(*February 11, 2024*)

Mapping subrings of $\mathbb{Q}$ to $\mathbb{Z}/N$?

Paul Garrett garrett@umn.edu https://www-users.cse.umn.edu/~garrett/

MathStackExchange question 4858256 asked why/whether something like

$$\frac{1}{3} - \frac{1}{4} = \frac{1}{12} \qquad \text{(in } \mathbb{Q}\text{)}$$

implies

$$3^{-1} - 4^{-1} = 12^{-1} \qquad \text{(in } \mathbb{Z}/17\text{)}$$

The equality of rational numbers is certainly a compelling heuristic for the corresponding equality mod 17. But, at an elementary level, that is not a proof. Yes, the same sort of argument

$$\frac{1}{3} - \frac{1}{4} = \frac{4}{12} - \frac{3}{12} = \frac{4-3}{12} = \frac{1}{12}$$

where "putting everything over a common denominator" is multiplying through by 12, immediately gives a proof of the mod-17 assertion:

$$3^{-1} - 4^{-1} = 12^{-1} \cdot (4-3) = 12^{-1} \bmod 17$$

But the identity in $\mathbb{Q}$ does not immediately, literally imply the corresponding identity mod 17, at a completely elementary level. But, with slightly less elementary considerations about *localization*, the identity in $\mathbb{Q}$ really *does* immediately give the identity in $\mathbb{Z}/17$!

---

1. *Localization*

Let R be a commutative ring with 1, with no (proper) 0-divisors. For present purposes, a *multiplicative subset* S of R is a subset closed under multiplication, containing 1, and not containing 0. Since R has no 0-divisors, it imbeds in its field of fractions K, and the *localization* $S^{-1}R$ of R can be described in a simpler fashion than the general case, as a subring of K: unsurprisingly,

$$S^{-1}R = \{\frac{r}{s} : s \in S,\ r \in R\} \subset K$$

Analogously, for a (proper, non-zero) ideal I of R, the localization $S^{-1}I$ is

$$S^{-1}I = \{\frac{i}{s} : s \in S,\ i \in R\} \subset S^{-1}R$$

The latter is an *ideal* of $S^{-1}R$: it is an abelian group, because

$$\frac{i}{s} + \frac{i'}{s'} = \frac{s'i + si'}{ss'} \qquad \text{(and } s'i, si' \in I \text{ because } I \text{ is an ideal)}$$

and it is closed under multiplication by $S^{-1}R$:

$$\frac{r}{s} \cdot \frac{i}{s'} = \frac{ri}{ss'} \qquad \text{(and } ri \in I \text{ because } I \text{ is an ideal)}$$

There is a natural commutative diagram

$$\begin{array}{ccc} R & \longrightarrow & S^{-1}R \\ \downarrow & & \downarrow \\ R/I & \longrightarrow & S^{-1}R/S^{-1}I \end{array}$$

[1.1] Claim: When the image of S in R/I lies inside the units $(R/I)^\times$, the map $\varphi : R/I \longrightarrow S^{-1}R/S^{-1}I$ is an *isomorphism.*

Proof: *(of claim)* First, the injectivity. For $\varphi(r+I) = 0$, it must be that $r = i/s$ for some $i \in I$ and $s \in S$. In R, this is equivalent to $s \cdot r = i$. Since s is has an inverse t mod I, this is equivalent to $r = t \cdot i \in I$.

For surjectivity: given r/s, find $r' \in R$ such that $r/s - r \in S^{-1}I$. For an inverse t of s mod I,

$$\frac{r}{s} - t \cdot r \;=\; \frac{r - st \cdot r}{s} \;=\; \frac{r(1-st)}{s}$$

Since $1 - st \in I$, which is an ideal, that last expression is in $S^{-1}I$. ///

[1.2] Corollary: Under the previous condition on I and S, any identity in $S^{-1}R$ gives the corresponding identity in R/I.

Proof: Since $R/I \longrightarrow S^{-1}R/S^{-1}I$ is an isomorphism, there is a composite homomorphism

$$S^{-1}R \;\longrightarrow\; S^{-1}R/S^{-1}I \;\longrightarrow\; R/S$$

Any equality in $S^{-1}R$ maps forward to a corresponding equality in R/I. ///

[1.3] Corollary: Any algebraic identity in $\mathbb{Q}$ maps forward to the corresponding identity in $\mathbb{Z}/N$, for every N relatively prime to all the denominators of the fractions in that identity. ///

[1.4] Corollary: For b prime to N, the image of the rational number a/b in $\mathbb{Z}/N$ is $ab^{-1}\mathrm{mod}\; N$.

Proof: The point is about b^{-1}. The equation $b \cdot c = 1$ maps forward to the same equation mod N, so the image of the inverse of b in $\mathbb{Q}$ maps to the inverse of b in $\mathbb{Z}/N$. ///

[1.5] Corollary: The identity $\frac{1}{3} - \frac{1}{4} = \frac{1}{12}$ in $\mathbb{Q}$ implies $3^{-1} - 4^{-1} = 12^{-1}$ in $\mathbb{Z}/N$ for all N prime to $2, 3$. ///
