MATH 361: NUMBER THEORY — FOURTH LECTURE

1. Introduction

Everybody knows that three hours after 10:00, the time is 1:00. That is, everybody is familiar with *modular arithmetic*, the usual arithmetic of the integers subject to the additional condition that some fixed integer (such as 12) is treated as 0. After noting some quick consequences of the Euclidean structure of the integer ring $(\mathbb{Z}, +, \cdot)$, this lecture places modular arithmetic in the context of quotient structures of this ring.

2. Some Loose Ends

2.1. **Euclid's Lemma.** *Euclid's Lemma* states that for positive integers a, b, n:

If $n \mid ab$ *and* $\gcd(n, a) = 1$ *then* $n \mid b$.

Note that Euclid's Lemma is similar to the definition of a prime element of an integral domain: both have the premise of an element dividing a product, and then the conclusion that the element divides one of the multiplicands. And, indeed, the proof of Euclid's Lemma is essentially the same as the proof that each irreducible element is prime in a Euclidean domain. Specifically, we have $n \mid ab$ and, because $\gcd(n, a) = 1$, we also have $Nn + Aa = 1$ for some N, A. Multiply this relation through by b to get $Nnb + Aab = b$. But n divides the left side, so n divides the right side, as desired.

We can also state and prove Euclid's Lemma in the language of ideals, notwithstanding that doing so is anti-historic. Again for positive integers a, b, n, now the statement is:

If $(ab) \subset (n)$ *and* $(n, a) = (1)$ *then* $(b) \subset (n)$.

Here the argument is that $(b) = (n, a)(b) = (nb, ab) \subset (nb, n) = (n)$. (We are multiplying ideals here. The definition is that if I and J are ideals then their product IJ is the ideal *generated* by all pairwise products ij where $i \in I$ and $j \in J$. Ideal properties show that in fact I is generated by all pairwise products of *generators* i and j, and this justifies the equality $(n, a)(b) = (na, nb)$ in the argument.)

A consequence of Euclid's Lemma is:

If $(a, b) = 1$ *then* $(a, bc) = (a, c)$.

Indeed, given that $(a, b) = 1$, any divisor d of a and bc satisfies $(d, b) = 1$ because $d \mid a$, and so Euclid's Lemma gives $d \mid c$ because $d \mid bc$. That is, any divisor of a and bc also divides c. Conversely, it is immediate that any divisor d of a and c divides bc. Alternatively, one can prove the consequence by a variant of proving the lemma: $\alpha a + \beta b = 1$ for some α and β, so $\alpha ac + \beta bc = c$, and so the linear combination c of a and bc is a multiple of their greatest common divisor (a, bc).

A particular instance of the consequence of Euclid's Lemma is:

The set of positive integers coprime to a given n is closed under multiplication.

Here the argument is that if $(n, b) = (n, c) = 1$ then because we have $(n, b) = 1$ Euclid's Lemma gives $(n, bc) = (n, c)$, and because we also have $(n, c) = 1$ indeed $(n, bc) = 1$.

2.2. **Least common multiple.** Any two positive integers a and b have a positive integer *least common multiple*, denoted $\operatorname{lcm}(a, b)$. If a and b are coprime then $\operatorname{lcm}(a, b) = ab$, because if a divides a multiple mb of b then a divides m by Euclid's Lemma. For general a and b, let $g = \gcd(a, b)$. With $a = ga'$ and $b = gb'$ where $\gcd(a', b') = 1$,

$$ab = g^2a'b' = g^2 \operatorname{lcm}(a', b') = g \operatorname{lcm}(ga', gb') = g \operatorname{lcm}(a, b).$$

That is, $\operatorname{lcm}(a, b) = ab/\gcd(a, b)$.

So far this writeup uses *global* methods, as compared to the *local* approach of factoring a and b uniquely into prime powers—as we can do essentially in consequence of Euclid's Lemma—and then working one prime at a time. To work locally instead, fix a prime p and suppose that

$$\text{the powers of } p \text{ in } a \text{ and } b \text{ are } p^{e_a} \text{ and } p^{e_b}$$

so that

$$\text{the powers of } p \text{ in } ab, \gcd(a, b), \operatorname{lcm}(a, b) \text{ are are } p^{e_a+e_b},\ p^{\min(e_a,e_b)},\ p^{\max(e_a,e_b)}.$$

Because $e_a+e_b = \min(e_a, e_b)+\max(e_a, e_b)$, again $ab = \gcd(a, b) \operatorname{lcm}(a, b)$. Similarly, it is easy to show the consequence of Euclid's Lemma in section 2.1 by local methods, taking unique factorization as morally in hand once Euclid's Lemma is proved. There are tradeoffs between local and global methods, depending on context. One issue in algorithmic/computational number theory is that factorization into primes can be intractable for large integers while global algorithms can be fast.

3. The Quotient Ring $\mathbb{Z}/n\mathbb{Z}$

Let $n \in \mathbb{Z}^+$ be a positive integer. Equality up to multiples of n partitions $\mathbb{Z}$ into n equivalence classes, called *cosets*,

$$\overline{0} = 0 + n\mathbb{Z}, \quad \overline{1} = 1 + n\mathbb{Z}, \quad \ldots, \quad \overline{n-1} = (n-1) + n\mathbb{Z}.$$

Let $\mathbb{Z}/n\mathbb{Z}$ denote the set of these cosets. The map

$$\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}, \qquad a \longmapsto \overline{a} = a + n\mathbb{Z}$$

is a well defined surjection. However, for now its domain is a ring but its codomain is only a set. We want it to be a ring-to-ring map, and this requires addition and multiplication in $\mathbb{Z}/n\mathbb{Z}$.

The natural addition and multiplication of $\mathbb{Z}/n\mathbb{Z}$ are obvious:

$$\overline{a} + \overline{b} \overset{\text{def}}{=} \overline{a+b}, \qquad \overline{a} \cdot \overline{b} \overset{\text{def}}{=} \overline{ab}.$$

Informally we are doing *remainder arithmetic*, but really an equivalence class such as $\overline{3}$ means *3 and all its n-translates*. The number of hours from *any* 10:00 to *any* 1:00 is $\overline{3}$ rather than 3.

> *The question is not what the operations of $\mathbb{Z}/n\mathbb{Z}$ must be, but whether what they must be makes sense.*

To address this question, we move to coset notation,

$$(a+n\mathbb{Z})+(b+n\mathbb{Z}) \stackrel{\text{def}}{=} (a+b)+n\mathbb{Z}, \qquad (a+n\mathbb{Z})(b+n\mathbb{Z}) \stackrel{\text{def}}{=} ab+n\mathbb{Z}.$$

The point is that conceivably $a+n\mathbb{Z} = a'+n\mathbb{Z}$ and $b+n\mathbb{Z} = b'+n\mathbb{Z}$ in $\mathbb{Z}/n\mathbb{Z}$ with $a \neq a'$ and/or $b \neq b'$ in $\mathbb{Z}$, and so the sum $(a+n\mathbb{Z})+(b+n\mathbb{Z}) = (a'+n\mathbb{Z})+(b'+n\mathbb{Z})$ is defined by two different formulas,

$$(a+n\mathbb{Z})+(b+n\mathbb{Z}) = a+b+n\mathbb{Z}, \qquad (a'+n\mathbb{Z})+(b'+n\mathbb{Z}) = a'+b'+n\mathbb{Z}.$$

Unless $a+b+n\mathbb{Z} = a'+b'+n\mathbb{Z}$, addition in $\mathbb{Z}/n\mathbb{Z}$ isn't sensible. And similarly for multiplication in $\mathbb{Z}/n\mathbb{Z}$,

$$(a+n\mathbb{Z})(b+n\mathbb{Z}) = ab+n\mathbb{Z}, \qquad (a'+n\mathbb{Z})(b'+n\mathbb{Z}) = a'b'+n\mathbb{Z},$$

so unless $ab+n\mathbb{Z} = a'b'+n\mathbb{Z}$, multiplication in $\mathbb{Z}/n\mathbb{Z}$ isn't sensible. However, the conditions

$$a+n\mathbb{Z} = a'+n\mathbb{Z} \quad \text{and} \quad b+n\mathbb{Z} = b'+n\mathbb{Z}$$

are

$$a'-a \in n\mathbb{Z} \quad \text{and} \quad b'-b \in n\mathbb{Z},$$

which give, crucially using the ideal properties of $n\mathbb{Z}$ in $\mathbb{Z}$ as compared to merely its subring properties,

$$\begin{aligned} (a'+b')-(a+b) &= (a'-a)+(b'-b) \in n\mathbb{Z} \\ a'b'-ab &= a'(b'-b)+b(a'-a) \in n\mathbb{Z}, \end{aligned}$$

and these conditions are the desired ones,

$$a+b+n\mathbb{Z} = a'+b'+n\mathbb{Z} \quad \text{and} \quad ab+n\mathbb{Z} = a'b'+n\mathbb{Z}.$$

That is, the quotient space $\mathbb{Z}/n\mathbb{Z}$ inherits ring structure from $\mathbb{Z}$ because the subring $n\mathbb{Z}$ of $\mathbb{Z}$ is an ideal. With the natural candidate inherited addition and multiplication operations of $\mathbb{Z}/n\mathbb{Z}$ confirmed as sensible, the reduction map

$$\overline{} : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$$

is innately a surjective ring homomorphism.

With these issues clearly addressed, from now on we allow ourselves to be situationally casual with the notations a, $\overline{a}$, and $a+n\mathbb{Z}$. For example, "$a \in \mathbb{Z}/n\mathbb{Z}$" and "$\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ where $a \in \mathbb{Z}$" are both literally correct, each assigning a different meaning to a—especially, a is not an integer in the first—but we may blur this distinction and let a denote both quantities simultaneously.

The unit group of $\mathbb{Z}/n\mathbb{Z}$ is

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{a \in \mathbb{Z}/n\mathbb{Z} : ab = 1 \text{ for some } b \in \mathbb{Z}/n\mathbb{Z}\}$$

Our earlier discussion of ideals and the Euclidean algorithm shows that for any integer $a \in \mathbb{Z}$,

$$\begin{aligned} \overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times &\iff \overline{a}\overline{b} = \overline{1} \text{ for some } \overline{b} \\ &\iff ab+kn = 1 \text{ for some } b \text{ and } k \\ &\iff (a,n) = 1. \end{aligned}$$

Consequently,

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} : (a,n) = 1\}.$$

Here we can note that for any integer k we have $(a+kn,n) = (a,n)$, so the value of (a,n) is independent of which a we use to name the coset $\overline{a}$. Thus the previous display is sensible. It shows that the elementary definition of the Euler totient function,

$$\varphi(n) = |\{a \in \{0, 1, \ldots, n-1\} : (a, n) = 1\}|$$

is equivalent to a more conceptual definition,

$$\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|.$$

4. Maps Among Quotient Rings of $\mathbb{Z}$

Let n and m be positive integers with $n \mid m$. The inclusion map $m\mathbb{Z} \longrightarrow n\mathbb{Z}$ of ideals of $\mathbb{Z}$ gives rise to a surjective map of quotient rings in the other direction,

$$^- : \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}, \qquad a + m\mathbb{Z} \longmapsto a + n\mathbb{Z}.$$

Similarly to the quotient ring operations, this quotient map is the obvious thing, but what needs to be shown is that thanks to the containment $m\mathbb{Z} \subset n\mathbb{Z}$, it makes sense. The problem is that conceivably an element $a+m\mathbb{Z}$ of $\mathbb{Z}/m\mathbb{Z}$ is also $a'+m\mathbb{Z}$ but $a + n\mathbb{Z}$ and $a' + n\mathbb{Z}$ are distinct in $\mathbb{Z}/n\mathbb{Z}$. However, this can't happen: the condition $a + m\mathbb{Z} = a' + m\mathbb{Z}$ is $a' - a \in m\mathbb{Z}$, implying $a' - a \in n\mathbb{Z}$ because of the containment, and this is the condition $a + n\mathbb{Z} = a' + n\mathbb{Z}$.

Still with $n \mid m$, the surjective map between quotient rings gives rise to a corresponding surjective map of multiplicative groups,

$$^- : (\mathbb{Z}/m\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times, \qquad a + m\mathbb{Z} \longmapsto a + n\mathbb{Z},$$

noting that if $(a, m) = 1$ then also $(a, n) = 1$, so indeed the quotient ring map takes units to units. We show that the unit group map surjects. In general, a surjection of commutative rings with 1 needn't give rise to a surjection of the unit groups, as shown by the map $\mathbb{Z} \longrightarrow \mathbb{Z}/5\mathbb{Z}$, so our argument must use specifics of the situation at hand. The issue is that the condition $(a, n) = 1$ doesn't imply $(a, m) = 1$. To address this, it suffices to consider the case $m = np$ with p prime, because the general case can be built from this one in finitely many steps. By the consequence of Euclid's Lemma noted early in this writeup, $(a, np) = (a, p)$. Now there are two cases.

- If $p \nmid a$ then $(a, np) = 1$. Thus $a + np\mathbb{Z}$ in $(\mathbb{Z}/np\mathbb{Z})^\times$ maps to $a + n\mathbb{Z}$ in $(\mathbb{Z}/n\mathbb{Z})^\times$.
- If $p \mid a$ then $(n, p) = 1$ because $(a, n) = 1$, and so $(a + n, p) = 1$. This gives $(a + n, np) = (a + n, n)$ by the consequence of Euclid's Lemma, and then $(a + n, n) = (a, n) = 1$, so altogether $(a + n, np) = 1$. Thus $a + n + np\mathbb{Z}$ in $(\mathbb{Z}/np\mathbb{Z})^\times$ maps to $a + n\mathbb{Z}$ in $(\mathbb{Z}/n\mathbb{Z})^\times$.

5. Congruence

Definition 5.1. *For any integers a, b, and n, we say that* **a equals b modulo n**, *notated*

$$a = b \bmod n,$$

if $n \mid b - a$. *Other notations for congruence are*

$$a =_n b, \qquad a \equiv b \pmod n, \qquad a = b\ (n),$$

and so on.

We recognize congruence modulo n in $\mathbb{Z}$ to mean equality in the quotient ring $\mathbb{Z}/n\mathbb{Z}$. Although there is nothing new in the definition other than notation, the notation lets us phrase arguments neatly and naturally. Here are some examples.

- $a = b \bmod 0$ if and only if $a = b$.
- $a = b \bmod 1$ for all a and b.
- $a = b \bmod 2$ if and only if a and b have the same parity.
- An exercise on the first homework set showed that
$$f(n_o + kf(n_o)) = 0 \bmod f(n_o).$$
- Let $f \in \mathbb{Z}[X_1, \dots, X_k]$, a polynomial in k variables with integer coefficients, be given. Suppose that we have k pairs of integer values that are congruent modulo some n,
$$(x_1, \dots, x_k) = (y_1, \dots, y_k) \bmod n, \quad \text{componentwise.}$$
Then also, because the map $\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ is a ring homomorphism,
$$f(x_1, \dots, x_k) = f(y_1, \dots, y_k) \bmod n.$$
- (*Decimal digits*) Because $10 = 1$ (9), it follows that for any decimal digits $a_0, \dots, a_n$,
$$\sum_{i=0}^{n} a_i 10^i = \sum_{i=0}^{n} a_i \bmod 9.$$
This is the grade school digit-sum test that a number is divisible by 9 if and only if the sum of its digits is divisible by 9. Because $10 = 1$ (3) the same result holds for divisibility by 3. Because $10 = -1$ (11) a similar result holds for divisibility by 11, but with the alternating sum of the digits. Because $10 = 0$ (2), a number's last digit determines whether it is divisible by 2, and similarly for divisibility by 5. Because $10 = 2$ (4) and $100 = 0$ (4), the sum of twice a number's second-to-last digit and its last digit determine whether it is divisible by 4.
- (*A variant of Euclid's argument*) Any odd n satisfies $n = 1$ (4) or $n = 3$ (4). Suppose that there are only finitely primes $p = 3$ (4); call them p_i for $i = 1, \dots, k$. (So here $p_1 = 3$.) Consider the odd number
$$n = 4p_2 \cdots p_k + 3 \quad \text{(note that } p_1 = 3 \text{ is excluded).}$$
Then $n \neq 0$ (3) and $n = 3$ $(p_i) \neq 0$ (p_i) for $i = 2, \dots, k$. Thus none of the p_i divide n, and neither does 2. It follows that n is a product of primes $q = 1$ (4). But any such product is again 1 (4), contradicting the fact that $n = 3$ (4). The conclusion is that there exist infinitely many primes $p = 3$ (4).

6. Euler's Rule and Fermat's Little Theorem

Proposition 6.1 (Euler's Rule)**.** *Let a, n be positive integers with $(a, n) = 1$. Then*
$$a^{\varphi(n)} = 1 \bmod n.$$

Proof. For an elementary proof, let $x_1, \dots, x_{\varphi(n)}$ be the elements of $\{0, \dots, n-1\}$ that are coprime to n. Then we have
$$ax_i = x_{j(i)} \bmod n, \quad i = 1, \dots, \varphi(n),$$
where the map
$$i \longmapsto j(i)$$
permutes $\{1, \dots, \varphi(n)\}$. Here one point is that the conditions $(a, n) = (x_i, n) = 1$ give $(ax_i, n) = 1$ by the observation after Euclid's Lemma toward the beginning of

this writeup that the set of positive integers coprime to a given n is closed under multiplication; thus we do have $ax_i = x_{j(i)} \bmod n$ for some $j(i)$. The second point is that if $ax_i = ax_{i'}$ (n) then $x_i = x_{i'}$ (n) also by Euclid's Lemma, because a is coprime to n, and so $x_i = x_{i'}$ because both come from $\{0, \ldots, n-1\}$. Thus $i = i'$, and the map $i \mapsto j(i)$ is a permutation, as claimed. Now, because the map is a permutation, we have

$$\prod_{i=1}^{\varphi(n)} x_i =_n \prod_{i=1}^{\varphi(n)} (ax_i) =_n a^{\varphi(n)} \prod_{i=1}^{\varphi(n)} x_i.$$

So $1 = a^{\varphi(n)}$ (n), because the product $\prod_{i=1}^{\varphi(n)} x_i$ is coprime to n in consequence of each x_i being so. □

The points addressed by explicit situational use of Euclid's Lemma in the previous argument are handled tacitly and automatically by the group structure of $(\mathbb{Z}/n\mathbb{Z})^\times$. Let G denote this group. Instead of making the elementary argument, let $x_1, \ldots, x_{\varphi(n)}$ be the elements of G, and identify a with its image $\overline{a}$ in G. The map $x \mapsto ax$ permutes G, and so

$$\prod_{x \in G} ax = \prod_{x \in G} x.$$

The left side is $a^{\varphi(n)} \prod_{x \in G} x$, and now multiplying by the inverse of the product, or noting that the cancellation law always holds in a group because we can multiply by inverses in general, gives the result.

Even more generally, Euler's Rule is a special case consequence of the beginning finite group theory result that the order of every subgroup divides the order of the group. Indeed, for any group element, the order of the cyclic subgroup that it generates divides the order of the group; the order of the cyclic subgroup is the order of its generator, so this latter order divides the order of the group. Thus, raising any group element to the order of the group gives 1. Specializing the group to $(\mathbb{Z}/n\mathbb{Z})^\times$ gives Euler's rule that for $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, $a^{\varphi(n)} = 1$ in $(\mathbb{Z}/n\mathbb{Z})^\times$.

Corollary 6.2 (Fermat's Little Theorem). *Let p be prime. For every integer a such that $p \nmid a$,*

$$a^{p-1} = 1 \bmod p.$$

In consequence of Fermat's Little Theorem,

$$a^p = a \bmod p \text{ for all integers } a \text{ and primes } p.$$

However, the slight gain of information here occurs outside the group setting of $(\mathbb{Z}/p\mathbb{Z})^\times$. In fact, the result in the previous display can be proved additively rather than multiplicatively, using induction on $a \geq 0$ with p fixed but generic, and using the binomial theorem. The base case $a = 0$ is clear, and if $a \geq 0$ and $a^p = a \bmod p$ then consequently

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

Because $(-a)^p = -a^p \bmod p$ for any integer a and prime p, including $p = 2$, we have the desired result for negative a as well, using the condition $-a \geq 1$ for the second congruence to follow,

$$a^p = -(-a)^p \bmod p = -(-a) \bmod p = a.$$

7. The Equation $ax + ny = b$

Consider the equation

$$ax + ny = b, \qquad a, n, b \in \mathbb{Z},\ n \neq 0.$$

Because the integer linear combinations of a and n are precisely the integer multiples of their greatest common divisor (a, n), the equation has integer solutions $[x\ y]$ if and only if $(a, n) \mid b$. When indeed $(a, n) \mid b$, the Euclidean algorithm gives $\tilde{x}_0$ and $\tilde{y}_0$ such that $a\tilde{x}_0 + n\tilde{y}_0 = (a, n)$, and so $[x_0\ y_0] = [\tilde{x}_0 b/(a, n)\ \ \tilde{y}_0 b/(a, n)]$ is one solution of our equation. We seek all solutions. If $[x_1\ y_1]$ is another solution then $a(x_0 - x_1) + n(y_0 - y_1) = 0$, so to find all solutions it suffices to solve the homogeneous equation $ax + ny = 0$. Let $g = (a, n)$. Divide the homogeneous equation by g to get

$$(a/g)x + (n/g)y = 0.$$

Note that $(a/g, n/g) = 1$ because $g = (a, n) = (ga/g, gn/g) = g(a/g, n/g)$. The previous display and the coprimality and Euclid's Lemma say that n/g divides x and a/g divides y. Consequently the solution set of the homogeneous equation is

$$\mathbb{Z}[n/g\ \ -a/g].$$

Altogether, when (a, n) divides b, the solutions of $ax + ny = b$ are

$$[x_0\ y_0] + \mathbb{Z}[n/g\ -a/g], \quad \text{where } ax_0 + ny_0 = b.$$

8. The Congruence $ax = b \bmod n$

Again consider $a, b, n \in \mathbb{Z}$ with $n \neq 0$. For any $x \in \mathbb{Z}$ we have the equivalences

$$ax = b \bmod n \iff ax + ny = b \text{ for some } y.$$

So the work that we just did shows the following result.

Proposition 8.1. *Let $a, b, n \in \mathbb{Z}$ with $n \neq 0$, and let $g = \gcd(a, n)$. The congruence*

$$ax = b \bmod n$$

has solutions if and only if $g \mid b$. When the congruence has a solution $x_0 \in \mathbb{Z}$ then its full integer solution set is

$$x_0 + \mathbb{Z}n/g.$$

It follows that the equation $ax = b$ in $\mathbb{Z}/n\mathbb{Z}$ has g solutions,

$$\{x_0 + tn/g + n\mathbb{Z} : t = 0, 1, \dots, g - 1\}.$$

In particular, if $g = 1$ then the equation $ax = b$ has one solution in $\mathbb{Z}/n\mathbb{Z}$.

Perhaps the proposition is most easily remembered as a procedure:

> *To solve the congruence*
>
> $$ax = b \bmod n,$$
>
> *let*
>
> $$g = \gcd(a, n), \quad a = a'g, \quad n = n'g.$$
>
> *Then the congruence is*
>
> $$a'gx = b \bmod n'g.$$
>
> *Unless $b = b'g$ there are no solutions. If $b = b'g$ then the congruence becomes*
>
> $$a'x = b' \bmod n', \quad \gcd(a', n') = 1,$$

with unique solution

$$x_0 = {a'}^{-1} b' \bmod n'.$$

Thus the original congruence has solutions $x_0 + tn' \bmod n$, $t = 0, 1, \ldots, g-1$.