Contents

Chapter 1

Unique Factorization

1.1 Unique Factorization in $\mathbb{Z}$

We say that a divides b if there is some c s.t. $b = ac$—we write $a \mid b$. A **prime** number is whose only divisors are 1 and p. Of great interest is the function $\pi(x)$—which outputs the number of primes between 1 and x.

Theorem 1. True facts about dividing

1. $a \mid a$ for $a \neq 0$.
2. If $a \mid b$ and $b \mid a$, then $a = \pm b$
3. If $a \mid b, b \mid c$, then $a \mid c$
4. If $a \mid b, a \mid c$, then $a \mid \alpha b + \beta c$

Definition (ord_p)**.** Let $n \in \mathbb{Z}$, p a prime. Then $\text{ord}(n) = a$ where a is the largest integer such that $p^a \mid n$ but $p^{a+1} \nmid n$. Define $\text{ord}(0) = \infty$.

ord gives the number of times that p divides n—the power of p in n's prime decomposition. On that note, every $n \in \mathbb{Z}$ has a unique prime decomposition:

Theorem 2. For every nonzero $n \in \mathbb{Z}$, there is a prime decomposition

$$n = (-1)^{\varepsilon(n)} \prod_p p^{a(p)}$$

with the exponents uniquely determined by n. In fact, we have that $a(p) = \text{ord}\, n$.

See that it must be the case that all but finitely many of $a(p)$ must be 0—or else we have some problems with n. The fact that $\mathbb{Z}$ is a PID plays nicely with the following definition

Definition (GCD)**.** Let $a, b \in \mathbb{Z}$. An integer d is called the gcd of a and b if every other common divisor of a and b divides d

You can use theorem 1 to show that the gcd is determined up to sign—so we can speak of *the* gcd. Even better (if you know some rings) is the following

Lemma 1. *Let $a, b \in \mathbb{Z}$. If $(a, b) = (d)$, then d is the gcd of a and b.*

We say that a, b are **relatively prime** is their only common divisors are ± 1. It is worth noting that if $a|bc$ and $(a, b) = 1$ (where (a, b) denotes the gcd), then it must be the case that $a|c$. This has two important consequences

Corollary 1. *If p is prime and $p|bc$, then either $p|b$ or $p|c$. (notice the hook into prime ideals)*

Corollary 2. *For p prime and $a, b \in \mathbb{Z}$, $\operatorname{ord} ab = \operatorname{ord} a + \operatorname{ord} b$.*

1.2 Unique Factorization in $k[x]$

This section retells the story of section 1 but in the case of a polynomial ring over a field — nothing to note if I'm being honest.

1.3 Unique Factorization in a PID

Definition (Euclidean Domain)**.** If R is a commutative domain, it is a Euclidean domain if there is a function $\lambda : R^+ \to \mathbb{N} \cup \{0\}$ such that if $a, b \in R, b \neq 0$, then there exists $c, d \in R$ with the property that $a = cb + d$ and either $d = 0$ or $\lambda(d) < \lambda(b)$.

Both $\mathbb{Z}$ and $k[x]$ (for k a field) are EDs. In $\mathbb{Z}$ we can use the standard absolute value function. For $p \in k[x]$, use $\lambda(p) = \deg(p)$.

In particular, it can be proven that every ED is a PID—the converse is not true but there aren't many readily available examples. Because of this nice structure, we inherit the same notion of divisibility. We say an element $u \in R$ is a **unit** if $u|1$—i.e. units have a mult. inverse. Two elements $a, b \in R$ are **associate** if $a = bu$ for some unit u. An element $p \in R$ is **irreducible** if $a|p$ means that a is a unit or an associate of p. A nonunit $p \in R$ is prime if $p \neq 0$ and $p|ab \implies p|a$ or $p|b$. Whiles these seem different, in a general PID we have that prime $\Leftrightarrow$ irreducible.

As seen in the previous two sections, our theory becomes richer when we utilize the language of ideals. Indeed, $a \mid b \Leftrightarrow (b) \subset (a)$, $u \in R$ is a unit $\Leftrightarrow (u) = R$ (since u has a multiplicative inverse), a, b are associate $\Leftrightarrow (a) = (b)$ (simply multiply by the correct unit), p is prime $\Leftrightarrow ab \in (p) \implies a \in (p)$ or $b \in p$). Even better, while the concept of a gcd does not exist in a general ring, since we are in a PID, we get the follwing resul:

Proposition 1. *Let R be a PID and $a, b \in R$. Then a and b have a greatest common divisor d, and $(a, b) = (d)$.*

Proof. Consider (a, b)—since R is a PID, there is an element d s.t. $(a, b) = (d)$. Further, $(a) \subset (d)$ and $(b) \subset (d)$ so $d \mid a, d \mid b$. Now suppose $d' \mid a, d' \mid b$. Then $(a) \subset (d'), (a) \subset (d')$. And so it must be the case that $(d) = (a, b) \subset (d')$—and hence $d \mid d'$, so d is our gcd. ■

Remark. *Note that in the above case we can have $(d) = (d')$, but then d and d' are associates—and we only care about gcd up to associates (in the same way that in $\mathbb{Z}$ we have $a \pm$ problem if we look for a "totally unique" gcd.)*

From this proposition, we get two immediate corollaries—if a, b are relatively prime, then $(a, b) = R$ (relatively prime means you can make a linear combination to get 1) and that irreducible $\implies$ prime.

We now endevor to prove that every nonzero $a \in R$ is a product of irreducible elements—we use the ascending chain condition!

Lemma 2. *A PID obeys the ASC.*

Proof. Let $(a_1) \subset (a_2) \subset \dots$ be an ascending chain of ideals in R, and let I be the union along the chain. Since R is a PID, $I = (a)$ for some $a \in R$. But then a is in the union along a chain, so it must be in one of the (a_k)—so $I \subset (a_k)$ and we have that chain must be eventually constant! ■

Proposition 2. *Every nonzero nonunit of a PID is a product of irreducibles.*

Proof. First we show that a is divisible by an irreducible. For there to be any meat, suppose that a is *not* irreducible. But then $a = a_1 b_1$ for a_1, b_1 nonunits. If a_1 is irrecducible, we are done! If it is not, then we can factor $a_1 = a_2 b_2$. Continuing, we get a chain $(a) \subset (a_1) \subset (a_2) \subset \cdots$—which must be eventually constant, giving us the required a_k, an irreducible which divides a.

Now we show that we can break down a entirely into irreducibles. For a nonirreducible a, we have some irred p_1 s.t. $p_1 \mid a$, so we can write $a = p_1 c_1$. If c_1 is a unit, we are done. If it is not we can factor further as $c_1 = p_2 c_2$. Continuing, we get a chain $(c) \subset (c_1) \subset (c_2) \subset \cdots$—which must be eventually constant, giving us the required c_k which is a unit. Thus, we can writ $a = p_1 p_2 \cdots p_k c_k$, a product of irreducibles. ■

Now this ASC is incredibly powerful. In fact, we use it to prove the following Lemma that will help us reproduce an analogue of the ord function in a general PID.

Lemma 3. *Let p be a prime and $a \neq 0$. Then there is an integer n such that $p^n \mid a$ but $p^{n+1} \nmid a$.*

Since this n is uniquely determined, we set $n = \operatorname{ord}_p a$. It is not difficult to show that ord obeys the same multiplicative $\to$ additive identity that it does in the $\mathbb{Z}$ and $k[x]$. Now we seek to take the previous proposition a bit further and show uniqueness of the decompostion. To do so, we need to deal with the case of associate primes. Let S be a set of primes in R such that

1. Every prime in R is associate to a prime in S
2. No two primes in R are associate

Theorem 3. Let R be a PID and S a set of primes as discussed above. Then if $a \in R, a \neq 0$, then we can write

$$a = u \prod_{p \in S} p^{e(p)}$$

where u is a unit. The units and exponents are uniquely determined and $e(p) = \operatorname{ord}_p a$.

Proof. Existence is already proven. Uniqueness follows directly from the properties that we have already stated about ord. ■

Remark. *Section 1.4 is uninteresting. Let ω be the primitive third root of unity. Then $Z[i]$ and $\mathbb{Z}[\omega]$ are Euclidean Domains. For $\mathbb{Z}[i]$, $\lambda(a+bi) = a^2+b^2$. For $\mathbb{Z}[\omega], \lambda(\alpha) = \lambda(a+b\omega) = \alpha\overline{\alpha}$.*

Chapter 1 Selected Problems

Problem 6: Let $a, b \in \mathbb{Z}$. Show that the equation $ax + by = c$ has solutions in the integers iff $(a, b) \mid c$.

Problem 10: Suppose that $(u, v) = 1$. Show that $(u + v, u - v)$ is either 1 or 2.

Problem 12: Suppose that we take several copies of a regular polygon and try to fit them evenly around a common vertex. Prove that this only possible polygons are triangles, squares, and hexagons

Problem 16: If $(u, v) = 1$ and $uv = a^2$, thow that u and v are both squares.

Chapter 2

Applications of Unique Factorization

Before we begin... I just couldn't get into this chapter. I tried so hard to care but none of it felt even remotely motivated. The mobius inversion theorem seemed cool and useful, but I just could not find myself *caring* about this. I feel bad about that, I really do, but this just isn't what I came to number theory for—I am much more interested in the ring theoretic side of things (chapters 3 and 4 and all that).

2.1 Infinitely Many Primes in $\mathbb{Z}$

Theorem 4 (Euclid)**.** In the ring $\mathbb{Z}$ there are infinitely many primes.

Proof. Suppose we have a finite list of positive primes $p_1, \ldots, p_n$. But then consider $N = (p_1 \cdots p_n) + 1$. Clearly N is not divisible by any of our primes—so it is either a prime in and of itself or is divisible by some prime larger that p_n. It follows that there must be infinite positive primes. ■

What about $k[x]$? If k is infinite then it is obvious as $x - a$ is monic and irreducible for all $a \in k$. If k is finite we can adapt the above proof as follows

Theorem 5. If k is a finite field, then there are infinitely many primes in $k[x]$.

Proof. Suppose we have a finite list of positive primes $f_1, \ldots, f_n$. But then consider $g = (f_1 \cdots f_n) + 1$. Clearly g is not divisible by any of our primes (since that would mean that $f_i \mid 1$ for some f_i)—so g is either a prime in and of itself or is divisible by some prime larger that f_n. It follows that there must be infinite positive primes. ■

See that in this case there are infinitely many primes which are not associate (differ by multiplication by a unit). This is not always the case. Let $p \in Z$ and let $\mathbb{Z}_{(p)}$ denote the localization of $\mathbb{Z}$ at $\mathbb{Z} \setminus (p)$—the set of all rational number a/b where $p \nmid b$. With a little bit of cross multiplying, we can show that every element of $\mathbb{Z}_{(p)}$ is a power of p times a unit—and so all primes in $\mathbb{Z}_{(p)}$ are associate.

2.2 Some Arithmetic Functions

We are interested in the number $a \in \mathbb{Z}$ that are "square-free". Why? It means that their prime decomposition has no repeated primes. Now given any $n \in \mathbb{Z}$ we can obviously separate n into its "square containing" and "square-free" parts.

Proposition 3. *If $n \in \mathbb{Z}$, n can be written in the form $n = ab^2$ where $a, b \in \mathbb{Z}$ and a is square-free.*

Note: it is *not* the case that b is square free—in fact often it is not. For example $8 = 2 \cdot 2^2$. This lemma can be used to prove that there are infinitely many primes in $\mathbb{Z}$, but we us proved that so there is no reason to do that again.

Now we define a handful of arithmetic functions (functions on the integers). First we define $v(n)$ to be the number of positive divisors of n and $\sigma(n)$ is the sum of the positive divisors of n. For example $v(3) = 2, v(6) = 4, v(12) = 6$ and $\sigma(3) = 4, \sigma(6) = 12, \sigma(12) = 28$. We can use the fundamental theorem of arithmetic to prove some nice formulas of v and σ:

Proposition 4. *If n is a positive integer and $n = p_1^{a_1} \cdots p_t^{a_t}$ is its prime decomposition, then*

(a) $v(n) = (a_1 + 1) \cdots (a_t + 1)$

(b) $\sigma(n) = \left(\frac{p_1^{a_1+1}}{p_1 - 1}\right) \cdots \left(\frac{p_t^{a_t+1}}{p_t - 1}\right)$

Proof. To prove (a), see that $m \mid n$ iff $m = p_1^{b_1} \cdots p_t^{b_t}$ and $0 \leq b_i \leq a_i$ for each i. Thus the positive divisors of n are in $1 - 1$ correspondence with n-tuples $(b_1, \ldots, b_t)$ with $0 \leq b_i \leq a_i$ and there are exactly $(a_1 + 1) \cdots (a_t + 1)$ such tuples ($a_i + 1$ choices for the i-th slot).

For (b), notice that $\sigma(n) = \sum p_1^{b_1} \cdots p_t^{b_t}$ where the sum is over all possible n-tuples of choices of the b_i mentioned above. Since these choices are independent we can also write $\sigma(n) = \left(\sum_{b_1=0}^{a_1} p_1^{b_1}\right) \cdots \left(\sum_{b_t=0}^{a_t} p_t^{b_t}\right)$—and we may use standard results relating to geometric sums to complete the proof. ■

One of the "most important" arithmetic functions is the Möbius μ function. It is defined for $n \in \mathbb{Z}^+$as follows:

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n \text{ is not square free} \\ (-1)^t & \text{if } n = p_1 p_2 \cdots p_t \text{ where the } p_i \text{ are distinct positive primes} \end{cases}$$

Proposition 5. *If $n > 1$, $\sum_{d|n} \mu(d) = 0$*

Proof. If $n = p_1^{a_1} \cdots p_t^{a_t}$, then $\sum_{d|n} \mu(d) = \sum_{(\varepsilon 1, \ldots, \varepsilon_t)} \mu(p_1^{\varepsilon_1} \cdots p_t^{\varepsilon_t})$ where the ε_i are either 1 or 0. Note that there are *technically* more terms in the sum, but μ makes them 0. Thus,

$$\sum_{d|n} \mu(d) = 1 - t + \binom{t}{2} - \binom{t}{3} + \cdots + (-1)^t = (1 - 1)^t = 0$$

■

While μ may seem like nonsense, it is useful in the context of the Dirichlet Product. If $f, g : \mathbb{Z}^+ \to \mathbb{C}$, then the **Dirichlet Product** of f and g is $f \circ g(n) := \sum f(d_1)g(d_2)$ where the sum ranges over all pairs (d_1, d_2) such that $d_1 d_2 = n$. It can be easily checked that this product is associative.

Define $\mathbb{I}$ to be 1 at 1 and 0 at all other positive integers—this it the identity for the Dirichlet product. Define $I(n) = 1$ for all $n \in \mathbb{Z}^+$. Then $f \circ I(n) = I \circ f(n) = \sum_{d|n} f(d)$.

Lemma 4. $I \circ \mu = \mu \circ I = \mathbb{I}$

Proof. Clearly they agree at 1. If $n > 1$, then $\mu \circ I(n) = \sum_{d|n} \mu(d) = 0$ and similarly for the other way. ■

Now comes (what appear to me) one of the biggest results of this chapter—I'm not going to lie to you and say that I understand why.

Theorem 6. Let $F(n) = \sum_{d|n} f(d)$. Then $f(n) = \sum_{d|n} \mu(d)F(n/d)$.

While I don't understand why it's important, I can say that the proof is pretty slick:

Proof. $F = f \circ I$, so $F \circ \mu = (f \circ I) \circ \mu = f \circ (I \circ \mu) = f \circ \mathbb{I} = f$. To be explicit, $f(n) = F \circ \mu(n) = \sum_{d|n} \mu(d)F(n/d)$. ■

A cool thing! While we considered complex valued functions, the same result holds if our functions (f and F) take value in *any* abelian group! In fact, the proof is identical! There only slight technicality is that we have multiplication in our sum. There are two ways to deal with this. For one, we can note that μ only output (0and ± 1), so we can interpret the multiplication as the sign of $F(n/d)$ in our sum. Alternatively, recall that we can see any abelian group as a $\mathbb{Z}$ module and then everything is fine!

We now introduce a new arithmetic function! The Euler ϕ function! For $n \in \mathbb{Z}^+$, $\phi(n)$ is the number of integer's between 1 and n that are prime to n. For example $\phi(1) = 1, \phi(5) = 4, \phi(6) = 2$. It is useful to know that if p is prime, then $\phi(p) = p - 1$.

Proposition 6. $\sum_{d|n} \phi(d) = n$

Proof. Consider the rationals $\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n}, 1$ each reduced to lowest terms. Each of the denominators divide n. If $d \mid n$, then there are exactly $\phi(d)$ entries in the list with d in the denominator. This proves our proposition. ■

Remark. *I'll be honest, this proof isn't entirely convincing in-and-of-itself. I worked out the case of $n = 12$, and I can see that this method holds water but I think that the proof (as presented in the text) is a little bit lacking.*

Proposition 7. *If $n = p_1^{a_1} \cdots p_t^{a_t}$, then*

$$\phi(n) = n(1 - (1/p_1)) \cdots (1 - (1/p_t))$$

Proof. Since $n = \sum_{d|n} \phi(d)$ we can use the Möbius inversion theorem so see that

$$\begin{aligned}\phi(n) &= \sum_{d|n} \mu(d)\frac{n}{d} \\ &= n - \sum_i \frac{n}{p_i} + \sum_{i<j} \frac{h}{p_i p_j} - \cdots \\ &= n(1-(1/p_1))\cdots(1-(1/p_t))\end{aligned}$$

■

This proof is... bad. Like just bad and unintuitive. Thankfully in the next chapter there is a better one.[1]

2.3 $\sum 1/p$ Diverges

Theorem 7. $\sum_{p \text{ prime}} \frac{1}{p}$ diverges.

Proof. Let $p_1, p_2, \ldots, p_{l(n)}$ be the list of primes less that n and let $\lambda(n) = \prod_{i=1}^{l(n)} (1-1/p)^{-1}$. Since $(1-1/p)^{-1} = \sum_{a_i=0}^{\infty} \frac{1}{p_i^{a_i}}$, we have that

$$\lambda(n) = \sum (p_1^{a_1} \cdots p_t^{a_t})^{-1}$$

where the sum runs over all t-tuples of nonnegative integers $(a_1, \ldots, a_t)$ [use some combo if you don't believe this]. Harder to believe (and I don't) is that $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} < \lambda(n)$ (and so $\lambda(n) \to \infty$).

Next consider $\log \lambda(n)$. Indeed,

$$\begin{aligned}\log \lambda(n) &= -\sum_{i=1}^{t} \log(1 - p_i^{-1}) \\ &= \sum_{i=1}^{t} \sum_{m=1}^{\infty} (m p_i^m)^{-1} \qquad = p_1^{-1} + p_2^{-1} + \cdots + p_t^{-1} + \sum_{i=1}^{t} \sum_{m=2}^{\infty} (m p_i^m)^{-1}\end{aligned}$$

But see that $\sum_{m=2}^{\infty} (m p_i^m)^{-1} < \sum_{m=2}^{\infty} < 2p_i^{-2}$. And so [at this point I am lost as to what is going on] $\log \lambda(n) < p_1^{-1} + p_2^{-1} + \cdots + p_t^{-1} + 2(p_1^{-2} + \cdots + p_t^{-2})$. As we know, $\sum n^{-2}$ converges, so it follows that $\sum p^{-2}$ also converges.

But then if $\sum p^{-1}$ converged there would be some integer N such that $\log \lambda(n) < N$ for all $n \in \mathbb{Z}$. This is false, so $\sum p^{-1}$ must diverge. ■

Next is a *wack* example that we couldn't quite understand during our meeting. I tried to make sense of it but it didn't go well.

[1] It would be good to note here that I am writing these notes after having written up chapter 3. I put this one off.

2.4 The Growth of $\pi(x)$

Recall that $\pi(x)$ gives the number of primes less than x. People are intensely interested in the growth of $\pi(x)$. We talked about it during our meeting and I see that their are applications to the growth of $\pi(x)$—esp when it comes to cryptography. At the same time, up just feels so arbitrary to me. Primes never really felt very important to me and spending 3 pages fiddling with inequalities feels even more tiring. From my conversations with Karl it seems like what is going on is some sort of asymptotic approximation, but the only time that I've seen/worked with asymptotics was the 2 weeks we spend on it in 530. Most (read: all) of the results in this section will simply be stated. I read them through in my initial pass through the text and I will be going through them again as I type—I will be including my comments on the proofs in the text.

Proposition 8. *$\pi(x) \leq \log\log x$ for $x \geq 2$.*

Comment. This one is cute! Bound each prime under $p_k < 2^{(2^k)}$ and then take double logs! ■

The bound above is then immediately tightened—we have that $\pi(x) \geq \frac{\log x}{2\log 2}$. Both of these show that $\pi(x) \to \infty$ as x gets large (yet another proof that there are infinite primes!). We define a new function $\theta(x) = \sum_{p \leq x} \log p$ (we set $\theta(1) = 0$), which is a close cousin of $\pi(x)$. In fact, we can use θ to bound $\pi(x)$ from above!

Proposition 9. *$\theta(x) < (4\log x)x$*

Comment. This bounding argument is clever! It uses $\binom{2n}{n}$ to bound $2^{2n} > \prod_{p>n}^{p<2n}$. Taking logs, the RHS turns into $\theta(2n) - \theta(n)$. We then sum this relation and simplify. ■

The next two corollaries return to tightening our bounds on $\pi(x)$. The thing that seems strange to me is the language of "positive constants" c_1, c_2. Do we know what they are? I have to think that they are computable, but the proofs skip that part under the guise of "the proof then follows from...".

Corollary 3. *There are positive constants c_1, c_2 such that*

$$c_2 \frac{x}{\log x} < \pi(x) < c_1 \frac{x}{\log x}$$

Proof. The only comment I can find to make is that in the proof of the lower bound what we actually do is bound

$$c_2 \frac{x}{\log x} < \frac{\theta(x)}{\log x} \leq \pi(x)$$

■

With these corollaries, we have that

$$\pi(x)\left(\frac{\log x}{x}\right) \to 1 \text{as} x \to \infty.$$

This a result that feels like it should be really cool. My understanding is that as x gets large $\frac{x}{\log x}$ becomes a better and better approximation for $\pi(x)$ which is (as I understand it) important for some reason or another. The main issue I have with seeing this as an important result is that I have only ever seen this used as a mathematical party trick. I'm sure it has an application somewhere but I'm not sure where or why.

Chapter 2 Selected Problems

to be selected

Chapter 3

Congruence

3.1 Elementary Observations

History: Diophantus asked when equations in x with integer coefficients have integer solutions. For example, does $x^2 - 117x + 31 = 0$? You solves my looking at the sign of the polynomial for even and odd values of x. We will show in this chapter that we can exploint properties of $\mathbb{Z}_m$ to answer these questions.

3.2 Congruence in ZZ

Definition (Congruence)**.** If $a, b, m \in \mathbb{Z}$, and $m \neq 0$, then we say that a is *congruent to* b *mod* m of $m|(b-a)$ and we write $a \equiv b(m)$

$\equiv$ is an equivalence relation. We will use the notation $\overline{a}$ for the class of integers equivalent to a. As long as we fix an m, we get the following characterization:

Proposition 10. *(a)* $\overline{a} = \overline{b}$ *iff* $a \equiv b(m)$

(b) $\overline{a} \neq \overline{b}$ *iff* $\overline{a} \cap \overline{b}$ *is empty*

(c) There are exactly m *distance congruence classes mod* m*.*

Why do we care? Well it turns out that the results allows us to turn $\mathbb{Z}_m$ into a ring! Not only that, the standard projection $\mathbb{Z} \to \mathbb{Z}_m$ is a homomorphism so it doesn't matter "when" we do the modulo! Even better—things cross over into the polynomial ring. If $p \in \mathbb{Z}[x]$ and $p(0)$ and $p(1)$ are both odd, then p can't have any integer roots!

3.3 On $ax \equiv b(m)$

How do we know when $ax \equiv b(m)$ is solvable? How many solutions should we expect it to have? The idea of a "number" of solutions may seem strange, but if we have $f(x_1, \ldots, x_n) \equiv 0(m)$, then we consider $(a_1, \ldots, a_n) \sim (b_1, \ldots, b_n)$ if they are the same class in ${\mathbb{Z}_m}^n$. For example, $3, 8, 13, 18$ all solve $6x \equiv 3(15)$, but $3 \equiv 18(15)$, so we say there are only 3 solutions.

Let $(a, m) = d > 0$ and $a' = \frac{a}{d}$, $m' = \frac{m}{d}$—note that this means that a' and m' are coprime

Proposition 11. *The congruence $ax \equiv b(m)$ has solutions if and only if $d \mid b$. If $d \mid b$, then there are exactly d solutions. If x_0 is a solution, then the other solutions are given by $x_0 + m', x_0 + 2m', \dots x_0 + (d-1)m'$.*

Proof. If x_0 is a solutins, then $ax_0 - b = my_0$ for some $y_0 \in \mathbb{Z}$. Thus, $ax_0 + my_0 = b$. d divides the LHS, so it must divide the RHS.

Conversely, if $d \mid b$, then there must be integers x_0', y_0' s.t. $ax_0' - my_0' = d$. Let $c = \frac{b}{d}$ and we have $a(x_0'c) - m(y_0'c) = b$—but if we let $x_0 = x_0'c$, we are done!

Now suppose that x_0, x_1 are solutions. $ax_0 \equiv b, ax_1 \equiv b \implies a(x_1 - x_0) \equiv 0$, and so $m \mid a(x_1 - x_0)$ *and* $m' \mid a'(x_1 - x_0)$. But we have already stated m' and a' are coprime, so $m' | x_1 - x_0$ and thus $x_1 = x_0 + km'$. The bounds on k are immediate. ■

Now this proposition has two immediate (and important) consequences when it comes to equivalences with unique solutions

Corollary 4. *If a and m are coprime, then $ax \equiv b(m)$ has exactly one solution*

Corollary 5. *If p is prime and $a \not\equiv 0(p)$, then $ax \equiv b(p)$ has exactly one solution.*

We can interpret these props and corrs in as ring theoretic statements. Recall that the units in $\mathbb{Z}_m$ are the invertable elements and for a multiplicative group. In particular, $a \in \mathbb{Z}_m$ is a unit iff $ax = 1$ is solvable—which happens precisely when a and m are coprime. It follows that there are $\phi(m)$ units in $\mathbb{Z}_m$.

In the special case that p is prime, all nonzero elements of $\mathbb{Z}_p$ are coprime to p and hence units. Thus, $\mathbb{Z}_p$ is field! If m is not prime, then $m = m_1 m_2$. But then in $\mathbb{Z}_p$, $\overline{m_1 m_2} = \overline{0}$—so we are not even a domain, let alone a field. To summarize,

Proposition 12. *An element $\overline{a} \in \mathbb{Z}_m$ is a unit iff $(a, m) = 1$. There are exactly $\phi(m)$ units in $\mathbb{Z}_m$. Further, $\mathbb{Z}_m$ is a field iff m is prime.*

Corollary 6 (Euler's Theorem)**.** *If $(a, m) = 1$, then $a^{\phi(m)} \equiv 1(m)$*

Proof. We know that the units of $\mathbb{Z}_m$ form a group of order $\phi(m)$. Since a is a unit, Lagagrange's theorem tells us that $\overline{a}^{\phi(m)} = \overline{1} \implies a^{\phi(m)} \equiv (m)$. ■

Corollary 7 (Fermat's Little Theorem)**.** *If p is prime and $p \nmid a$, then $a^{p-1} \equiv 1(p)$.*

Proof. The above corr and the fact that for p prime we have that $\phi(p) = p - 1$. ■

3.4 The Chinese Remainder Theorem

When our m is composite, we can sometimes simplify our correspondence so a system of congruences. Indeed, such a simplification is possible in a much larger class of rings (the PID case is in the selected problems for this chapter).

Lemma 5. *If $a_1, \dots, a_n$ are all relatively prime to m, then so is their product.*

Proof. $U(\mathbb{Z}_m)$ is a group, and hence closed under multiplication. ■

Lemma 6. *Suppose $a_1, \dots a_t$ all divide n and that the a_i are pairwise coprime. Then $a_1 \cdots a_t \mid n$.*

Proof. We proceed by induction on t. $t = 1$ is immediate. Now assume that our lemma is true for $t-1$, so $a_1 \cdots a_{t-1} \mid n$. By the previous lemma, a_t is prime to $a_1 \cdots a_{t-1}$. It follows that there are $r, s \in \mathbb{Z}$ s.t. $ra_t + sa_1 \cdots a_{t-1} = 1$. If we multiply both sides by n, see that the LHS is divisible by $a_1 \cdots a_t$—so n must be as well! ■

Now we state the big boy theorem feared by many an undergraduate:

Theorem 8 (Chinese Remainder Theorem)**.** Suppose $m = m_1 \cdots m_t$ where the m_i are pairwise coprime. Let $b_1, \dots, b_t \in \mathbb{Z}$ and consider the system

$$x \equiv b_1(m_1), x \equiv b_2(m_2), \dots, x \equiv b_t(m_t)$$

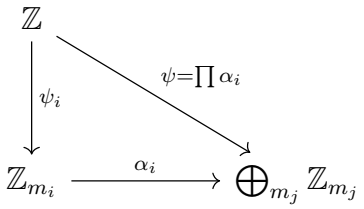
This system always has solutions and any two solutions differ by a multiple of m.

Proof. Let $n_i = \frac{m}{m_i}$. From two lemmas ago (using `\ref` is too much work) we have that $(m_i, n_i) = 1$. Thus, we have $r_i, s_i \in \mathbb{Z}$ s.t. $r_i m_i + s_i n_i = 1$. Let $e_i = s_i n_i$—and so $e_i \equiv 1(m_i)$ but $e_i \equiv 0(m_j)$ for $i \neq j$. Now define $x_0 = \sum_{i=0}^{t} b_i e_i$. Notice that this means that $x_0 \equiv b_i e_i(m_i) \implies x_0 \equiv b_i(m_i)$ and so x_0 is a solution![1]

Now suppose that x_1 is another solution. Then $x_1 - x_0 \equiv 0(m_i)$ for all i. In other words, each $m_i \mid x_1 - x_0$, and so by the other previous lemma $m = m_1 \cdots m_t | x_1 - x_0$. ■

This has a nice ring theoretic interpretation. Recall that if we have a handful of rings, $R_1, \dots, R_t$, we can form a new ring $S = R_1 \oplus \cdots \oplus R_t$ with operations done component-wise. In this case $U(S) = U(R_1) \times \cdots \times U(R_t)$.

Now we turn our attention back to the ring $\mathbb{Z}_m$. Recalling some category theory, recall that both we have canonical maps $\psi_i : Z \to \mathbb{Z}_{m_i}$ and $\alpha_i : \mathbb{Z}_{m_i} \hookrightarrow \oplus \mathbb{Z}_{m_j}$. Since α_i exists for each m_i, we have an induced map:



Now we consider the image and kernel of ψ. By the CRT above, we have that ψ is onto. Further, the kernel is precisely the ideal $m\mathbb{Z}$. Thus, we have an isomorphism between

$$\mathbb{Z}_m \simeq \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_t}$$

whenever $m = m_1 \cdots m_t$ and the m_i are pairwise coprime. This immedately tells us about the units of $\mathbb{Z}_m$: $\phi(m) = \phi(m_1) \cdots \phi(m_t)$. If we consider the prime decompositon of m, $m =$

[1] I'm not sure what do with this, but it sure smells like some sort of orthogonal decomp. What are the vectors? What is the inner product? Honestly, it might be a bit more clear in the context of the more general statement of the theorem—linear algebra over a PID has a ton of structure.

$p_1^{a_1} \cdots p_t^{a_t}$, then $\phi(m) = \phi(p_1^{a_1}) \cdots \phi(p_t^{a_t})$. Now we know that $\phi(p^a) = p^a - p^{a-1} = p^a(1 - 1/p)$ and it follows that

$$\begin{aligned}
\phi(m) &= \prod p_i^{a_i} \left(1 - \frac{1}{p_i}\right) \\
&= p_1^{a_1} \cdots p_t^{a_t} \prod \left(1 - \frac{1}{p_i}\right) \\
&= m \prod \left(1 - \frac{1}{p_i}\right)
\end{aligned}$$

Chapter 3 Selected Problems

Problem 1: Show that there are infinitely many primes congruent to -1 modulo 6.

Proof. Before we show that there are inifinetly many primes of this form, we need to show that there are *any* primes of the for $6k-1$. Division by 6 gives remainder of $-1, 0, 1, 2, 3, 4$—so any odd number is necessarily of the form $6k+1, 6k+3, 6k-1$. Some algebra gives that

$$(6k+1)(\overline{6k}+1) = 6(6k\overline{k} - k - \overline{k}) + 1$$
$$(6k+3)(\overline{6k}+3) = 6(6k\overline{k} - 3k - 3\overline{k} + 1) + 3$$

and so any odd number of the form $6k-1$ must be divisible by a prime of the form $6k-1$—otherwise how did we leave the closed systems of $6k+1$ and $6k+3$.

Not suppose that there were a finite list of positive primes, $p_1, \ldots, p_n$ of the form $p_i = 6k_i - 1$ and set $N = 6\prod_i p_i - 1$. Now N can be divisible by any of the p_i but is of the form discussed above—so our list must be incomplete! Therefore there must be infinite primes of the for $6k-1$ and we are done! ■

Problem 4: Show that the equation $3x^2 + 2 = y^2$ has no solutions in the integers.

Proof. Seeking to use the result from the text, we set $f(x, y) = 3x^2 - y + 2$ and see what happens when we plug in odd or even numbers:

$$f(0,0) = 2$$
$$f(1,0) = 3 + 2 = 5$$
$$f(0,1) = -1 + 2 = 1$$
$$f(1,1) = 3 - 1 + 2 = 4$$

This rules out solutions of the form (e, o) and (o, e). But tells us nothing about the cases of (e, e) or (o, o). The natural next step would be to check solutions mod 4. Notice that this only helps us in the case that we are (e, e)—as the o, o case is equal to 4. Before we deal with that, we show there can't be any solutions of the for (e, e) by show that $f(e, e)$ is never

0 mod 4

$$\begin{aligned} f(0,0) &= 2 \\ f(2,0) &= 0 - 2^2 + 2 \equiv 2 \\ f(0,2) &= 3 \cdot 2^2 - 0 + 2 \equiv 2 \\ f(2,2) &= 3 \cdot 2^2 - 2^2 + 2 \equiv 2 \end{aligned}$$

Since the (e,e) case always gives us 2 (mod 4), we can't have a solution of the form (e,e).

Now we turn our attention back to the case of (o,o). We will check these solutions mod 3. There are 4 cases to check, but since we consider 3 to be 0, we can use our previous computation:

$$\begin{aligned} f(0,0) &= 2 \equiv 2(3) \\ f(1,0) &= 3 + 2 = 5 \equiv 1(3) \\ f(0,1) &= -1 + 2 = 1 \equiv 1(3) \\ f(1,1) &= 3 - 1 + 2 = 4 \equiv 1(3) \end{aligned}$$

And so any solution of the form (o,o) fails mod 3 and we have exhausted all the possible cases! ■

Problem 12: Show that if p is prime and $1 \leq k \leq p-1$, then $p \mid \binom{p}{k}$. Deduce that $(a+1)^p \equiv a^p + 1(p)$.

Proof. See that if $1 \leq k \leq p-1$, then

$$\binom{p}{k} = \frac{1 \cdot 2 \cdots p}{(1 \cdot 2 \cdots k)(1 \cdot 2 \cdots (p-k))} = \frac{(p-k) \cdot (p-k+1) \cdots p}{1 \cdot 2 \cdots (p-k)}$$

but since p is prime and p does not appear in the denominator, $p \mid \binom{p}{k}$

For the second part, consider the fact that

$$(a+1)^p = \sum_{k=0}^{p} \binom{p}{k} a^{b-k}.$$

By the above work, everything except for the $k = 0, p$ drops to 0 mod p. The $k = 0$ gives a^p and the $k = p$ case gives 1. Thus, we have recovered the freshmans dream:

$$(a+1)^p \equiv a^p + 1(p)$$

■

Problem 17 : Let $f \in \mathbb{Z}[x]$ and $n = p_1^{a_1} \cdots p_t^{a_t}$. Show that $f(x) \equiv 0(n)$ has a solution iff $f(x) \equiv 0(p_i^{a_i})$ has a solution for each i.

Proof. ($\implies$) This direction is obvious. Since $p_i^{a_i} \mid n$ for all i, if $n \mid f(x)$, then $p_i^{a_i} \mid f(x)$.

($\impliedby$) We know that $p_1^{a_1} \mid f(x)$, so $f(x) = p_1^{a_1} k_1$. But since $p_2^{a_2} \mid f(x)$ and $p_2^{a_2} \nmid p_1^{a_1}$, we know that $f(x) = p_1^{a_1} p_2^{a_2} k_2$. Continuing for all the p_i, we have that $f(x) = p_1^{a_1} \cdots p_t^{a_t} k_t$. It follows immediately that $n | f(x)$. ■

Problem 18: Let N be the number of solutions to $f(x) \equiv 0(m)$ and N_i the number of solutions to $f(x) \equiv 0(p_i^{a_i})$. Show that $N = \prod_i N_i$.

Proof. As seen above, a solution to $f(x) \equiv 0(n)$ can be constructed from a product of solutions to solutions to $f(x) \equiv 0(p_i^{a_i})$. If we view this product as a t-tuple of integers x_i, where each x_i solve the related equivalence (to $p_i^{a_i}$), then our solution is given by the map $(x_1, \ldots, x_t) \mapsto \prod x_i$. There are N_i solutions for each entry, so some basic combinatorics tells us that there are $\prod_i N_i$ possible combinations, and hence $\prod_i N_i$ possible solutions! ■

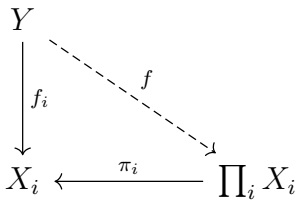
Problem 22: Formulate and prove the Chinese Remainder Theorem for a PID. I was actually able to prove it for any commutative ring with unity!

Solution: First we need a concept of coprime ideals. Given two ideals $I, J \subset R$, we say that they are **coprime** if these are elements $r \in I, s \in J$ such that $r + s = 1$—Notice that this says that $I + J = R$. It is will known that $IJ \subset I \cap J$, but the opposite containment can occasionally hold:

Lemma. *If R is any commutative ring with 1 and I, J are coprime ideals, then $IJ = I \cap J$.*

Proof. As mentioned above, $\subset$ is well known, so let $a \in I \cap J$. Since I, J are coprime, we have that there are $r \in I, s \in J$ such that $r + s = 1$. We can write $a = a(r + s) = ar + as$—this a linear combination of r and s, so it lives in IJ, hence $a \in IJ$. ■

With our lemma proven, we can proceed. For those fearful of category theory, we recommend that you look away because we invoke the universal property of products: given a product $\prod X_i$ and any set of maps $f_i : Y \to X_i$, there is a unique map f such that the following diagram commutes for every i:



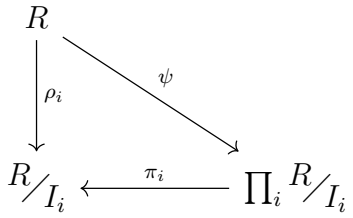
With this background, we can finally state and prove our theorem.

Theorem. *Let $I_1, \ldots, I_n$ be pairwise coprime ideals in R, a commutative ring with unity and $I = \prod_i I_i$. Then the natural map*

$$\varphi : {}^{R}\!/_{I} \to \prod_i {}^{R}\!/_{I_i}$$

is an isomorphism.

Proof. Let $\rho_i : R \to {}^{R}\!/_{I_i}$ and $\pi : \prod_i {}^{R}\!/_{I_i} \to {}^{R}\!/_{I_i}$ be the standard quotient and projection maps. Invoking the universal property of products, we have a map φ such that the following diagram commutes for all i:



Category also guarantees that ψ is a ring homomorphism, so there is no need to check that! Further, it must be the case that ψ is onto. See that both π_i and ρ_i are onto. This, combined with the fact that π_i is a projection onto ${}^{R}\!/_{I_i}$ and the commutativity of the diagram gives us that ψ must be onto as well.

What is the kernel of ψ? It is precisely the elements which are in each of the I_i (as the must be zero in each component)—meanning the kernel is $\bigcap_i I_i = \prod_i I_i$ (by the lemma). Thus by the first isomorphism theorem, ψ descends to an isomorphism.

$$\varphi : {}^{R}\!/_{I} \to \prod_i {}^{R}\!/_{I_i}$$

■

■