7. 2/21

7.1. There will be a test on Friday of next week (3/3). It will consist of 6–8 problems, the majority computation-based, not proof-based.

7.2. Let's write out $(\mathbf{Z}/m\mathbf{Z})^\times$ for some small values of m, and in the cases where a primitive root mod m exists, determine what they are. Recall that the size of $(\mathbf{Z}/m\mathbf{Z})^\times$ is the Euler totient $\varphi(m)$.

(1) $(\mathbf{Z}/2\mathbf{Z})^\times = \{\boxed{1}\}$.
(2) $(\mathbf{Z}/3\mathbf{Z})^\times = \{1, \boxed{2}\}$.
(3) $(\mathbf{Z}/4\mathbf{Z})^\times = \{1, \boxed{3}\}$.
(4) $(\mathbf{Z}/5\mathbf{Z})^\times = \{1, \boxed{2}, \boxed{3}, 4\}$.
(5) $(\mathbf{Z}/6\mathbf{Z})^\times = \{1, \boxed{5}\}$.
(6) $(\mathbf{Z}/7\mathbf{Z})^\times = \{1, 2, \boxed{3}, 4, \boxed{5}, 6\}$.
(7) $(\mathbf{Z}/8\mathbf{Z})^\times = \{1, 3, 5, 7\}$. No primitive roots mod 8.
(8) $(\mathbf{Z}/9\mathbf{Z})^\times = \{1, \boxed{2}, 4, \boxed{5}, 7, 8\}$.

Above, $\{a_1, a_2, \ldots\}$ is an abuse of notation for $\{a_1 + m\mathbf{Z}, a_2 + m\mathbf{Z}, \ldots\}$, as usual.

We conclude: For general a and m, it's hard to tell whether or not a gives rise to a primitive root mod m.

7.3. *Artin's conjecture on primitive roots* The following conjecture was posed in a letter by the number theorist Emil Artin on September 27, 1927, and remains unsolved. Emil Artin was the father of Professor Mike Artin here at MIT.

Conjecture 7.1. *Suppose $a \in \mathbf{Z}$ is neither a perfect square nor -1. Then there are infinitely many primes p such that $a + p\mathbf{Z}$ is a primitive root mod p.*

7.4. We define the *order* of a mod m to be the smallest positive integer $k \in \mathbf{N}$ such that $a^k \equiv 1 \pmod{m}$. Equivalently, it is the number of distinct congruence classes that appear as you take higher and higher powers of a. Thus a is a primitive root mod m if and only if its order is $\varphi(m)$.

What are the orders of the elements of $(\mathbf{Z}/7\mathbf{Z})^\times$?

a	1	2	$\boxed{3}$	4	$\boxed{5}$	6
$\mathrm{ord}_7(a)$	1	3	6	3	6	2

To build more intuition, here is the table for $(\mathbf{Z}/21\mathbf{Z})^\times$.

a	1	2	4	5	8	10	11	13	16	17	19	20
$\mathrm{ord}_{21}(a)$	1	6	3	6	2	6	6	2	3	6	6	2

We see that no element has order $\varphi(21) = 12$, so there are no primitive roots mod 21.

The tables are related. Anything coprime to 21 must be coprime to 7, so there is a well-defined map $(\mathbf{Z}/21\mathbf{Z})^\times \to (\mathbf{Z}/7\mathbf{Z})^\times$ that sends $a + 21\mathbf{Z} \mapsto a + 7\mathbf{Z}$. Similarly, there is a well-defined map $(\mathbf{Z}/21\mathbf{Z})^\times \to (\mathbf{Z}/3\mathbf{Z})^\times$.

How do $\mathrm{ord}_7(a)$ and $\mathrm{ord}_3(a)$ compare to $\mathrm{ord}_{21}(a)$? A third table:

a	1	2	4	5	8	10	11	13	16	17	19	20
$\mathrm{ord}_7(a)$	1	3	3	6	1	6	3	2	3	6	6	2
$\mathrm{ord}_3(a)$	1	2	1	2	2	1	2	1	1	2	1	2

It looks like $\mathrm{ord}_{21}(a)$ is the least common multiple of $\mathrm{ord}_7(a)$ and $\mathrm{ord}_3(a)$.

7.5. In general, we are led to guess that the structure of $(\mathbf{Z}/mn\mathbf{Z})^\times$ is built up from that of $(\mathbf{Z}/m\mathbf{Z})^\times$ and $(\mathbf{Z}/n\mathbf{Z})^\times$ in a certain precise way. However, the story seems clearest when m and n coprime.

By contrast, consider the case where $m = 6$ and $n = 3$, so that $mn = 18$. We see that $\mathrm{ord}_{18}(7) = 3$, whereas $\mathrm{ord}_6(7) = 1$ and $\mathrm{ord}_3(7) = 1$. Certainly, $3 \neq \mathrm{lcm}(1, 1)$.

7.6. *Interlude on sets and functions* For what follows, we need to review some terminology from set theory.

If X and Y are sets, then $X \times Y$ is the set of ordered pairs (x, y) with $x \in X$ and $y \in Y$.

A map $f : X \to Y$ is *injective* iff it sends different elements in X to different elements in Y. It is *surjective* iff every element in Y has a preimage in X. It is *bijective* iff it has a two-sided inverse: This means we can find a map $f^{-1} : Y \to X$ such that $(f^{-1} \circ f)(x) = x$ for all $x \in X$ and $(f \circ f^{-1})(y) = y$ for all $y \in Y$.

Theorem 7.2. *f is bijective if and only if it is both injective and surjective.*

Theorem 7.3. *If X and Y are finite sets of the same size, then f is injective if and only if it is surjective.*

7.7. *Chinese Remainder Theorem* Fix natural numbers $m, n \in \mathbf{N}$. Let $F : \mathbf{Z}/mn\mathbf{Z} \to \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ be defined by

$$F(a + mn\mathbf{Z}) = (a + m\mathbf{Z}, a + n\mathbf{Z}).$$

Theorem 7.4. *If m, n are coprime, then F is bijective.*

Proof. Note that $\mathbf{Z}/mn\mathbf{Z}$ and $\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ are both of size mn. So by Theorem 7.3, it is enough to show that F is surjective.

A general element of $\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ looks like $(b + m\mathbf{Z}, c + n\mathbf{Z})$. We must exhibit some $a + mn\mathbf{Z}$ such that $a \equiv b \pmod{m}$ and $a \equiv c \pmod{n}$. Since m, n are coprime, our theorem about linear Diophantine equations gives $x, y \in \mathbf{Z}$ such that $mx + ny = 1$. We claim that $a \equiv cmx + bny \pmod{mn}$ is our solution. Indeed,

$$a \equiv bny \equiv b(1 - mx) \equiv b \pmod{m},$$

and the argument that $a \equiv c \pmod{n}$ is analogous. □

Tomorrow, we will discuss what this theorem implies about the subset of units $(\mathbf{Z}/mn\mathbf{Z})^\times \subseteq \mathbf{Z}/mn\mathbf{Z}$.

8. 2/22

8.1. *Review* Yesterday, we introduced a map

$$F : \mathbf{Z}/mn\mathbf{Z} \to \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}.$$

It sends a congruence class $a + mn\mathbf{Z}$ to the ordered pair $(a + m\mathbf{Z}, a + n\mathbf{Z})$. (We are writing out these congruence classes as explicit sets in order to avoid ambiguity.)

The domain and range always have the same size, mn. The Chinese Remainder Theorem says that in the special case where m and n are coprime, F is bijective.

Example 8.1. If $m = 2$ and $n = 3$, then $mn = 6$ and F looks like:

a	0	1	2	3	4	5
$F(a)$	$(0,0)$	$(1,1)$	$(0,2)$	$(1,0)$	$(0,1)$	$(1,2)$

The bijectivity of F means that we can always reconstruct a uniquely from the knowledge of $F(a)$.

Example 8.2. If $m = 2$ and $n = 4$, then $mn = 8$ and F looks like:

a	0	1	2	3	4	5	6	7
$F(a)$	$(0,0)$	$(1,1)$	$(0,2)$	$(1,3)$	$(0,0)$	$(1,1)$	$(0,2)$	$(1,3)$

The map F fails to be injective because, *e.g.*, $F(0) = F(4)$; more generally, $F(a) = F(a + 4)$ for any a. It also fails to be surjective because, *e.g.*, there is no a such that $F(a) = (0, 1)$.

8.2. Earlier, we observed that if a is invertible mod mn, then a is invertible mod m and n separately. Therefore, F restricts to a well-defined map

$$F^\times : (\mathbf{Z}/mn\mathbf{Z})^\times \to (\mathbf{Z}/m\mathbf{Z})^\times \times (\mathbf{Z}/n\mathbf{Z})^\times.$$

Theorem 8.3. *If m, n are coprime, then $F^\times$ is bijective.*

Proof. The restriction of an injective map to a smaller domain is still injective, so $F^\times$ remains injective. (The analogous statement with "surjective" in place of "injective" is not true, so to prove surjectivity, we need more work.)

Suppose b, *resp.* c, is invertible mod m, *resp.* n. By the bijectivity of F, we can at least find a such that $a \equiv b \pmod{m}$ and $a \equiv c \pmod{n}$. It remains to show a is invertible mod mn.

We proved earlier that this happens precisely when $\gcd(a, mn) = 1$. So if a is not invertible mod mn, then a and mn have some common divisor greater than 1, which we can take to be a prime p. But then, by the prime divisor property on Stillwell page 29, p divides either m or n. So either $\gcd(a, m) > 1$ or $\gcd(a, n) > 1$, contradicting either the invertibility of b mod m or that of c mod n. □

Corollary 8.4. *If m, n are coprime, then $\varphi(mn) = \varphi(m)\varphi(n)$.*

Ultimately, we'd like to use Theorem 8.3 to prove our conjecture that if m, n are coprime and a is invertible mod mn, then

$$\mathrm{ord}_{mn}(a) = (\mathrm{ord}_m(a), \mathrm{ord}_n(a)).$$

I would like to put statements like this in a somewhat broader context: namely, that of group theory.

8.3. *Groups* A *group* is a set G together with a map $\star : G \times G \to G$, called a *binary operation* or *group law*, such that the following properties hold:

(1) Associativity. $(x \star y) \star z = x \star (y \star z)$ for all $x, y, z \in G$.
(2) Identity. There is some element $e \in G$ such that $e \star x = x \star e = x$ for all $x \in G$.
(3) Inverses. For all $x \in G$, there is some element $y \in G$ such that $x \star y = y \star x = e$.

Lemma 8.5. *The identity element is unique.*

Proof. If e, e' are identity elements of the same group, then $e = e \star e' = e'$. □

Lemma 8.6. *For any $x \in G$, the inverse of x is unique.*

Proof. If $y, z \in G$ are both inverses of x, then $x \star y = e = x \star z$. Therefore,

$$(y \star x) \star y = y \star (x \star y) = y \star (x \star z) = (y \star x) \star z.$$

The left-hand side simplifies to $e \star y = y$, and the right-hand side to $e \star z = z$. Thus $y = z$. □

8.4. Going forward, we will use associativity wherever it is needed without comment. In particular, we will drop the use of parentheses.

8.5. In this course, we are only interested in *abelian groups*. A group is *abelian* iff it additionally satisfies:

(4) Commutativity. $x \star y = y \star x$ for all $x, y \in G$.

Example 8.7. The integers form an abelian group under addition. That is, if we take $G = \mathbf{Z}$ and $\star = +$, then the axioms are satisfied: $+$ is associative and commutative, 0 is an identity element, and every integer n has an inverse under $+$ that is also an integer: namely, $-n$.

The integers do not form an abelian group under multiplication. What goes wrong? The identity element is forced to be 1. But then most integers cannot have an inverse that is also an integer.

Example 8.8. Similarly, for any $m \in \mathbf{Z}$, the set of congruence classes $\mathbf{Z}/m\mathbf{Z}$ forms an abelian group under addition. It does not form an abelian group under multiplication, except when $m = 1$.

Example 8.9. For any $m \in \mathbf{Z}$, the set of invertible congruence classes $(\mathbf{Z}/m\mathbf{Z})^\times$ forms an abelian group under multiplication. Indeed, the axiom about inverses is satisfied precisely because of how we defined invertibility mod m.

However, $(\mathbf{Z}/m\mathbf{Z})^\times$ does not form a group under addition, because the sum of two elements of $(\mathbf{Z}/m\mathbf{Z})^\times$ need not belong to $(\mathbf{Z}/m\mathbf{Z})^\times$. (Example?)

8.6. *Products of groups* If $(G, \star)$ and $(H, *)$ are groups, then we can form a new group in which the underlying set is $G \times H$ and the group law is the operation $\diamond$ defined by

$$(x, y) \diamond (x', y') = (x \star x', y * y').$$

If e_G and e_H are the respective identity elements of G and H, then the identity element of the new group is (e_G, e_H).

This is clearly relevant to the study of F and $F^\times$. We see that $\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ forms a group under coordinate-wise addition, and $(\mathbf{Z}/m\mathbf{Z})^\times \times (\mathbf{Z}/n\mathbf{Z})^\times$ forms a group under coordinate-wise multiplication.

8.7. *Orders of group elements* If $x \in G$, then the *order* of x is the smallest positive integer $k \in \mathbf{N}$ such that

$$\overbrace{x \star \cdots \star x}^{k \text{ copies of } x} = e.$$

In the case where $G = (\mathbf{Z}/m\mathbf{Z})^\times$ and $\star$ is multiplication, this recovers the definition we gave yesterday.

We will prove later that if $x \in G$ has order k and $y \in H$ has order ℓ, then $(x, y) \in G \times H$ has order $\operatorname{lcm}(k, \ell)$.

8.8. *Homomorphisms* A *homomorphism (of groups)* $(G, \star) \to (H, *)$ is a map $f : G \to H$ such that for all $x, y \in G$, we have

$$f(x \star y) = f(x) * f(y).$$

Intuitively, this means f transforms the operation $\star$ on G into the operation $*$ on H.

Lemma 8.10. *If $f : G \to H$ is a homomorphism, then f sends the identity of G to the identity of H.*

Proof. Writing e_G and e_H for the respective identity elements, we see $f(e_G) = f(e_G \star e_G) = f(e_G) * f(e_G)$. Multiplying both sides by the inverse of $f(e_G)$ in H, we get $e_H = f(e_G)$. □

An *isomorphism* is a bijective homomorphism. When two groups are related by an isomorphism, we say they are *isomorphic*. The isomorphism is like a Rosetta stone that perfectly translates either group law into the other, allowing us to treat the groups as the "same".

Example 8.11. For any fixed constant $c > 0$, the exponential map $f(x) = c^x$ defines a homomorphism $(\mathbf{R}, +) \to (\mathbf{R}_{>0}, \times)$. In fact, it is an isomorphism, because it has the two-sided inverse $f^{-1}(x) = \log_c(x)$.

Example 8.12. F is an isomorphism $(\mathbf{Z}/mn\mathbf{Z}, +) \to (\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}, +)$ (where the latter "+" is coordinate-wise addition). Similarly, the map $F^\times$ is an isomorphism $((\mathbf{Z}/mn\mathbf{Z})^\times, \times) \to ((\mathbf{Z}/m\mathbf{Z})^\times \times (\mathbf{Z}/n\mathbf{Z})^\times, \times)$.

9. 2/24

9.1. Recall that a homomorphism $(G, \star) \to (H, *)$ is a map $f : G \to H$ such that $f(x \star y) = f(x) * f(y)$.

We always have at least one: namely, the map that sends every element of G to the identity element of H, which we call the *trivial homomorphism*. Decide whether or not there is a *nontrivial* homomorphism...

(1) ... $(\mathbf{Z}, +) \to (\mathbf{Z}/6\mathbf{Z}, +)$.

(2) ... $(\mathbf{Z}/6\mathbf{Z}, +) \to (\mathbf{Z}, +)$.

(3) ... from $(G, \star)$ into $(G, \star)$, for general $(G, \star)$.

(4) ... $(\mathbf{Z}/15\mathbf{Z}, +) \to (\mathbf{Z}/5\mathbf{Z}, +)$.

(5) ... $((\mathbf{Z}/15\mathbf{Z})^\times, \times) \to ((\mathbf{Z}/5\mathbf{Z})^\times, \times)$.

(6) ... $(\mathbf{Z}/4\mathbf{Z}, +) \to ((\mathbf{Z}/5\mathbf{Z})^\times, \times)$.

9.2. The "mod 6" map $(\mathbf{Z}, +) \to (\mathbf{Z}/6\mathbf{Z}, +)$ is indeed a homomorphism: For any integers a and b, the very definition of addition mod 6 gives us

$$(a + b) + 6\mathbf{Z} = (a + 6\mathbf{Z}) + (b + 6\mathbf{Z}),$$

so the map does preserve addition. And this homomorphism is nontrivial.

9.3. By contrast, we claim the only homomorphism $f : (\mathbf{Z}/6\mathbf{Z}, +) \to (\mathbf{Z}, +)$ is the trivial one.

We know that a general element of this group can be written $a + 6\mathbf{Z}$ for some integer a. Adding this element to itself 6 times always results in $0 + 6\mathbf{Z}$. Since the homomorphism f must send the identity element $0 + 6\mathbf{Z} \in \mathbf{Z}/6\mathbf{Z}$ to the identity element $0 \in \mathbf{Z}$, we get

$$\begin{aligned} \overbrace{f(a + 6\mathbf{Z}) + \cdots + f(a + 6\mathbf{Z})}^{6 \text{ times}} &= f(\overbrace{(a + 6\mathbf{Z}) + \cdots + (a + 6\mathbf{Z})}^{6 \text{ times}}) \\ &= f(0 + 6\mathbf{Z}) \\ &= 0. \end{aligned}$$

That is, $6f(a + 6\mathbf{Z}) = 0$. This can happen only if $f(a + 6\mathbf{Z}) = 0$.

9.4. The last example is the most interesting, because we aren't used to seeing addition and multiplication mixed together.

Yet nontrivial homomorphisms $f : (\mathbf{Z}/4\mathbf{Z}, +) \to ((\mathbf{Z}/5\mathbf{Z})^\times, \times)$ do exist. For any integer a, there is a homomorphism given by

$$f(n + 4\mathbf{Z}) = a^n + 5\mathbf{Z},$$

and it is nontrivial when $a \not\equiv 1 \pmod 5$.

Note that on the left-hand side, $n + 4\mathbf{Z}$ is a congruence class, while on the right-hand side, the exponent n is an integer! So we are implicitly claimiing that this formula doesn't depend on how we choose the integer representing the congruence class. Once you grant this, f is a homomorphism because

$$f(n + n') \equiv a^{n+n'} \equiv a^n a^{n'} \equiv f(n) f(n'). \tag{9.1}$$

It is an analogue, for modular or congruence arithmetic, of the exponential maps that we study in precalculus.

We claim that if a is a primitive root mod 5, then f is also bijective, hence an isomorphism. Since $|\mathbf{Z}/4\mathbf{Z}| = 4 = |(\mathbf{Z}/5\mathbf{Z})^\times|$, it suffices to show that f is surjective: in other words, that every element of $(\mathbf{Z}/5\mathbf{Z})^\times$ takes the form a^n. But this is precisely what it means for a to be a primitive root.

Example 9.1. If $a \equiv 3 \pmod 5$, then the table of values is:

$$\begin{array}{cccccc} a & 0 & 1 & 2 & 3 \\ f(a) & 1 & 3 & 4 & 2 \end{array}$$

The table shows that $f(a)$ determines a uniquely (injectivity), and that every element mod 5 takes the form $f(a)$ (surjectivity). So f is bijective. Indeed, 3 gives a primitive root mod 5.

9.5. There is a slight generalization of the preceding setup. Let $(G, \star)$ be an arbitrary group with identity e. For any $a \in G$, write

$$a^{\star n} := \overbrace{a \star \cdots \star a}^{n \text{ copies of } a}.$$

Lemma 9.2. *If $a^{\star k} = e$, then there is a homomorphism:*

$$\begin{array}{ccc} (\mathbf{Z}/k\mathbf{Z}, +) & \to & (G, \star) \\ n + k\mathbf{Z} & \mapsto & a^{\star n} \end{array}$$

Proof. We will check that the map is well-defined. Then the proof that it is a homomorphism is basically (9.1).

Suppose n and n' are representatives of the same congruence class mod k. Then $n' = n + kd$ for some $d \in \mathbf{Z}$. But then

$$a^{\star n'} = a^{\star n} \star a^{\star kd} = a^{\star n} \star (a^{\star k})^{\star d} = a^{\star n}.$$

So $a^{\star n'} = a^{\star n}$, meaning this element of G is independent of whether we used n or n' to define it. □

9.6. By the way, note that any homomorphism f out of the group $(\mathbf{Z}/k\mathbf{Z}, +)$ is wholly determined by the value of f at $1 + k\mathbf{Z}$. Indeed,

$$\begin{aligned} f(n + k\mathbf{Z}) &= f(\overbrace{(1 + k\mathbf{Z}) + \cdots + (1 + k\mathbf{Z})}^{n \text{ times}}) \\ &= \overbrace{f(1 + k\mathbf{Z}) + \cdots + f(1 + k\mathbf{Z})}^{n \text{ times}}, \end{aligned}$$

so $f(n + k\mathbf{Z})$ is determined by $f(1 + k\mathbf{Z})$.