Jumbled up thoughts

Stefanus Koesno[1]

[1] Somewhere in California
San Jose, CA 95134 USA

(Dated: March 21, 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, we need to take care some subtleties, *e.g.* say we want $a = 5$, $b = 3$, and $x = 7$. If we blindly calculate it

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

which is wrong since 5 is not between $[7, 7 + 3)$. Note that Theorem 1.4 is not the usual division statement. We might think that $-2/3 = 0$ (at least that's what you'll get using a computer when both numbers are integers since $|-2| < |3|$). However, Theorem 1.4 requires that the **remainder** be positive, also the quotient is defnied as $q = \lfloor a/b \rfloor \to \lfloor -2/3 \rfloor = -1$. Thus the right way is

$$\begin{aligned} -2 &= 3q + r \\ -2 &= 3(-1) + 1 \\ 5 &= 3(-1) + 8 \end{aligned}$$

which is correct since now 8 in in the range of $[7, 7 + 3)$.

Exercise 1.7. Show that Theorem 1.5 also holds for the interval $(x, x + b]$. Does it hold in general for the intervals $[x, x + b]$ or $(x, x + b)$?

The key here is the observation that $(x, x+b]$ contains b integers $\lfloor x \rfloor + 1, \lfloor x \rfloor + 2, \ldots, \lfloor x \rfloor + b$. Since there are b integers we can apply the same trick, applying Theorem 1.4 with $a - (\lfloor x \rfloor + 1)$ we obtain our goal.

The intervals $[x, x+b]$ or $(x, x+b)$ don't work because $[x, x+b]$ can contain $b+1$ integers and $(x, x+b)$ can contain $b-1$ integers, those happen when x itself is an integer. We need b integers in the range since r can contain b different values $0, 1, \ldots, b-1$.

Exercise 1.2. Let n be a composite integer. Show that there exists a prime p dividing n, with $p \leq n^{1/2}$.

First, we utilize the fundamental theorem that n must have prime factors. Next, we use contradiction. If all primes factors p_i of n are bigger than $n^{1/2}$ this means that every product $p_i p_j > n$ which is a contradiction. Thus there must be a factor p that is $\leq n^{1/2}$.

Theorem 1.6 This is one cool theorem, it also brings up the dillema on whether we need some intuitive understanding before attacking a problem or do we just blindly follows the mathematical consequence from one statement to another to get to where we want to go. I came from a physics background where you need to have (physical) intuitions on the theories you have, not just some mathematical tricks to get you somewhere (something that Feynman himself corroborated).

However, this approach might not be profitable in mathematics. The proof of this theorem just utilizes contradiction and some keen observation as always. Mechanically going from one deduction reasoning to another seems to be the fastest route for this particular problem. Note that the proof doesn't give us an intuition as to how we can compute it or what it is.

Note that the goal of is to massage any ideal into $d\mathbb{Z}$, *i.e.* d must be the smallest positive element $\in I$ that divides any element in I. So, in some sense, given any two elements $a, b \in I$, we can find another number d that divides both a and b. However, what we want is **not** the smallest number that divides a and b, that would be 1, we want the largest number d that divides a and b since that will be sufficient for $d\mathbb{Z}$ to contain both a and b or in other words since $as + bt \in I$ and $g \in I$ is a must

$$as + bt = g$$

where s, t are some integers and $g = \gcd(a, b)$. This statement more naturally flows as a consequence of the “ideal” formalism rather than its precedence since it is not immediately clear how we can systematically compute s and t, “idealism” is indeed a powerful tool.

To intuitively prove this theorem we can use Euclid’s gcd algorithm

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1 q_2 + r_2 \\ &\vdots \\ r_{n-1} &= r_n q + g \end{aligned}$$

Since $b \in I \to q_1 b \in I$ as well which means that $r_1 = a - q_1 b \in I$ which in turn means that r_2 is also $\in I$ and so on. Hence $g \in I$.

We now need to repeat the process, we calculate the pairwise gcd of all the positive numbers in I and then the pairwise gcd of all the gcd’s and so on. The smallest gcd of gcd of gcd of $\ldots$ of the numbers will be d since it obviously divides all elements of I.

The “astute reader” would have also noticed that we can use Euclid’s gcd algorithm to get s and t in $as + bt = g$ by simply keeping track the residue of each step

$$\begin{aligned} & a = bq_0 + r_0 \\ & a = r_0 q_1 + r_1, \quad r_0 = a - bq_0 \\ & a = r_1 q_2 + r_2, \quad r_1 = a - r_0 q_1 = a - (a - bq_0) q_1 \\ & \quad \vdots \\ & a = r_{n-1} q_n + g, \quad r_{n-1} = a - q_{n-1}(a - q_{n-1}(a - \ldots q_1(a - bq_0))) \end{aligned}$$

where $g \equiv \gcd(a, b)$, by substituting each r_i we will get the values for s and t. Let’s see an example

$$\begin{aligned} 7 &= 5 \cdot 1 + 2, \quad 2 = 7 - 5 \\ 7 &= 2 \cdot 3 + 1 = (7 - 5) \cdot 3 + 1 \\ \to 1 &= (-2)7 + (3)5 \end{aligned}$$

In conclusion, everytime you do the gcd calculation ala Euclid, you practically generate other elements in I (due to the closure property of an ideal) and because of that g is included as well, that’s the reasoning behind this theorem.

So which way reigns supreme? Do we need some sort of intuition of how things work or just heartlessly traverse through logical conclusions to get to our main goal? Intuition takes time to develop (although it gives you a deeper understanding) while mechanical derivation is faster, so ¯\(º_o)/¯

Exercise 1.8. Let I be a non-empty set of integers that is closed under addition (i.e., $a + b \in I$ for all $a, b \in I$). Show that I is an ideal if and only if $-a \in I$ for all $a \in I$.

If I is an ideal and $a \in I$ then $(-1)a = -a \in I, \ -1 \in \mathbb{Z}$ per the definition of an ideal.

Going the other direction requires more work. Since I is closed under addition this means that I is also closed under multiplication by a positive integer $za \in I, a \in I, z \in \mathbb{Z}, z > 0$. Since a multiplication is nothing but repeated additions

$$za = \underbrace{a + a + a + a + \cdots + a}_{z \text{ numbers of } a}$$

thus closed under addition means closed under positive multiplication. If for every $a \in I$, $-a \in I$ is also true this means that $-a + a = 0 \in I$ and I is closed under negative multiplication as

$$za = \underbrace{-a + -a + -a + -a + \cdots + -a}_{z \text{ numbers of } -a}$$

$z < 0$. Thus I is closed under $za \in I, z \in \mathbb{Z}$ and this completes the proof.

Exercise 1.9 (c). $\gcd(a, 0) = \gcd(a, a) = |a|$ and $\gcd(a, 1) = 1$

Using Theorem 1.8

$$\begin{aligned} as + 0 \cdot t &= \gcd(a, 0) \\ as &= \gcd(a, 0) \end{aligned}$$

Since gcd is the smallest of $|as + bt|$, the only solution above is $s = \pm 1$. Also

$$\begin{aligned} as + at &= \gcd(a, a) \\ a(s + t) &= \gcd(a, a) \end{aligned}$$

gcd is the smallest of $|a(s + t)|$, the only solution above is $s + t = \pm 1$.

Exercise 1.9 (d). $\gcd(ca, cb) = |c| \gcd(a, b)$

In ent.pdf a sick induction proof was employed, we can avoid it by using ideals. First $g \equiv \gcd(a,b)$, by Theorem 1.8 we have

$$\begin{aligned} as + bt &= g \\ c \times (as+bt) &= c \times g \\ (ca)s + (cb)t &= cg \end{aligned}$$

Thus $g' \equiv \gcd(ca, cb) | cg$. The question is now whether $g' < cg$ or $g' = cg$? Applying Theorem 1.8 to g'

$$\begin{aligned} cas' + cbt' &= g' \\ c(as' + bt') &= g' \end{aligned}$$

Thus $c|g' \rightarrow g' = ck$, now suppose $g' < cg$

$$\begin{aligned} \cancel{c}(as' + bt') &= \cancel{c}k \\ ck < cg &\rightarrow k < g \end{aligned}$$

which is a contradiction as g is the smallest $as + bt$ possible.

Exercise 1.10. Show that for all integers a, b with $d := \gcd(a,b) \neq 0$, we have $\gcd(a/d, b/d) = 1$.

Again, using Theorem 1.8

$$\begin{aligned} as + bt &= d \\ \frac{a}{d}s + \frac{b}{d}t &= 1 \end{aligned}$$

Exercise 1.11. Let n be an integer. Show that if a, b are relatively prime integers, each of which divides n, then ab divides n.

$a|n \rightarrow n = aa'$, $b|n \rightarrow n = bb'$, $aa' = bb'$ which means that $a|bb'$ but since $\gcd(a,b) = 1$ according to Theorem 1.9 $a|b' \rightarrow b' = am$. Thus $n = bb' = (ab)m \rightarrow ab|n$.

Exercise 1.14. Let p be a prime and k an integer, with $0 < k < p$. Show that the binomial coefficient

$$\binom{p}{k} = \frac{p!}{k!(p-k)!},$$

which is an integer (see §A2), is divisible by p.

I'm more interested in the fact that $\binom{p}{k}$ is an integer. If you check (§A2), you need two identities to prove this

$$\binom{p}{p} = \binom{p}{0} = 1$$

and **Pascal identity**

$$\binom{p}{k} = \binom{p-1}{k-1} + \binom{p-1}{k}$$

So the goal is to reduce $\binom{p}{k}$ into a sum of $\binom{p}{p}$ and $\binom{p}{0}$

$$\begin{aligned}
\binom{p}{k} &= \binom{p-1}{k-1} + \binom{p-1}{k} \\
&= \left\{\binom{p-2}{k-2} + \binom{p-2}{k-1}\right\} + \binom{p-1}{k} \\
&\vdots \\
&= \binom{p-k}{k-k} + \binom{p-k}{k-k+1} + \binom{p-k+1}{2} + \cdots + \binom{p-2}{k-1} + \binom{p-1}{k} \\
&= 1 + (p-k) + \binom{p-k+1}{2} + \cdots + \binom{p-2}{k-1} + \binom{p-1}{k}
\end{aligned}$$

So we substitute A at each step with a lower p and k, we now need to substitute each term again using Pascal identity, very laborious indeed but it does the job.

Note that for this particular problem p needs to be prime, otherwise it won't work, *e.g.* $\binom{18}{6} = 18564$ and $18 \nmid 18564$.

Exercise 1.17. Let a, b, c be positive integers satisfying $\gcd(a, b) = 1$ and $c \geq (a-1)(b-1)$. Show that there exist non-negative integers s, t such that $c = as + bt$.

$$\begin{aligned}
(a-1)(b-1) &= ab - a - b + 1 \\
&\to c > ab - a - b + 1 \\
(as + bt) + a + b &> ab + 1 \\
a(s+1) + b(t+1) &> ab + 1
\end{aligned}$$

$s \geq b, t \geq 0$ will do.

Theorem 2.4. This is a spin off of Theorem 1.4 and Theorem 1.5 as explained in the previous paragraph. Theorem 1.4 is $a = bq + r$ here $a = nq + z \to z = a - nq \to z = a + ny$

with $y = -q$. z plays the role of the remainder here and as such it can always be shifted to $[x, x + n)$ according to Theorem 1.5.

Exercise 2.7. Let $a, b, n \in \mathbb{Z}$ with $n > 0$ and $a \equiv b(\text{mod } n)$. Show that $\gcd(a, n) = \gcd(b, n)$.

We know that $a \equiv b(\text{mod } n)$ means $n|(a - b)$. Say $\gcd(a, n) = g_a$ and $\gcd(b, n) = g_b$ and $g_a \neq g_b$. Since $a - b = nn'$,

$$\begin{aligned} a &= b + nn' \\ &= g_b b' + (g_b n_b)n', \quad n = g_b n_b \\ &= g_b(b' + n_b n') \\ \rightarrow g_b &\mid a \end{aligned}$$

By the same token $g_a|b$. Denote $g_{ab} \equiv \text{lcm}(g_a, g_b)$. Since g_a, g_b both divide a, b, and n, $\gcd(a, n)$ and $\gcd(b, n)$ are $g_{ab} \neq g_a \neq g_b$ which is a contradiction. (g_{ab} can be equal to g_a but that requires $g_a = g_b$)

Exercise 2.9. Let e be a positive integer. For $a \in \{0, \ldots, 2^e - 1\}$, let $\tilde{a}$ denote the integer obtained by inverting the bits in the e-bit, binary representation of a (note that $\tilde{a} \in \{0, \ldots, 2^e - 1\}$). Show that $\tilde{a} + 1 \equiv -a(\text{mod } 2^e)$. This justfies the usual rule for computing negatives in 2's complement arithmetic (which is really just arithmetic modulo 2^e).

First thing to clarify, even though $\tilde{a} \in \{0, \ldots, 2^e - 1\}$ it doesn't mean that $\tilde{a}$ can take any value, *e.g.* say $e = 3$, $2^e - 1 = 7$ then if $a = 1(001)$ then $\tilde{a} = 6(110)$ otherwise $\tilde{a} + 1 \equiv -a(\text{mod } 2^e)$ doesn't hold.

We can rewrite $\tilde{a} + 1 \equiv -a(\text{mod } 2^e)$ as $\tilde{a} + a + 1 \equiv 0(\text{mod } 2^e)$ since $\tilde{a}$ is just the binary complement of a

$$\tilde{a} + a = \underbrace{111\ldots1}_{e \text{ number of ones}} = 2^e - 1$$

Thus

$$\begin{aligned} \tilde{a} + a + 1 &= 2^e - 1 + 1 \\ &= 2^e \\ &\equiv 0(\text{mod } 2^e) \end{aligned}$$

Exercise 2.10. Show that the equation $7y^3 + 2 = z^3$ has no solutions $y, z \in \mathbb{Z}$.

The LHS is $7y^3 + 2 \equiv 2 (\text{mod } 7)$ since $7y^3$ is a multiple of 7. This means that the RHS has to be $z^3 \equiv 2 (\text{mod } 7)$ as well. But there's no integer z' such that $z'^3 = 2$ thanks to Theorem 2.3. Since if there is then $z \equiv z' (\text{mod } 7) \rightarrow z^3 \equiv z'^3 (\text{mod } 7)$ meaning $z'^3 = 2$.

Except that that was a flawed argument in which I mixed up "if" and "if and only if". If $x = y' (\text{mod } n)$ then $x^3 = y'^3 (\text{mod } n)$ but not the other way round, *i.e.* $x = y' (\text{mod } n) \rightarrow \sqrt[3]{x} = \sqrt[3]{y'} (\text{mod } n)$ is WRONG!

The correct way to prove the above is to list the cube of all members of $\mathbb{Z}/7\mathbb{Z}$ except for 0, *i.e.*

$$\begin{array}{ll} 1^3 \equiv 1 (\text{mod } 7) & 2^3 \equiv 1 (\text{mod } 7) \\ 3^3 \equiv 6 (\text{mod } 7) & 4^3 \equiv 1 (\text{mod } 7) \\ 5^3 \equiv 6 (\text{mod } 7) & 6^3 \equiv 6 (\text{mod } 7) \end{array}$$

We don't see any $2 (\text{mod } 7)$, thus $x^3 = 2 (\text{mod } 7)$ has no solution. But wait, how about cube of numbers greater than 7? Well any number can be brought under 7 by $x \equiv y (\text{mod } 7)$, *e.g.* $17 \equiv 3 (\text{mod } 7)$ such that $17^3 \equiv 3^3 (\text{mod } 7) \equiv 6 (\text{mod } 7)$. Thus the above list is enough to proof that there is no x such that $x^3 \equiv 2 (\text{mod } 7)$.

Theorem 2.5 *(i)*. It's cool to see an alternative proof, he uses the alternative definition of gcd $as + bt = d$ and Theorem 1.8 to prove it.

Theorem 2.5 *(ii)*. This also relates to the statement on page 20 "The image of τ_a consists of the n/d integers $i \cdot d (i = 0, \dots, n/d - 1)$".

Remember that $\gcd(a, n) = d$, let's denote $n_d = n/d$, therefore

$$az = ny + r$$
$$(da')z = (dn_d)y + r$$

Therefore $d|r$

$$d(a'z) = d(n_d y) + dr'$$
$$\rightarrow a'z = n_d y + r'$$

Since $0 < r' < n_d$, there are only $n_d - 1$ different values of r' and therefore there are only $n_d - 1$ different values of $r = dr'$. This explains $i \cdot d (i = 0, \dots, n/d - 1)$.

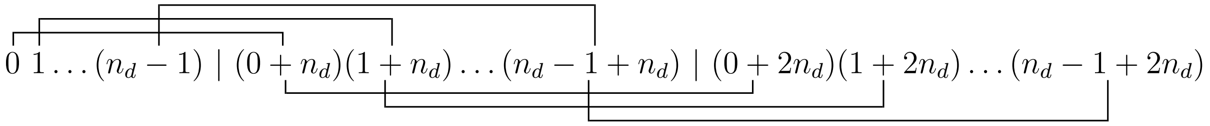
For the next statement "Moreover, every element b in the image of τ_a has precisely d pre-images $z_0 + j \cdot (n/d)(j = 0, \dots, d-1)$, where $z_0 \in \{0, ..., n/d - 1\}$". This is because

$$a'(z + n_d x) = n_d y + r'$$

i.e. shifting z by $n_d x$ doesn't change r' and therefore doesn't change $r = dr'$ either. So for each r there are a few z's related to it. How many? Well, we can rearrange the numbers $0, 1, \dots, n-1$ into groups of $n_d - 1$ clusters

$$\overbrace{\underbrace{0,\dots,n_d-1}_{n_d\text{ remainders}}\quad \underbrace{0+n_d,\dots,n_d-1+n_d}_{n_d\text{ remainders}}\quad \dots\quad \underbrace{0+(d-1)n_d,\dots,n_d-1+(d-1)n_d}_{n_d\text{ remainders}}}^{d\text{ repetitions of }n_d\text{ remainders}}$$

The preimages of z are shown below


$0\ 1 \dots (n_d - 1) \mid (0 + n_d)(1 + n_d) \dots (n_d - 1 + n_d) \mid (0 + 2n_d)(1 + 2n_d) \dots (n_d - 1 + 2n_d)$

i.e. $0, n_d, 2n_d, \dots, (d-1)n_d$ have the same remainder, ditto for $1, 1 + n_d, 1 + 2n_d, \dots, 2 + (d-1)n_d$ and so on.

Therefore there are d preimages for each z.