MODULAR ARITHMETIC

TIM SMITS

The integers $\mathbb{Z}$ are our first example of a ring. Our goal is to now construct a finite ring of size n for any $n > 1$, $\mathbb{Z}/n\mathbb{Z}$.

Some set theory

Before beginning the construction, we'll first review some set theory.

Definition 0.1. A (binary) **relation** R between sets X and Y is is a subset of $X \times Y$. If $X = Y$ we say that R is a relation on X. If $(x, y) \in R$, we write $x \sim y$ and say that x relates to y.

The way to interpret the relation is that R is the set of values where $x \sim y$ is true.

Example 0.2. Let $X = Y = \{0, 1, 2, 3\}$. Define the relation $R = \{(0, 0), (1, 1), (2, 2), (3, 3)\}$. This is the relation $=$, e.g. since $1 = 1$ we have $(1, 1) \in R$.

Example 0.3. With $R = \{(0, 0), (0, 1), (0, 2), (0, 3), (1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3)\}$ and $X = Y = \{0, 1, 2, 3\}$ as above, then R is the relation $\leq$.

Definition 0.4. Let $\sim$ be a relation on a set S. Then $\sim$ is called an **equivalence relation** if the following conditions hold:

1. (Reflexive) $x \sim x$ for all $x \in S$
2. (Symmetric) For all $x, y \in S$, if $x \sim y$ then $y \sim x$
3. (Transitive) For all $x, y, z \in S$, if $x \sim y$ and $y \sim z$ then $x \sim z$.

A relation $\sim$ is called reflexive, symmetric, or transitive if it satisfies the respective conditions above. Familiar examples of equivalence relations include $=$ on $\mathbb{R}$, and similarity of matrices in $M_n(F)$ for a field F.

Definition 0.5. Let $\sim$ be a relation on S. The **conjugacy class** of an element $a \in S$, denoted $[a]$ (or $\overline{a}$), is defined by $[a] = \{b \in S : b \sim a\}$. An element a' is called a **representative** of $[a]$ if $a' \in [a]$.

Equivalences relations are nice because they give a partition of S into the different conjugacy classes under $\sim$.

Proposition 1. *Let $\sim$ be an equivalence relation on S. For two conjugacy classes $[a]$ and $[b]$, either $[a] = [b]$ or $[a] \cap [b] = \emptyset$.*

Proof. Note that because $\sim$ is reflexive, for any $a \in S$, $[a]$ is non-empty. Pick conjugacy clases $[a]$ and $[b]$ of S. First, suppose that $a \sim b$. If $x \in [a]$ by definition $x \sim a$, and since $a \sim b$ we have $x \sim b$ by transitivity. Therefore $x \in [b]$, giving $[a] \subseteq [b]$. Similarly, $[b] \subseteq [a]$ so $[a] = [b]$. Now if $a \not\sim b$, suppose for contradiction that $[a] \cap [b] \neq \emptyset$. Then pick $x \in [a] \cap [b]$, so by definition $x \sim a$ and $x \sim b$, so $a \sim b$ by symmetry and transitivity, a contradiction. Therefore, $[a] \cap [b] = \emptyset$. $\square$

Proposition 2. *Let $\sim$ be an equivalence relation on S. Then $S = \bigcup_{a \in S}[a]$.*

Proof. Let $s \in S$. Then $s \sim s$ by reflexivity, so $s \in [s] \subseteq \bigcup_{a \in S}[a]$. Therefore, $S \subseteq \bigcup_{a \in S}[a]$. If $s \in \bigcup_{a \in S}[a]$, then $s \in [a]$ for some $a \in S$. However, $[a] \subset S$, so $s \in S$ giving $\bigcup_{a \in S}[a] \subseteq S$. □

It's worth pointing out that since two conjugacy classes $[a]$ and $[b]$ are either equal or disjoint, we can refine the above union to a disjoint union by just taking it over the distinct conjugacy classes.

Construction of $\mathbb{Z}/n\mathbb{Z}$

The key to our construction will be the fact that the integers have division with remainder.

Theorem 0.6 (Division algorithm)**.** *Let a and b be integers with $b > 0$. Then there exist unique integers q and r such that $a = bq + r$ with $0 \leq r < b$.*

Fix an integer $n > 1$ and define a relation on $\mathbb{Z}$ as follows: $a \sim_n b \iff n \mid (a - b)$.

Proposition 3. *The relation $\sim_n$ as defined above is an equivalence relation on $\mathbb{Z}$.*

Proof. For $a \in \mathbb{Z}$, we have $a \sim_n a$ because $n \mid 0$. If $a \sim_n b$, then $n \mid (a - b)$ so $n \mid (b - a)$, because $b - a = (-1)(a - b)$ giving $b \sim_n a$. If $a \sim_n b$ and $b \sim_n c$, then $n \mid (a - b)$ and $n \mid (b - c)$. We then have that $n \mid (a - b) + (b - c) = a - c$, so $a \sim_n c$, so that $\sim_n$ is an equivalence relation as desired.

□

The set theory above says that $\sim_n$ gives a partition of the integers into disjoint sets, and for an integer a we have $[a] = \{\ldots, a-2n, a-n, a, a+n, a+2n, \ldots\}$, the set of integers that differ from a by a multiple of n. The division algorithm tells us that any integer a is of the form $a = qn + r$ with $0 \leq r \leq n - 1$, i.e. that $a \sim r$ for some r with $0 \leq r \leq n - 1$. In other words, $\mathbb{Z} = \bigsqcup_{i=0}^{n-1}[i]$.

Let $\mathbb{Z}/n\mathbb{Z} = \{[0], \ldots, [n-1]\}$ be the set of equivalence classes under $\sim_n$. We define addition and multiplication operations on $\mathbb{Z}/n\mathbb{Z}$ by $[a] + [b] = [a + b]$ and $[a] \cdot [b] = [ab]$. Notationally, we use the convention that the conjugacy class $[a]$ is written as $a \bmod n$, and if $a \sim_n b$ then we write $a \equiv b \bmod n$. Using this new notation, the above operations are $(a \bmod n) + (b \bmod n) = (a + b) \bmod n$ and $(a \bmod n) \cdot (b \bmod n) = ab \bmod n$. We'll use both notations fairly often, so make sure both make sense!

Proposition 4. *The operations $+$ and $\cdot$ as defined above are well defined, i.e. do not depend on the choice of representative in the conjugacy class.*

Proof. To check the operation is well defined, we must show that if $a \bmod n = a' \bmod n$ and $b \bmod n = b' \bmod n$, then $a + b \bmod n = a' + b' \bmod n$. Translating this into a statement using the definition of $\sim_n$, we want to show that if $a \equiv a' \bmod n$ and $b \equiv b' \bmod n$, that $a + b \bmod n \equiv a' + b' \bmod n$. If $a \equiv a' \bmod n$, then by definition we have $n \mid (a - a')$, and similarly we have $n \mid (b - b')$. Then $a' = a + kn$ and $b' = b + \ell n$ for some integers k and ℓ. Adding shows that $a' + b' = a + b + n(k + \ell)$, so $a + b \equiv a' + b' \bmod n$. Similarly for multiplication, we have $a'b' = (a+kn)(b+n\ell) = ab+n(a\ell+bk+nk\ell)$, so $a'b' \equiv ab \bmod n$. □

Definition 0.7. The set $\mathbb{Z}/n\mathbb{Z}$ with the operations of $+$ and $\cdot$ as defined above is called the **integers modulo n**.

The proposition above says that addition and multiplication do not depend on the choice of representatives for the conjugacy classes of $\mathbb{Z}/n\mathbb{Z}$. We may as well take the integers $0, 1, \ldots, n-1$ to be representatives of the conjugacy classes of $0 \bmod n, \ldots, n-1 \bmod n$, although we'll see in a little bit that sometimes it's more convenient to pick different representatives. As the operations of addition and multiplication are very closely tied to the usual addition and multiplication of integers, it should be fairly unsurprising that many of the same properties carry over to $\mathbb{Z}/n\mathbb{Z}$:

Proposition 5. *The operations $+$ and $\cdot$ on $\mathbb{Z}/n\mathbb{Z}$ satisfy the following properties for any $a, b, c \in \mathbb{Z}$:*

1. $a + b \equiv b + a \bmod n$ *and* $ab \equiv ba \bmod n$.
2. $(a + b) + c \equiv a + (b + c) \bmod n$ *and* $a(bc) \equiv (ab)c \bmod n$.
3. $a(b + c) \equiv ab + ac \bmod n$.
4. $a + 0 \equiv a \bmod n$.
5. $a + (n - a) \equiv 0 \bmod n$.
6. $a \cdot 1 \equiv a \bmod n$.

Proof. Exercise. □

Arithmetic in $\mathbb{Z}/n\mathbb{Z}$

Before doing anything else, it will be helpful to familiarize ourselves with how arithmetic in $\mathbb{Z}/n\mathbb{Z}$ works.

Example 0.8. $a \equiv 0 \bmod n$, is equivalent to saying that $n \mid a$, i.e. $a = nk$ for some integer k.

Example 0.9. In $\mathbb{Z}/6\mathbb{Z}$, we have $20 \equiv 2 \bmod 6$ because $20 = 2 + 3 \cdot 6$. In $\mathbb{Z}/11\mathbb{Z}$, $-20 \equiv 13 \bmod 11$ because $-20 = 13 - 3 \cdot 11$. Similarly, $13 \bmod 11 \equiv 2 \bmod 11$.

Example 0.10. In $\mathbb{Z}/17\mathbb{Z}$, $15 + 7 \bmod 17 \equiv 22 \bmod 17 \equiv 5 \bmod 17$ because $22 = 1 \cdot 17 + 5$. We have $15 \cdot 7 \bmod 17 \equiv 105 \bmod 17 \equiv 3 \bmod 17$ because $105 = 6 \cdot 17 + 3$.

Example 0.11. To compute $a \bmod n$, add or subtract multiples of n to a (since this does not affect the value of $a \bmod n$) until you reduce to something you can handle. For example, to compute $-533 \bmod 7$, add 700 to -533 and then subtract 140 from 167 to get $-533 \bmod 7 \equiv 167 \bmod 7 \equiv 27 \bmod 7 \equiv 6 \bmod 7$.

Example 0.12. For every integer n, we have $n \equiv 0 \bmod 2$ or $n \equiv 1 \bmod 2$. Saying $n \equiv 0 \bmod 2$ is the same as saying $n = 2k$ for some k, i.e. n is even and $n \equiv 1 \bmod 2$ is the same as saying $n = 2\ell + 1$ for some ℓ, i.e. n is odd. Notice that $a \equiv b \bmod 2$ if and only if a and b have the same parity.

Example 0.13. To carry out arithmetic quickly, it may be helpful to change the representatives of conjugacy classes. In $\mathbb{Z}/7\mathbb{Z}$, we have $16 \cdot 3 \bmod 7 \equiv 48 \bmod 7 \equiv -1 \bmod 7 \equiv 6 \bmod 7$. One could first reduce $16 \bmod 7 \equiv 2 \bmod 7$ to conclude $16 \cdot 3 \bmod 7 \equiv 2 \cdot 3 \bmod 7 \equiv 6 \bmod 7$.

Example 0.14. To compute $10^4 \bmod 19$, instead of computing 10^4 and then reducing mod 19, it's easier to compute success powers and reduce as you go along: $10^4 \bmod 19 \equiv (100)^2 \bmod 19 \equiv 5^2 \bmod 19 \equiv 6 \bmod 19$.

Solving $ax \equiv b \bmod n$

Perhaps one of the most basic questions we can ask about $\mathbb{Z}/n\mathbb{Z}$ is how to solve linear equations of the form $[a][x] = [b]$. This is a subtle question however, since the structure of $\mathbb{Z}/n\mathbb{Z}$ is different for different values of n.

Example 0.15. In $\mathbb{Z}/4\mathbb{Z}$, we have $2 \cdot 2 \equiv 0 \bmod 4$, however $2 \not\equiv 0 \bmod 4$. This says that $\mathbb{Z}/n\mathbb{Z}$ does not have the zero product property.

Example 0.16. In $\mathbb{Z}/5\mathbb{Z}$, every non-zero element has a multiplicative inverse: $1 \cdot 1 \equiv 1 \bmod 5$, $2 \cdot 3 \equiv 3 \cdot 2 \equiv 1 \bmod 5$, and $4 \cdot 4 \equiv 1 \bmod 5$. This says that $\mathbb{Z}/5\mathbb{Z}$ is a field!

We introduce some new terminology to talk about the structural differences:

Definition 0.17. An element $[a] \in \mathbb{Z}/n\mathbb{Z}$ is called a **unit** if $[a]$ has a multiplicative inverse, i.e. there is $[b] \in \mathbb{Z}/n\mathbb{Z}$ such that $[a][b] = [1]$. An element $[a] \in \mathbb{Z}/n\mathbb{Z}$ is called a **zero divisor** if $[a] \neq [0]$ and there is non-zero $[b] \in \mathbb{Z}/n\mathbb{Z}$ such that $[a][b] = [0]$. The set of units in $\mathbb{Z}/n\mathbb{Z}$ is denoted by $(\mathbb{Z}/n\mathbb{Z})^\times$.

Notice that because every element of $\mathbb{Z}/5\mathbb{Z}$ has a multiplicative inverse, if $[a][b] = [0]$ in $\mathbb{Z}/5\mathbb{Z}$, multiplying by said inverse says that $[b] = [0]$, i.e. $[a]$ is *not* a zero divisor. We can then distinguish $\mathbb{Z}/5\mathbb{Z}$ from $\mathbb{Z}/4\mathbb{Z}$ (apart from the obviously different number of elements) by noting that $\mathbb{Z}/4\mathbb{Z}$ has zero divisors, while $\mathbb{Z}/5\mathbb{Z}$ does not. Our first order of business is to figure out what the possible units of $\mathbb{Z}/n\mathbb{Z}$ are.

Theorem 0.18. *Let $[a] \in \mathbb{Z}/n\mathbb{Z}$. Then $[a]$ is a unit if and only if $(a, n) = 1$.*

Proof. The proof is largely just understanding what the above statement actually means. Saying that $[a]$ is a unit in $\mathbb{Z}/n\mathbb{Z}$ is the same thing as saying that $[a][b] = [1]$ for some $[b] \in \mathbb{Z}/n\mathbb{Z}$. By definition, this means that $ab \equiv 1 \bmod n$, so that there is some integer k with $nk = ab - 1$. This says that $ab + n(-k) = 1$, so clearly this means that $(a, n) = 1$. Conversely, if $(a, n) = 1$ then by Bezout's lemma there are integers x, y with $ax + ny = 1$. Taking this equation mod$n$ says that $ax \equiv 1 \bmod n$, i.e. $[a][x] = [1]$ in $\mathbb{Z}/n\mathbb{Z}$. □

This theorem is rather simple, but it has important consequences:

Corollary 0.19. *$\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is prime. In particular, $\mathbb{Z}/n\mathbb{Z}$ has the zero product property if and only if n is prime.*

Proof. $\mathbb{Z}/n\mathbb{Z}$ satisfies all but one of the field axioms by construction, the exception being all non-zero elements having a multiplicative inverse. This happens if and only if all non-zero elements are units, i.e. $(a, n) = 1$ for $1 < a < n$. This happens if and only if n is prime. If n is a prime, then $[a][b] = [0]$ says $[b] = [0]$ after multiplying by $[a]^{-1}$. If n is composite, write $n = ab$ for some integers a, b so that $[a][b] = [0]$ in $\mathbb{Z}/n\mathbb{Z}$, so that $\mathbb{Z}/n\mathbb{Z}$ does not have the zero product property. □

By classifying all the units of $\mathbb{Z}/n\mathbb{Z}$, we've determined the special linear equation $[a][x] = [1]$ in $\mathbb{Z}/n\mathbb{Z}$ has a solution if and only if $[a]$ is invertible in $\mathbb{Z}/n\mathbb{Z}$. This then says the (unique) solution is given by $[x] = [a]^{-1}$. The general case is very similar:

Theorem 0.20. *Let $d = (a, n)$. The equation $[a][x] = [b]$ is solvable in $\mathbb{Z}/n\mathbb{Z}$ if and only if $d \mid b$. The solutions are of the form $[x_0 + kn/d]$ for $0 \leq k \leq d - 1$, where $[x_0]$ is any solution.*

Proof. Saying that $[a][x] = [b]$ in $\mathbb{Z}/n\mathbb{Z}$ is the same as saying that $ax \equiv b \bmod n$, i.e. there is some integer ℓ with $n\ell = ax - b$, or that $ax + n(-\ell) = b$. Certainly for this to be true, we must have that $d \mid b$. Now suppose that $d \mid b$. By Bezout, we can write $ax + by = d$ for some integers x, y. Suppose that $b = dm$ for some integer m. Then multiplying this equation by m says that $a(mx) + n(my) = b$, so taking this mod n says that $[a][mx] = [b]$, i.e. the equation is solvable.

We now classify the solutions. Suppose that $[x_0]$ is a solution to $[a][x] = [b]$. Then $[x_0 + kn/d]$ for $0 \leq k \leq d-1$ is also a solution, because $[a][x_0 + kn/d] = [ax_0 + akn/d] = [ax_0]$ because $n \mid akn/d$. Now we show that any such solution has this form. Let $[x_0]$ be a solution and $[x]$ any other solution. Then $[a][x] = [a][x_0]$ says that $[a(x - x_0)] = [0]$, i.e. $a(x - x_0) = n\ell$ for some integer ℓ. Dividing out by d says that $\frac{a}{d}(x - x_0) = \ell\frac{n}{d}$, and because $(\frac{a}{d}, \frac{n}{d}) = 1$, this says that $\frac{n}{d} \mid x - x_0$, i.e. $x = x_0 + t\frac{n}{d}$ for some integer t. The final observation is that if $t \equiv k \bmod d$ for some $0 \leq k \leq d - 1$, then $t\frac{n}{d} \equiv k\frac{n}{d} \bmod n$, so that $x \equiv x_0 + k\frac{n}{d} \bmod n$, where $0 \leq k \leq d - 1$, i.e. $[x] = [x_0 + k\frac{n}{d}]$ for some $0 \leq k \leq d - 1$. □

As the above theorem shows, once we find a single solution, we know what all solutions are. To find an initial solution, we can run the Euclidean algorithm backwards.

Example 0.21. Suppose we want to solve $[72][x] = [1]$ in $\mathbb{Z}/89\mathbb{Z}$. It's clear that $(72, 89) = 1$, so that the unique solution is given by $[x] = [72]^{-1}$. To compute the inverse, running the Euclidean algorithm backwards says that $1 = 89 \cdot 17 + 72 \cdot (-21)$, so taking this mod 89 says $72 \cdot (-21) \equiv 1 \bmod 89$. Since $-21 \equiv 68 \bmod 89$, we see that $[72]^{-1} = [68]$ is the solution.

Example 0.22. Suppose we want to solve $[42][x] = [12]$ in $\mathbb{Z}/78\mathbb{Z}$. We see that $(42, 78) = 6$, so there are a total of 6 different solutions, which we can list once we have found one. Saying that $[42][x] = [12]$ in $\mathbb{Z}/78\mathbb{Z}$ is the same thing as finding integers x, y such that $42x + 78y = 12$. Running the Euclidean algorithm backwards says that $6 = 42 \cdot 2 + 78 \cdot (-1)$, so $12 = 42 \cdot 4 + 78 \cdot (-2)$. Taking this mod 78 says that $42 \cdot 4 \equiv 12 \bmod 78$, so that $[4]$ is a solution. We then find that the solutions are $[4], [17], [30], [43], [56], [69]$.

Systems of congruence equations

Now that we know how to solve linear equations in $\mathbb{Z}/n\mathbb{Z}$, the next natural question is how to solve *systems* of linear equations in $\mathbb{Z}/n\mathbb{Z}$. From linear algebra, we know that a system of k linear equations in m variables in $\mathbb{Z}/n\mathbb{Z}$ is the same thing as a matrix equation of the form $Ax = b$ where $A \in M_{k\times m}(\mathbb{Z}/n\mathbb{Z})$ and $x, b \in (\mathbb{Z}/n\mathbb{Z})^k$. If $n = p$ is a prime, then the theory of abstract linear algebra over fields tells us all we need to know about how to solve such equations, and therefore how to solve systems of linear equations in $\mathbb{Z}/p\mathbb{Z}$. When n is not prime, $\mathbb{Z}/n\mathbb{Z}$ is not a field, and the theory of linear algebra breaks down completely. In general, solving systems of equations in $\mathbb{Z}/n\mathbb{Z}$ is quite hard.

The next best thing we can do is work with systems of *congruences*, where instead of trying to solve k linear equations in m unknowns in $\mathbb{Z}/n\mathbb{Z}$ we try and solve k linear equations in one unknown by varying the modulus.

Theorem 0.23. *Let $(m, n) = 1$. Then the system of congruences*

$$x \equiv a \bmod m$$
$$x \equiv b \bmod n$$

has a unique solution in $\mathbb{Z}/mn\mathbb{Z}$.

Proof. Suppose a solution exists. Since $x \equiv a \bmod m$, we can write $x = a + mk$ for some integer k. Plugging this into the second equation, $a + mk \equiv b \bmod n$ says that $mk \equiv b - a \bmod n$. Since $(m, n) = 1$, we have that $[m]$ is a unit mod n so $k \equiv t(b - a) \bmod n$, where t is a representative of $[m]^{-1}$. Translating back into a statement about integers, we have $k = t(b - a) + n\ell$ for some ℓ, so that $x = a + m(t(b - a) + n\ell) = a + mt(b - a) + nm\ell$, so that $x \equiv a + mt(b - a) \bmod mn$. This says any solution must look like this, and note that this certainly is a solution to the above system of congruences, so now we need only show there is a single solution of this type. Since a, b, m are fixed, the only thing to do is to check that our choice of t doesn't matter. If t' is any other representative of $[m]^{-1}$, then $t' = t + ny$ for some integer y, so running the same argument with t' instead of t says that $x = a + m(t + ny)(b - a) + nm\ell$, which still gives $x \equiv a + mt(b - a) \bmod mn$, so this is the only solution modulo mn. □

Note that this proof *explicitly* tells us the solution!

Example 0.24. Suppose we wish to solve the system of congruences

$$x \equiv 5 \bmod 6$$
$$x \equiv 3 \bmod 35$$

The above theorem tells us that there is a unique solution in $\mathbb{Z}/210\mathbb{Z}$, given by $x \equiv 5 - 12t \bmod 210$, where t is a representative of $[6]^{-1}$ in $\mathbb{Z}/35\mathbb{Z}$. By inspection, we see that $[6]^{-1} = [6]$, so we may choose $t = 6$ to get $x \equiv -67 \bmod 210 \equiv 143 \bmod 210$ as the solution.

Of course, trying to remember a formula to solve a system is not a very good technique. Let's see how you would solve this by hand, in practice. The first equation says $x = 5 + 6k$ for some $k \in \mathbb{Z}$. Plugging into the second equation, we have $5 + 6k \equiv 3 \bmod 35$, so $6k \equiv 33 \bmod 35$. Since 6 is invertible mod 35 with inverse given by $6 \bmod 35$, we see $k \equiv 33 \cdot 6 \equiv 23 \bmod 35$, so $k = 23 + 35\ell$ for some $\ell \in \mathbb{Z}$. Plugging back in, we find $x = 5 + 6(23 + 35\ell) = 143 + 210\ell$, i.e. $x \equiv 143 \bmod 210$.

In more algebraic language, we can restate the above theorem as follows:

Theorem 0.25. *Let* $(m, n) = 1$. *There is a bijection* $\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ *given by* $x \bmod mn \to (x \bmod m, x \bmod n)$. *The inverse map is given by* $(a \bmod m, b \bmod n) \to a + mt(b - a) \bmod mn$ *where* t *is any representative of* $[m]^{-1}$ *in* $\mathbb{Z}/n\mathbb{Z}$.

The map above is stronger than just a bijection. If we let φ denote the map from $\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, then φ has the property that $\varphi([x] + [y]) = \varphi([x]) + \varphi[y])$ and $\varphi([x][y]) = \varphi([x])\varphi([y])$, so that it preserves the additive and multiplicative structure of both sides. This is our first example of a *ring isomorphism*, which will be one of our basic objects of study when we discuss arbitrary rings. By factoring $n = p_1^{e_1} \cdots p_k^{e_k}$ into a product of primes, we get the following more general result:

Theorem 0.26 (Chinese Remainder Theorem)**.** *Write* $n = p_1^{e_1} \cdots p_k^{e_k}$ *as a product of primes. Then* $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{e_k}\mathbb{Z}$ *via the ring isomorphism* $x \bmod n \to (x \bmod p_1^{e_1}, \ldots, x \bmod p_k^{e_k})$.

Proof. Theorem 0.25 says the map $f : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is a bijection. It's easy to see that f is also a ring homomorphism (and therefore an isomorphism), because of the

definitions of addition and multiplication in the product ring. To prove the Chinese Remainder Theorem, we induct on the number of distinct prime factors k of n. If $k = 1$, there is nothing to show. Now suppose that the theorem is true for any integer with $k-1$ prime factors. Note that $p_1^{e_1} \cdots p_k^{e_k} = p_1^{e_1}(p_2^{e_2} \cdots p_k^{e_k})$, so $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p^{e_1}\mathbb{Z} \times \mathbb{Z}/p_2^{e_2} \cdots p_k^{e_k}\mathbb{Z}$ via the map $x \bmod n \to (x \bmod p_1^{e_1}, x \bmod p_2^{e_2} \cdots p_k^{e_k})$ by applying theorem 0.25. By induction hypothesis, $\mathbb{Z}/p_2^{e_2} \cdots p_k^{e_k}\mathbb{Z} \cong \mathbb{Z}/p_2^{e_2}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_k^{e_k}\mathbb{Z}$ via the map $x \bmod p_2^{e_2} \cdots p_k^{e_k} \to (x \bmod p_2^{e_2}, \ldots, x \bmod p_k^{e_k})$. The composition of ring isomorphisms $x \bmod n \to (x \bmod p_1^{e_1}, x \bmod p_2^{e_2} \cdots p_k^{e_k}) \to (x \bmod p_1^{e_1}, (x \bmod p_2^{e_2}, \ldots, x \bmod p_k^{e_k})) \to (x \bmod p_1^{e_1}, \ldots, x \bmod p_k^{e_k})$ is the map $x \bmod n \to (x \bmod p_1^{e_1}, \ldots, x \bmod p_k^{e_k})$. This is still an isomorphism because the composition of isomorphisms remains an isomorphism. Therefore, the theorem is true for any integer with k prime factors as well. By induction, it's therefore true for all integers $n > 1$. □

In the language of congruences, this says there is a unique solution in $\mathbb{Z}/n\mathbb{Z}$ to the system of congruences $x \equiv a_i \bmod p_i^{e_i}$ for $1 \leq i \leq k$.

Example 0.27. Suppose we wish to solve the system of congruences

$$x \equiv 1 \bmod 8$$
$$x \equiv 3 \bmod 9$$
$$x \equiv 2 \bmod 5$$

We solve the system by solving it in pairs. First, we solve the system $x \equiv 1 \bmod 8$ and $x \equiv 3 \bmod 5$. This has solution given by $x \equiv 57 \bmod 72$ using the method from before. We then need to solve the system $x \equiv 57 \bmod 72$ and $x \equiv 2 \bmod 5$, which has solution $x \equiv 57 \bmod 360$.

The Chinese Remainder Theorem has very important number theoretic consequences: understanding the ring $\mathbb{Z}/n\mathbb{Z}$ is the same thing as understanding the rings $\mathbb{Z}/p_i^{e_i}\mathbb{Z}$ where $n = p_1^{e_1} \cdots p_k^{e_k}$. Therefore, one really only needs to understand the structure of the rings $\mathbb{Z}/p^e\mathbb{Z}$ for p prime and $e \geq 1$. Often times, one can deduce facts about $\mathbb{Z}/p^e\mathbb{Z}$ by first working in $\mathbb{Z}/p\mathbb{Z}$ and then inductively working up to $\mathbb{Z}/p^e\mathbb{Z}$, therefore making $\mathbb{Z}/p\mathbb{Z}$ the "most important" one of these rings to study.

There is a very important philosophy in number theory, the so called "local-global principle", based on the idea that if one knows information mod p for all primes p, then the Chinese Remainder Theorem should allow one to "glue" this information to gain information back in $\mathbb{Z}$. the simplest illustration is the following:

Proposition 6. *Suppose that $x \in \mathbb{Z}$ and $x \equiv 0 \bmod p$ for all prime p. Then $x = 0$.*

Proof. If $x \neq 0$, then we can write $x = p_1^{e_1} \ldots p_k^{e_k}$ as a product of primes. Then for $p \neq p_i$, we have $x \not\equiv 0 \bmod p$, a contradiction. □

The next example is too difficult to prove with the tools that we will have available to use, but still illustrates the principle nicely:

Theorem 0.28. *Let $x \in \mathbb{Z}$ and suppose that $[x]$ is a square in $\mathbb{Z}/p\mathbb{Z}$ for all prime p. Then x is a square in $\mathbb{Z}$.*