(p) &= |\{k : 1 \leq k \leq p \wedge k \perp p\}| \\ &= |\{k : 1 \leq k \leq p - 1 \wedge k \perp p\}| + |\{k : k = p \wedge k \perp p\}| \\ &= (p - 1) + (0) \\ &= p - 1\end{aligned}$$

as we needed to show. □

We may evaluate $\varphi(p^e)$ when e is a positive integer by noting there are p^e numbers in total, and of those, p^{e-1} are multiples of p such that $k \not\perp p^e$, $1 \leq k \leq p^e$. (Intuitively, these are $k \in \{p, 2p, 3p, \ldots, (p^{e-1})p\}$.) This yields

$$\begin{aligned}\varphi(p^e) &= |\{k : 1 \leq k \leq p^e \wedge k \perp p^e\}| \\ &= |\{k : 1 \leq k \leq p^e\}| - |\{k : 1 \leq k \leq p^e \wedge k \not\perp p^e\}| \\ &= p^e - p^{e-1} \\ &= p^{e-1}(p - 1) \\ &= p^e(1 - \frac{1}{p}).\end{aligned}$$

► **28.** [*M25*] Show that the method used to prove Theorem F can be used to prove the following extension, called *Euler's theorem*: $a^{\varphi(m)} \equiv 1 \pmod m$, for *any* positive integer m, when $a \perp m$. (In particular, the number n' in exercise 19 may be taken to be $n^{\varphi(m)-1} \bmod m$.)

Proposition (*Euler's theorem*)**.** $a^{\varphi(m)} \equiv 1 \pmod m$, *for any integer* $m > 0$, *when* $a \perp m$.

Proof. Let a and m be arbitrary integers such that $m > 0$ and $a \perp m$. We must show that $a^{\varphi(m)} \equiv 1 \pmod m$.

Since $a \perp m$, we have that

$$a \equiv 1 \pmod m.$$

Let $x_1, x_2, \ldots, x_{\varphi(m)}$ be the $\varphi(m)$ integers such that $x_i \perp p$, $1 \leq i \leq \varphi(m)$. For each, we have that

$$x_i \equiv x_i \pmod m$$

and by Law A, we can multiply each to obtain

$$ax_i \equiv x_i \pmod m.$$

Similarly, we may multiply for $1 \leq i \leq \varphi(m)$ to obtain

$$\prod_{1 \leq i \leq \varphi(m)} ax_i \equiv \prod_{1 \leq i \leq \varphi(m)} x_i \pmod m$$

or equivalently

$$a^{\varphi(m)} \prod_{1 \leq i \leq \varphi(m)} x_i \equiv \prod_{1 \leq i \leq \varphi(m)} x_i \pmod m.$$

Finally, as each $x_i \perp m$, we may cancel out the products to obtain

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

as we needed to show. □

29. [*M22*] A function $f(n)$ of positive integers n is called *multiplicative* if $f(rs) = f(r)f(s)$ whenever $r \perp s$. Show that each of the following functions is multiplicative: (a) $f(n) = n^c$, where c is any constant; (b) $f(n) = [n$ is not divisible by k^2 for any integer $k > 1]$; (c) $f(n) = c^k$, where k is the number of distinct primes that divide n; (d) the product of any two multiplicative functions.

We may prove that the various functions are multiplicative.

Proposition (A)**.** *The function $f(n) = n^c$, where c is any constant, is multiplicative.*

Proof. Let f be a function such that $f(n) = n^c$, where c is an arbitrary constant; and let r and s be arbitrary integers such that $r \perp s$. We must show that f is multiplicative; that is, that $f(rs) = f(r)f(s)$. But

$$\begin{aligned} f(rs) &= (rs)^c \\ &= r^c s^c \\ &= f(r)f(s) \end{aligned}$$

as we needed to show. □

Proposition (B)**.** *The function $f(n) = [k^2 \nmid n]$ for any integer $k > 1$, is multiplicative.*

Proof. Let f be a function such that $f(n) = [k^2 \nmid n]$ for any integer $k > 1$; and let r and s be arbitrary integers such that $r \perp s$. We must show that f is multiplicative; that is, that $f(rs) = f(r)f(s)$.

First, we have that $k^2 \nmid n$ for any integer $k > 1$. But we also have that $n \nmid k^2$, since k^2 being a multiple of n would require n to be a square, a possibility precluded by the fact that $k^2 \nmid n$ for any integer $k > 1$. Therefore, we have the stronger condition that $n \perp k^2$.

Then

$$\begin{aligned} f(rs) &= [rs \perp k^2] \\ &= [k^2 \equiv 1 \pmod{rs}] \\ &= [k^2 \equiv 1 \pmod{r} \wedge k^2 \equiv 1 \pmod{s}] && \text{by Law D} \\ &= [k^2 \equiv 1 \pmod{r}][k^2 \equiv 1 \pmod{s}] \\ &= [r \perp k^2][s \perp k^2] \\ &= f(r)f(s) \end{aligned}$$

as we needed to show. □

Proposition (C)**.** *The function $f(n) = c^k$, where c is any constant and k is the number of distinct primes that divide n, is multiplicative.*

Proof. Let f be a function such that $f(n) = c^k$, where c is any constant and k is the number of distinct primes that divide n; and let r and s be arbitrary integers such that $r \perp s$. We must show that f is multiplicative; that is, that $f(rs) = f(r)f(s)$.

Let k_n denote the number of distinct primes that divide n. Since $r \perp s$, the prime factors of r must be distinct from the prime factors of s, and so we must that have $k_{rs} = k_r + k_s$.

Then,

$$\begin{aligned} f(rs) &= c_{rs}^k \\ &= c^{k_r + k_s} \\ &= c^{k_r} c^{k_s} \\ &= f(r)f(s) \end{aligned}$$

as we needed to show. □

Proposition (D)**.** *The function $f(n) = g(n)h(n)$, where g and h are multiplicative functions, is multiplicative.*

Proof. Let f be a function such that $f(n) = g(n)h(n)$, where g and h are multiplicative functions; and let r and s be arbitrary integers such that $r \perp s$. We must show that f is multiplicative; that is, that $f(rs) = f(r)f(s)$. But

$$\begin{aligned} f(rs) &= g(rs)h(rs) \\ &= g(r)g(s)h(r)h(s) \\ &= g(r)h(r)g(s)h(s) \\ &= f(r)f(s) \end{aligned}$$

as we needed to show. □

30. [*M30*] Prove that the function $\varphi(n)$ of exercise 27 is multiplicative. Using this fact, evaluate $\varphi(1000000)$, and give a method for evaluating $\varphi(n)$ in a simple way once n has been factored into primes.

We may prove that Euler's totient function $\varphi(n)$ is multiplicative.

Proposition. *Euler's totient function $\varphi(n)$ is multiplicative.*

Proof. Let

$$\varphi(n) = |\{k : 1 \leq k \leq n \wedge k \perp n\}|$$

be Euler's totient function; and r and s arbtrary integers such that $r \perp s$. We must show that $\varphi(rs) = \varphi(r)\varphi(s)$.

Let $R = \{r_1, r_2, \ldots, r_{\varphi(r)}\}$ be those integers such that $r_k \perp r$, $1 \leq k \leq r$; and $S = \{s_1, s_2, \ldots, s_{\varphi(s)}\}$ be those integers such that $s_k \perp s$, $1 \leq k \leq s$; and define

$$T = \{t_i = rs' + sr' : r' \in R \wedge s' \in S\}.$$

T has the following properties:

1. $t_i \perp rs$. Suppose not. That is, suppose that $\gcd(rs' + sr', rs) > 1$ had a prime divisor p. Then, without loss of generality, p divides both r and not s (since $r \perp s$) and r'. But $r' \perp r$, so $p = 1$, which is a contradiction, similarly for the case p divides s and not r, and so, $t_i \perp rs$.
2. $t_i \not\equiv t_j \pmod{rs}$. Suppose $rs' + sr' \equiv rs'' + sr'' \pmod{rs}$. Then rs divides $r(s' - s'') + s(r' - r'')$ and s divides $r(s' - s'')$. But $r \perp s$, so s divides $s' - s''$, or equivalently, $s' \equiv s'' \pmod{s}$. As s' and s'' are both relatively prime and less than s, $s' = s''$. Similarly for rs dividing $s(r' - r'')$ to discover $r' = r''$. And so, no two $t_i \not\equiv t_j \pmod{rs}$.

3. $(\forall n \perp rs)\,(\exists t_i)\,(n \equiv t_i \pmod{rs})$. Suppose $n \perp rs$. Since $r \perp s$, n can be expressed as $n = rv + su$ for arbitrary integers u and v. We have $u \not\perp r$ and $v \not\perp s$ since $rv + su \perp rs$ and $r \perp s$. Expressing u as $u = r' + ra$ and v as $v = s' + sb$ for arbitrary integers a and b, we have $n = rv + su = r(s' + sb) + s(r' + ra) = rs' + rsb + sr' + sra = rs' + sr' + rs(a + b)$, or equivalently, $n \equiv t_i \pmod{rs}$.

Since each $t_i \perp rs$, no two $t_i \not\equiv t_j \pmod{rs}$, and for any integer $n \perp rs$ there is a t_i such that $n \equiv t_i \pmod{rs}$, $i \neq j$; we have that $T = \{t_1, t_2, \ldots, t_{\varphi(rs)}\}$, those integers such that $t_k \perp rs$, $1 \leq k \leq rs$; and that $\varphi(rs) = |R||S| = \varphi(r)\varphi(s)$.

Then

$$\varphi(rs) = \varphi(r)\varphi(s)$$

as we needed to show. □

We can use this fact and the result of exercise 27, that $\varphi(p^e) = p^e - p^{e-1}$ for any prime p, to evaluate $\varphi(1000000)$ as

$$\begin{aligned}\varphi(1000000) &= \varphi((2^6)(5^6)) \\ &= \varphi(2^6)\varphi(5^6) \\ &= (2^6 - 2^5)(5^6 - 5^5) \\ &= (32)(12500) \\ &= 400000.\end{aligned}$$

A method for evaluating $\varphi(z)$ in a simple way once z has been factored into n primes p_i raised to powers w_i as $\prod_{1 \leq i \leq n} p_i^{w_i}$ is

$$\begin{aligned}\varphi(z) &= \prod_{1 \leq i \leq n} \varphi(p_i^{w_i}) \\ &= \prod_{1 \leq i \leq n} p_i^{w_i} - p_i^{w_i - 1} \\ &= \left(\prod_{1 \leq i \leq n} p_i^{w_i}\right)\left(\prod_{1 \leq i \leq n} 1 - \frac{1}{p_i}\right) \\ &= z \prod_{\substack{p \mid z \\ p \text{ prime}}} 1 - \frac{1}{p}.\end{aligned}$$

31. [*M22*] Prove that if $f(n)$ is multiplicative, so is $g(n) = \sum_{d \backslash n} f(d)$.

Proposition. *If $f(n)$ is multiplicative, so is $g(n) = \sum_{d \backslash n} f(d)$.*

Proof. Let $f(n)$ be a multiplicative function; $g(n) = \sum_{d|n} f(d)$; and r and s arbitrary integers such that $r \perp s$. We must show that $g(rs) = g(r)g(s)$. But since $r \perp s$, the divisors d of rs may be partitioned into those that divide r and those that divide s; let these be denoted a and b such that $a|r$ and $b|s$. Then, as $a \perp b$ since $\gcd(r, s) =$

$\gcd(a, s) = \gcd(a, b) = 1$,

$$\begin{aligned} g(rs) &= \sum_{d|rs} f(d) \\ &= \sum_{\substack{a|r \\ b|s}} f(ab) \\ &= \sum_{\substack{a|r \\ b|s}} f(a)f(b) \\ &= \left(\sum_{a|r} f(a)\right)\left(\sum_{b|s} f(b)\right) \\ &= g(r)g(s). \end{aligned}$$

□

32. [*M18*] Prove the double-summation identity

$$\sum_{d\backslash n}\sum_{c\backslash d} f(c,d) = \sum_{c\backslash n}\sum_{d\backslash(n/c)} f(c,cd),$$

for any function $f(x, y)$.

Proposition. $\sum_{d|n}\sum_{c|d} f(c,d) = \sum_{c|n}\sum_{d|(n/c)} f(c,cd)$.

Proof. Let $f(a, b)$ be an arbitrary function. We must show that

$$\sum_{d|n}\sum_{c|d} f(c,d) = \sum_{c|n}\sum_{d|(n/c)} f(c,cd).$$

But, since $n = cd'k$ if and only if $n = ck' \wedge n/c = d'k$ for arbitrary integers k and k',

$$\begin{aligned} \sum_{d|n}\sum_{c|d} f(c,d) &= \sum_{d|n\wedge c|d} f(c,d) \\ &= \sum_{cd'|n\wedge c|cd'} f(c,cd') && \text{let } d = cd' \\ &= \sum_{cd'|n} f(c,cd') \\ &= \sum_{cd'|n\wedge cd'|n} f(c,cd') \\ &= \sum_{c|n\wedge d'|(n/c)} f(c,cd') \\ &= \sum_{c|n}\sum_{d'|(n/c)} f(c,cd') \\ &= \sum_{c|n}\sum_{d|(n/c)} f(c,cd) \end{aligned}$$

as we needed to show. □

33. [*M18*] Given that m and n are integers, evaluate (a) $\lfloor\frac{1}{2}(n+m)\rfloor + \lfloor\frac{1}{2}(n-m+1)\rfloor$; (b) $\lceil\frac{1}{2}(n+m)\rceil + \lceil\frac{1}{2}(n-m+1)\rceil$. (The special case $m = 0$ is worth noting.)

We may evaluate the equations.

(a) We want to evalute

$$\left\lfloor \frac{1}{2}(n+m) \right\rfloor + \left\lfloor \frac{1}{2}(n-m+1) \right\rfloor.$$

We consider two cases, depending on whether $n \pm m$ is odd or even.

Case 1. [$n \pm m$ *odd*] In the case that $n \pm m$ is odd,

$$\begin{aligned} \left\lfloor \frac{1}{2}(n+m) \right\rfloor + \left\lfloor \frac{1}{2}(n-m+1) \right\rfloor &= \frac{n+m-1}{2} + \frac{n-m+1}{2} \\ &= \frac{n+m-1+n-m+1}{2} \\ &= \frac{2n}{2} \\ &= n. \end{aligned}$$

Case 2. [$n \pm m$ *even*] In the case that $n \pm m$ is even,

$$\begin{aligned} \left\lfloor \frac{1}{2}(n+m) \right\rfloor + \left\lfloor \frac{1}{2}(n-m+1) \right\rfloor &= \frac{n+m}{2} + \frac{n-m}{2} \\ &= \frac{n+m+n-m}{2} \\ &= \frac{2n}{2} \\ &= n. \end{aligned}$$

In either case, we have

$$\left\lfloor \frac{1}{2}(n+m) \right\rfloor + \left\lfloor \frac{1}{2}(n-m+1) \right\rfloor = n.$$

(b) We want to evaluate

$$\left\lceil \frac{1}{2}(n+m) \right\rceil + \left\lceil \frac{1}{2}(n-m+1) \right\rceil.$$

We consider two cases, depending on whether $n \pm m$ is odd or even.

Case 1. [$n \pm m$ *odd*] In the case that $n \pm m$ is odd,

$$\begin{aligned} \left\lceil \frac{1}{2}(n+m) \right\rceil + \left\lceil \frac{1}{2}(n-m+1) \right\rceil &= \frac{n+m+1}{2} + \frac{n-m+1}{2} \\ &= \frac{n+m+1+n-m+1}{2} \\ &= \frac{2n+2}{2} \\ &= n+1. \end{aligned}$$

Case 2. [$n \pm m$ *even*] In the case that $n \pm m$ is even,

$$\begin{aligned} \left\lceil \frac{1}{2}(n+m) \right\rceil + \left\lceil \frac{1}{2}(n-m+1) \right\rceil &= \frac{n+m}{2} + \frac{n-m+2}{2} \\ &= \frac{n+m+n-m+2}{2} \\ &= \frac{2n+2}{2} \\ &= n+1. \end{aligned}$$

In either case, we have

$$\left\lceil \frac{1}{2}(n+m) \right\rceil + \left\lceil \frac{1}{2}(n-m+1) \right\rceil = n+1.$$

The special case $m = 0$ yields

$$\left\lfloor \frac{n}{2} \right\rfloor + \left\lfloor \frac{n+1}{2} \right\rfloor = n$$

and

$$\left\lceil \frac{n}{2} \right\rceil + \left\lceil \frac{n+1}{2} \right\rceil = n+1.$$

► **34.** [*M21*] What conditions on the real number $b > 1$ are necessary and sufficient to guarantee that $\lfloor \log_b x \rfloor = \lfloor \log_b \lfloor x \rfloor \rfloor$ for all real $x \geq 1$?

For real numbers $x \geq 1$ and $b > 1$ we have for some arbitrary integer n that

$$\begin{aligned}
\lfloor \log_b x \rfloor = n \quad &\iff \quad n \leq \log_b x < n+1 \\
&\iff \quad b^n \leq x < b^{n+1} \\
&\iff \quad b^n \leq \lfloor x \rfloor < b^{n+1} \qquad\qquad b \in \mathbb{Z} \\
&\iff \quad n \leq \log_b \lfloor x \rfloor < n+1 \\
&\iff \quad \lfloor \log_b \lfloor x \rfloor \rfloor = n.
\end{aligned}$$

That is, b an integer such that $b \geq 2$ are necessary and sufficient conditions to guarantee that

$$\lfloor \log_b x \rfloor = \lfloor \log_b \lfloor x \rfloor \rfloor$$

for all real $x \geq 1$.

Note that we have the same conditions for ceilings, as

$$\begin{aligned}
\lceil \log_b x \rceil = n \quad &\iff \quad n < \log_b x \leq n+1 \\
&\iff \quad b^n < x \leq b^{n+1} \\
&\iff \quad b^n < \lceil x \rceil \leq b^{n+1} \qquad\qquad b \in \mathbb{Z} \\
&\iff \quad n < \log_b \lceil x \rceil \leq n+1 \\
&\iff \quad \lceil \log_b \lceil x \rceil \rceil = n.
\end{aligned}$$

► **35.** [*M20*] Given that m and n are integers and $n > 0$, prove that

$$\lfloor (x+m)/n \rfloor = \lfloor (\lfloor x \rfloor + m)/n \rfloor$$

for all real x. (When $m = 0$, we have an important special case.) Does an analogous result hold for the ceiling function?

We may prove the result for floors.

Proposition. $\lfloor (x+m)/n \rfloor = \lfloor (\lfloor x \rfloor + m)/n \rfloor$ *for integers* m, n, $n > 0$ *and real* x.

Proof. Let m and n be arbitrary integers such that $n > 0$, and x an arbitrary real number. We must show that

$$\lfloor (x+m)/n \rfloor = \lfloor (\lfloor x \rfloor + m)/n \rfloor.$$

But for an arbitary integer z

$$\begin{aligned}
\lfloor (x+m)/n \rfloor = z &\iff z \le (x+m)/n < z+1 \\
&\iff nz \le (x+m) < n(z+1) \\
&\iff nz - m \le x < n(z+1) - m \\
&\iff nz - m \le \lfloor x \rfloor < n(z+1) - m \\
&\iff nz \le \lfloor x \rfloor + m < n(z+1) \\
&\iff z \le (\lfloor x \rfloor + m)/n < z+1 \\
&\iff \lfloor (\lfloor x \rfloor + m)/n \rfloor = z
\end{aligned}$$

as we needed to show. □

Note the important special case for $m = 0$,

$$\lfloor x/n \rfloor = \lfloor \lfloor x \rfloor / n \rfloor.$$

An analogous result holds for ceilings.

Proposition. $\lceil (x+m)/n \rceil = \lceil (\lceil x \rceil + m)/n \rceil$ *for integers* m, n, $n > 0$ *and real* x.

Proof. Let m and n be arbitrary integers such that $n > 0$, and x an arbitrary real number. We must show that

$$\lceil (x+m)/n \rceil = \lceil (\lceil x \rceil + m)/n \rceil.$$

But for an arbitary integer z

$$\begin{aligned}
\lceil (x+m)/n \rceil = z &\iff z < (x+m)/n \le z+1 \\
&\iff nz < (x+m) \le n(z+1) \\
&\iff nz - m < x \le n(z+1) - m \\
&\iff nz - m < \lceil x \rceil \le n(z+1) - m \\
&\iff nz < \lceil x \rceil + m \le n(z+1) \\
&\iff z < (\lceil x \rceil + m)/n \le z+1 \\
&\iff \lceil (\lceil x \rceil + m)/n \rceil = z
\end{aligned}$$

as we needed to show. □

36. [*M23*] Prove that $\sum_{k=1}^{n} \lfloor k/2 \rfloor = \lfloor n^2/4 \rfloor$; also evaulate $\sum_{k=1}^{n} \lceil k/2 \rceil$.

We may prove the sum for floors.

Proposition. $\sum_{1 \le k \le n} \left\lfloor \frac{k}{2} \right\rfloor = \left\lfloor \frac{n^2}{4} \right\rfloor$.

Proof. Let n be an arbitary positive integer. We must show that

$$\sum_{1 \le k \le n} \left\lfloor \frac{k}{2} \right\rfloor = \left\lfloor \frac{n^2}{4} \right\rfloor.$$

We consider two cases, depending on whether $n = 2m$ is even or $n = 2m+1$ is odd for an arbitrary integer m. We also will utilize the equality

$$\sum_{1 \le k \le n} \left\lfloor \frac{k}{2} \right\rfloor = \sum_{1 \le k \le n} \left\lfloor \frac{n+1-k}{2} \right\rfloor.$$

Case 1. $[n = 2m]$ We have the equality

$$\left\lfloor \frac{k}{2} \right\rfloor + \left\lfloor \frac{n+1-k}{2} \right\rfloor = m$$

since for an arbitrary integer q, if $k = 2q$ is even

$$\left\lfloor \frac{k}{2} \right\rfloor + \left\lfloor \frac{n+1-k}{2} \right\rfloor = \left\lfloor \frac{2q}{2} \right\rfloor + \left\lfloor \frac{2m+1-2q}{2} \right\rfloor = m + \left\lfloor \frac{1}{2} \right\rfloor = m;$$

and if $k = 2q+1$ is odd

$$\left\lfloor \frac{k}{2} \right\rfloor + \left\lfloor \frac{n+1-k}{2} \right\rfloor = \left\lfloor \frac{2q+1}{2} \right\rfloor + \left\lfloor \frac{2m+1-2q-1}{2} \right\rfloor = \left\lfloor \frac{1}{2} \right\rfloor + m = m.$$

In this case then

$$\begin{aligned}
\sum_{1 \le k \le n} \left\lfloor \frac{k}{2} \right\rfloor &= \frac{1}{2} \sum_{1 \le k \le n} \left(\left\lfloor \frac{k}{2} \right\rfloor + \left\lfloor \frac{n+1-k}{2} \right\rfloor \right) \\
&= \frac{1}{2} \sum_{1 \le k \le n} m \\
&= \frac{nm}{2} \\
&= \frac{n^2}{4}.
\end{aligned}$$

Case 2. $[n = 2m+1]$ In this case,

$$\begin{aligned}
\sum_{1 \le k \le n} \left\lfloor \frac{k}{2} \right\rfloor &= \left(\sum_{1 \le k \le 2m} \left\lfloor \frac{k}{2} \right\rfloor \right) + \left\lfloor \frac{n}{2} \right\rfloor \\
&= \frac{(2m)^2}{4} + m \\
&= m^2 + m \\
&\frac{n^2}{4} - \frac{1}{4}.
\end{aligned}$$

And so, in either case,

$$\frac{(n-1)^2}{4} < \frac{n^2}{4} - \frac{1}{4} \le \sum_{1 \le k \le n} \left\lfloor \frac{k}{2} \right\rfloor \le \frac{n^2}{4}$$

or equivalently,

$$\sum_{1 \le k \le n} \left\lfloor \frac{k}{2} \right\rfloor = \left\lfloor \frac{n^2}{4} \right\rfloor$$

as we needed to show. □

For the second sum, we may prove another result.

Proposition. $\sum_{1 \le k \le n} \left\lceil \frac{k}{2} \right\rceil = \left\lceil \frac{n(n+2)}{4} \right\rceil$.

Proof. Let n be an arbitary positive integer. We must show that

$$\sum_{1\leq k\leq n}\left\lceil\frac{k}{2}\right\rceil=\left\lceil\frac{n(n+2)}{4}\right\rceil.$$

We consider two cases, depending on whether $n=2m$ is even or $n=2m+1$ is odd for an arbitrary integer m. We also will utilize the equality

$$\sum_{1\leq k\leq n}\left\lceil\frac{k}{2}\right\rceil=\sum_{1\leq k\leq n}\left\lceil\frac{n+1-k}{2}\right\rceil.$$

Case 1. $[n=2m]$ We have the equality

$$\left\lceil\frac{k}{2}\right\rceil+\left\lceil\frac{n+1-k}{2}\right\rceil=m+1$$

since for an arbitrary integer q, if $k=2q$ is even

$$\left\lceil\frac{k}{2}\right\rceil+\left\lceil\frac{n+1-k}{2}\right\rceil=\left\lceil\frac{2q}{2}\right\rceil+\left\lceil\frac{2m+1-2q}{2}\right\rceil=m+1;$$

and if $k=2q+1$ is odd

$$\left\lceil\frac{k}{2}\right\rceil+\left\lceil\frac{n+1-k}{2}\right\rceil=\left\lceil\frac{2q+1}{2}\right\rceil+\left\lceil\frac{2m+1-2q-1}{2}\right\rceil=m+1.$$

In this case

$$\begin{aligned}\sum_{1\leq k\leq n}\left\lceil\frac{k}{2}\right\rceil&=\frac{1}{2}\sum_{1\leq k\leq n}\left(\left\lceil\frac{k}{2}\right\rceil+\left\lceil\frac{n+1-k}{2}\right\rceil\right)\\&=\frac{1}{2}\sum_{1\leq k\leq n}m+1\\&=\frac{n(m+1)}{2}\\&=\frac{n((n/2)+1)}{2}\\&=\frac{n(n+2)}{4}.\end{aligned}$$

Case 2. $[n=2m+1]$ In this case

$$\begin{aligned}\sum_{1\leq k\leq n}\left\lceil\frac{k}{2}\right\rceil&=\left(\sum_{1\leq k\leq 2m}\left\lceil\frac{k}{2}\right\rceil\right)+\left\lceil\frac{n}{2}\right\rceil\\&=\frac{2m(2m+2)}{4}+m+1\\&=(m+1)^2\\&\frac{(n+1)^2}{4}.\end{aligned}$$

And so, in either case,

$$\frac{n(n+2)}{4}\leq\sum_{1\leq k\leq n}\left\lceil\frac{k}{2}\right\rceil\leq\frac{(n+1)^2}{4}<\frac{(n+1)(n+3)}{4}$$

or equivalently,

$$\sum_{1\le k\le n}\left\lceil\frac{k}{2}\right\rceil=\left\lceil\frac{n(n+2)}{4}\right\rceil$$

as we needed to show. □

► **37.** [*M30*] Let m and n be integers, $n>0$. Show that

$$\sum_{0\le k<n}\left\lfloor\frac{mk+x}{n}\right\rfloor=\frac{(m-1)(n-1)}{2}+\frac{d-1}{2}+d\lfloor x/d\rfloor,$$

where d is the greatest common divisor of m and n, and x is any real number.

We may prove the result for floors.

Proposition. $\sum_{0\le k<n}\left\lfloor\frac{mk+x}{n}\right\rfloor=\frac{(m-1)(n-1)}{2}+\frac{d-1}{2}+d\lfloor x/d\rfloor$ *for* $d=\gcd(m,n)$.

Proof. Let m, n, and d be arbitrary integers such that $d=\gcd(m,n)$ and x an arbitrary real number. We must show that

$$\sum_{0\le k<n}\left\lfloor\frac{mk+x}{n}\right\rfloor=\frac{(m-1)(n-1)}{2}+\frac{d-1}{2}+d\left\lfloor\frac{x}{d}\right\rfloor.$$

But since for an arbitrary real z, $z=\lfloor x\rfloor+x \bmod 1=\lfloor x\rfloor+\{x\}$,

$$\sum_{0\le k<n}\left\lfloor\frac{mk+x}{n}\right\rfloor=\sum_{0\le k<n}\frac{mk+x}{n}-\sum_{0\le k<n}\left\{\frac{mk+x}{n}\right\}.$$

We have that

$$\begin{aligned}\sum_{0\le k<n}\frac{mk+x}{n}&=\frac{m}{n}\left(\sum_{0\le k<n}k\right)+\frac{1}{n}\left(\sum_{0\le k<n}x\right)\\&=\frac{m}{n}\frac{(n-1)n}{2}+\frac{1}{n}nx\\&=\frac{m(n-1)}{2}+x.\end{aligned}$$

And so

$$\sum_{0\le k<n}\left\lfloor\frac{mk+x}{n}\right\rfloor=\frac{m(n-1)}{2}+x-\sum_{0\le k<n}\left\{\frac{mk+x}{n}\right\}.$$

Then, for $n' = n/d$ and $m' = m/d$, we have

$$\begin{aligned}
\sum_{0\le k<n} \left\{\frac{mk+x}{n}\right\} &= \sum_{0\le k<n} \left\{\frac{m'k}{n'} + \frac{x}{n}\right\} \\
&= \sum_{0\le i<d} \sum_{n'i\le j<n'(i+1)} \left\{\frac{m'j}{n'} + \frac{x}{n}\right\} \\
&= \sum_{0\le i<d} \sum_{0\le j<n'} \left\{\frac{m'(j+n'i)}{n'} + \frac{x}{n}\right\} \\
&= \sum_{0\le i<d} \sum_{0\le j<n'} \left\{\frac{m'j}{n'} + m'i + \frac{x}{n}\right\} \\
&= \sum_{0\le i<d} \sum_{0\le j<n'} \left\{\frac{m'j}{n'} + \frac{x}{n}\right\} && \text{since } m'i \equiv 0 \pmod 1 \\
&= d \sum_{0\le j<n'} \left\{\frac{m'j}{n'} + \frac{x}{n}\right\} \\
&= d \sum_{0\le j<n'} \left\{\frac{m'j}{n'} + \frac{x/d}{n'}\right\} \\
&= d \sum_{0\le j<n'} \left\{\frac{m'j + x/d}{n'}\right\} \\
&= d \sum_{0\le j<n'} \left\{\frac{m'j + \lfloor x/d\rfloor + \{x/d\}}{n'}\right\} \\
&= d \sum_{0\le j<n'} \left\{\frac{m'j}{n'} + \frac{\lfloor x/d\rfloor}{n'} + \frac{\{x/d\}}{n'}\right\} \\
&= d \sum_{0\le j<n'} \left\{\frac{j}{n'} + \frac{\lfloor x/d\rfloor}{n'} + \frac{\{x/d\}}{n'}\right\} && \text{since } m'j/n' \equiv j/n' \pmod 1 \\
&= d \sum_{0\le j<n'} \left\{\frac{j + \lfloor x/d\rfloor}{n'} + \frac{\{x/d\}}{n'}\right\}
\end{aligned}$$

$$
\begin{aligned}
&= d\left(\left(\sum_{0\le j<n'}\left\{\frac{j}{n'}+\frac{\{x/d\}}{n'}\right\}\right)+\left(\sum_{0\le j<n'}\left\{\frac{\lfloor x/d\rfloor}{n'}\right\}\right)\right)\\
&= d\left(\left(\sum_{0\le j<n'}\left\{\frac{j}{n'}+\frac{\{x/d\}}{n'}\right\}\right)+n'\left\{\frac{\lfloor x/d\rfloor}{n'}\right\}\right)\\
&= d\left(\left(\sum_{0\le j<n'}\left\{\frac{j}{n'}+\frac{\{x/d\}}{n'}\right\}\right)+\{\lfloor x/d\rfloor\}\right)\\
&= d\left(\left(\sum_{0\le j<n'}\left\{\frac{j}{n'}+\frac{\{x/d\}}{n'}\right\}\right)+0\right) && \text{since } \lfloor x/d\rfloor \equiv 0 \pmod 1\\
&= d\sum_{0\le j<n'}\left\{\frac{j}{n'}+\frac{\{x/d\}}{n'}\right\}\\
&= d\sum_{0\le j<n'}\frac{j}{n'}+\frac{\{x/d\}}{n'} && \text{since } 0\le j+\{x/d\}<n'\\
&= d\sum_{0\le j<n'}\frac{j+\{x/d\}}{n'}\\
&= d\frac{(n'-1)n'}{2n'}+\frac{dn'}{n'}\{x/d\}\\
&= \frac{n-d}{2}+\frac{dn'}{n'}(x/d-\lfloor x/d\rfloor)\\
&= \frac{n-d}{2}+x-d\lfloor x/d\rfloor.
\end{aligned}
$$

For justifications of certain steps, note that

$$m'\equiv 0 \pmod 1 \wedge i\equiv 0 \pmod 1 \iff m'i\equiv 0 \pmod 1;$$

$$
\begin{aligned}
m\equiv \gcd(m,n) \pmod n &\iff m\equiv d \pmod n\\
&\iff m'd\equiv d \pmod{n'd}\\
&\iff m'\equiv 1 \pmod{n'}\\
&\iff m'j\equiv j \pmod{n'}\\
&\iff m'j/n'\equiv j/n' \pmod 1;
\end{aligned}
$$

and

$$0\le j\le n'-1 \wedge \{x/d\}<1 \iff 0\le j+\{x/d\}<n'.$$

And so

$$
\begin{aligned}
\sum_{0\le k<n}\left\lfloor\frac{mk+x}{n}\right\rfloor &= \frac{m(n-1)}{2}+x-\frac{n-d}{2}-x+d\lfloor x/d\rfloor\\
&= \frac{mn-m-n+d}{2}+d\lfloor x/d\rfloor\\
&= \frac{(m-1)(n-1)}{2}+\frac{d-1}{2}+d\lfloor x/d\rfloor
\end{aligned}
$$

as we needed to show. □

For ceilings, note that by negating both sides of the equality yields

$$\begin{aligned} -\sum_{0\le k<n}\left\lfloor\frac{mk+x}{n}\right\rfloor &= \sum_{0\le k<n} -\left\lfloor\frac{mk+x}{n}\right\rfloor \\ &= \sum_{0\le k<n}\left\lceil\frac{-mk-x}{n}\right\rceil \end{aligned}$$

and

$$\begin{aligned} -\left(\frac{(m-1)(n-1)}{2}+\frac{d-1}{2}+d\lfloor x/d\rfloor\right) &= \frac{(-m+1)(n-1)}{2}-\frac{d-1}{2}-d\lfloor x/d\rfloor \\ &= \frac{(-m+1)(n-1)}{2}-\frac{d-1}{2}+d\lceil -x/d\rceil \end{aligned}$$

or equivalently since x and m are arbitrary

$$\sum_{0\le k<n}\left\lceil\frac{mk+x}{n}\right\rceil = \frac{(m+1)(n-1)}{2}-\frac{d-1}{2}+d\lceil x/d\rceil.$$

38. [*M26*] (E. Busche, 1909.) Prove that, for all real x and y with $y>0$,

$$\sum_{0\le k<y}\left\lfloor x+\frac{k}{y}\right\rfloor = \lfloor xy+\lfloor x+1\rfloor(\lceil y\rceil-y)\rfloor.$$

In particular, when y is a positive integer n, we have the important formula

$$\lfloor x\rfloor+\left\lfloor x+\frac{1}{n}\right\rfloor+\cdots+\left\lfloor x+\frac{n-1}{n}\right\rfloor = \lfloor nx\rfloor.$$

Proposition. $\sum_{0\le k<y}\left\lfloor x+\frac{k}{y}\right\rfloor = \lfloor xy+\lfloor x+1\rfloor(\lceil y\rceil-y)\rfloor$.

Proof. Let x and y be artbitrary real numbers such that $y>0$. We must show that

$$\sum_{0\le k<y}\left\lfloor x+\frac{k}{y}\right\rfloor = \lfloor xy+\lfloor x+1\rfloor(\lceil y\rceil-y)\rfloor.$$

Let n be that unique integer such that $n=\lceil(1-\{x\})y\rceil$ so that

$$\begin{aligned} n-1<(1-\{x\})y\le n \quad &\iff \quad \frac{n-1}{y}<1-\{x\}\le\frac{n}{y} \\ &\iff \quad \frac{n-1}{y}<1+\lfloor x\rfloor-x\le\frac{n}{y} \\ &\iff \quad x+\frac{n-1}{y}<1+\lfloor x\rfloor\le x+\frac{n}{y} \\ &\iff \quad x+\frac{n-1}{y}<\lfloor x+1\rfloor\le x+\frac{n}{y} \\ &\iff \quad \frac{n-1}{y}<\lfloor x+1\rfloor-x\le\frac{n}{y} \\ &\iff \quad n-1<(\lfloor x+1\rfloor-x)y\le n \\ &\iff \quad n-1<\lfloor x+1\rfloor y-xy\le n \end{aligned}$$

or equivalently

$$n = \lceil \lfloor x+1 \rfloor y - xy \rceil.$$

Note that for $0 \le k \le n-1 < n$

$$\lfloor x \rfloor \le x + \frac{k}{y} < \lfloor x+1 \rfloor \quad \Longleftrightarrow \quad \left\lfloor x + \frac{k}{y} \right\rfloor = \lfloor x \rfloor$$

and that for $n \le k \le \lceil y \rceil - 1 < y$

$$\lfloor x+1 \rfloor \le x + \frac{k}{y} < \lfloor x+2 \rfloor \quad \Longleftrightarrow \quad \left\lfloor x + \frac{k}{y} \right\rfloor = \lfloor x+1 \rfloor.$$

Then

$$\begin{aligned}
\sum_{0 \le k < y} \left\lfloor x + \frac{k}{y} \right\rfloor &= \sum_{0 \le k \le \lceil y \rceil - 1} \left\lfloor x + \frac{k}{y} \right\rfloor \\
&= \sum_{0 \le k \le n-1} \left\lfloor x + \frac{k}{y} \right\rfloor + \sum_{n \le k \le \lceil y \rceil - 1} \left\lfloor x + \frac{k}{y} \right\rfloor \\
&= n\lfloor x \rfloor + ((\lceil y \rceil - 1) - n + 1)\lfloor x+1 \rfloor \\
&= n\lfloor x \rfloor + (\lceil y \rceil - n)\lfloor x+1 \rfloor \\
&= n\lfloor x \rfloor + \lceil y \rceil \lfloor x+1 \rfloor - n\lfloor x+1 \rfloor \\
&= \lceil y \rceil \lfloor x+1 \rfloor - n \\
&= \lfloor x+1 \rfloor \lceil y \rceil - \lceil \lfloor x+1 \rfloor y - xy \rceil \\
&= \lfloor x+1 \rfloor \lceil y \rceil + \lfloor -\lfloor x+1 \rfloor y + xy \rfloor \\
&= \lfloor xy + \lfloor x+1 \rfloor \lceil y \rceil - \lfloor x+1 \rfloor y \rfloor \\
&= \lfloor xy + \lfloor x+1 \rfloor (\lceil y \rceil - y) \rfloor
\end{aligned}$$

as we needed to show. □

[*Crelle* **136** (1909), 42; the case $y = n$ is due to C. Hermite, *Acta Math.* **5** (1884), 315.]

39. [*HM35*] A function f for which $f(x) + f(x + \frac{1}{n}) + \cdots + f(x + \frac{n-1}{n}) = f(nx)$, whenever n is a positive integer, is called a *replicative function*. The previous exercise establishes the fact that $\lfloor x \rfloor$ is replicative. Show that the following functions are replicative:

a) $f(x) = x - \frac{1}{2}$;

b) $f(x) = [x \text{ is an integer}]$;

c) $f(x) = [x \text{ is a positive integer}]$;

d) $f(x) = [\text{there exists a rational number } r \text{ and an integer } m \text{ such that } x = r\pi + m]$;

e) three other functions like the one in (d), with r and/or m restricted to positive values;

f) $f(x) = \log|2 \sin \pi x|$, if the value $f(x) = -\infty$ is allowed;

g) the sum of any two replicative functions;

h) a constant multiple of a replicative function;

i) the function $g(x) = f(x - \lfloor x \rfloor)$, where $f(x)$ is replicative.

We may prove that numerous functions are replicative.

Proposition (A)**.** *$f(x) = x - \frac{1}{2}$ is replicative.*

Proof. Let f be a function defined as

$$f(x) = x - \frac{1}{2}$$

and let n be an arbitrary positive integer. We must show that

$$\sum_{0 \le k \le n-1} f\left(x + \frac{k}{n}\right) = f(nx).$$

But

$$\begin{aligned}
\sum_{0 \le k \le n-1} f\left(x + \frac{k}{n}\right) &= \sum_{0 \le k \le n-1} x + \frac{k}{n} - \frac{1}{2} \\
&= \frac{1}{x} \sum_{0 \le k \le n-1} 1 + \frac{1}{n} \sum_{0 \le k \le n-1} k - \frac{1}{2} \sum_{0 \le k \le n-1} 1 \\
&= \frac{n}{x} + \frac{(n-1)n}{2n} - \frac{n}{2} \\
&= \frac{n}{x} + \frac{n-1}{2} - \frac{n}{2} \\
&= \frac{n}{x} + \frac{n-1-n}{2} \\
&= \frac{n}{x} - \frac{1}{2} \\
&= f(nx)
\end{aligned}$$

as we needed to show. □

Proposition (B)**.** $f(x) = [x \bmod 1 = 0]$ *is replicative.*

Proof. Let f be a function defined as

$$f(x) = [x \bmod 1 = 0]$$

and let n be an arbitrary positive integer. We must show that

$$\sum_{0 \le k \le n-1} f\left(x + \frac{k}{n}\right) = f(nx).$$

But for some $k' = n - nx \bmod n - 1$, $0 \le k' \le n - 1$, we have

$$\begin{aligned}
x &= \lfloor x \rfloor + x \bmod 1 \\
&= \left\lfloor \frac{nx}{n} \right\rfloor + \frac{nx \bmod n}{n} \\
&= \left\lfloor \frac{nx}{n} \right\rfloor + \frac{n - k' - 1}{n}
\end{aligned}$$

if and only if $x - \frac{n-k'-1}{n}$ is an integer, or equivalently, if and only if $\left(x + \frac{k'}{n}\right) \bmod 1 = 0$. In the case that such a k' exists, then clearly $n \mid x$ and nx is an integer, or equivalently,

$nx \bmod 1 = 0$, and

$$\begin{aligned}
\sum_{0\le k\le n-1} f\left(x+\frac{k}{n}\right) &= \sum_{0\le k\le n-1} \left[\left(x+\frac{k}{n}\right) \bmod 1 = 0\right] \\
&= \sum_{\substack{0\le k\le n-1 \\ k\neq k'}} \left[\left(x+\frac{k}{n}\right) \bmod 1 = 0\right] \\
&\quad + \sum_{\substack{0\le k\le n-1 \\ k= k'}} \left[\left(x+\frac{k}{n}\right) \bmod 1 = 0\right] \\
&= 0 + 1 \\
&= 1 \\
&= [nx \bmod 1 = 0] \\
&= f(nx).
\end{aligned}$$

In the case that such a k' does not exist, then clearly $n \nmid x$ and nx is not an integer, or equivalently, $nx \bmod 1 \neq 0$, and

$$\begin{aligned}
\sum_{0\le k\le n-1} f\left(x+\frac{k}{n}\right) &= \sum_{0\le k\le n-1} \left[\left(x+\frac{k}{n}\right) \bmod 1 = 0\right] \\
&= 0 \\
&= [nx \bmod 1 = 0] \\
&= f(nx).
\end{aligned}$$

In either case, we find that

$$\sum_{0\le k\le n-1} f\left(x+\frac{k}{n}\right) = f(nx)$$

as we needed to show. □

Proposition (C)**.** $f(x) = [x \bmod 1 = 0 \wedge x > 0]$ *is replicative.*

Proof. Let f be a function defined as

$$f(x) = [x \bmod 1 = 0 \wedge x > 0] = [x > 0][x \bmod 1 = 0]$$

and let n be an arbitrary positive integer. We must show that

$$\sum_{0\le k\le n-1} f\left(x+\frac{k}{n}\right) = f(nx).$$

But similar to **Proposition B**, for some $k' = n - nx \bmod n - 1$, $0 \le k' \le n-1$, we have

$$\begin{aligned}
x &= \lfloor x \rfloor + x \bmod 1 \\
&= \left\lfloor \frac{nx}{n} \right\rfloor + \frac{nx \bmod n}{n} \\
&= \left\lfloor \frac{nx}{n} \right\rfloor + \frac{n - k' - 1}{n}
\end{aligned}$$

if and only if $x - \frac{n-k'-1}{n}$ is an integer, or equivalently, if and only if $\left(x + \frac{k'}{n}\right) \bmod 1 = 0$. In the case that such a k' exists, then clearly $n \mid x$ and nx is an integer, or equivalently, $nx \bmod 1 = 0$, and

$$\begin{aligned}
\sum_{0\le k\le n-1} f\left(x+\frac{k}{n}\right) &= \sum_{0\le k\le n-1} \left[x+\frac{k}{n}>0\right]\left[\left(x+\frac{k}{n}\right) \bmod 1 = 0\right] \\
&= \sum_{\substack{0\le k\le n-1\\ k\ne k'}} \left[x+\frac{k}{n}>0\right]\left[\left(x+\frac{k}{n}\right) \bmod 1 = 0\right] \\
&\quad + \sum_{\substack{0\le k\le n-1\\ k= k'}} \left[x+\frac{k}{n}>0\right]\left[\left(x+\frac{k}{n}\right) \bmod 1 = 0\right] \\
&= \sum_{\substack{0\le k\le n-1\\ k\ne k'}} \left[x+\frac{k}{n}>0\right](0) \\
&\quad + \left[x+\frac{k'}{n}>0 \wedge \left(x+\frac{k}{n}\right) \bmod 1 = 0\right]\left[\left(x+\frac{k}{n}\right) \bmod 1 = 0\right] \\
&= 0 + \left[x+\frac{k'}{n}>0\right]\left[\left(x+\frac{k'}{n}\right) \bmod 1 = 0\right] \\
&= \left[x+\frac{k'}{n}>0 \wedge \left(x+\frac{k'}{n}\right) \bmod 1 = 0\right] \\
&= \left[x+\frac{k'}{n}\ge 1 \wedge \left(x+\frac{k'}{n}\right) \bmod 1 = 0\right] \\
&= \left[x>0 \wedge \left(x+\frac{k'}{n}\right) \bmod 1 = 0\right] \\
&= \left[nx>0 \wedge \left(x+\frac{k'}{n}\right) \bmod 1 = 0\right] \\
&= [nx>0]\left[\left(x+\frac{k'}{n}\right) \bmod 1 = 0\right] \\
&= [nx>0](1) \\
&= [nx>0][nx \bmod 1 = 0] \\
&= f(nx)
\end{aligned}$$

since $x \le 0$ if and only if $x + \frac{k'}{n} < 1$, and so neither it nor any multiple a positive integer such as nx.

In the case that such a k' does not exist, then clearly $n \nmid x$ and nx is not an integer, or equivalently, $nx \bmod 1 \ne 0$, and

$$\begin{aligned}
\sum_{0\le k\le n-1} f\left(x+\frac{k}{n}\right) &= \sum_{0\le k\le n-1} \left[x+\frac{k}{n}>0\right]\left[\left(x+\frac{k}{n}\right) \bmod 1 = 0\right] \\
&= \sum_{0\le k\le n-1} \left[x+\frac{k}{n}>0\right](0) \\
&= 0 \\
&= [nx>0](0) \\
&= [nx>0][nx \bmod 1 = 0] \\
&= f(nx).
\end{aligned}$$

In either case, we find that

$$\sum_{0\leq k\leq n-1} f\left(x+\frac{k}{n}\right) = f(nx)$$

as we needed to show. □

Proposition (D)**.** *$f(x) = [\exists r \in \mathbb{Q}, m \in \mathbb{Z} : x = r\pi + m]$ is replicative.*

Proof. Let f be a function defined as

$$f(x) = [\exists r \in \mathbb{Q}, m \in \mathbb{Z} : x = r\pi + m]$$

and let n be an arbitrary positive integer. We must show that

$$\sum_{0\leq k\leq n-1} f\left(x+\frac{k}{n}\right) = f(nx).$$

In the case that we may find an integer k' such that

$$x + \frac{k'}{n} = r\pi + m$$

it must be unique since if we found an integer k'' such that $x+\frac{k''}{n} = r'\pi+m'$, $(r-r')\pi$ can only be an integer if $r = r'$ and $(m-m')$ can only be a rational if $m = m'$, and so $k' = k''$. Then,

$$\begin{aligned} x + \frac{k'}{n} = r\pi + m \quad &\iff \quad nx + k' = nr\pi + nm \\ &\iff \quad nx = nr\pi + nm - k' \\ &\iff \quad nx = r'\pi + m' \end{aligned}$$

for a rational $r' = nr$ and an integer $m' = nm - k'$. Hence

$$\begin{aligned} \sum_{0\leq k\leq n-1} f\left(x+\frac{k}{n}\right) &= \sum_{0\leq k\leq n-1} [\exists r \in \mathbb{Q}, m \in \mathbb{Z} : x + \frac{k}{n} = r\pi + m] \\ &= \sum_{\substack{0\leq k\leq n-1 \\ k\neq k'}} [\exists r \in \mathbb{Q}, m \in \mathbb{Z} : x + \frac{k}{n} = r\pi + m] \\ &\quad + \sum_{\substack{0\leq k\leq n-1 \\ k=k''}} [\exists r \in \mathbb{Q}, m \in \mathbb{Z} : x + \frac{k}{n} = r\pi + m] \\ &= \sum_{\substack{0\leq k\leq n-1 \\ k\neq k'}} (0) + [\exists r \in \mathbb{Q}, m \in \mathbb{Z} : x + \frac{k'}{n} = r\pi + m] \\ &= 0 + 1 \\ &= 1 \\ &= [\exists r \in \mathbb{Q}, m \in \mathbb{Z} : nx = r\pi + m] \\ &= f(nx). \end{aligned}$$

In the case that we may not find such an integer k', even $k' = 0$, then clearly $x \neq r\pi+m$

if and only if $nx \neq r'\pi + m'$ for $r' = nr$ and $m' = nm$, and in such a case

$$\begin{aligned}\sum_{0\leq k\leq n-1} f\left(x+\frac{k}{n}\right) &= \sum_{0\leq k\leq n-1} [\exists r\in\mathbb{Q}, m\in\mathbb{Z} : x+\frac{k}{n} = r\pi + m] \\ &= \sum_{0\leq k\leq n-1} (0) \\ &= 0 \\ &= [\exists r\in\mathbb{Q}, m\in\mathbb{Z} : nx = r\pi + m] \\ &= f(nx).\end{aligned}$$

In either case, we find that

$$\sum_{0\leq k\leq n-1} f\left(x+\frac{k}{n}\right) = f(nx)$$

as we needed to show. □

Proposition (E1)**.** *$f(x) = [\exists r\in\mathbb{Q}^+, m\in\mathbb{Z} : x = r\pi + m]$ is replicative.*

Proof. Let f be a function defined as

$$f(x) = [\exists r\in\mathbb{Q}^+, m\in\mathbb{Z} : x = r\pi + m]$$

and let n be an arbitrary positive integer. We must show that

$$\sum_{0\leq k\leq n-1} f\left(x+\frac{k}{n}\right) = f(nx).$$

But we may rely on the proof of **Proposition D**, and specifically, the determination of the rational r' such that $r' = nr$. $r > 0$ if and only if $nr > 0$, since $n > 0$. Hence the result. □

Proposition (E2)**.** *$f(x) = [\exists r\in\mathbb{Q}, m\in\mathbb{Z}^+ : x = r\pi + m]$ is replicative.*

Proof. Let f be a function defined as

$$f(x) = [\exists r\in\mathbb{Q}, m\in\mathbb{Z}^+ : x = r\pi + m]$$

and let n be an arbitrary positive integer. We must show that

$$\sum_{0\leq k\leq n-1} f\left(x+\frac{k}{n}\right) = f(nx).$$

But we may rely on the proof of **Proposition D**, and specifically, the determination of the integer m' such that $m' = nm - k'$. $m > 0$ if and only if $nr > 0$, since $n > k' \geq 0$. Hence the result. □

Proposition (E3)**.** *$f(x) = [(\exists r\in\mathbb{Q}^+, m\in\mathbb{Z}^+ : x = r\pi + m]$ is replicative.*

Proof. Let f be a function defined as

$$f(x) = [\exists r\in\mathbb{Q}^+, m\in\mathbb{Z}^+ : x = r\pi + m]$$

and let n be an arbitrary positive integer. We must show that

$$\sum_{0\leq k\leq n-1} f\left(x+\frac{k}{n}\right) = f(nx).$$

But we may rely on the proofs of **Proposition E1** and **Proposition E2**, and specifically, the determination of both the rational r' such that $r' = nr$ and the integer m' such that $m' = nm - k'$ simultaneously. Hence the result. □

Proposition (F)**.** *$f(x) = \log|2\sin\pi x|$ is replicative, if the value $f(x) = -\infty$ is allowed.*

Proof. Let f be a function defined as

$$f(x) = \log|2\sin\pi x|$$

and let n be an arbitrary positive integer. We must show that

$$\sum_{0\le k\le n-1} f\left(x+\frac{k}{n}\right) = f(nx)$$

allowing for $f(x) = -\infty$.

Note that we have the equalities

$$2\sin\theta = (e^{i\theta} - e^{-i\theta})/i = (1-e^{-2i\theta})e^{i\theta - i\pi/2},$$

$$\prod_{0\le k\le n-1} (1 - e^{-2i\pi(x+k/n)}) = 1 - e^{-2i\pi nx},$$

and

$$\prod_{0\le k\le n-1} e^{i\pi(x-(1/2)+(k/n))} = e^{i\pi(nx-1/2)}.$$

Then

$$\begin{aligned}
\sum_{0\le k\le n-1} f\left(x+\frac{k}{n}\right) &= \sum_{0\le k\le n-1} \log\left|2\sin\pi\left(x+\frac{k}{n}\right)\right| \\
&= \log\left|\prod_{0\le k\le n-1} 2\sin\pi\left(x+\frac{k}{n}\right)\right| \\
&= \log\left|\prod_{0\le k\le n-1} (e^{i\pi\left(x+\frac{k}{n}\right)} - e^{-i\pi\left(x+\frac{k}{n}\right)})/i\right| \\
&= \log\left|\prod_{0\le k\le n-1} (1-e^{-2i\pi\left(x+\frac{k}{n}\right)})e^{i\pi\left(x+\frac{k}{n}\right)-i\pi/2}\right| \\
&= \log\left|\left(\prod_{0\le k\le n-1} 1-e^{-2i\pi\left(x+\frac{k}{n}\right)}\right)\left(\prod_{0\le k\le n-1} e^{i\pi\left(x+\frac{k}{n}\right)-i\pi/2}\right)\right| \\
&= \log\left|(1-e^{-2i\pi nx})(e^{i\pi(nx-1/2)})\right| \\
&= \log\left|(e^{i\pi nx} - e^{-i\pi nx})/i\right| \\
&= \log|2\sin\pi nx|
\end{aligned}$$

as we needed to show. □

Proposition (G)**.** *The sum of any two replicative functions is replicative.*

Proof. Let f and g be replicative functions, h a function defined as

$$h(x) = f(x) + g(x),$$

and let n be an arbitrary positive integer. We must show that

$$\sum_{0 \le k \le n-1} h\left(x + \frac{k}{n}\right) = h(nx).$$

But

$$\begin{aligned}\sum_{0 \le k \le n-1} h\left(x + \frac{k}{n}\right) &= \sum_{0 \le k \le n-1} f\left(x + \frac{k}{n}\right) + g\left(x + \frac{k}{n}\right) \\ &= \sum_{0 \le k \le n-1} f\left(x + \frac{k}{n}\right) + \sum_{0 \le k \le n-1} g\left(x + \frac{k}{n}\right) \\ &= f(xn) + g(xn) \\ &= h(xn)\end{aligned}$$

as we needed to show. □

Proposition (H)**.** *A constant multiple of a replicative function is replicative.*

Proof. Let f be a replicative function, c an arbitrary real number, g a function defined as

$$g(x) = cf(x),$$

and let n be an arbitrary positive integer. We must show that

$$\sum_{0 \le k \le n-1} g\left(x + \frac{k}{n}\right) = g(nx).$$

But

$$\begin{aligned}\sum_{0 \le k \le n-1} g\left(x + \frac{k}{n}\right) &= \sum_{0 \le k \le n-1} cf\left(x + \frac{k}{n}\right) \\ &= c \sum_{0 \le k \le n-1} f\left(x + \frac{k}{n}\right) \\ &= cf(xn) \\ &= g(xn)\end{aligned}$$

as we needed to show. □

Proposition (I)**.** *The function $g(x) = f(x - \lfloor x \rfloor)$, where $f(x)$ is replicative is itself replicative.*

Proof. Let f be a replicative function, g a function defined as

$$g(x) = f(x - \lfloor x \rfloor),$$

and let n be an arbitrary positive integer. We must show that

$$\sum_{0 \le k \le n-1} g\left(x + \frac{k}{n}\right) = g(nx).$$

Let k' be the unique integer such that

$$\{x\} + \frac{k'-1}{n} < 1 \le \{x\} + \frac{k'}{n}$$

so that $k' = \lceil n(1-\{x\}) \rceil$. Then

$$\begin{aligned}
\sum_{0\le k\le n-1} g\left(x+\frac{k}{n}\right) &= \sum_{0\le k\le n-1} f\left(\left\{x+\frac{k}{n}\right\}\right) \\
&= \sum_{0\le k\le k'-1} f\left(\left\{x+\frac{k}{n}\right\}\right) + \sum_{k'\le k\le n-1} f\left(\left\{x+\frac{k}{n}\right\}\right) \\
&= \sum_{0\le k\le k'-1} f\left(\{x\}+\frac{k}{n}\right) + \sum_{k'\le k\le n-1} f\left(\{x\}+\frac{k}{n}-1\right) \\
&= \sum_{0\le k\le k'-1} f\left(\{x\}+\frac{k}{n}\right) + \sum_{k'\le k\le n-1} f\left(\{x\}+\frac{k-n}{n}\right) \\
&= \sum_{n-k'\le k\le n-1} f\left(\{x\}+\frac{k'-n+k}{n}\right) + \sum_{0\le k\le n-k'-1} f\left(\{x\}+\frac{k'-n+k}{n}\right) \\
&= \sum_{0\le k\le n-1} f\left(\{x\}+\frac{k'-n}{n}+\frac{k}{n}\right) \\
&= f\left(n\left(\{x\}+\frac{k'-n}{n}\right)\right) \\
&= f\left(n\{x\}+k'-n\right) \\
&= f\left(n\{x\}+\lceil n(1-\{x\})\rceil - n\right) \\
&= f\left(n\{x\}+\lceil n-n\{x\}-n\rceil\right) \\
&= f\left(n\{x\}+\lceil -n\{x\}\rceil\right) \\
&= f\left(n\{x\}-\lfloor n\{x\}\rfloor\right) \\
&= f\left(\{n\{x\}\}\right) \\
&= f\left(\{nx-n\lfloor x\rfloor\}\right) \\
&= f\left(\{nx-\lfloor nx\rfloor\}\right) \\
&= f\left(\{nx\}\right) \\
&= f\left(nx-\lfloor nx\rfloor\right) \\
&= g(nx)
\end{aligned}$$

as we needed to show. □

40. [*HM46*] Study the class of replicative functions; determine all replicative functions of a special type. For example, is the function in (a) of exercise 39 the only continuous replicative function? It may be interesting to study also the more general class of functions for which

$$f(x) + f\left(x+\frac{1}{n}\right) + \cdots + f\left(x+\frac{n-1}{n}\right) = a_n f(nx) + b_n.$$

Here a_n and b_n are numbers that depend on n but not on x. Derivatives and (if $b_n = 0$) integrals of these functions are of the same type. If we require that $b_n = 0$, we have, for example, the Bernoulli polynomials, the trigonometric functions $\cot \pi x$ and $\csc^2 \pi x$, as well as Hurwitz's generalized zeta function $\zeta(s,x) = \sum_{k\ge 0} 1/(k+x)^s$ for fixed s. With $b_n \neq 0$ we have still other well-known functions, such as the psi function.

n.a.

... For further results see L. J. Mordell, *J. London Math. Soc.* **33** (1958), 371–375.; M. F. Yoder, *Æquationes Mathematcæ* **13** (1975), 251–261.

41. [*M23*] Let $a_1, a_2, a_3, \ldots$ be the sequence $1, 2, 2, 3, 3, 3, 4, 4, 4, 4, \ldots$; find an expression for a_n in terms of n, using the floor and/or ceiling function.

We want to find a kind of inverse of the sum of the first n integers. That is, we want to know $a_n = k$ such that

$$\sum_{1\le i\le k-1} i = \frac{(k-1)k}{2} < n \le \frac{k(k+1)}{2} = \sum_{1\le i\le k} i.$$

Solving for k yields

$$k - 1 < \frac{\sqrt{8n+1}-1}{2} \le k$$

or equivalently

$$k = a_n = \left\lceil \frac{\sqrt{8n+1}-1}{2} \right\rceil.$$

42. [*M24*] (a) Prove that

$$\sum_{k=1}^{n} a_k = na_n - \sum_{k=1}^{n-1} k(a_{k+1} - a_k), \qquad \text{if } n > 0.$$

(b) The preceding formula is useful for evaluating certain sums involving the floor function. Prove that, if b is an integer ≥ 2,

$$\sum_{k=1}^{n} \lfloor \log_b k \rfloor = (n+1)\lfloor \log_b n \rfloor - (b^{\lfloor \log_b n \rfloor + 1} - b)/(b-1).$$

Proposition (A). $\sum_{1\le k\le n} a_k = na_n - \sum_{1\le k\le n-1} k(a_{k+1} - a_k)$ *if* $n > 0$.

Proof. Let n be an arbitrary integer such that $n > 0$. We must show that

$$\sum_{1\le k\le n} a_k = na_n - \sum_{1\le k\le n-1} k(a_{k+1} - a_k).$$

But

$$\begin{aligned}
\sum_{1\le k\le n} a_k &= \sum_{1\le k\le n} (1)a_k \\
&= \sum_{1\le k\le n} (k-k+1)a_k \\
&= \sum_{1\le k\le n} ka_k - (k-1)a_k \\
&= -\sum_{1\le k\le n} (k-1)a_k + \sum_{1\le k\le n} ka_k \\
&= (0)a_1 - \sum_{2\le k\le n} (k-1)a_k + \sum_{1\le k\le n} ka_k \\
&= -\sum_{2\le k\le n} (k-1)a_k + \sum_{1\le k\le n} ka_k \\
&= na_n - \sum_{2\le k\le n} (k-1)a_k + \sum_{1\le k\le n-1} ka_k \\
&= na_n - \sum_{1\le k\le n-1} ka_{k+1} + \sum_{1\le k\le n-1} ka_k \\
&= na_n - \sum_{1\le k\le n-1} ka_{k+1} - ka_k \\
&= na_n - \sum_{1\le k\le n-1} k(a_{k+1} - a_k)
\end{aligned}$$

as we needed to show. □

Proposition (B)**.** $\sum_{1\le k\le n}\lfloor \log_b k\rfloor = (n+1)\lfloor \log_b n\rfloor - (b^{\lfloor \log_b n\rfloor+1} - b)/(b-1)$ *if* $b \ge 2$.

Proof. Let b be an arbitrary integer such that $b \ge 2$. We must show that

$$\sum_{1\le k\le n} \lfloor \log_b k\rfloor = (n+1)\lfloor \log_b n\rfloor - (b^{\lfloor \log_b n\rfloor+1} - b)/(b-1).$$

But from **Proposition A**, we have

$$\begin{aligned}
\sum_{1\le k\le n}\lfloor\log_b k\rfloor &= \sum_{1\le k\le n-1}\lfloor\log_b k\rfloor + \sum_{n\le k\le n}\lfloor\log_b k\rfloor \\
&= \sum_{1\le k\le n-1}\lfloor\log_b k\rfloor + \sum_{b^{\lfloor\log_b n\rfloor}\le k\le n}\lfloor\log_b k\rfloor \\
&= \sum_{b^0\le k<b^{\lfloor\log_b n\rfloor}}\lfloor\log_b k\rfloor + \sum_{b^{\lfloor\log_b n\rfloor}\le k\le n}\lfloor\log_b k\rfloor \\
&= \sum_{0\le j<\lfloor\log_b n\rfloor}\ \sum_{b^j\le k<b^{j+1}}\lfloor\log_b k\rfloor + \sum_{b^{\lfloor\log_b n\rfloor}\le k\le n}\lfloor\log_b k\rfloor \\
&= \sum_{0\le j<\lfloor\log_b n\rfloor} j(b^{j+1}-b^j) + \sum_{b^{\lfloor\log_b n\rfloor}\le k\le n}\lfloor\log_b k\rfloor \\
&= \left(\sum_{0\le j<\lfloor\log_b n\rfloor} j(b^{j+1}-b^j)\right) + (n-b^{\lfloor\log_b n\rfloor}+1)\lfloor\log_b n\rfloor \\
&= -\left(\lfloor\log_b n\rfloor b^{\lfloor\log_b n\rfloor} - \sum_{0\le j\le\lfloor\log_b n\rfloor-1} j(b^{j+1}-b^j)\right) + (n+1)\lfloor\log_b n\rfloor \\
&= -\left(\sum_{0\le j\le\lfloor\log_b n\rfloor-1} b^{j+1}\right) + (n+1)\lfloor\log_b n\rfloor \\
&= (n+1)\lfloor\log_b n\rfloor - \sum_{1\le j\le\lfloor\log_b n\rfloor} b^j \\
&= (n+1)\lfloor\log_b n\rfloor - (b^{\lfloor\log_b n\rfloor+1}-b)/(b-1)
\end{aligned}$$

as we needed to show. □

43. [*M23*] Evaluate $\sum_{k=1}^{n}\lfloor\sqrt{k}\rfloor$.

We have by exercise 42

$$\begin{aligned}
\sum_{1\le k\le n}\lfloor\sqrt{k}\rfloor &= \sum_{1\le k\le n-1}\lfloor\sqrt{k}\rfloor + \sum_{n\le k\le n}\lfloor\sqrt{k}\rfloor \\
&= \sum_{1^2\le k<\lfloor n\rfloor^2}\lfloor\sqrt{k}\rfloor + \sum_{\lfloor\sqrt{n}\rfloor^2\le k\le n}\lfloor\sqrt{k}\rfloor \\
&= \sum_{1\le j<\lfloor n\rfloor}\sum_{j^2\le k<(j+1)^2}\lfloor\sqrt{k}\rfloor + \sum_{\lfloor\sqrt{n}\rfloor^2\le k\le n}\lfloor\sqrt{k}\rfloor \\
&= \sum_{1\le j<\lfloor n\rfloor} j((j+1)^2-j^2) + \sum_{\lfloor\sqrt{n}\rfloor^2\le k\le n}\lfloor\sqrt{k}\rfloor \\
&= \left(\sum_{1\le j<\lfloor n\rfloor} j((j+1)^2-j^2)\right) + (n-\lfloor\sqrt{n}\rfloor^2+1)\lfloor\sqrt{n}\rfloor \\
&= (n-\lfloor\sqrt{n}\rfloor^2+1)\lfloor\sqrt{n}\rfloor + \left(\sum_{1\le j<\lfloor n\rfloor} j((j+1)^2-j^2)\right) \\
&= (n+1)\lfloor\sqrt{n}\rfloor - \left(\lfloor\sqrt{n}\rfloor\lfloor\sqrt{n}\rfloor^2 - \left(\sum_{1\le j<\lfloor n\rfloor} j((j+1)^2-j^2)\right)\right) \\
&= (n+1)\lfloor\sqrt{n}\rfloor - \sum_{1\le k\le\lfloor\sqrt{n}\rfloor} k^2 \\
&= (n+1)\lfloor\sqrt{n}\rfloor - \frac{\lfloor\sqrt{n}\rfloor(\lfloor\sqrt{n}\rfloor+1)(2\lfloor\sqrt{n}\rfloor+1)}{6} \\
&= \lfloor\sqrt{n}\rfloor\left((n+1) - \frac{(\lfloor\sqrt{n}\rfloor+1)(2\lfloor\sqrt{n}\rfloor+1)}{6}\right) \\
&= \lfloor\sqrt{n}\rfloor\left(n - \frac{(\lfloor\sqrt{n}\rfloor+1)(2\lfloor\sqrt{n}\rfloor+1)-6}{6}\right) \\
&= \lfloor\sqrt{n}\rfloor\left(n - \frac{(2\lfloor\sqrt{n}\rfloor+5)(\lfloor\sqrt{n}\rfloor-1)}{6}\right).
\end{aligned}$$

44. [*M24*] Show that $\sum_{k\ge0}\sum_{1\le j<b}\lfloor(n+jb^k)/b^{k+1}\rfloor = n$, if b and n are integers, $n\ge0$, and $b\ge2$. What is the value of this sum when $n<0$?

We may prove the equality for nonnegative n.

Proposition. $\sum_{k\ge0}\sum_{1\le j<b}\left\lfloor\frac{n+jb^k}{b^{k+1}}\right\rfloor = n$ *if* b *and* n *are integers,* $n\ge0$*, and* $b\ge2$*.*

Proof. Let b and n be arbitrary integers such that $n\ge0$ and $b\ge2$. We must show that

$$\sum_{k\ge0}\sum_{1\le j<b}\left\lfloor\frac{n+jb^k}{b^{k+1}}\right\rfloor = n.$$

By exercise 38 with $x = \frac{n}{b^{k+1}}$ and $y = b$ we have

$$\begin{aligned}
\sum_{1\le j<b} \left\lfloor \frac{n+jb^k}{b^{k+1}} \right\rfloor &= \left(\sum_{0\le j<b} \lfloor \frac{n+jb^k}{b^{k+1}} \rfloor \right) - \left\lfloor \frac{n}{b^{k+1}} \right\rfloor \\
&= \left(\sum_{0\le j<b} \left\lfloor \frac{n}{b^{k+1}} + \frac{j}{b} \right\rfloor \right) - \left\lfloor \frac{n}{b^{k+1}} \right\rfloor \\
&= \left\lfloor \frac{nb}{b^{k+1}} + \left\lfloor \frac{n}{b^{k+1}} + 1 \right\rfloor (\lceil b \rceil - b) \right\rfloor - \left\lfloor \frac{n}{b^{k+1}} \right\rfloor \\
&= \left\lfloor \frac{nb}{b^{k+1}} \right\rfloor - \left\lfloor \frac{n}{b^{k+1}} \right\rfloor \\
&= \left\lfloor \frac{n}{b^k} \right\rfloor - \left\lfloor \frac{n}{b^{k+1}} \right\rfloor .
\end{aligned}$$

In the case that $n > 0$, for some arbitrary k

$$\begin{aligned}
\left\lfloor \frac{n}{b^k} \right\rfloor = 0 \quad &\iff \quad 0 \le \frac{n}{b^k} < 1 \\
&\implies \quad n < b^k \\
&\iff \quad \log_b n < \log_b b^k \\
&\iff \quad \log_b n < k \\
&\iff \quad k \ge \lfloor \log_b n \rfloor + 1.
\end{aligned}$$

Then

$$\begin{aligned}
\sum_{k\ge 0} \sum_{1\le j<b} \left\lfloor \frac{n+jb^k}{b^{k+1}} \right\rfloor &= \sum_{k\ge 0} \left\lfloor \frac{n}{b^k} \right\rfloor - \left\lfloor \frac{n}{b^{k+1}} \right\rfloor \\
&= \left(\sum_{0\le k\le \lfloor \log_b n \rfloor} \left\lfloor \frac{n}{b^k} \right\rfloor - \left\lfloor \frac{n}{b^{k+1}} \right\rfloor \right) + \left(\sum_{k\ge \lfloor \log_b n \rfloor + 1} \left\lfloor \frac{n}{b^k} \right\rfloor - \left\lfloor \frac{n}{b^{k+1}} \right\rfloor \right) \\
&= \left(\sum_{0\le k\le \lfloor \log_b n \rfloor} \left\lfloor \frac{n}{b^k} \right\rfloor - \left\lfloor \frac{n}{b^{k+1}} \right\rfloor \right) + 0 \\
&= \sum_{0\le k\le \lfloor \log_b n \rfloor} \left\lfloor \frac{n}{b^k} \right\rfloor - \sum_{0\le k\le \lfloor \log_b n \rfloor} \left\lfloor \frac{n}{b^{k+1}} \right\rfloor \\
&= \left\lfloor \frac{n}{b^0} \right\rfloor + \sum_{1\le k\le \lfloor \log_b n \rfloor} \left\lfloor \frac{n}{b^k} \right\rfloor - \sum_{1\le k\le \lfloor \log_b n \rfloor + 1} \left\lfloor \frac{n}{b^k} \right\rfloor \\
&= \left\lfloor \frac{n}{b^0} \right\rfloor + \sum_{1\le k\le \lfloor \log_b n \rfloor} \left\lfloor \frac{n}{b^k} \right\rfloor - \left(\sum_{1\le k\le \lfloor \log_b n \rfloor} \left\lfloor \frac{n}{b^k} \right\rfloor \right) - \left\lfloor \frac{n}{b^{\lfloor \log_b n \rfloor + 1}} \right\rfloor \\
&= \left\lfloor \frac{n}{b^0} \right\rfloor + 0 - \left\lfloor \frac{n}{b^{\lfloor \log_b n \rfloor + 1}} \right\rfloor \\
&= n - 0 \\
&= n.
\end{aligned}$$

In the case that $n = 0$, then clearly

$$\sum_{k\ge 0} \sum_{1\le j<b} \left\lfloor \frac{0+jb^k}{b^{k+1}} \right\rfloor = \sum_{k\ge 0} \left\lfloor \frac{0}{b^k} \right\rfloor - \left\lfloor \frac{0}{b^{k+1}} \right\rfloor = 0 = n.$$

Hence, in either case

$$\sum_{k\geq 0}\sum_{1\leq j<b}\left\lfloor\frac{n+jb^k}{b^{k+1}}\right\rfloor = n$$

as we needed to show. □

When $n<0$, we may find an arbitrary k such that

$$\begin{aligned}\left\lfloor\frac{n}{b^k}\right\rfloor = -1 &\iff -1\leq\frac{n}{b^k}<0\\ &\iff 0<\frac{-n}{b^k}\leq 1\\ &\implies -n\leq b^k\\ &\iff \log_b -n\leq\log_b b^k\\ &\iff \log_b -n\leq k\\ &\iff k\geq\lfloor\log_b -n\rfloor.\end{aligned}$$

Then

$$\begin{aligned}\sum_{k\geq 0}\sum_{1\leq j<b}\left\lfloor\frac{n+jb^k}{b^{k+1}}\right\rfloor &= \sum_{k\geq 0}\left\lfloor\frac{n}{b^k}\right\rfloor-\left\lfloor\frac{n}{b^{k+1}}\right\rfloor\\ &= \left(\sum_{0\leq k\leq\lfloor\log_b -n\rfloor-1}\left\lfloor\frac{n}{b^k}\right\rfloor-\left\lfloor\frac{n}{b^{k+1}}\right\rfloor\right)+\left(\sum_{k\geq\lfloor\log_b -n\rfloor}\left\lfloor\frac{n}{b^k}\right\rfloor-\left\lfloor\frac{n}{b^{k+1}}\right\rfloor\right)\\ &= \left(\sum_{0\leq k\leq\lfloor\log_b -n\rfloor-1}\left\lfloor\frac{n}{b^k}\right\rfloor-\left\lfloor\frac{n}{b^{k+1}}\right\rfloor\right)+\left(\sum_{k\geq\lfloor\log_b -n\rfloor}-1+1\right)\\ &= \left(\sum_{0\leq k\leq\lfloor\log_b -n\rfloor-1}\left\lfloor\frac{n}{b^k}\right\rfloor-\left\lfloor\frac{n}{b^{k+1}}\right\rfloor\right)+0\\ &= \sum_{0\leq k\leq\lfloor\log_b -n\rfloor-1}\left\lfloor\frac{n}{b^k}\right\rfloor-\sum_{0\leq k\leq\lfloor\log_b -n\rfloor-1}\left\lfloor\frac{n}{b^{k+1}}\right\rfloor\\ &= \left\lfloor\frac{n}{b^0}\right\rfloor+\sum_{1\leq k\leq\lfloor\log_b -n\rfloor-1}\left\lfloor\frac{n}{b^k}\right\rfloor-\sum_{1\leq k\leq\lfloor\log_b -n\rfloor}\left\lfloor\frac{n}{b^k}\right\rfloor\\ &= \left\lfloor\frac{n}{b^0}\right\rfloor+\sum_{1\leq k\leq\lfloor\log_b -n\rfloor-1}\left\lfloor\frac{n}{b^k}\right\rfloor-\left(\sum_{1\leq k\leq\lfloor\log_b -n\rfloor-1}\left\lfloor\frac{n}{b^k}\right\rfloor\right)-\left\lfloor\frac{n}{b^{\lfloor\log_b -n\rfloor}}\right\rfloor\\ &= \left\lfloor\frac{n}{b^0}\right\rfloor+0-\left\lfloor\frac{n}{b^{\lfloor\log_b -n\rfloor}}\right\rfloor\\ &= n+1.\end{aligned}$$

► **45.** [*M28*] The result of exercise 37 is somewhat surprising, since it implies that when m and n are positive integers

$$\sum_{0\leq k<n}\left\lfloor\frac{mk+x}{n}\right\rfloor=\sum_{0\leq k<m}\left\lfloor\frac{nk+x}{m}\right\rfloor.$$

This "reciprocity relationship" is one of many similar formulas (see Section 3.3.3). Show that for any function f, we have

$$\sum_{0\leq j<n}f\left(\left\lfloor\frac{mj}{n}\right\rfloor\right)=\sum_{0\leq r<m}\left\lceil\frac{rn}{m}\right\rceil(f(r-1)-f(r))+nf(m-1).$$

In particular, prove that

$$\sum_{0\le j<n}\binom{\lfloor mj/n\rfloor+1}{k}+\sum_{0\le j<m}\left\lfloor\frac{jn}{m}\right\rfloor\binom{j}{k-1}=n\binom{m}{k}.$$

[*Hint:* Consider the change of variable $r=\lfloor mj/n\rfloor$. Binomial coefficients $\binom{m}{k}$ are discussed in Section 1.2.6.]

Proposition. $\sum_{0\le j<n} f\left(\left\lfloor\frac{mj}{n}\right\rfloor\right)=nf(m-1)+\sum_{0\le r<m}\left\lceil\frac{rn}{m}\right\rceil(f(r-1)-f(r))$ *for any function* f *and positive integers* m *and* n.

Proof. Let f be any function and m and n arbitrary positive integers. We must show that

$$\sum_{0\le j<n} f\left(\left\lfloor\frac{mj}{n}\right\rfloor\right)=nf(m-1)+\sum_{0\le r<m}\left\lceil\frac{rn}{m}\right\rceil(f(r-1)-f(r)).$$

Note that

$$\begin{aligned}
\left\lfloor\frac{mj}{n}\right\rfloor=r &\iff r\le\frac{mj}{n}<r+1\\
&\iff nr\le mj<n(r+1)\\
&\iff \frac{nr}{m}\le j<\frac{n(r+1)}{m}\\
&\iff \frac{nr}{m}\le j<\frac{n(r+1)}{m}.\\
&\iff \left\lceil\frac{nr}{m}\right\rceil\le j<\left\lceil\frac{n(r+1)}{m}\right\rceil.
\end{aligned}$$

Then

$$\begin{aligned}
\sum_{0\le j<n} f\left(\left\lfloor\frac{mj}{n}\right\rfloor\right)&=\sum_{0\le r<m}\sum_{\lceil\frac{nr}{m}\rceil\le j<\lceil\frac{n(r+1)}{m}\rceil} f\left(\left\lfloor\frac{mj}{n}\right\rfloor\right)\\
&=\sum_{0\le r<m}\sum_{\lceil\frac{nr}{m}\rceil\le j<\lceil\frac{n(r+1)}{m}\rceil} f(r)\\
&=\sum_{0\le r<m}\left(\left\lceil\frac{n(r+1)}{m}\right\rceil-\left\lceil\frac{nr}{m}\right\rceil\right)f(r)\\
&=\sum_{0\le r<m}\left\lceil\frac{n(r+1)}{m}\right\rceil f(r)-\left\lceil\frac{nr}{m}\right\rceil f(r)\\
&=\sum_{0\le r<m}\left\lceil\frac{n(r+1)}{m}\right\rceil f(r)-\sum_{0\le r<m}\left\lceil\frac{nr}{m}\right\rceil f(r)\\
&=\sum_{1\le r<m+1}\left\lceil\frac{nr}{m}\right\rceil f(r-1)-\sum_{0\le r<m}\left\lceil\frac{nr}{m}\right\rceil f(r)\\
&=\left\lceil\frac{nm}{m}\right\rceil f(m-1)+\left\lceil\frac{n(0)}{m}\right\rceil f(0-1)+\sum_{1\le r<m}\left\lceil\frac{nr}{m}\right\rceil f(r-1)-\sum_{0\le r<m}\left\lceil\frac{nr}{m}\right\rceil f(r)\\
&=nf(m-1)+\sum_{0\le r<m}\left\lceil\frac{nr}{m}\right\rceil f(r-1)-\sum_{0\le r<m}\left\lceil\frac{nr}{m}\right\rceil f(r)\\
&=nf(m-1)+\sum_{0\le r<m}\left\lceil\frac{nr}{m}\right\rceil(f(r-1)-f(r))
\end{aligned}$$

as we needed to show. □

Proposition. $\sum_{0\le j<n}\binom{\lfloor mj/n\rfloor+1}{k}+\sum_{0\le j<m}\left\lceil\frac{jn}{m}\right\rceil\binom{j}{k-1}=n\binom{m}{k}$ *for any function* f *and positive integers* k, m, *and* n.

Proof. Let f be any function and k, m, and n arbitrary positive integers. We must show that

$$\sum_{0\le j<n}\binom{\lfloor mj/n\rfloor+1}{k}+\sum_{0\le j<m}\left\lceil\frac{jn}{m}\right\rceil\binom{j}{k-1}=n\binom{m}{k}.$$

But by the preceding proposition for

$$f(x)=\binom{x+1}{k}$$

we have that

$$\sum_{0\le j<n}\binom{\lfloor mj/n\rfloor+1}{k}=n\binom{m}{k}+\sum_{0\le r<m}\left\lceil\frac{rn}{m}\right\rceil\left(\binom{r}{k}-\binom{r+1}{k}\right);$$

and

$$\binom{r+1}{k}=\binom{r}{k}+\binom{r}{k-1}\quad\Longleftrightarrow\quad\binom{r}{k}-\binom{r+1}{k}=-\binom{r}{k-1};$$

so

$$\begin{aligned}\sum_{0\le j<n}\binom{\lfloor mj/n\rfloor+1}{k}&=n\binom{m}{k}+\sum_{0\le r<m}\left\lceil\frac{rn}{m}\right\rceil\left(\binom{r}{k}-\binom{r+1}{k}\right)\\&=n\binom{m}{k}-\sum_{0\le r<m}\left\lceil\frac{rn}{m}\right\rceil\binom{r}{k-1}\\&=n\binom{m}{k}-\sum_{0\le j<m}\left\lceil\frac{jn}{m}\right\rceil\binom{j}{k-1}.\end{aligned}$$

Hence

$$\sum_{0\le j<n}\binom{\lfloor mj/n\rfloor+1}{k}+\sum_{0\le j<m}\left\lceil\frac{jn}{m}\right\rceil\binom{j}{k-1}=n\binom{m}{k}$$

as we needed to show. □

46. [*M29*] (*General reciprocity law.*) Extend the formula of exercise 45 to obtain an expression for $\sum_{0\le j<\alpha n}f(\lfloor mj/n\rfloor)$, where α is *any* positive real number.

For any positive real number α, since by the first proposition of exercise 45

$$\left\lfloor\frac{mj}{n}\right\rfloor=r\quad\Longleftrightarrow\quad\left\lceil\frac{rn}{m}\right\rceil\le j<\left\lceil\frac{(r+1)n}{m}\right\rceil,$$

we have

$$\begin{aligned}
\sum_{0\le j<\alpha n} f\left(\left\lfloor\frac{mj}{n}\right\rfloor\right) &= \sum_{0\le r<\alpha m}\ \sum_{\lceil\frac{rn}{m}\rceil\le j<\lceil\frac{(r+1)n}{m}\rceil} f\left(\left\lfloor\frac{mj}{n}\right\rfloor\right)\\
&= \sum_{0\le r<\alpha m}\ \sum_{\lceil\frac{rn}{m}\rceil\le j<\lceil\frac{(r+1)n}{m}\rceil} f(r)\\
&= \sum_{0\le r<\alpha m}\left(\left\lceil\frac{(r+1)n}{m}\right\rceil-\left\lceil\frac{rn}{m}\right\rceil\right)f(r)\\
&= \sum_{0\le r<\alpha m}\left\lceil\frac{(r+1)n}{m}\right\rceil f(r)-\left\lceil\frac{rn}{m}\right\rceil f(r)\\
&= \sum_{0\le r<\alpha m}\left\lceil\frac{(r+1)n}{m}\right\rceil f(r)-\sum_{0\le r<\alpha m}\left\lceil\frac{rn}{m}\right\rceil f(r)\\
&= \sum_{1\le r<\alpha m+1}\left\lceil\frac{rn}{m}\right\rceil f(r-1)-\sum_{0\le r<\alpha m}\left\lceil\frac{rn}{m}\right\rceil f(r)\\
&= \lceil\frac{\alpha nm}{m}\rceil f(\lceil\alpha m\rceil-1)+\left\lceil\frac{(0)n}{m}\right\rceil f(0-1)+\sum_{1\le r<\alpha m}\left\lceil\frac{rn}{m}\right\rceil f(r-1)-\sum_{0\le r<\alpha m}\left\lceil\frac{rn}{m}\right\rceil f(r)\\
&= \lceil\alpha n\rceil f(\lceil\alpha m\rceil-1)+\sum_{0\le r<\alpha m}\left\lceil\frac{rn}{m}\right\rceil f(r-1)-\sum_{0\le r<\alpha m}\left\lceil\frac{rn}{m}\right\rceil f(r)\\
&= \lceil\alpha n\rceil f(\lceil\alpha m\rceil-1)+\sum_{0\le r<\alpha m}\left\lceil\frac{rn}{m}\right\rceil (f(r-1)-f(r)).
\end{aligned}$$

► **47.** [*M31*] When p is an odd prime number, the *Legendre symbol* $\left(\frac{q}{p}\right)$ is defined to be $+1$, 0, or -1, depending on whether $q^{(p-1)/2} \bmod p$ is 1, 0, or $p-1$. (Exercise 26 proves that these are the only possible values.)

a) Given that q is not a multiple of p, show that the numbers

$$(-1)^{\lfloor 2kq/p\rfloor}(2kq \bmod p), \qquad 0<k<p/2,$$

are congruent in some order to the numbers $2, 4, \ldots, p-1$ (modulo p). Hence $\left(\frac{q}{p}\right)=(-1)^\sigma$ where $\sigma=\sum_{0\le k<p/2}\lfloor 2kq/p\rfloor$.

b) Use the result of (a) to calculate $\left(\frac{2}{p}\right)$.

c) Given that q is odd, show that $\sum_{0\le k<p/2}\lfloor 2kq/p\rfloor \equiv \sum_{0\le k<p/2}\lfloor kq/p\rfloor$ (modulo 2) unless q is a multiple of p. [*Hint:* Consider the quantity $\lfloor(p-1-2k)q/p\rfloor$.]

d) Use the general reciprocity formula of exercise 46 to obtain the *law of quadratic reciprocity*, $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{(p-1)(q-1)/4}$, given that p and q are distinct odd primes.

Answers to exercise 47 follow below.

(a) We may prove the congruence relation in order to deduce that $\left(\frac{q}{p}\right)=(-1)^{\sum_{0\le k<p/2}\lfloor 2kq/p\rfloor}$ if $p \not\perp q$, p an odd prime.

Proposition (A). $\prod_{0<k<p/2}(-1)^{\lfloor 2kq/p\rfloor}(2kq \bmod p) \equiv \prod_{0<k<p/2} 2k \pmod p$ *if* $p \not\perp q$, p *an odd prime.*

Proof. Let p and q be arbitrary integers such that $p \not\perp q$ and p an odd prime. We must show that

$$\prod_{0<k<p/2} (-1)^{\lfloor 2kq/p \rfloor} (2kq \bmod p) \equiv \prod_{0<k<p/2} 2k \pmod{p}.$$

Let k be an arbitrary integer such that $0 < k < p/2$. Then

$$2kq = p \left\lfloor \frac{2kq}{p} \right\rfloor + (2kq) \bmod p$$

or equivalently

$$(2kq \bmod p) \equiv 2kq \pmod{p}.$$

Since $p \not\perp q$, $q \equiv 1 \pmod{p}$, and so

$$(2kq \bmod p) \equiv 2k \pmod{p}.$$

Also, in the case that $\left\lfloor \frac{2kq}{p} \right\rfloor$ is even, then so is $2kq \bmod p$, and

$$\begin{aligned} &(-1)^{\lfloor 2kq/p \rfloor} (2kq \bmod p) \equiv 2kq \bmod p \pmod{p} \\ \implies \quad &(-1)^{\lfloor 2kq/p \rfloor} (2kq \bmod p) \equiv 2kq \pmod{p}; \end{aligned}$$

in the case that $\left\lfloor \frac{2kq}{p} \right\rfloor$ is odd, then so is $2kq \bmod p$ since p is an odd prime, and

$$\begin{aligned} &(-1)^{\lfloor 2kq/p \rfloor} (2kq \bmod p) \equiv 2kq - p \pmod{p} \\ \implies \quad &(-1)^{\lfloor 2kq/p \rfloor} (2kq \bmod p) \equiv 2kq \pmod{p}; \end{aligned}$$

and in either case

$$(-1)^{\lfloor 2kq/p \rfloor} (2kq \bmod p) \equiv 2k \pmod{p}.$$

Hence,

$$\prod_{0<k<p/2} (-1)^{\lfloor 2kq/p \rfloor} (2kq \bmod p) \equiv \prod_{0<k<p/2} 2k \pmod{p}$$

as we needed to show.

□

(b) In order to calculate $\left(\frac{2}{p}\right)$, we let $q = 2$ and p be an odd prime. Then

$$\left(\frac{2}{p}\right) = (-1)^{\sum_{0 \le k < p/2} \lfloor 4k/p \rfloor}$$

has solutions for $p = 4n + 1$ or $4n + 3$ for some integer n; in particular, $(-1, 1, 1, -1)$ for $p \equiv (1, 3, 5, 7) \pmod{8}$, respectively; or expressed as the formula

$$\left(\frac{2}{p}\right) = (-1)^{\lfloor \frac{p+2}{4} \rfloor}.$$

(c) We may show the relation.

Proposition (C)**.** $\sum_{0\le k<p/2}\lfloor 2kq/p\rfloor \equiv \sum_{0\le k<p/2}\lfloor kq/p\rfloor \pmod 2$ *if* q *odd and* $p \not\perp q$*.*

Proof. Let p and q be arbitrary integers such that p is an odd prime, $p \not\perp q$, and q odd. We must show that

$$\sum_{0\le k<p/2}\lfloor 2kq/p\rfloor \equiv \sum_{0\le k<p/2}\lfloor kq/p\rfloor. \pmod 2$$

But

$$\begin{aligned}
\sum_{0\le k<p/2}\lfloor 2kq/p\rfloor &= \sum_{0\le k<p/4}\lfloor 2kq/p\rfloor + \sum_{p/4\le k<p/2}\lfloor 2kq/p\rfloor \\
&= \sum_{0\le k<p/4}\lfloor 2kq/p\rfloor + \sum_{-1/2<k\le(p-2)/4}\lfloor 2(\frac{p-1}{2}-k)q/p\rfloor \\
&= \sum_{0\le k<p/4}\lfloor 2kq/p\rfloor + \sum_{0\le k<p/4}\lfloor 2(\frac{p-1}{2}-k)q/p\rfloor \\
&= \sum_{0\le k<p/4}\lfloor 2kq/p\rfloor + \sum_{0\le k<p/4}\lfloor (p-1-2k)q/p\rfloor \\
&= \sum_{0\le k<p/4}\lfloor 2kq/p\rfloor + \sum_{0\le k<p/4} q-\lceil (2k+1)q/p\rceil \\
&= \sum_{0\le k<p/4}\lfloor 2kq/p\rfloor + \sum_{0\le k<p/4} q-1-\lfloor (2k+1)q/p\rfloor.
\end{aligned}$$

Then, since $p \not\perp q$ and q odd

$$\begin{aligned}
\sum_{0\le k<p/2}\lfloor 2kq/p\rfloor &\equiv \sum_{0\le k<p/4}\lfloor 2kq/p\rfloor + \sum_{0\le k<p/4} q-1-\lfloor (2k+1)q/p\rfloor \\
&\equiv \sum_{0\le k<p/4}\lfloor 2kq/p\rfloor + \sum_{0\le k<p/4}\lfloor (2k+1)q/p\rfloor \\
&\equiv \sum_{0\le k<p/2}\lfloor kq/p\rfloor \pmod 2
\end{aligned}$$

as we needed to show. □

(d) We may use the general reciprocity formula of exercise 46 to obtain the *law of quadratic reciprocity.*

Proposition (D)**.** $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}$ *if* p *and* q *are distinct odd primes.*

Proof. Let p and q be arbitrary integers such that p and q are distinct odd primes. We must show that

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}.$$

From exercise 46

$$\begin{aligned}\sum_{0\le k<p/2}\left\lfloor\frac{kq}{p}\right\rfloor &= \lceil p/2\rceil(\lceil q/2\rceil-1)+\sum_{0\le r<q/2}\left\lceil\frac{pr}{q}\right\rceil((r-1)-r)\\ &= \frac{(p+1)(q-1)}{4}-\sum_{0\le r<q/2}\left\lceil\frac{pr}{q}\right\rceil\\ &= \frac{(p+1)(q-1)}{4}-\frac{q-1}{2}-\sum_{0\le r<q/2}\left\lfloor\frac{pr}{q}\right\rfloor\\ &= \frac{(p-1)(q-1)}{4}-\sum_{0\le r<q/2}\left\lfloor\frac{pr}{q}\right\rfloor.\end{aligned}$$

Then, since

$$\begin{aligned}\sum_{0\le k<p/2}\left\lfloor\frac{2kq}{p}\right\rfloor+\sum_{0\le k<q/2}\left\lfloor\frac{2kp}{q}\right\rfloor &\equiv \sum_{0\le k<p/2}\left\lfloor\frac{kq}{p}\right\rfloor+\sum_{0\le k<q/2}\left\lfloor\frac{kp}{q}\right\rfloor\\ &\equiv \frac{(p-1)(q-1)}{4}\pmod 2\end{aligned}$$

we have

$$\begin{aligned}\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) &= (-1)^{\sum_{0\le k<p/2}\lfloor 2kq/p\rfloor+\sum_{0\le k<q/2}\lfloor 2kp/q\rfloor}\\ &= (-1)^{(p-1)(q-1)/4}\end{aligned}$$

as we needed to show. □

... The idea of this proof goes back to G. Eisenstein, *Crelle* **28** (1844), 246–248; Eisenstein also gave several other proofs of this and other reciprocity laws in the same volume.

48. [*M26*] Prove or disprove the following identities, for integers m and n:

$$\text{(a)}\quad\left\lfloor\frac{m+n-1}{n}\right\rfloor=\left\lceil\frac{m}{n}\right\rceil;\qquad\text{(b)}\quad\left\lfloor\frac{n+2-\lfloor n/25\rfloor}{3}\right\rfloor=\left\lfloor\frac{8n+24}{25}\right\rfloor.$$

Some but not all of the identities may be proven.

(a) The identity

$$\left\lfloor\frac{m+n-1}{n}\right\rfloor=\left\lceil\frac{m}{n}\right\rceil$$

may be disproven by counterexample. Let $m = 0$ and $n = -1$. Then

$$\begin{aligned}\left\lfloor \frac{m+n-1}{n} \right\rfloor &= \left\lfloor \frac{0+-1-1}{-1} \right\rfloor \\ &= \left\lfloor \frac{-2}{-1} \right\rfloor \\ &= \lfloor 2 \rfloor \\ &= \lfloor 2 \rfloor \\ &= 2 \\ &\neq 0 \\ &= \lceil 0 \rceil \\ &= \left\lceil \frac{0}{-1} \right\rceil \\ &= \left\lceil \frac{m}{n} \right\rceil .\end{aligned}$$

Note, however, that we may prove the identity in the case that $n > 0$.

Proposition (A)**.** $\left\lfloor \frac{m+n-1}{n} \right\rfloor = \left\lceil \frac{m}{n} \right\rceil$ *if* $n > 0$.

Proof. Let m and n be arbitrary integers such that $n > 0$. We must show that

$$\left\lfloor \frac{m+n-1}{n} \right\rfloor = \left\lceil \frac{m}{n} \right\rceil .$$

But since $n > 0$ implies $\frac{n-1}{n} < 1$,

$$\begin{aligned}f(x) = c(x) - 1 \left\lfloor \frac{m+n-1}{n} \right\rfloor &= \left\lfloor \frac{m}{n} + \frac{n-1}{n} \right\rfloor \\ &= \left\lceil \frac{m}{n} \right\rceil\end{aligned}$$

as we needed to show. □

(b) The second identity may be proven.

Proposition (B)**.** $\left\lfloor \frac{n+2-\lfloor n/25 \rfloor}{3} \right\rfloor = \left\lfloor \frac{8n+24}{25} \right\rfloor$.

Proof. Let n be an arbitrary integer. We must show that

$$\left\lfloor \frac{n+2-\lfloor n/25 \rfloor}{3} \right\rfloor = \left\lfloor \frac{8n+24}{25} \right\rfloor .$$

But

$$\begin{aligned}\left\lfloor \frac{n+2-\lfloor n/25 \rfloor}{3} \right\rfloor &= \left\lceil \frac{n-\lfloor n/25 \rfloor}{3} \right\rceil \\ &= \left\lceil \frac{n+\lceil -n/25 \rceil}{3} \right\rceil \\ &= \left\lceil \frac{\lceil 24n/25 \rceil}{3} \right\rceil \\ &= \left\lceil \frac{8n}{25} \right\rceil \\ &= \left\lceil \frac{8n+24}{25} \right\rceil\end{aligned}$$

as we needed to show. □

49. [*M30*] Suppose the integer-valued function $f(x)$ satisfies the two simple laws (i) $f(x+1) = f(x)+1$; (ii) $f(x) = f(f(nx)/n)$ for all positive integers n. Prove that either $f(x) = \lfloor x \rfloor$ for all rational x, or $f(x) = \lceil x \rceil$ for all rational x.

We may prove the result.

Proposition. *If an integer-valued function $f(x)$ satisfies $f(x+1) = f(x)+1$ and $f(x) = f(f(nx)/n)$ for all positive integers n, either $(\forall x \in \mathbb{Q})\,(f(x) = \lfloor x \rfloor)$ or $(\forall x \in \mathbb{Q})\,(f(x) = \lceil x \rceil)$.*

Proof. Let f be an integer-valued function such that

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

and

$$f(x) = f(f(nx)/n).$$

We must show that either

$$(\forall x \in \mathbb{Q})\,(f(x) = \lfloor x \rfloor)$$

or

$$(\forall x \in \mathbb{Q}\,(f(x) = \lceil x \rceil)\,.$$

First, we consider the domain of integers. From

$$f(0) = f(f((1)0)/1) = f(f(0))$$

we may deduce that $f(0) = 0$. Then, from the inductive hypotheses $f(k) = k$ and $f(-k) = -k$ for an arbitrary integer $k \geq 0$, we are able to show that $f(k+1) = f(k)+1$ and $f(1-k) = f(-k)+1$ respectively, proving by mathematical induction that $f(n) = n$ for all integers n.

Second, we consider the domain of rationals. If $f\left(\frac{1}{2}\right) \leq 0$, we have

$$\begin{aligned}f\left(\frac{1}{2}\right) &= f\left(\frac{1}{1-2f(1/2)} f\left(\frac{1}{2}\left(1-2f(1/2)\right)\right)\right) \\ &= f\left(\frac{1}{1-2f(1/2)} f\left(\frac{1}{2}-f\left(\frac{1}{2}\right)\right)\right) \\ &= f\left(\frac{1}{1-2f(1/2)} f\left(f\left(\frac{1}{2}\right)-f\left(\frac{1}{2}\right)\right)\right) \\ &= f(0) \\ &= 0;\end{aligned}$$

also, if $f\left(\frac{1}{n-1}\right) = 0$, we have

$$\begin{aligned} f\left(\frac{1}{n-1}\right) &= f\left(\frac{1}{n} f\left(\frac{n}{n-1}\right)\right) \\ &= f\left(\frac{1}{n} f\left(1 + \frac{1}{n-1}\right)\right) \\ &= f\left(\frac{1}{n}\left(1 + f\left(\frac{1}{n-1}\right)\right)\right) \\ &= f\left(\frac{1}{n}\left(1+0\right)\right) \\ &= f\left(\frac{1}{n}\right) \\ &= 0; \end{aligned}$$

and furthermore, if $1 \leq m < n$, by induction on m and since $m\lceil n/m \rceil - n \leq 0$,

$$\begin{aligned} f\left(\frac{m}{n}\right) &= f\left(\frac{1}{\lceil n/m \rceil} f\left(\frac{\lceil n/m \rceil m}{n}\right)\right) \\ &= f\left(\frac{1}{\lceil n/m \rceil} f\left(\frac{\lceil n/m \rceil m + n - n}{n}\right)\right) \\ &= f\left(\frac{1}{\lceil n/m \rceil} f\left(\frac{\lceil n/m \rceil m + n - nm/m}{n}\right)\right) \\ &= f\left(\frac{1}{\lceil n/m \rceil} f\left(\frac{n + m\left(\lceil n/m \rceil - n/m\right)}{n}\right)\right) \\ &= f\left(\frac{1}{\lceil n/m \rceil} f\left(1 + \frac{m}{n}\left(\left\lceil \frac{n}{m} \right\rceil - \frac{n}{m}\right)\right)\right) \\ &= f\left(\frac{1}{\lceil n/m \rceil}\left(1 + f\left(\frac{m}{n}\left(\left\lceil \frac{n}{m} \right\rceil - \frac{n}{m}\right)\right)\right)\right) \\ &= f\left(\frac{1}{\lceil n/m \rceil}\left(1 + f\left(\frac{1}{n}\left(m\lceil n/m \rceil - n\right)\right)\right)\right) \\ &= f\left(\frac{1}{\lceil n/m \rceil}\left(1+0\right)\right) \\ &= f\left(\frac{1}{\lceil n/m \rceil}\right) \\ &= 0. \end{aligned}$$

Therefore, in the case that $f\left(\frac{1}{2}\right) \leq 0$, $(\forall x \in \mathbb{Q})\,(f(x) = \lfloor x \rfloor)$.

On the other hand, in the case that $f\left(\frac{1}{2}\right) > 0$, we may define $f'(x) = -f(-x)$ so that

$f'(x+1) = f'(x) + 1$ and $f'(x) = f'(f'(nx)/n)$, and

$$\begin{aligned} f'\left(\frac{1}{2}\right) &= f'\left(\frac{1}{2}\right) - 1 + 1 \\ &= f'\left(\frac{1}{2} - 1\right) + 1 \\ &= -f\left(\frac{-1}{2} + 1\right) + 1 \\ &= 1 - f\left(\frac{1}{2}\right) \\ &\leq 0. \end{aligned}$$

Therefore, $f'(x) = -f(-x) = -\lfloor -x \rfloor = \lceil x \rceil$; that is, in the case that $f\left(\frac{1}{2}\right) > 0$, $(\forall x \in \mathbb{Q})\,(f'(x) = \lceil x \rceil)$.

Hence, either $(\forall x \in \mathbb{Q})\,(f(x) = \lfloor x \rfloor)$ or $(\forall x \in \mathbb{Q})\,(f'(x) = \lceil x \rceil)$, as we needed to show. □

[P. Eisele and K. P. Hadeler, *AMM* **97** (1990), 475–477.]

[G. Hamel, *Math. Annalen* **60** (1905), 459–462.]