Math 313/623 Notes 3

David L. Meretzky

Tuesday February 5th, 2019

> There is no problem in all Mathematics that cannot be solved by direct counting.
>
> Mach Ernst

Recall from last class that the major theorem we obtained was that every number has a unique prime factorization. We saw two proofs of this. Today we will see that this theorem gives us an easy way to discover the greatest common divisor of two numbers. Then we will define and discuss some basic properties of commutative rings.

2 Congruences of the First Degree, Continued

2.1 Preliminary theorems regarding prime numbers, factors etc. Continued

Article 17. If A is a product of numbers a, b, c, etc. Then the prime decomposition of A is the products of the prime decompositions of a, b, c, etc.

Proof. Form a product of the prime factors of a, b, c, etc. then this must be the unique prime factorization of A. □

Thus B divides A if and only if every prime in B appears in the factorization of A, and if p^n appears in B then p^m appears in A with $n \leq m$. Thus if the prime factorization of A is $p^\alpha q^\beta r^\gamma$, then A has $(\alpha+1)(\beta+1)(\gamma+1)$ different divisors. That is, all divisors of A are of the form $p^i q^j r^k$ where $0 \leq i \leq \alpha$, $0 \leq j \leq \beta$, and $0 \leq k \leq \gamma$.

Article 18. If A and B have no primes in common in their prime factorization, then their greatest common divisor is 1.

Proof. If a number d divides both A and B then every prime in the prime factorization of d must appear in the prime factorizations of both A and B. Since A and B have no primes in common in their prime factorization, then $d = 1$. □

Now we have a method for finding the greatest common divisor of numbers A and B. Write the prime factorizations of A and B and list the primes which appear in both. For each of these primes their multiplicity will be the minimum of both A and B.

Example 1. Let $A = 504 = 2^3 3^2 7$, $B = 2880 = 2^6 3^2 5$, and $C = 864 = 2^5 3^3$. Then their greatest common divisor is $2^{min(\{3,6,5\})} 3^{min(\{2,2,3\})} = 2^3 3^2 = 72$.

Article 19. If some numbers a, b, c etc. are relatively prime to some number k, then their product abc etc. is relatively prime to k.

Proof. The product abc etc. has no prime factors which are not present in a, b, c etc. but by the preceding article, none of these numbers share any prime factors with k, thus abc etc. has no prime factors which are also in k. Again, by the preceding article, the product abc etc. is relatively prime to k. □

If some numbers a, b, c etc. are relatively prime to each other and they all divide some number k, then their product divides k.

Proof. Let p be a prime factor of the product which appears n times. Then since p must appear in the factors a total of n times it must appear in only one of a, b, c etc. exactly n times since a, b, c etc. are relatively prime to each other. Since that factor divides k, p^n appears in the prime factorization of k. Continue in this manner to guarantee that all prime factors of the product appear in k. □

If two numbers a and b are congruent to several moduli m, n but m and n are relatively prime, then a and b are congruent relative to the product mn.

Proof. We have that $m|a - b$, and $n|a - b$ and m and n are relatively prime, then by the previous statement, letting $k = a - b$ we have $mn|a - b$. □

If a and b are relatively prime and if $b|ak$ then $b|k$. See proposition 1 from lecture 2.

Proof. Since $a|ak$ and $b|ak$ we have $ab|ak$ and therefore $ak/ab = x = k/b$ so $b|k$ as desired. □

Article 20. Suppose p, q, r, etc. are unequal primes and $A = p^\alpha q^\beta r^\gamma$ etc. then if $A = k^n$ for some number k, all of the powers α, β, γ, etc. must be divisible by n.

Proof. By article 17, $k^n = A$ contains no prime factors not present in k. Thus, if p appears in k exactly α' times, it will appear in k^n exactly $n\alpha' = \alpha$ times. Thus $n|\alpha$. □

Article 21. If a, b, c, etc. are relatively prime and their product is k^n for some k, then each factor a will be of the form l^n for some l.

Proof. Let a have prime factorization $p^\lambda q^\mu r^\pi$. Then since a, b, c, etc. are relatively prime p, q, and r appear in k^n with powers λ, μ, and π respectively. Thus by the previous article, λ, μ, and π are all divisible by n. Therefore a is is of the form l^n where $l = p^{\lambda/n} q^{\mu/n} r^{\pi/n}$. □

This concludes the preliminaries on prime factorization. We will finish up some preliminaries on congruences.

Article 22. If a and b are divisible by k and they are congruent relative to a modulus m which is relatively prime to k then $a/k \equiv b/k \pmod{m}$.

Proof. Since $k|(a-b)$ and therefore $kx = (a-b)$ since $m|(a-b)$ we have $m|kx$ since m is relatively prime to k, $m|x$. Note that $x = (a-b)/k$. Thus $m|(a-b)/k$ which is equivalent to $a/k \equiv b/k \pmod{m}$. □

If a and b are divisible by k and they are congruent relative to a modulus m such that the greatest common divisor of m and k is e then $a/k \equiv b/k \pmod{m/e}$.

Proof. It must be true that k/e and m/e are relatively prime. Otherwise there is an even greater common divisor contradicting that e is the greatest common divisor. Clearly since $e|m$ we have $e|a-b$. If $mx = (a-b)$ then $\frac{m}{e}x = \frac{(a-b)}{e}$ since $k|a-b$ we must have $\frac{k}{e}|\frac{(a-b)}{e}$ and therefore, $\frac{k}{e}|\frac{m}{e}x$. But since k/e and m/e are relatively prime, we have that $\frac{k}{e}|x$. Thus $x = \frac{k}{e}l$. So $\frac{m}{e}\frac{k}{e}l = \frac{(a-b)}{e}$. Multiplying both sides by $\frac{e}{k}$ we obtain $\frac{m}{e}l = \frac{(a-b)}{k}$ which is the same as $a/k \equiv b/k \pmod{m/e}$ as desired. □

Article 23. If a is a prime relative to m and e and f are noncongruent relative to m, then ae and af will be noncongruent relative to m.

Proof. We need to show that if $m \not| (e-f)$ then $m \not| (ae-af)$. Suppose $m|(ae-af)$, this is the same as $ae \equiv af \pmod{m}$, then since a and m are relatively prime, by Article 22, we have that $ae/a \equiv af/a \pmod{m}$ that is $m|(e-f)$, a contradiction. □

Take all the residues 0 to $m-1$, these are all noncongruent relative to m, then $a0$, $a1$, $a2$,...,$a(m-1)$ will all be noncongruent relative to m, thus when reduced to their least positive residues $a0$, $a1$, $a2$,...,$a(m-1)$ must be the whole set 0 to $m-1$.

For instance let $a = 7$ and $m = 4$, we have $0(7) = 0 \pmod{4}$, $1(7) \equiv 3 \pmod{4}$, $2(7) \equiv 2 \pmod{4}$ and $3(7) \equiv 1 \pmod{4}$.

Article 24. Let a, b be numbers and x a variable. The expression $ax+b$ can be made congruent to any number c relative to a modulus m provided m is prime relative to a.

Proof. Let e be the least positive residue of $c-b$ relative to m. By the comment after the previous article, since a is relatively prime to m there is some number j in the range from 0 to $m-1$ such that $aj \equiv e \pmod{m}$. Then $aj \equiv e \equiv c-b$, and therefore $aj+b \equiv c \pmod{m}$. □

Article 25. We say that a congruence is solved when we find a value of the unknown which makes the congruence true. We can talk about congruences like we talk about equations. One way in which we will classify congruences is by highest degree of unknown.

Rings

Preliminary definitions

Before we continue talking about congruences of the first degree we will go back to *A Classical Introduction to Modern Number Theory* where we will see that the theory of residues and unique factorization holds for polynomials. We need some definitions first.

What is a number system? Numbers are things we can add and multiply. They have other properties like unique factorization perhaps. There are special numbers that are primes. The integers are clearly a different number system than the rationals or the reals or the complex numbers. What do all of these number systems share? They share many properties. Some are more important than others. We will be looking at number systems which are called commutative rings.

Given here are some definitions.

Definition 1. Given a set X, an operation on X of arity n is a function d from $X \times X \times ... \times X = X^n$ to X. That is, d takes in n elements of X, they do not have to be different, and returns a single element of X.

Example 2. Addition and multiplication are operations of arity 2 on the integers. Note that subtraction is not an operation on the positive integers because $2 - 5 = -3$ is not in the positive integers. Addition is takes in two integers $(\ ) + (\ )$ and outputs another integer. We could also write this as $+ : \mathbb{Z}^2 \to \mathbb{Z}$. Note that $\mathbb{Z}^2 = \{(x, y) : x, y \in \mathbb{Z}\}$, the pairs of all integers. Addition and multiplication take in a pair of integers and return a single integer.

Definition 2. A commutative ring is a set R together with two operations called addition, $+$, and multiplication, $*$, both of arity 2 which satisfy some properties:

For all $a, b, c \in R$, we have the following additive properties:

1. $(a + b) + c = a + (b + c)$. (associativity)
2. There exists an element $0 \in R$ such that $0 + a = a + 0 = a$. (identity)
3. For every $x \in R$ there exists a $y \in R$ such that $x + y = 0$. (inverses)

4. $a + b = b + a$. (commutativity)

For all $a, b, c \in R$, we have the following multiplicative properties:

1. $(a * b) * c = a * (b * c)$. (associativity)
2. There exists an element $1 \in R$ such that $1 * a = a * 1 = a$. (identity)
3. $a * b = b * a$. (commutativity)

For all $a, b, c \in R$, multiplication and addition interact in the following ways:

1. $a * (b + c) = a * b + a * c = (b + c) * a$ (distributivity)

The integers are the quintessential example of a commutative ring. From now on, by number, we mean an element of a ring.

We will now examine some things about the above definition. Notice that the multiplication is not required to have an inverse property. What would an inverse property for the multiplication look like? Something like this:

For every non-zero $x \in R$ there exists a $y \in R$ such that $x * y = 1$. (inverses)

This property is true for the rationals, reals, and complex numbers.

Definition 3. A ring which has this additional property that every number has a multiplicative inverse is called a field.

But this property does not hold for $\mathbb{Z}$. Note for instance that there is no integer x such that $2 * x = 1$.

Example 3. Here are some examples of rings:

1. $\mathbb{Z}$, the integers.
2. $\mathbb{Q}$, the rationals.
3. $\mathbb{R}$, the reals.
4. $\mathbb{C}$, the complex numbers.
5. $R[x]$, the collection of polynomials with coefficients in a ring R with indeterminate x.
6. $\mathbb{Z}/n\mathbb{Z}$, the set of integer residues mod n with addition and multiplication defined in the exercises from lecture 1.

Here are some examples of fields

1. $\mathbb{Q}$, the rationals.

2. $\mathbb{R}$, the reals.

3. $\mathbb{C}$, the complex numbers.

4. $\mathbb{Z}/p\mathbb{Z}$, when p is prime.

Note that $\mathbb{N}$ the natural numbers (positve integers including 0) fail to be a ring. They fail the additive inverses property.

Mostly we are investigating the multiplicative properties of rings. There are some important definitions we need.

Fields and integral domains

Definition 4. A non-zero element of a ring, $x \in R$, is called a zero divisor if there exists an element $y \in R$ such that $y \neq 0$ and $xy = 0$.

For instance 2 and 3 are zero divisors in $\mathbb{Z}/6\mathbb{Z}$ since $2 * 3 \equiv 0 \pmod 6$. $\mathbb{Z}$ has no zero divisors.

Definition 5. A non-zero element of a ring, $x \in R$, is called left cancelative if for any other $y, z \in R$ such that

$$xy = xz$$

we must have that

$$y = z$$

also. Note that this does not imply that x has a multiplicative inverse.[1]

Proposition 1. An element is left cancelative if and only if it is not a zero divisor.

Proof. With the notation of the previous definition, if $xy = xz$ then $xy - xz = 0$. By the distributive law we have $x(y - z) = 0$. Since x is not a zero divisor and $x \neq 0$, we have that $y - z = 0$. Thus $y = z$. □

For instance, since 2 is not a zero divisor in $\mathbb{Z}$, we have that $2x = 2y$ implies that $x = y$. You can combine this with either article 3 (Gauss) or lemma 2 (Ireland and Rosen) to show that every number has a unique even or odd representation of the form $2k$ or $2k + 1$.

Definition 6. A non-zero element of a ring, $x \in R$, is called a unit if there exists an element $y \in R$ such that $xy = 1$.

Example 4. For example, 5 is a unit in $\mathbb{Z}/6\mathbb{Z}$ because $5 * 5 \equiv 1 \pmod 6$. The only units of $\mathbb{Z}$ are 1 and -1.

[1] In a commutative ring, where $xy = yx$ for all ring elements, there is no distinction between right or left cancelative, there is just cancelative.

Proposition 2. A number cannot be both a unit and a zero divisor.

Proof. Let x be a unit. Then there exists a nonzero y such that $x * y = 1$. Suppose now that x is also a zero divisor. Then there exists a nonzero z such that $zx = 0$. But then $z*(x*y) = z*1 = z$. Since $z*(x*y) = (z*x)*y = 0*y = 0$ we have that $z = 0$. Which is a contradiction. □

Note, there are numbers which are neither zero divisors nor units. Take for instance $2 \in \mathbb{Z}$. It is neither a unit nor a zero divisor.

Proposition 3. A ring R is a field if and only if every non-zero element is a unit.

Proposition 4. Let p be a prime. Then $\mathbb{Z}/p\mathbb{Z}$ is a field.

Proof. Let $a \in \mathbb{Z}/p\mathbb{Z}$ such that $a \neq 0$. We need to show that a has a multiplicative inverse. In article 24 let $c = 1$ and $b = 0$ then since a is clearly relatively prime to p, we have that there is some $x \in \mathbb{Z}/p\mathbb{Z}$ such that $ax \equiv 1 \pmod{p}$. □

Definition 7. We say that a ring R is an integral domain if none of its elements are zero divisors.

It is clear that every field is an integral domain. Not every integral domain however is a field. For instance, the integers have elements which are not units but none of its elements are zero divisors. The integers are the major example of an integral domain. Roughly speaking, all of the elements of a commutative ring can be placed into one of three buckets, units, zero divisors, and things that are neither units nor zero divisors. Said another way, every ring element divides 0, 1, or neither. When every non-zero ring element either divides 1 or neither, we have an integral domain. When every non-zero ring element either divides 1 we have a field.

We have the following set of inclusions so far.

$$\text{Fields} \subset \text{Integral Domains} \subset \text{Commutative Rings}$$