## 1. Proof of Generalized CRT

I will begin with a definition of a **commutative ring with unity**. Don't worry about the name.

DEFINITION 0.1. A ring is a set $R$ with two binary operations $+$ and $\times$ with a few conditions:

(1) There exists a zero element $0 \in R$ so that for all $a \in R$, $a + 0 = a$. (This is just zero in the integers).
(2) For any $a, b \in R$, $a + b \in R$ (adding two things give you an object in the ring).
(3) FOr any $a, b \in R$, we get $a + b = b + a$.
(4) For any $a \in R$, there is a $b \in R$ so that $a + b = 0$. We write $b$ as $-a$ (there exists negative elements i.e. additive inverses).
(5) Addition is associative. That is, $(a + b) + c = a + (b + c)$.
(6) For any $a, b \in R$, $a \times b \in R$ (multiplication gives you something in the ring) (we will omit $\times$ if it is obvious).
(7) For $a, b, c \in R$, we get $a(b + c) = ab + ac$ (multiplication distrbutes over addition).

For a commutative ring with unit, we add two conditions.

(1) * For any $a, b \in R$, we get $ab = ba$ (the commutative part in commutative ring).
(2) * There exists a $1 \in R$ so that $a \times 1 = 1 \times a$ (the unity part of a ring).

EXAMPLE 0.2. Notice that $\mathbb{Z}$, the integers, form a commutative ring with unity. It has $0, 1 \in \mathbb{Z}$. Also, all of the other conditions make sense!

EXAMPLE 0.3. We will write $\mathbb{Z}/n\mathbb{Z}$ to be the integers modulo $n$.

For example, $\mathbb{Z}/3\mathbb{Z}$ is just the set $\{\bar{0}, \bar{1}, \bar{2}\}$. Addition in this follows your usual understanding of modular arithmetic.

$$\bar{0} + \bar{2} = \bar{2}, \quad \bar{2} + \bar{2} = \bar{1}, \quad \bar{2} + \bar{1} = \bar{0}.$$

Now, we come to something you are less familiar with.

DEFINITION 0.4. A subset $I \subseteq R$ of a ring is called an **ideal** if it satisfies certain properties.

(1) For any $a, b \in I$, $a + b \in I$.
(2) For any $r \in R$ and any $a \in I$, we have $ra \in I$.

EXAMPLE 0.5. The even numbers $2\mathbb{Z}$ form an ideal in $\mathbb{Z}$.

Notice that if we take any number in $2\mathbb{Z}$, say 8 and 16, we get $8 + 16 = 24$ which is also in $2\mathbb{Z}$.

If $3 \in \mathbb{Z}$ and $2 \in 2\mathbb{Z}$, we get $2 \times 3 = 6 \in 2\mathbb{Z}$.
More generally, if can be seen that $2\mathbb{Z}$ is an ideal!

Now, we define **modulo of a ring by an ideal**.

DEFINITION 0.6. If $I$ is an ideal of a commutative ring with unity $R$, $R/I$ is the ring where every element of $R$ that is in $I$ is set to 0. (This is informal).

EXAMPLE 0.7. Consider the example $\mathbb{Z}/3\mathbb{Z}$.
We know that 9 modulo 3 is 0. This is because $9 \in 3\mathbb{Z}$. What about 5? Well, $5 = 2 + 3$ and $3 \in 3\mathbb{Z}$. This forces 5 equal to 2 modulo 3 inside $\mathbb{Z}/3\mathbb{Z}$.

This motivates the next definition!

DEFINITION 0.8. We get a map $R \to R/I$ which sends elements of $R$ in the obvious way to elements of $R/I$.

EXAMPLE 0.9. We get a mapping $\mathbb{Z} \to \mathbb{Z}/8\mathbb{Z}$ defined by sending $a$ to $a \pmod 8$.

DEFINITION 0.10. A ring morphism $f : R \to S$ between rings $R$ and $S$ is a just a mapping preserving the ring structure. That is,

(1) $f(a + b) = f(a) + f(b)$
(2) $f(a \times b) = f(a) \times f(b)$.

EXAMPLE 0.11. Notice that $f : \mathbb{Z} \to \mathbb{Z}/8\mathbb{Z}$ preserves the ring structure!
For example, $f(8 + 3) = f(11) = 3$, but $f(8) + f(3) = 0 + 3 = 3$. Also, $f(8 \times 9) = f(72) = 0$ and $f(8) \times f(9) = 0 \times 1 = 0$.

DEFINITION 0.12. Two ideals $I$ and $J$ of a ring is said to be **comaximal** or **relatively prime** if $I + J$ is the whole ring.
Note: $I + J = \{i + j | i \in I, j \in J\}$.

EXAMPLE 0.13. An obvious example will be in the case of the integers $\mathbb{Z}$. The ideals $2\mathbb{Z}$ and $5\mathbb{Z}$ are comaximal (or 2 and 5 are relatively prime).
This is because $1 = (-2)2 + 5$ and $(-2)2 \in 2\mathbb{Z}$ and $5 \in 5\mathbb{Z}$. Now, this implies that $1 \in 2\mathbb{Z} + 5\mathbb{Z}$. Now, we can multiply 1 by anything in $\mathbb{Z}$. For example, $9 \times 1$. This implies that

$$9 = 9 \times 1 = 9((-2)2 + 5) = (-18)2 + 45.$$

So, $9 \in 2\mathbb{Z} + 5\mathbb{Z}$. Since we can really just multiply by anything $a$ and get $a \in 2\mathbb{Z} + 5\mathbb{Z}$, we conclude that $2\mathbb{Z} + 5\mathbb{Z} = \mathbb{Z}$!

I am sorry this last part, but we are going to do this part in with a few more definitions.

DEFINITION 0.14. If $R$ and $S$ are rings, $R \times S = \{(r, s) | r \in R, s \in S\}$ is a ring.

EXAMPLE 0.15. Take $\mathbb{Z}$ and $\mathbb{Z}$. Then $\mathbb{Z} \times \mathbb{Z}$ is just the set of ordered pairs! We define addition and multiplication component wise.

For example, $(2, 3) + (4, 9) = (6, 12)$ and $(2, 2) + (3, 7) = (6, 14)$.

DEFINITION 0.16. If $f : R \to S$, then $\ker f$ is called the kernel of the ring morphism. It is defined as "everything in $R$ that is sent to 0 in $S$". More formally

$$\ker f = \{r \in R | f(r) = 0\}.$$

Also, $\ker f$ is an ideal of $R$! Verify the conditions.

EXAMPLE 0.17. Look at $f : \mathbb{Z} \to \mathbb{Z}/8\mathbb{Z}$. What is the kernel? What is sent to zero?

It is everything in $8\mathbb{Z}$!

Now, you are going to have to take some faith in me when I make this claim.

THEOREM 0.18. *If $f : R \to S$ is a surjective ring morphism, then $R$ is the same as $S/\ker f$. (Surjective means that $S$ is small enough so that for every $s \in S$ there is a $r \in R$ so that $f(r) = s$).*

*More formally, $R$ is isomorphic to $S/\ker f$ (isomorphic/isomorphism just means there is a ring morphisms so that $R$ and $S/\ker f$ look essentially the same i.e. have the same ring structure).*

EXAMPLE 0.19. Again, look at $f : \mathbb{Z} \to \mathbb{Z}/8\mathbb{Z}$. This surjective. For example, if we have $\overline{3} \in \mathbb{Z}/8\mathbb{Z}$, then $11 \in \mathbb{Z}$ is such that $f(11) = 3$.

The kernel $\ker f$ was conclude to be just $8\mathbb{Z}$. So, applying the previous theorem, $R = \mathbb{Z}$ and $\ker f = 8\mathbb{Z}$, we actually have $\mathbb{Z}/8\mathbb{Z}$ is the same as $\mathbb{Z}/8\mathbb{Z}$!

THEOREM 0.20 (Number Theoretic CRT Simple Case). *If $m\mathbb{Z}$ and $n\mathbb{Z}$ are ideals of $\mathbb{Z}$, $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$ i.e. are comaximal, then we get an isomorphism*

$$\mathbb{Z}/(mn\mathbb{Z}) \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

PROOF. My proof here is a bit informal.

We have define $f : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ as follows,

$$a \mapsto (a \pmod m, a \pmod n).$$

This can be checked to be a ring morphism and that it is well-defined i.e. if $a = b$, then the get mapped to the same thing.

We want to apply Theorem 0.18 to get the isomorphism. So, we need to figure out what the kernel is. What element gets sent to $(0 \pmod m, a \pmod n) = (\overline{0}, \overline{0})$? This comes down to solving the congruence

$$z \equiv 0 \mod m, \text{ and } z \equiv 0 \mod n$$

for $z$. Well, clearly, $z$ has to be a multiple of both $m$ and $n$! But a multiple of both $m$ and $n$ is an element of both $m\mathbb{Z}$ and $n\mathbb{Z}$. That is, $z$ must be in $m\mathbb{Z} \cap n\mathbb{Z}$! Also, $n\mathbb{Z} \cap m\mathbb{Z} = nm\mathbb{Z}$.

So, by Theorem 0.18, we get

$$\mathbb{Z}/(mn\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

an isomorphism! □

Remark: You might find it strange I didn't use the comaximal condition $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$ in the proof! It is actually very subtle. We know we *need* the condition since if not, we get an easy counter example.

Take $2\mathbb{Z}$ and $4\mathbb{Z}$. Obviously, $2\mathbb{Z} + 4\mathbb{Z} = 2\mathbb{Z}$ so they are not comaximal. Also, $2\mathbb{Z} \cap 4\mathbb{Z} = 2\mathbb{Z}$. However, it is obvious that $\mathbb{Z}/2\mathbb{Z}$ is not eh same thing as $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$!

The subtlety is when I said $n\mathbb{Z} \cap m\mathbb{Z} = nm\mathbb{Z}$! If two ideals $I$ and $J$ are not comaximal, we cannot conclude that $I \cap J = IJ$. At best, we get $I \cap J \subseteq IJ$!

THEOREM 0.21. *Knowing the Number Theoretic Simple Case, we can quickly get the general case!*

*If $n_1\mathbb{Z}, \ldots, n_j\mathbb{Z}$ are ideals of $\mathbb{Z}$ so that they are pairwise comaximal i.e. $n_i\mathbb{Z} + n_k\mathbb{Z} = \mathbb{Z}$ for any $n_i, n_k$, then we get an isomorphism*

$$\mathbb{Z}/(n_1 n_2 \ldots n_j\mathbb{Z}) \to \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_j\mathbb{Z}.$$

Remark: This gives you the solving of the congruence $x \equiv 122 \pmod{233}$, $x \equiv 141 \pmod{233}$, and $x \equiv 9 \pmod{199}$.

Also, without really doing much more work, we **come to the general case in Commutative Ring Theory**.

THEOREM 0.22. *If $I_1, \ldots, I_n$ are ideals of a commutative ring with unity $R$, and the $I_i$'s are pairwise comaximal, we get an isomorphism*

$$R/(I_1 I_2 \ldots I_n) \cong R/I_1 \times R/I_2 \times \cdots \times R/I_n.$$