Math 4527 (Number Theory 2)

Lecture #20 of 38 $\sim$ March 8, 2021

Rings and Ideals

- Tunnell's Theorem on Congruent Numbers
- Ideals of Commutative Rings
- Quotient Rings

This material represents §8.1.1-8.1.2 from the course notes.

Congruent Numbers, I

Definition

We say a positive integer n is a congruent number if there exists a right triangle with rational side lengths whose area is n.

Proposition (Congruent Numbers)

The positive integer n is a congruent number if and only if the congruent-number elliptic curve $E_n : y^2 = x^3 - n^2x$ has a rational point with $y \neq 0$.

Explicitly, $a = \dfrac{y}{x}$, $b = \dfrac{2nx}{y}$, and $c = \dfrac{2x^2}{y} - \dfrac{y}{x} = \dfrac{x^2 + n^2}{y}$.

Congruent Numbers, II

We have an efficient way to determine if n is a congruent number:

Theorem (Tunnell's Theorem)

If n is an odd congruent number then the number of solutions in integers to $n = 2x^2 + y^2 + 32z^2$ is equal to half the number of solutions of $n = 2x^2 + y^2 + 8z^2$, while if n is an even congruent number then the number of solutions to $n/2 = 4x^2 + y^2 + 32z^2$ is equal to half the number of solutions of $n/2 = 4x^2 + y^2 + 8z^2$.

We can use Tunnell's theorem in combination with a search for rational points on E_n to determine (provably) whether n is a congruent number.

Congruent Numbers, III

Examples:

1. If $n = 2$ then there are two solutions to $n/2 = 4x^2 + y^2 + 32z^2$ (namely, $(0, \pm 1, 0)$) and also two solutions to $n/2 = 4x^2 + y^2 + 8z^2$ (namely, $(0, \pm 1, 0)$). Thus, 2 is not a congruent number.
2. If $n = 3$ then there are four solutions to $n = 2x^2 + y^2 + 32z^2$ (namely, $(\pm 1, \pm 1, 0)$ and also four solutions to $n = 2x^2 + y^2 + 8z^2$ (also $(\pm 1, \pm 1, 0)$). Thus, 3 is not a congruent number.

Congruent Numbers, IV

Examples (continued):

3. If $n = 13$ then there are no solutions to $n = 2x^2 + y^2 + 32z^2$ or to $n = 2x^2 + y^2 + 8z^2$.

- This suggests n is in fact a congruent number, and indeed, searching for rational points on $y^2 = x^3 - 13^2x$ will eventually identify the point $(x, y) = (-36/25, 1938/125)$, which yields the triangle sides $(a, b, c) = (323/30, 780/323, 106921/9690)$.
- Thus, 13 is a congruent number.

Quadratic Integer Rings

We now move into the next chapter of the course $\sim$ §8: Quadratic Integer Rings.

- The goal, reasonably enough, is to study the quadratic integer rings, which are essentially the rings $\mathbb{Z}[\sqrt{D}]$ we have already encountered in our study of Pell's equation.
- We begin with an overview of some properties of integral domains related to division algorithms, common divisors, and unique factorization.
- These topics are of independent interest since they will allow us to generalize many of the arithmetic properties of $\mathbb{Z}$ to other rings with more solid footing.
- We then narrow our focus to quadratic integer rings, with the primary goal of studying unique (and non-unique!) factorization.

Motivation for Ideals, I

We start by introducing ideals of commutative rings, which (in the study of general rings) are primarily motivated by their use in constructing quotient rings.

- The basic idea is that ideals are the objects in the world of rings that we can take quotients by, in analogy to how normal subgroups are the objects in the world of groups that we can take quotients by.
- So let me motivate the definition of an ideal by working out what properties we need in order to have residue classes work properly.

Motivation for Ideals, II

In a group G, we have a natural notion of a subgroup (namely, a subset that also carries the structure of a group under the operation from G).

- If H is a subgroup of G, then we define the natural analogue of residue classes in G (namely, left cosets of H) as sets of the form $gH = \{gh : h \in H\}$.
- We then try to define a composition operation on the left cosets of H by writing $(g_1H)(g_2H) = g_1g_2H$.
- However, this is not always well-defined: in order for this operation to be consistent, we have to impose an additional property on H, namely, that it is a normal subgroup of G.

Motivation for Ideals, III

We can try to play the same game inside a ring R: we again have a natural notion of a subring (namely, a subset that also carries the structure of a ring under the operations from R).

- If S is a subring of R, then we define the residue classes in R as the (left) cosets of S under addition: namely, as $a + S = \{a + s : s \in S\}$.
- We can then add these residue classes via $(a + S) + (b + S) = (a + b) + S$, and this will be well-defined as long as S is a subgroup of R under addition.
- We'd also like to be able to multiply residue classes (since we want to have both ring operations) via $(a + S)(b + S) = ab + S$.
- But to make multiplication well-defined, we will have to impose an additional property on S, which we now investigate.

Motivation for Ideals, IV

So, if I is a subset of R (whose properties we intend to characterize in a moment) let us say that two elements $a, b \in R$ are "congruent modulo I" if $a - b \in I$.

- The connection to cosets is that the coset $a + I$ is exactly the set of elements congruent to a modulo I.
- First, we would like "congruence modulo I" to be an equivalence relation: this requires $a \equiv a \pmod{I}$, $a \equiv b \pmod{I}$ implies $b \equiv a \pmod{I}$, and $a \equiv b \pmod{I}$ and $b \equiv c \pmod{I}$ implies $a \equiv c \pmod{I}$.
- It is not hard to see that these three conditions require $0 \in I$, that I be closed under additive inverses, and that I be closed under addition.
- This just means that I is a subgroup of R under addition.

Motivation for Ideals, V

We also want congruences to respect addition and multiplication.

- If $a \equiv b \pmod{I}$ and $c \equiv d \pmod{I}$, then we want $a + c \equiv b + d \pmod{I}$ and $ac \equiv bd \pmod{I}$.
- In terms of ring elements, this is equivalent to the following: if $b = a + r$ and $d = c + s$ for some $r, s \in I$, then we want $(b + d) - (a + c) = r + s$ to be in I, and we also want $bd - ac = (a + r)(c + s) - ac = as + rc + rs$ to be in I.
- The first condition clearly follows from the requirement that I is closed under addition. It is a bit less obvious how to handle the second condition, but one immediate implication follows by setting $a = c = 0$: namely, that $rs \in I$.
- Thus, I must be closed under $\cdot$, so it must be a subring.
- But more is needed: since $0 \in I$, we can set $r = 0$ to see that $as \in I$, and we can also set $s = 0$ to see that $rc \in I$.

Motivation for Ideals, VI

- So in fact, I must be closed under (left and right) multiplication by *arbitrary* elements of R, in addition to being a subgroup.
- In fact, this condition is also sufficient to ensure that $a \equiv b \pmod{I}$ and $c \equiv d \pmod{I}$ imply $a + c \equiv b + d \pmod{I}$ and $ac \equiv bd \pmod{I}$.
- Once we impose these conditions, everything will be well-defined with our choices of addition and multiplication of residue classes.
- Explicitly, we define $a + I = \overline{a}$ to be the set of ring elements b congruent to a modulo I, and then we take the operations $\overline{a} + \overline{b} = \overline{a + b}$ and $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$ that we wanted earlier.

Ideals of Commutative Rings, I

Let's now start in with ideals, and then build back up to quotient rings:

Definition

If R is a commutative ring with 1, a subset I is called a (two-sided) ideal of R if it contains 0, is closed under subtraction, and is closed under arbitrary multiplication by elements of R.

Explicitly, I is an ideal if I contains 0 and for any $x, y \in I$ and any $r \in R$, the elements $x - y$ and rx are in I.

- I is an ideal of R if and only if I is a subgroup of $(R, +)$ that is also closed under multiplication by arbitrary elements of R.
- If R is not commutative, there are various other flavors of ideals (left ideals, right ideals) to worry about. We will not deal with these since our focus is on commutative rings.

Ideals of Commutative Rings, II

Examples:

1. The subrings $n\mathbb{Z}$ are ideals of $\mathbb{Z}$, since they are clearly closed under arbitrary multiplication by elements of $\mathbb{Z}$.
2. If $R = F[x]$ and p is any polynomial, the subring pR of multiples of p is an ideal of $F[x]$, since it is closed under arbitrary multiplication by polynomials in $F[x]$.
3. The subset $\mathbb{Z}$ of $\mathbb{Q}$ is **not** an ideal of $\mathbb{Q}$, since it is not closed under arbitrary multiplication by elements of $\mathbb{Q}$. For example, if we take $r = 1/3 \in \mathbb{Q}$ and $x = 4 \in \mathbb{Z}$, the element $rx = 4/3$ is not in $\mathbb{Z}$.
4. For any ring R, the sets $\{0\}$ and R are ideals of R. We refer to $\{0\}$ as the trivial ideal (or the "zero ideal") and refer to any ideal $I \neq R$ as a proper ideal (since it is a proper subset of R).

Ideals of Commutative Rings, III

Examples:

5. In the polynomial ring $\mathbb{Z}[x]$, the set S of polynomials with even constant term forms an ideal: it contains 0, is closed under subtraction, and if we multiply an element of S by an arbitrary polynomial in $\mathbb{Z}[x]$, we again obtain a polynomial with even constant term.
6. The set $S = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}\}$ of "even" residue classes is an ideal of $\mathbb{Z}/8\mathbb{Z}$: it contains 0, is closed under subtraction, and any multiple of something in S is again in S because 8 is even.
7. The set $S = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}\}$ of "even" residue classes is **not** an ideal of $\mathbb{Z}/9\mathbb{Z}$: it is not closed under addition, because for example $\overline{2} + \overline{8} = \overline{1}$ mod 9. (The problem is that 9 is odd.)

Ideals of Commutative Rings, IV

Examples:

9. Is the set $S = \{\overline{0}, \overline{3}, \overline{6}\}$ is an ideal of $\mathbb{Z}/9\mathbb{Z}$?

Ideals of Commutative Rings, IV

Examples:

9. Is the set $S = \{\overline{0}, \overline{3}, \overline{6}\}$ is an ideal of $\mathbb{Z}/9\mathbb{Z}$?
   Yes: it contains 0, is closed under subtraction, and any multiple of anything in S is again in S since 3 divides 9.
10. Is the set $T = \{(2a, 3a) : a \in \mathbb{Z}\}$ an ideal of $\mathbb{Z} \times \mathbb{Z}$?

Ideals of Commutative Rings, IV

Examples:

9. Is the set $S = \{\overline{0}, \overline{3}, \overline{6}\}$ is an ideal of $\mathbb{Z}/9\mathbb{Z}$?
   Yes: it contains 0, is closed under subtraction, and any multiple of anything in S is again in S since 3 divides 9.
10. Is the set $T = \{(2a, 3a) : a \in \mathbb{Z}\}$ an ideal of $\mathbb{Z} \times \mathbb{Z}$?
    No: although it contains 0 and is closed under subtraction, it is not closed under arbitrary multiplication since for example $(2, 3) \in S$ but $(1, 2) \cdot (2, 3) = (2, 6) \notin S$.
11. Is the set $T = \{(2a, 3b) : a, b \in \mathbb{Z}\}$ an ideal of $\mathbb{Z} \times \mathbb{Z}$?

Ideals of Commutative Rings, IV

Examples:

9. Is the set $S = \{\overline{0}, \overline{3}, \overline{6}\}$ is an ideal of $\mathbb{Z}/9\mathbb{Z}$?
   Yes: it contains 0, is closed under subtraction, and any multiple of anything in S is again in S since 3 divides 9.
10. Is the set $T = \{(2a, 3a) : a \in \mathbb{Z}\}$ an ideal of $\mathbb{Z} \times \mathbb{Z}$?
    No: although it contains 0 and is closed under subtraction, it is not closed under arbitrary multiplication since for example $(2, 3) \in S$ but $(1, 2) \cdot (2, 3) = (2, 6) \notin S$.
11. Is the set $T = \{(2a, 3b) : a, b \in \mathbb{Z}\}$ an ideal of $\mathbb{Z} \times \mathbb{Z}$?
    Yes: it contains 0, is closed under subtraction, and we can see $(c, d) \cdot (2a, 3b) = (2ac, 3bd) \in S$ for any $(c, d) \in \mathbb{Z} \times \mathbb{Z}$.

Ideals of Commutative Rings, V

In order to study the structure of ideals, we would like a simpler way to describe them.

- A convenient way is to describe ideals as being "generated" by subsets of a ring, in much the same way that we describe subspaces of a vector space as being generated by a subset that spans it.
- So, following the parallel, if R is a commutative ring with 1 and A is a subset of R, we would like to define "the ideal generated by A" to be the smallest ideal containing A.
- But... it is not obvious that there is such a smallest ideal.

Ideals of Commutative Rings, VI

We need a fact about intersections of ideals:

Proposition (Intersections of Ideals)

Let R be a commutative ring with 1. If S is any indexing set and $\{I_s\}_{s\in S}$ is any collection of ideals of R, then the intersection $\bigcap_{s\in S} I_s$ is also an ideal of R. (In short: the intersection of any collection of ideals is also an ideal.)

Proof:

- Suppose x, y are elements of $\bigcap_{s\in S} I_s$ and $r \in R$.
- Then by definition, $x, y \in I_s$ for all $s \in S$. Since each I_s is an ideal, that means 0, $x - y$, and rx are all in I_s for each s.
- But then by definition, this means 0, $x - y$, and rx are all in $\bigcap_{s\in S} I_s$, which is therefore an ideal of R.

Ideals of Commutative Rings, VII

Now, back to this business about generating ideals:

Definition

Suppose R is a commutative ring with 1 and A is a subset of R. We define the ideal generated by A, denoted (A), to be the intersection of all ideals of R containing A.

Our proposition assures us that this definition is well-posed.

- Specifically, the intersection makes sense because A is contained in at least one ideal (namely the whole ring R),
- Then the intersection of any nonempty collection of ideals is also an ideal, so (A) is a well-defined ideal.
- It is also easy to see that (A) is the smallest ideal containing A: any other ideal containing A is among those in the intersection, so it contains (A).

Ideals of Commutative Rings, VIII

This is all perfectly nice, but we'd like to write down the elements that are actually in (A)! Fortunately, this is not so hard:

- If $a_1, a_2, \ldots, a_n$ are any elements of A, we see that (A) must contain the elements $r_1 a_1$, $r_2 a_2$, ... , $r_n a_n$ for any $r_i \in R$.
- (A) must therefore contain the sum $r_1 a_1 + r_2 a_2 + \cdots + r_n a_n$.
- On the other hand, if we let S be the set of elements of the form $r_1 a_1 + r_2 a_2 + \cdots + r_n a_n$ for any $a_i \in A$ and $r_i \in R$ (and some $n \geq 0$), then it is easy to see that S contains 0, is closed under subtraction, and is closed under multiplication by elements of R, so S is an ideal.
- Furthermore, since R contains 1, S contains A.
- Since S is an ideal, that means S contains (A), but since everything in (A) must be in S, we see $S = (A)$.

Ideals of Commutative Rings, IX

We have just proven the following proposition:

Proposition (Generation of Ideals)

Let R be a commutative ring with 1 and A be a subset of R. Then the set $(A) = \{r_1a_1 + r_2a_2 + \cdots + r_na_n : r_i \in R \text{ and } a_i \in A\}$ is the smallest ideal containing A.

Example:

- Inside $\mathbb{Z}$, we have $(2) = \{2a : a \in \mathbb{Z}\}$ and $(4, 6) = \{4a + 6b : a, b \in \mathbb{Z}\}$.
- Note that $(4, 6)$ contains $6 - 4 = 2$, and so since it is an ideal, in fact it is the ideal (2).

Ideals of Commutative Rings, X

The simplest class of ideals are those generated by a finite set, and (in particular) those generated by a single element:

Definition

If R is a ring with 1, we say an ideal I is finitely generated if I is generated by a finite set, and we say I is principal if I is generated by a single element. Thus, a finitely generated ideal has the form $I = (a_1, a_2, \ldots, a_n)$, while a principal ideal has the form $I = (a)$.

Note that the principal ideal (a) is simply the set of R-multiples of a: $(a) = \{ra : r \in R\}$.

Ideals of Commutative Rings, XI

Examples:

1. If R is any commutative ring with 1, then $R = (1)$ is principal. Likewise, the zero ideal $0 = (0)$ is also principal.
2. In $\mathbb{Z}$, for any integer n we have $(n) = n\mathbb{Z}$. Since every ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z}$, we see that every ideal of $\mathbb{Z}$ is principal. We remark that the notation $n\mathbb{Z}$ we have already used is consistent with the definition above.
3. Inside $\mathbb{Z}$, if $\gcd(a, b) = d$, then $(a, b) = (d)$.[1] This follows from the pair of observations that a and b are both contained in (d) because $d|a$ and $d|b$, meaning that that $(a, b) \subseteq (d)$, and also that $d = xa + yb$ for some integers x and y by the Euclidean algorithm, so that d is contained in (a, b).

[1] Indeed, as a reflection of this fact, many authors write (a, b) to denote the greatest common divisor of a and b.

Ideals of Commutative Rings, XII

Since principal ideals are the easiest to describe, it is often useful to try to determine whether a particular ideal is principal, though this task is not always so easy!

- Indeed, as we will see over the next few weeks, the question of whether ideals are principal is closely related to various facts regarding unique factorization.

Ideals of Commutative Rings, XIII

Example: Show that the ideal $I = (2, x)$ in $\mathbb{Z}[x]$ is not principal.

- Note that $I = \{2p(x) + xq(x) : p, q \in \mathbb{Z}[x]\}$ is the collection of polynomials in $\mathbb{Z}[x]$ with even constant term.
- If I were principal and generated by some polynomial $r(x)$, then every polynomial in I would be divisible by $r(x)$.
- In particular, $r(x)$ would divide 2, so since 2 is a constant polynomial and a prime number, $r(x)$ would have to be one of $\{\pm 1, \pm 2\}$.
- However, since $r(x)$ must also divide x, the only possibility is that $r(x)$ would be either 1 or -1.
- But it is easy to see that the ideal generated by 1 (or -1) is all of $\mathbb{Z}[x]$, so $r(x)$ cannot be 1 or -1, since $I \neq \mathbb{Z}[x]$.
- Thus, there is no possible choice for r, so I is not principal.

Ideals of Commutative Rings, XIV

Example: Show that $I = (2, 1 + \sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}]$ is not principal.

- Suppose I were principal with generator $r = a + b\sqrt{-5}$.
- Then r must divide 2, meaning that $2 = rs$ for some $s \in \mathbb{Z}[\sqrt{-5}]$. Taking norms yields $4 = N(2) = N(r)N(s)$.
- Likewise, since r divides $1 + \sqrt{-5}$, we would have $1 + \sqrt{-5} = rt$ for some $t \in \mathbb{Z}[\sqrt{-5}]$. Taking norms yields $6 = N(1 + \sqrt{-5}) = N(r)N(t)$.
- Since $N(r) = a^2 + 5b^2$ is a nonnegative integer, we see that $N(r)$ must divide both 4 and 6, hence is either 1 or 2. However, it is easy to see that there are no integer solutions to $a^2 + 5b^2 = 2$, and the only elements of norm 1 are 1 and -1.
- As in the examples above, the ideal generated by 1 (or -1) is all of $\mathbb{Z}[\sqrt{-5}]$, but $(2, 1 + \sqrt{-5}) \neq \mathbb{Z}[\sqrt{-5}]$ since every element $a + b\sqrt{-5}$ in the ideal has $a + b$ even.
- Thus, I is not principal.

Ideals of Commutative Rings, XV

The non-principal ideal in the last example is related to a situation of non-unique factorization.

- We had the non-principal ideal $I = (2, 1 + \sqrt{-5})$.
- Now observe that $2 \cdot 3 = 6 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$.
- Unlike the situation with the factorization $5 = (2 + i)(2 - i) = (1 + 2i)(1 - 2i)$ in the Gaussian integers, the terms in the factorization of 6 in $\mathbb{Z}[\sqrt{-5}]$ are not obtained by scaling one another by unit factors (and they are also all "irreducible", meaning that they cannot be factored further).

Our main goal in this chapter is to understand this kind of behavior: when do rings have unique factorization, and when do they fail to have unique factorization?

Ideals of Commutative Rings, XVI

As we noted in both of the examples, we always have $(1) = R$. We can generalize this statement somewhat:

Proposition (Ideals and Units)

If I is an ideal of the ring R with 1, then $I = R$ if and only if I contains a unit.

Proof:

- If $I = R$ then certainly I contains a unit (namely, 1).
- Conversely, if $u \in I$ is a unit with $ur = 1$, then since I is an ideal we have $1 = ur \in I$.
- Then for any $s \in R$, the element $s = 1s$ is also in I, and so $I = R$.

Ideals of Commutative Rings, XVII

Since every nonzero element in a field is a unit, the only nonzero ideal of a field F is F itself. The converse is also true:

Corollary (Ideals of Fields)

A commutative ring R with 1 is a field if and only if the only ideals of R are 0 and R.

Proof:

- If F is a field and $I \neq (0)$, then I contains some nonzero r. Since F is a field, r is a unit, so $I = R$ by the proposition.
- Conversely, if the only ideals of R are 0 and R, let $r \in R$ be any nonzero element. Then (r) contains $r \neq 0$ so it cannot be the zero ideal, so we must have $(r) = R$.
- By the previous proposition, this means (r) contains 1: then $rs = 1$ for some $s \in R$, so r is a unit. Hence every nonzero element of R is a unit, so R is a field as claimed.

Quotient Rings, I

Now we can get back to constructing quotient rings:

Definition

If I is an ideal of the ring R, then we say a is congruent to b modulo I, written $a \equiv b \pmod{I}$, if $a - b \in I$.

Proposition (Ideal Congruences)

Let I be an ideal of R and $a, b, c, d \in R$. The following are true:

1. $a \equiv a \pmod{I}$.
2. $a \equiv b \pmod{I}$ if and only if $b \equiv a \pmod{I}$.
3. If $a \equiv b \pmod{I}$ and $b \equiv c \pmod{I}$, then $a \equiv c \pmod{I}$.
4. If $a \equiv b \pmod{I}$ and $c \equiv d \pmod{I}$, then $a + c \equiv b + d \pmod{I}$.
5. If $a \equiv b \pmod{I}$ and $c \equiv d \pmod{I}$, then $ac \equiv bd \pmod{I}$.

Quotient Rings, II

Proofs:

1. $a \equiv a \pmod{I}$.
   - Since $a - a = 0 \in I$, the statement is immediate.
2. $a \equiv b \pmod{I}$ if and only if $b \equiv a \pmod{I}$.
   - If $a - b \in I$ then $-(a - b) = b - a \in I$ since I is closed under additive inverses, and conversely if $b - a \in I$ then so is $-(b - a) = a - b$.
3. If $a \equiv b \pmod{I}$ and $b \equiv c \pmod{I}$, then $a \equiv c \pmod{I}$.
   - We are given $a - b \in I$ and $b - c \in I$, so since I is closed under addition, we see $(a - b) + (b - c) = a - c \in I$.

Quotient Rings, III

Proofs (continued):

4. If $a \equiv b \pmod{I}$ and $c \equiv d \pmod{I}$, then $a + c \equiv b + d \pmod{I}$.
   - We are given $a - b \in I$ and $c - d \in I$, so since I is closed under addition, $(a - b) + (c - d) = (a + c) - (b + d) \in I$.
5. If $a \equiv b \pmod{I}$ and $c \equiv d \pmod{I}$, then $ac \equiv bd \pmod{I}$.
   - We are given $a - b \in I$ and $c - d \in I$.
   - Then since I is closed under arbitrary left and right multiplication, $(a - b)c$ and $b(c - d)$ are also in I.
   - Hence $ac - bd = (a - b)c + b(c - d)$ is also in I since I is closed under addition.

Quotient Rings, IV

Now we can define residue classes:

Definition

If I is an ideal of the ring R, then for any $a \in R$ we define the residue class of a modulo I to be the set $\overline{a} = a + I = \{a + x : x \in I\}$. This set is the left coset of I (under the addition operation of R) represented by a.

- We will use the notation $\overline{a}$ and $a + I$ interchangeably. (The latter is intended to evoke the idea of "adding" a to the set I.)
- It follows from properties of cosets that two residue classes are either disjoint or identical and that they partition R: $\overline{a} = \overline{b}$ if and only if $a \equiv b \pmod{I}$ if and only if $a - b \in I$.

Quotient Rings, V

All that remains is to verify that the residue classes form a ring.

Theorem (Quotient Rings)

Let I be an ideal of the ring R. Then the collection of residue classes modulo I forms a ring, denoted R/I (read as "R mod I"), under the operations $\overline{a} + \overline{b} = \overline{a+b}$ and $\overline{a} \cdot \overline{b} = \overline{ab}$. (This ring is called the quotient ring of R by I.) If R is commutative then so is R/I, and likewise if R has a 1 then so does R/I.

The notation R/I is intended to emphasize the idea that I represents a single element (namely, $\overline{0}$) in the quotient ring R/I, and the other elements in R/I are "translates" of I. In this way, R/I is the ring obtained from R by "collapsing" or "dividing out" by I, whence the name "quotient ring".

Quotient Rings, V

Proof:

- The proof is essentially bookkeeping, and the only real content is to show that the operations are well-defined: that is, if we choose different elements $a' \in \bar{a}$ and $b' \in \bar{b}$, the residue class of $a' + b'$ is the same as that of $a + b$, and similarly for the product.
- To see this, if $a' \in \bar{a}$ then $a' \equiv a \pmod{I}$, and similarly if $b' \in \bar{b}$ then $b' \equiv b \pmod{I}$.
- Then $a' + b' \equiv a + b \pmod{I}$, so $\overline{a' + b'} = \overline{a + b}$. Likewise, $a'b' \equiv ab \pmod{I}$, so $\overline{a'b'} = \overline{ab}$.
- Thus, the operations are well-defined.

Quotient Rings, VI

Proof (continued):

- Now we just observe that the ring axioms are essentially inherited from R.
- For the ring axioms, we observe that associativity, commutativity, and the distributive laws follow immediately from the corresponding properties in R: the additive identity in R/I is $\overline{0}$, the multiplicative identity is $\overline{1}$, and the additive inverse of $\overline{a}$ is $\overline{-a}$.
- For example, we have $\overline{a} + \overline{b} = \overline{a+b} = \overline{b+a} = \overline{b} + \overline{a}$.

Summary

We discussed Tunnell's theorem on congruent numbers.

We introduced ideals of commutative rings and discussed some of their properties.

We defined quotient rings.

Next lecture: More with quotient rings, maximal and prime ideals.