Math 313/623 Notes 7

David L. Meretzky

Tuesday March 26th, 2019

> We're gonna rock around the clock tonight
>
> Bill Haley

In these notes we will investigate some important arithmetic functions and the Möbius Inversion Formula.

Back to Gauss Section 2

Solutions of Congruences of the first degree

Article 26. In the case $(a, m) = 1$ we know that $ax + b \equiv c \pmod{m}$. Suppose that x_0 solves this congruence, that is $ax_0 + b \equiv c \pmod{m}$. It should follow from article 9 that if for any $x_1 \in \mathbb{Z}$ such that $x_1 \equiv x_0 \pmod{m}$, x_1 is also a solution to the congruence. Furthermore, if t is any other root of the congruence $ax + b \equiv c \pmod{m}$, then it must be congruent to x_0. Spelling it all out, if $(a, m) = 1$, then given any solution x_0, all solutions are given by the set $x_0 + m\mathbb{Z}$.

I will now say the same thing in about 5 different ways. Pick whichever way makes sense to you. This justifies why we say that the equation $ax + b \equiv c \pmod{m}$ only has a single root. It's "root" is the set of all numbers congruent to x_0 modulo m. More precisely, there is exactly one least residue of x_0 in the set $x_0 + m\mathbb{Z}$. More modernly, $x_0 + m\mathbb{Z}$ is a single element of $\mathbb{Z}/m\mathbb{Z}$, usually identitfied with the aforementioned least residue.

Note that these results do not hold if $(a, m) \neq 1$ or if the degree of the congruence is greater than 1, say $ax^2 + b \equiv c \pmod{m}$.

Proof. I wouldn't dare. □

Article 27. Gauss makes a delightful but somewhat hard to parse observation that if we want to solve a congruence of the form $ax + t \equiv u \pmod{b}$, where now $(a, b) = 1$, we only need to solve $ax \equiv \pm 1 \pmod{b}$. We can easily check that that if there is some solution r such that $ar \equiv \pm 1 \mod b$, then $\pm(u - t)r$ will be a solution to $ax + t \equiv u \pmod{b}$. That is,

$$a \pm (u - t)r + t \equiv (u - t) + t \equiv u \pmod{b}$$

since $ar \equiv \pm 1 \mod b$. Furthermore, we note by the definition of congruence that solving $ax \equiv \pm 1 \pmod{b}$ amounts to finding an $x, y \in mathbbZ$ such that

$ax + by = \pm 1$.

Here we outline the algorithm for actually finding a solution to such a congruence again given the condition on a. Note that the condition $(a, b) = 1$ is exactly enough to guarantee solutions $x, y \in \mathbb{Z}$. See the related discussion in Notes 2 definition 4: for fixed $(a, b) = 1$, the set of all possible linear combinations $\{ax + by | x, y \in \mathbb{Z}\} = (a, b) = (1) = \mathbb{Z}$ where the parentheses now denote ideals.

Start with $(a, b) = 1$ How do we find the associated x and y such that $ax + by = 1$? Apply Lemma 2 of Notes 2. Without loss of generality say that $a > b$. Then there exist unique q_0, $0 < r_0 < b$ such that $a = bq_0 + r_0$. Note that $(a, b) = (b, r_0) = 1$, that is, $0 < r_0 < b$ guarantees that b and r_0 are relatively prime. Moreover, suppose there were x_0,y_0 such that $x_0r_0 + y_0b = 1$, then since $r_0 = a - bq_0$, we have

$$\begin{aligned} x_0r_0 + y_0b =& x_0(a - bq_0) + y_0b \\ =& x_0a + (y_0 - q_0)b \\ =& 1 \end{aligned}$$

which gives us our initial x and y as $x = x_0$, $y = (y_0 - q_0)$.

We are not finished however, this relies upon the assumption that we know how to solve $x_0r_0 + y_0b = 1$. Use the same process on this equation to obtain x_0 and y_0 in terms of some x_1 and y_1. Again, begin by dividing b by r_0.

This method must terminate eventually when some $r_n = 1$ at which point it becomes easy to find the x_n and y_n coefficents. This is called the Euclidean Algorithm.

We skip article 28.

Article 29. Now we investigate $ax + t \equiv u \pmod{m}$ the case where a, the coefficient on the unknown, is not relatively prime to the modulus m. Suppose $(a, m) = \delta > 1$. By article 5, if x satisfies the congruence relative to the modulus m, then it certainly satisfies the congruence relative to the modulus δ. However, $ax \equiv 0 \pmod{\delta}$ since $\delta | a$. Thus $t \equiv u \pmod{\delta}$ is the only case where the congruence has a solution. In this case, $\delta | t - u$. Thus applying article 22, we obtain

$$(a/\delta)x \equiv (u - t)/\delta \pmod{m/\delta}$$

since a/δ and m/δ are relatively prime we can use the machinery of the previous articles to solve this case now, i.e. the coefficient of x and the modulus are relatively prime.

In the rest of section 2 Gauss proves the chinese remainder theorem and then uses this to give the simpler proof of Notes 6. Proposition 8 which is contained in the exercises of notes 6.

Exercises