# Math 313/623 Notes 1

David L. Meretzky

Tuesday January 29, 2019

> Integral numbers are the
> fountainhead of all mathematics.
>
> *Minkowski, H.*

Gauss once said "Mathematics is the queen of the sciences and number-theory the queen of mathematics." If this be true we may add that the Disquisitiones is the Magna Charta of number-theory. The advantage which science gained by Gauss' long-lingering method of publication is this: What he put into print is as true and important today as when first published; his publications are statutes, superior to other human statutes in this, that nowhere and never has a single error been detected in them. This justifies and makes intelligible the pride with which Gauss said in the evening of his life of the first larger work of his youth: "The Disquisitiones arithmeticae belong to history."

— Cantor, M.

The following is copied from an english translation of Gauss's 1798 masterpiece *Disquisitiones Arithmeticae*. Unless otherwise specified, by numbers we mean integers, that is whole numbers both positive and negative. The integers will be denoted $\mathbb{Z}$.

# 1 Congruent Numbers in General

## 1.1 Congruent numbers, moduli, residues, and nonresidues

Let $a$ and $c$ be integers. If there exists an integer $b$ such that $ab = c$ we say that $a$ divides $c$ and write $a|c$.

**Article 1.** Let $a$, $b$, and $m$ be integers. If $m$ divides $a - b$, then we say that $a$ and $b$ are *congruent relative to* $m$ or *congruent modulo* $m$ or *congruent mod* $m$. We call $m$ the *modulus*. If $a$ and $b$ are congruent, each is called a *residue* of the other. If they are noncongruent, they are called nonresidues.

For instance, $-9$ and 16 are congruent relative to 5.
Furthermore, $-7$ is a residue of both 4 and 15 relative to 11.
We can see that, $-7$ is a nonresidue of both 4 and 15 relative to the modulus 3.
Since every number divides 0, every number is congruent to itself relative to any modulus.
For example, $5|(11 - 11)$ thus 11 is congruent to itself modulo 5.

**Article 2.** Given a number $a$, and a modulus $m$, its residues are exactly the set $\{a + km : k \in \mathbb{Z}\}$.

*Proof.* Suppose $b \in \{a + km : k \in \mathbb{Z}\}$, then for some $k$, $b = a + km$. Therefore, $km = b - a$ and consequently, $m|(b - a)$. Therefore $b$ is a residue of $a$ mod $m$. To prove the reverse implication, that any residue of $a$ modulo $m$ must be contained in the set $\{a + km : k \in \mathbb{Z}\}$, reverse the argument. □

We will denote "$a$ is congruent to $b$ modulo $m$" as $a \equiv b \pmod{m}$. We will denote the set $\{a + km : k \in \mathbb{Z}\}$ by $a + m\mathbb{Z}$.

**Article 3.** Given an integer $A$, and a list of $m$ integers, $a$, $a + 1$, $a + 2$, ..., $a + m - 1$, prove that only one of the list of $m$ integers is congruent to $A$ mod $m$.

For example, given any number $A$, $A$ is only congruent to one of 7, 8, 9 modulo 3. Let $A = 17$, one can check that $17 \not\equiv 7 \pmod{3}$, $16 \equiv 8 \pmod{3}$, $16 \not\equiv 9 \pmod{3}$. We have $\frac{7-17}{3} = -3 - \frac{1}{3}$, $\frac{8-17}{3} = -3$, $\frac{9-17}{3} = -2 - \frac{2}{3}$. Thus, $8 = 17 - 3(3) \in \{17 + k(3)|k \in \mathbb{Z}\}$.

*Proof.* If $\frac{a-A}{m}$ is an integer, then $a \equiv A \pmod{m}$ and let $k = \frac{a-A}{m}$. Otherwise, if $\frac{a-A}{m}$ is a positive fraction, let $k$ be the next largest integer. These two cases give us the less than or equal sign in the below expression,

$$0 < \frac{a - A}{m} \leq k < \frac{a - A}{m} + 1 \tag{1}$$

From which it follows that

$$a \leq A + km < a + m$$

and $A + km$ will be the desired number which is congruent to $A$.

To show that there is only one number in the list $a$, $a + 1$, $a + 2$, ..., $a + m - 1$, which is congruent to $A$, note that, only one of the list $\frac{a-A}{m}$, $\frac{a+1-A}{m}$, $\frac{a+2-A}{m}$, etc. can be a whole number because (by equation 1) they all lie between $\frac{a-A}{m}$ and $\frac{a-A}{m} + 1$ and therefore since $k - 1 < \frac{a-A}{m}$ and $\frac{a-A}{m} + 1 < k + 1$, they all lie between $k - 1$ and $k + 1$, and since they are all different, only one of them can equal the whole number $k$.

In the case that $\frac{a-A}{m}$ is a negative fraction, we can still let $k$ be the next largest integer, note $-3$ is larger than $-3 - \frac{1}{2}$. □

The result above should be obvious even if the argument is tricky in places. We retrace the proof in the context of the example of $A = 17$, $a = 7$, and $m = 3$.

Note that since $\frac{a-A}{m} = \frac{7-17}{3} = -3 - \frac{1}{3}$ is a negative fraction in this case, let $k$ be the next largest integer, $k = -3$. Equation (1) then becomes

$$\frac{7 - 17}{3} \leq k = -3 < \frac{7 - 17}{3} + 1 < 0$$

Thus at least one of either 7, 8, or 9 will be equal to $17 - 3(3)$ and hence congruent to 17 modulo 3.

To show that at most one of the three numbers has this property we note that $\frac{7-17}{3}$, $\frac{7+1-17}{3}$, and $\frac{7+2-17}{3}$ lie between $\frac{7-17}{3}$ and $\frac{7-17}{3}+1$, and therefore, between $k-1=-4$ and $k+1=-2$. Therefore, only one of $\frac{7-17}{3}$, $\frac{7+1-17}{3}$, and $\frac{7+2-17}{3}$ can be a whole number, $-3$.

We obtain the next article as a corollary, and with it, a definition.

## 1.2 Least Residues

**Article 4.** Let $A$ be a number and $m$ a modulus, $A$ will be congruent to exactly one of 0, 1, 2, ... $m-1$ modulo $m$. Furthermore, $A$ will be congruent to exactly one of $-(m-1)$, $-(m-2)$,...,$-2$, $-1$, 0 modulo $m$. We call these two unique numbers the least positive residue and the greatest negative residue respectively.

Note that Gauss's terminology here is slightly different.

*Proof.* Examine the case $a=0$ and $a=-(m-1)$ in the previous article. □

For example, the positive least residue of $-13$ relative to the modulus 5 is 2. Write out some elements of the set $\{-13+k(5) : k \in \mathbb{Z}\}$. What is the greatest negative residue?

Note that in the case $a=0$, the set $\{a+km : k \in \mathbb{Z}\}$ is denoted simply $m\mathbb{Z}$. Denote the set of least positive residues mod $m$, $\{0,1,2,....,(m-1)\}$, by $\mathbb{Z}/m\mathbb{Z}$.

## 1.3 Elementary propositions regarding congruences

**Article 5.** Here are two elementary propositions.

1. If $a$ and $b$ are congruent relative to a composite[1] modulus, then they are congruent relative to any divisor of the modulus. Said another way, if $a \equiv b \pmod{m}$ where $m=kl$, then $a \equiv b \pmod{k}$.
2. Congruence is an equivalence relation.

The proofs are left as exercises.

**Article 6.** If $A \equiv a$, $B \equiv b$, $C \equiv c$ and so on, relative to some modulus, then $A+B+C+... \equiv a+b+c....$ Also $A-B \equiv a-b$.

The proof is left as an exercise.

**Article 7.** If $A \equiv a$, then $kA \equiv ka$.

[1] neither 1 nor a prime

*Proof.* While this can be proven directly, note that if $k$ is a positive integer, then this is a special case of the preceding article. If $k$ is negative then $-k$ is positive and so $-kA \equiv -ka$ which then implies $kA \equiv ka$. □

If $A \equiv a$ and $B \equiv b$, then $AB \equiv ab$ because $AB \equiv Ab \equiv ab$ by the previous article and by transitivity in article 5 part 2.

**Article 8.** Given numbers $A$, $B$, $C$, etc. and other numbers $a$, $b$, $c$, etc. which are congruent to them, the products $ABC$ etc. $\equiv abc$ etc.

*Proof.* From the preceding article it follows that $AB \equiv ab$. For the same reason $ABC \equiv abc$ and so forth. □

It follows that if $A \equiv a$ and $k$ is a positive integer then $A^k \equiv a^k$.

**Article 9.** Let $X$ be an algebraic function in indeterminate $x$, of the form

$$X(x) = Ax^a + Bx^b + Cx^c + ...$$

where $A$, $B$, $C$, etc. are any integers and $a$, $b$, $c$, etc. are nonnegative integers. Then if $x \equiv y \pmod{m}$ then $X(x) \equiv X(y) \pmod{m}$ for any modulus $m$.

*Proof.* Fix a modulus $m$, let $x \equiv y$. Then by the preceding articles, $x^a \equiv y^a$ and $Ax^a \equiv Ay^a$ and $Ax^a + Bx^b + .. \equiv Ay^a + By^b + ...$ □

As an exercise, come up with a similar theorem for functions of several variables.

We call the collection of all polynomials in indeterminate $x$ with integer coefficients $\mathbb{Z}[x]$.

**Article 10.** If all integers are substituted consecutively for $x$ in an algebraic equation, and the corresponding values of the function, $X(1)$, $X(2)$, ... are reduced by some modulus $m$ to their least positive residue, they will form a sequence which will repeat every $m$ terms.

*Proof.* Let $0 \leq a < m$. Then $\{a + km : k \in \mathbb{Z}\}$ are all congruent modulo $m$, and therfore, $\{X(a + km) : k \in \mathbb{Z}\}$ are all congruent modulo $m$. □

Find the sequence for $X(x) = x^3 - 8x + 6$ with $m = 5$. Check that 0 and 2 do not appear in this sequence.

**Article 11.** Since no $x$ makes $X(x) \equiv 0 \pmod{5}$, conclude that $x^3 - 8x + 6 = 0$ has no integer solutions.[2] Since no $x$ makes $X(x) \equiv 2 \pmod{5}$, conclude that $x^3 - 8x + 6 = 2$ has no integer solutions. If for some modulus, an element $X(x) \in \mathbb{Z}[x]$, the congruence $X(x) \equiv 0$ cannot be satisfied, then $X(x)$ has no rational root.

[2]From this we may actually conclude that $X(x) = 0$ has no solutions in rationals either. Try to prove this yourself.

## 1.4 Certain applications

**Article 12.** There are certain divisibility tricks which are useful and seeminly miraculous. Now we have the machinery to show that they are natural and sound.

If the sum of the digits of a number are divisible by 9, then that number is divisible by 9. The same is true for 3. Other divisibility tricks can be derived similarly.

*Proof.* Every number can be expressed as $a + 10b + 100c + ....$ This is our usual representation. For instance, $573 = 3 + 7 * 10 + 5 * 100$. Note however that since $10 \equiv 1 \pmod 9$, then by article 8, $10^k \equiv 1 \pmod 9$ for any positive integer $k$. Thus $a + 10b + 100c + ... \equiv a + b + c + ... \pmod 9$. □

Derivation of a divisibility trick for 11: $10 \equiv -1 \pmod{11}$. Thus $a+10b+100c+1000d+... \equiv a+(-1)b+(-1)^2c+(-1)^3d+... \pmod{11}$. So a number is divisible by 11 if and only if the alternating sum of it's digits is divisible by 11. It is easy to check that 121 is divisible by 11 since $1 - 2 + 1 = 0$. It is easy to check that 1000 is congruent to $-1$ mod 11, since $0 + (-1)0 + (-1)^2 0 + (-1)^3 1 = -1$.

## Exercises

1. Prove articles 5 and 6.
2. Derive divisibility tricks for 2, 3, 4, 5, 6 and 8.
3. Figure out why there is no easy divisibility trick for 7.
4. Prove, for a number $a \neq 0$, $a|a$.
5. Prove that if $a|b$ and $b|a$ then $a = \pm b$.
6. Prove that if $a|b$ and $b|c$ then $a|c$.
7. Prove that if $a|b$ and $a|c$ then $a|(b + c)$.
8. What moduli $m$ make the congruence $X(x) \equiv 0$ fail for $X(x) = x^2 + 1$, $X(x) = x^2 - 2$, $X(x) = x^2 + x + 1$? (see article 10)

   Give the set $\mathbb{Z}/m\mathbb{Z}$ operations of multiplication and addition as follows: perform the usual addition or multiplication in the integers and then take the least positive residue of this as the answer.
9. Compute $5 \times 4$ in $\mathbb{Z}/6\mathbb{Z}$.
10. Show that adding 4 in $\mathbb{Z}/6\mathbb{Z}$ behaves like subtracting 2.
11. Prove that for $n \in \mathbb{Z}/m\mathbb{Z}$, addition by $n$ is the same as adding $n + km$ for any $k \in \mathbb{Z}$.
12. Rewrite these notes and make sure you understand every line.
13. Do the other exercises within these notes.