Jumbled up thoughts

Stefanus Koesno[1]

[1] Somewhere in California

San Jose, CA 95134 USA

(Dated: February 28, 2016)

Abstract

Stray thoughts of a stray man. This is a collection of things that I thought was fun to do and also things that I always come back to after forgetting it :) There's no order or structure here just whatever my mind facies at the moment.

The second book on number theory that I use is ntb v2 by Victor Shoup, I'm reading it concurrently with William Stein's ent.pdf.

Theorem 1.5. He said that by "Applying Theorem 1.4 with $a - \lceil x \rceil$ in place of a we obtain"

Theorem 1.4 is the statement that for $a, b \in \mathbb{Z}$, $a = bq + r$. Although it is somewhat obvious there are a few things to consider.

First the range of x is $[x, x + b)$, here b is not included because otherwise we will have too many integers in the range. This only happens if x coincides with an integer, *e.g.* $x = 1$, $b = 1$, if the range is $[x, x + b]$ then there will be two integers in the range, 1 and 2. By excluding $x + b$ we only have one integer in the range, which is $x = 1$.

Second, substituting $a \to a - \lceil x \rceil$ is not so straightforward in practice, *e.g.* say we want $a = 5$, $b = 3$, and $x = 7$. What we want to calculate is then

$$\begin{aligned} 5 - 7 &= 3q + r \\ -2 &= 3q + r \\ -2 &= 3 \cdot 0 + -2 \\ 5 &= 3 \cdot 0 + 5 \end{aligned}$$

which is wrong since 5 is not between $[7, 7 + 5)$ Although merely substituting $a - \lceil x \rceil$ into a seems like a good idea at first, *i.e.*

$$\begin{aligned} a - \lceil x \rceil &= bq + r \\ a &= bq + (r + \lceil x \rceil) \end{aligned}$$

and also $0 \le r < b \to x \le r + \lceil x \rceil < x + b$ everything seems ok. However, the quotient q is $\lfloor a - \lceil x \rceil / b \rfloor$, *i.e.* the quotient of $a - \lceil x \rceil$ instead of a.

The right way to do it is

$$\begin{aligned} \lceil x \rceil &= bq' + r' \\ a - \lceil x \rceil &= bq + r \\ a &= bq + r + \lceil x \rceil \\ &= bq + r + bq' + r' \\ a &= b(q + q') + (r + r') \end{aligned}$$