You will be given the following definitions on the exam.

Definition. *Two integers a and b are* **congruent modulo** m *if* $b - a = km$ *for some* $k \in \mathbb{Z}$. *This equivalence is written* $a \equiv b \pmod{m}$.

Definition. *Given a set S, a* **binary operator** $\star$ *is a rule that takes two elements $a, b \in S$ and manipulates them to give us a third, not necessarily distinct, element $a \star b$.*

Definition. *A* **group** *is a set G and binary operator $\star$ such that:*

- *(closure) For every $a, b \in G$ we have $a \star b \in G$.*
- *(identity) There exists a special element $e \in G$ so that for every $a \in G$ we have $a \star e = e \star a = a$; we often call this the identity element.*
- *(inverses) For every $a \in G$, there exists an element $a' \in G$ so that $a \star a' = a' \star a = e$.*
- *(associativity) For all $a, b, c \in G$ we have $a \star (b \star c) = (a \star b) \star c$.*

Definition. *A binary operator $\star$ on S is* **commutative** *if $a \star b = b \star a$ for all $a, b \in S$.*

Definition. *The* **order** *of a group $(G, \star)$ is the number of elements in G.*

Theorem. *If $a \equiv b$ and $c \equiv d \pmod m$ then $a + c \equiv b + d \pmod m$.*

Proof. This can be proved by applying the definition of congruence and doing some basic algebraic manipulation. By the definition of congruence we know that a and b differ by some multiple of m, i.e., $b - a = km$ for some $k \in \mathbb{Z}$. Likewise we know that c and d also differ by some multiple of m, i.e., $d - c = jm$ for some $j \in \mathbb{Z}$. Note that we used j instead of k since the multiple of m by which c and d differ might be different from the multiple by which a and b differ. We can then add these equations to get:

$$(b - a) + (d - c) = km + jm$$

or

$$(b + d) - (a + c) = (j + k)m.$$

By the definition of congruence modulo m, this is the same as saying $a + c$ is congruent to $b + d$ mod m, since the two sums differ by a multiple of m. □

Theorem. *If $a \equiv b$ and $c \equiv d \pmod m$ then $a \times c \equiv b \times d \pmod m$.*

Proof. By the definition of congruence we know that a and b differ by some multiple of m, i.e., $b - a = km$ for some $k \in \mathbb{Z}$. Likewise we know that c and d also differ by some multiple of m, i.e., $d - c = jm$ for some $j \in \mathbb{Z}$.

It is then helpful to rewrite these equations as

$$\begin{aligned} b &= km + a \\ d &= jm + c \end{aligned}$$

We multiply both sides by each other to obtain

$$\begin{aligned} bd &= (km + a)(jm + c) \\ &= jkm^2 + jma + kmc + ac \\ &= (jkm + ja + kc)m + ac. \end{aligned}$$

We then subtract ac from both sides to obtain

$$bd - ac = (jkm + ja + kc)m.$$

By the definition of congruence modulo m, this is the same as saying that $a \times c$ and $b \times d$ differ by an integer multiple of m, and so by definition are congruent mod m. □

Theorem. *If $a^2 + b^2 = 1 \pmod 4$, then exactly one of a or b is even/odd.*

Proof. On homework 8, you proved (and Dominick also posted solutions) that if n is even, then $n^2 \equiv 0 \pmod 4$, and if n is odd then $n^2 \equiv 1 \pmod 4$; you would need to prove this again on the exam if asked for this proof. You have also proved that we can add two congruence relations to obtain a third congruence relation (the first proof).

Therefore, if a and b are both even, then $a^2 \equiv 0$ (mod 4) and $b^2 \equiv 0$ (mod 4), and so $a^2+b^2 \equiv 0 \pmod 4$. If both are odd, then $a^2 \equiv 1$ (mod 4) and $b^2 \equiv 1 \pmod 4$, and so $a^2+b^2 \equiv 2 \pmod 4$. Therefore, if $a^2+b^2 \equiv 1 \pmod 4$, then it is not possible for both to be even or both to be odd, and so one must be even and the other odd. □

Theorem. *If $a^2 + b^2 + c^2 = 3 \pmod 4$, then a, b, c must all be odd*

Proof. On homework 8, you proved (and Dominick also posted solutions) that if n is even, then $n^2 \equiv 0 \pmod 4$, and if n is odd then $n^2 \equiv 1 \pmod 4$. You have also proved that we can add congruence relations to obtain a new congruence relation.

Therefore, if all of a, b, and c are odd, then all of a^2, b^2, and c^2 are congruent to 1 mod 4, and so $a^2 + b^2 + c^2 \equiv 3 \pmod 4$. If only 2 of them are odd, then $a^2+b^2+c^2 \equiv 2 \pmod 4$, if only 1 of them is odd then $a^2+b^2+c^2 \equiv 0 \pmod 4$, and if all are even then the sum is congruent to 0 mod 4. □

While the definition itself of a group guarantees the existence of an identity element, it does not tell us how many there are. Can we have five identity elements? Can we have even two? The following theorem tells us that a group has at most one identity element.

Theorem. *A group cannot have more than one identity element.*

Proof. Suppose that e and f are both identity elements of a group $G, \star$. We know the following two statements from the definition of any identity element of a group:

$$\begin{aligned} e &= e \star f \\ e \star f &= f. \end{aligned}$$

The first equation is true by definition of f being an identity element of G; the second equation is true by definition of e being an identity element of G. We can combine these two equations to conclude that $e = f$, showing that there can only be one identity element of a group. □

While the definition itself of a group guarantees that every element has an inverse, it does not say anything about how many inverses an element can have. Is it possible for a single element $a \in G$ to have more than one inverse? That is, can we find multiple elements in G so that combining any of them with a will give us the identity element?

Theorem. *An element of a group cannot have more than one inverse.*

Proof. We want to show that if some element a has two inverses, then those two inverse elements must be the same. To see this consider, let us consider two hypothetical inverses of a which we will call b and c. If b is an inverse of a, then we have:

$$a \star b = e. \tag{1}$$

We can combine c with both sides of this equation to obtain:

$$c \star (a \star b) = c \star e. \tag{2}$$

The associative property of the group operation $\star$ allows us to rewrite the left-hand side, and since e is the identity element, we can also rewrite the right-hand side. We obtain:

$$(c \star a) \star b = c. \tag{3}$$

Since we began by assuming that c is an inverse element of a, then $c \star a = e$, and $(c \star a) \star b = e \star b = b$. Equation (3) then becomes just:

$$b = c, \tag{4}$$

showing that if b and c are both inverse elements of a, then they must be the same element. In other words, a can only have one inverse. □