Math 417 – Fourth Day – Class

Bruce Reznick
University of Illinois at Urbana-Champaign

August 31, 2020

The Euclidean Algorithm computes $gcd(56, 200)$.

$$\underline{200} = 3 \cdot \underline{56} + \underline{32}$$

The Euclidean Algorithm computes $gcd(56, 200)$.

$$\underline{200} = 3 \cdot \underline{56} + \underline{32}$$

$$\underline{56} = 1 \cdot \underline{32} + \underline{24}$$

The Euclidean Algorithm computes $gcd(56, 200)$.

$$\underline{200} = 3 \cdot \underline{56} + \underline{32}$$
$$\underline{56} = 1 \cdot \underline{32} + \underline{24}$$
$$\underline{32} = 1 \cdot \underline{24} + \underline{8}$$

The Euclidean Algorithm computes $gcd(56, 200)$.

$$\underline{200} = 3 \cdot \underline{56} + \underline{32}$$
$$\underline{56} = 1 \cdot \underline{32} + \underline{24}$$
$$\underline{32} = 1 \cdot \underline{24} + \underline{8}$$
$$\underline{24} = 3 \cdot \underline{8}.$$

The Euclidean Algorithm computes $gcd(56, 200)$.

$$\underline{200} = 3 \cdot \underline{56} + \underline{32}$$
$$\underline{56} = 1 \cdot \underline{32} + \underline{24}$$
$$\underline{32} = 1 \cdot \underline{24} + \underline{8}$$
$$\underline{24} = 3 \cdot \underline{8}.$$

The Euclidean Algorithm computes $gcd(56, 200)$.

$$\underline{200} = 3 \cdot \underline{56} + \underline{32}$$
$$\underline{56} = 1 \cdot \underline{32} + \underline{24}$$
$$\underline{32} = 1 \cdot \underline{24} + \underline{8}$$
$$\underline{24} = 3 \cdot \underline{8}.$$

$$8 = 32 - 1 \cdot 24; \quad 24 = 56 - 1 \cdot 32 \implies$$

The Euclidean Algorithm computes $gcd(56, 200)$.

$$\underline{200} = 3 \cdot \underline{56} + \underline{32}$$
$$\underline{56} = 1 \cdot \underline{32} + \underline{24}$$
$$\underline{32} = 1 \cdot \underline{24} + \underline{8}$$
$$\underline{24} = 3 \cdot \underline{8}.$$

$$8 = 32 - 1 \cdot 24; \quad 24 = 56 - 1 \cdot 32 \implies$$
$$8 = 32 - (56 - 32) = 2 \cdot 32 - 56; \quad 32 = 200 - 3 \cdot 56 \implies$$

The Euclidean Algorithm computes $gcd(56, 200)$.

$$\underline{200} = 3 \cdot \underline{56} + \underline{32}$$
$$\underline{56} = 1 \cdot \underline{32} + \underline{24}$$
$$\underline{32} = 1 \cdot \underline{24} + \underline{8}$$
$$\underline{24} = 3 \cdot \underline{8}.$$

$$8 = 32 - 1 \cdot 24; \quad 24 = 56 - 1 \cdot 32 \implies$$
$$8 = 32 - (56 - 32) = 2 \cdot 32 - 56; \quad 32 = 200 - 3 \cdot 56 \implies$$
$$8 = 2 \cdot (200 - 3 \cdot 56) - 56 = 2 \cdot 200 - (2 \cdot 3 + 1) \cdot 56.$$

The Euclidean Algorithm computes $gcd(56, 200)$.

$$\underline{200} = 3 \cdot \underline{56} + \underline{32}$$
$$\underline{56} = 1 \cdot \underline{32} + \underline{24}$$
$$\underline{32} = 1 \cdot \underline{24} + \underline{8}$$
$$\underline{24} = 3 \cdot \underline{8}.$$

$$8 = 32 - 1 \cdot 24; \quad 24 = 56 - 1 \cdot 32 \implies$$
$$8 = 32 - (56 - 32) = 2 \cdot 32 - 56; \quad 32 = 200 - 3 \cdot 56 \implies$$
$$8 = 2 \cdot (200 - 3 \cdot 56) - 56 = 2 \cdot 200 - (2 \cdot 3 + 1) \cdot 56.$$
$$2 \cdot 200 = 400; \quad 7 \cdot 56 = 392, \qquad 400 - 392 = 8$$

The Euclidean Algorithm computes $gcd(56, 200)$.

$$\underline{200} = 3 \cdot \underline{56} + \underline{32}$$
$$\underline{56} = 1 \cdot \underline{32} + \underline{24}$$
$$\underline{32} = 1 \cdot \underline{24} + \underline{8}$$
$$\underline{24} = 3 \cdot \underline{8}.$$

$$8 = 32 - 1 \cdot 24; \quad 24 = 56 - 1 \cdot 32 \implies$$
$$8 = 32 - (56 - 32) = 2 \cdot 32 - 56; \quad 32 = 200 - 3 \cdot 56 \implies$$
$$8 = 2 \cdot (200 - 3 \cdot 56) - 56 = 2 \cdot 200 - (2 \cdot 3 + 1) \cdot 56.$$
$$2 \cdot 200 = 400; \quad 7 \cdot 56 = 392, \qquad 400 - 392 = 8 \quad \checkmark$$

The Euclidean Algorithm computes $gcd(56, 200)$.

$$\underline{200} = 3 \cdot \underline{56} + \underline{32}$$
$$\underline{56} = 1 \cdot \underline{32} + \underline{24}$$
$$\underline{32} = 1 \cdot \underline{24} + \underline{8}$$
$$\underline{24} = 3 \cdot \underline{8}.$$

$$8 = 32 - 1 \cdot 24; \quad 24 = 56 - 1 \cdot 32 \implies$$
$$8 = 32 - (56 - 32) = 2 \cdot 32 - 56; \quad 32 = 200 - 3 \cdot 56 \implies$$
$$8 = 2 \cdot (200 - 3 \cdot 56) - 56 = 2 \cdot 200 - (2 \cdot 3 + 1) \cdot 56.$$
$$2 \cdot 200 = 400; \quad 7 \cdot 56 = 392, \qquad 400 - 392 = 8 \quad \checkmark$$

And, as predicted, $gcd(\frac{56}{8}, \frac{200}{8}) = gcd(7, 25) = 1$. You can find the Euclidean Algorithm for this by dividing everything above by 8.

I'd like to spend a little more time on C_6 and on powers of elements forming a subgroup. Remember

$$G = \{e, a, a^2, a^3, a^4, a^5\}, \qquad a^6 = e.$$

I'd like to spend a little more time on C_6 and on powers of elements forming a subgroup. Remember

$$G = \{e, a, a^2, a^3, a^4, a^5\}, \qquad a^6 = e.$$

I'll talk about what the powers of a^j look like and $\langle a^j \rangle$.

I'd like to spend a little more time on C_6 and on powers of elements forming a subgroup. Remember

$$G = \{e, a, a^2, a^3, a^4, a^5\}, \qquad a^6 = e.$$

I'll talk about what the powers of a^j look like and $\langle a^j \rangle$.

The powers of e aren't exciting, because $e * e = e$, so $\langle e \rangle = \{e\}$. Since a generates the group, $\langle a \rangle = C_6$. I talked about $\langle a^2 \rangle$ and $\langle a^3 \rangle$ without details in the lecture. Here they are:

I'd like to spend a little more time on C_6 and on powers of elements forming a subgroup. Remember

$$G = \{e, a, a^2, a^3, a^4, a^5\}, \qquad a^6 = e.$$

I'll talk about what the powers of a^j look like and $\langle a^j \rangle$.

The powers of e aren't exciting, because $e * e = e$, so $\langle e \rangle = \{e\}$. Since a generates the group, $\langle a \rangle = C_6$. I talked about $\langle a^2 \rangle$ and $\langle a^3 \rangle$ without details in the lecture. Here they are:

$$a^2, (a^2)^2 = a^4, (a^2)^3 = a^6 = e; \qquad a^3, (a^3)^2 = a^6 = e.$$

I'd like to spend a little more time on C_6 and on powers of elements forming a subgroup. Remember

$$G = \{e, a, a^2, a^3, a^4, a^5\}, \qquad a^6 = e.$$

I'll talk about what the powers of a^j look like and $\langle a^j \rangle$.

The powers of e aren't exciting, because $e * e = e$, so $\langle e \rangle = \{e\}$. Since a generates the group, $\langle a \rangle = C_6$. I talked about $\langle a^2 \rangle$ and $\langle a^3 \rangle$ without details in the lecture. Here they are:

$$a^2, (a^2)^2 = a^4, (a^2)^3 = a^6 = e; \qquad a^3, (a^3)^2 = a^6 = e.$$

We can always stop when we get back to e because, for example, $(a^2)^4 = (a^2)^3 * a^2 = e * a^2 = a^2$. They just start repeating. So, as before,

I'd like to spend a little more time on C_6 and on powers of elements forming a subgroup. Remember

$$G = \{e, a, a^2, a^3, a^4, a^5\}, \qquad a^6 = e.$$

I'll talk about what the powers of a^j look like and $\langle a^j \rangle$.

The powers of e aren't exciting, because $e * e = e$, so $\langle e \rangle = \{e\}$. Since a generates the group, $\langle a \rangle = C_6$. I talked about $\langle a^2 \rangle$ and $\langle a^3 \rangle$ without details in the lecture. Here they are:

$$a^2, (a^2)^2 = a^4, (a^2)^3 = a^6 = e; \qquad a^3, (a^3)^2 = a^6 = e.$$

We can always stop when we get back to e because, for example, $(a^2)^4 = (a^2)^3 * a^2 = e * a^2 = a^2$. They just start repeating. So, as before,

$$\langle a^2 \rangle = \{e, a^2, a^4\}, \quad \langle a^3 \rangle = \{e, a^3\}.$$

This leaves $\langle a^4 \rangle$ and $\langle a^5 \rangle$. We have

This leaves $\langle a^4 \rangle$ and $\langle a^5 \rangle$. We have

$$a^4, (a^4)^2 = a^8 = a^2, (a^4)^3 = a^{12} = e;$$

This leaves $\langle a^4 \rangle$ and $\langle a^5 \rangle$. We have

$$a^4, (a^4)^2 = a^8 = a^2, (a^4)^3 = a^{12} = e;$$
$$a^5, (a^5)^2 = a^{10} = a^4, (a^5)^3 = a^{15} = a^3, (a^5)^4 = a^{20} = a^2,$$
$$(a^5)^5 = a^{25} = a, (a^5)^6 = a^{30} = e.$$

This leaves $\langle a^4 \rangle$ and $\langle a^5 \rangle$. We have

$$a^4, (a^4)^2 = a^8 = a^2, (a^4)^3 = a^{12} = e;$$
$$a^5, (a^5)^2 = a^{10} = a^4, (a^5)^3 = a^{15} = a^3, (a^5)^4 = a^{20} = a^2,$$
$$(a^5)^5 = a^{25} = a, (a^5)^6 = a^{30} = e.$$

That is,

$$\langle a^4 \rangle = \{e, a^4, a^2\} = \langle a^2 \rangle$$

This leaves $\langle a^4 \rangle$ and $\langle a^5 \rangle$. We have

$$a^4, (a^4)^2 = a^8 = a^2, (a^4)^3 = a^{12} = e;$$
$$a^5, (a^5)^2 = a^{10} = a^4, (a^5)^3 = a^{15} = a^3, (a^5)^4 = a^{20} = a^2,$$
$$(a^5)^5 = a^{25} = a, (a^5)^6 = a^{30} = e.$$

That is,

$$\langle a^4 \rangle = \{e, a^4, a^2\} = \langle a^2 \rangle$$

and

$$\langle a^5 \rangle = \{e, a^5, a^4, a^3, a^2, a\} = \langle a \rangle = G.$$

This leaves $\langle a^4 \rangle$ and $\langle a^5 \rangle$. We have

$$a^4, (a^4)^2 = a^8 = a^2, (a^4)^3 = a^{12} = e;$$
$$a^5, (a^5)^2 = a^{10} = a^4, (a^5)^3 = a^{15} = a^3, (a^5)^4 = a^{20} = a^2,$$
$$(a^5)^5 = a^{25} = a, (a^5)^6 = a^{30} = e.$$

That is,

$$\langle a^4 \rangle = \{e, a^4, a^2\} = \langle a^2 \rangle$$

and

$$\langle a^5 \rangle = \{e, a^5, a^4, a^3, a^2, a\} = \langle a \rangle = G.$$

There is a general principle at work. Note that $a^2 * a^4 = a * a^5 = e$.

This leaves $\langle a^4 \rangle$ and $\langle a^5 \rangle$. We have

$$a^4, (a^4)^2 = a^8 = a^2, (a^4)^3 = a^{12} = e;$$
$$a^5, (a^5)^2 = a^{10} = a^4, (a^5)^3 = a^{15} = a^3, (a^5)^4 = a^{20} = a^2,$$
$$(a^5)^5 = a^{25} = a, (a^5)^6 = a^{30} = e.$$

That is,

$$\langle a^4 \rangle = \{e, a^4, a^2\} = \langle a^2 \rangle$$

and

$$\langle a^5 \rangle = \{e, a^5, a^4, a^3, a^2, a\} = \langle a \rangle = G.$$

There is a general principle at work. Note that $a^2 * a^4 = a * a^5 = e$.

THEOREM If G is a group, $k \in \mathbb{N}$, and $x \in G$, then $\langle x^k \rangle \subseteq \langle x \rangle$.

This leaves $\langle a^4 \rangle$ and $\langle a^5 \rangle$. We have

$$a^4, (a^4)^2 = a^8 = a^2, (a^4)^3 = a^{12} = e;$$
$$a^5, (a^5)^2 = a^{10} = a^4, (a^5)^3 = a^{15} = a^3, (a^5)^4 = a^{20} = a^2,$$
$$(a^5)^5 = a^{25} = a, (a^5)^6 = a^{30} = e.$$

That is,

$$\langle a^4 \rangle = \{e, a^4, a^2\} = \langle a^2 \rangle$$

and

$$\langle a^5 \rangle = \{e, a^5, a^4, a^3, a^2, a\} = \langle a \rangle = G.$$

There is a general principle at work. Note that $a^2 * a^4 = a * a^5 = e$.

THEOREM If G is a group, $k \in \mathbb{N}$, and $x \in G$, then $\langle x^k \rangle \subseteq \langle x \rangle$.

PROOF By definition, $\langle g \rangle = \{g^i : i \in \mathbb{N}\}$. Thus if $y \in \langle x^k \rangle$, then $y = (x^k)^i$ for some i. That is, $y = x^{ki} \in \langle x \rangle$. □

THEOREM If $x \in G$ has order m, then $\langle x \rangle = \langle x^{-1} \rangle$.

THEOREM If $x \in G$ has order m, then $\langle x \rangle = \langle x^{-1} \rangle$.

PROOF The situation is that $\{e, x, x^2, \ldots, x^{m-1}\}$ are distinct and $x^m = e$. Then $x * x^{m-1} = x^{1+(m-1)} = x^m = e$, so $x^{-1} = x^{m-1}$. What are the powers of x^{-1}? We have

THEOREM If $x \in G$ has order m, then $\langle x \rangle = \langle x^{-1} \rangle$.

PROOF The situation is that $\{e, x, x^2, \ldots, x^{m-1}\}$ are distinct and $x^m = e$. Then $x * x^{m-1} = x^{1+(m-1)} = x^m = e$, so $x^{-1} = x^{m-1}$. What are the powers of x^{-1}? We have

$$(x^{-1})^2 = x^{-1} * x^{-1} = x^{m-1} * x^{m-1} = x^{2m-2} = x^m * x^{m-2} = x^{m-2},$$

THEOREM If $x \in G$ has order m, then $\langle x \rangle = \langle x^{-1} \rangle$.

PROOF The situation is that $\{e, x, x^2, \ldots, x^{m-1}\}$ are distinct and $x^m = e$. Then $x * x^{m-1} = x^{1+(m-1)} = x^m = e$, so $x^{-1} = x^{m-1}$. What are the powers of x^{-1}? We have

$$(x^{-1})^2 = x^{-1} * x^{-1} = x^{m-1} * x^{m-1} = x^{2m-2} = x^m * x^{m-2} = x^{m-2},$$

and, more generally,

$$(x^{-1})^k = (x^{m-1})^k = x^{km-k} = x^{(k-1)m+m-k} = (x^m)^{k-1} x^{m-k} = x^{m-k}.$$

THEOREM If $x \in G$ has order m, then $\langle x \rangle = \langle x^{-1} \rangle$.

PROOF The situation is that $\{e, x, x^2, \ldots, x^{m-1}\}$ are distinct and $x^m = e$. Then $x * x^{m-1} = x^{1+(m-1)} = x^m = e$, so $x^{-1} = x^{m-1}$. What are the powers of x^{-1}? We have

$$(x^{-1})^2 = x^{-1} * x^{-1} = x^{m-1} * x^{m-1} = x^{2m-2} = x^m * x^{m-2} = x^{m-2},$$

and, more generally,

$$(x^{-1})^k = (x^{m-1})^k = x^{km-k} = x^{(k-1)m+m-k} = (x^m)^{k-1} x^{m-k} = x^{m-k}.$$

Thus, $\langle x^{-1} \rangle = \{e, x^{m-1}, x^{m-2}, \ldots x\} = \langle x \rangle$. □

THEOREM If $x \in G$ has order m, then $\langle x \rangle = \langle x^{-1} \rangle$.

PROOF The situation is that $\{e, x, x^2, \ldots, x^{m-1}\}$ are distinct and $x^m = e$. Then $x * x^{m-1} = x^{1+(m-1)} = x^m = e$, so $x^{-1} = x^{m-1}$. What are the powers of x^{-1}? We have

$$(x^{-1})^2 = x^{-1} * x^{-1} = x^{m-1} * x^{m-1} = x^{2m-2} = x^m * x^{m-2} = x^{m-2},$$

and, more generally,

$$(x^{-1})^k = (x^{m-1})^k = x^{km-k} = x^{(k-1)m+m-k} = (x^m)^{k-1} x^{m-k} = x^{m-k}.$$

Thus, $\langle x^{-1} \rangle = \{e, x^{m-1}, x^{m-2}, \ldots x\} = \langle x \rangle$. □

Taking powers of x^{-1} just gives us the same elements in reverse order, as we saw with $x = a, x = a^2$ in C_6.

One thing new that I wanted to prove was to show that the only groups of order 4 are C_4 and V up to isomorphism. This will use the fact that the rows and the columns of a group multiplication table have to be different.

One thing new that I wanted to prove was to show that the only groups of order 4 are C_4 and V up to isomorphism. This will use the fact that the rows and the columns of a group multiplication table have to be different.

Suppose G is a group of order 4. I want to distinguish two cases:

One thing new that I wanted to prove was to show that the only groups of order 4 are C_4 and V up to isomorphism. This will use the fact that the rows and the columns of a group multiplication table have to be different.

Suppose G is a group of order 4. I want to distinguish two cases:
(i) For every $g \in G$, $g^2 = e$.

One thing new that I wanted to prove was to show that the only groups of order 4 are C_4 and V up to isomorphism. This will use the fact that the rows and the columns of a group multiplication table have to be different.

Suppose G is a group of order 4. I want to distinguish two cases:
(i) For every $g \in G$, $g^2 = e$.

(ii) There exists (at least one) element $x \in G$ so that $x^2 \neq e$.

One thing new that I wanted to prove was to show that the only groups of order 4 are C_4 and V up to isomorphism. This will use the fact that the rows and the columns of a group multiplication table have to be different.

Suppose G is a group of order 4. I want to distinguish two cases:
(i) For every $g \in G$, $g^2 = e$.

(ii) There exists (at least one) element $x \in G$ so that $x^2 \neq e$.

We'll fill out the multiplication tables and show that (i) forces an isomorphism to V and (ii) forces an isomorphism to C_4.

(i) So, let's call the elements of the group $\{e, x, y, z\}$, so they are all different and we know by hypothesis that $x^2 = y^2 = z^2 = e$.

(i) So, let's call the elements of the group $\{e, x, y, z\}$, so they are all different and we know by hypothesis that $x^2 = y^2 = z^2 = e$.

G	e	x	y	z
e	e	x	y	z
x	x	e	?	?
y	y	?	e	?
z	z	?	?	e

(i) So, let's call the elements of the group $\{e, x, y, z\}$, so they are all different and we know by hypothesis that $x^2 = y^2 = z^2 = e$.

G	e	x	y	z
e	e	x	y	z
x	x	e	?	?
y	y	?	e	?
z	z	?	?	e

What can $x * y$ be? It can't be x or e because it shares a row with them and it can't be y because it shares a column, and it has to be in G, so it has to be z. Similarly, any product of two of these gives the third. So we have, on the next page,

G	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

V	I	X	Y	Z
I	I	X	Y	Z
X	X	I	Z	Y
Y	Y	Z	I	X
Z	Z	Y	X	I

G	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

V	I	X	Y	Z
I	I	X	Y	Z
X	X	I	Z	Y
Y	Y	Z	I	X
Z	Z	Y	X	I

There is an isomorphism Φ between G and V and it is defined by $\Phi(e) = I$, $\Phi(x) = X$, $\Phi(y) = Y$, $\Phi(z) = Z$.

Now we consider (ii). There is an element $x \in G$ so that $x^2 = x * x \neq e$. Let's write the elements of the group as $\{e, x, x^2, y\}$, and complete the table as far as we can.

Now we consider (ii). There is an element $x \in G$ so that $x^2 = x * x \neq e$. Let's write the elements of the group as $\{e, x, x^2, y\}$, and complete the table as far as we can.

G	e	x	x^2	y
e	e	x	x^2	y
x	x	x^2	?	?
x^2	x^2	?	?	?
y	y	?	?	?

Now we consider (ii). There is an element $x \in G$ so that $x^2 = x * x \neq e$. Let's write the elements of the group as $\{e, x, x^2, y\}$, and complete the table as far as we can.

G	e	x	x^2	y
e	e	x	x^2	y
x	x	x^2	?	?
x^2	x^2	?	?	?
y	y	?	?	?

The first thing you might think about is $x * x^2$, but all the table tells you is that it's not x, x^2, so it has to be e or y.

Now we consider (ii). There is an element $x \in G$ so that $x^2 = x * x \neq e$. Let's write the elements of the group as $\{e, x, x^2, y\}$, and complete the table as far as we can.

G	e	x	x^2	y
e	e	x	x^2	y
x	x	x^2	?	?
x^2	x^2	?	?	?
y	y	?	?	?

The first thing you might think about is $x * x^2$, but all the table tells you is that it's not x, x^2, so it has to be e or y.

It is faster to look at $x * y$, which can't be x, x^2 or y, so it has to be e. The same thing holds for $y * x$, as we'll see on the next page.

G	e	x	x^2	y
e	e	x	x^2	y
x	x	x^2	?	e
x^2	x^2	?	?	?
y	y	e	?	?

G	e	x	x^2	y
e	e	x	x^2	y
x	x	x^2	?	e
x^2	x^2	?	?	?
y	y	e	?	?

Now we can fill out the rows and see that $x * x^2$ has to be y and $x^2 * x$ has to be y, so $y = x^3$, and the table starts to look familiar

G	e	x	x^2	y
e	e	x	x^2	y
x	x	x^2	?	e
x^2	x^2	?	?	?
y	y	e	?	?

Now we can fill out the rows and see that $x * x^2$ has to be y and $x^2 * x$ has to be y, so $y = x^3$, and the table starts to look familiar

G	e	x	x^2	x^3
e	e	x	x^2	x^3
x	x	x^2	x^3	e
x^2	x^2	x^3	?	?
x^3	x^3	e	?	?

G	e	x	x^2	y
e	e	x	x^2	y
x	x	x^2	?	e
x^2	x^2	?	?	?
y	y	e	?	?

Now we can fill out the rows and see that $x * x^2$ has to be y and $x^2 * x$ has to be y, so $y = x^3$, and the table starts to look familiar

G	e	x	x^2	x^3
e	e	x	x^2	x^3
x	x	x^2	x^3	e
x^2	x^2	x^3	?	?
x^3	x^3	e	?	?

We don't even have to finish the table, we have $x * x^3 = e = x^4$ and $G = \{e, x, x^2, x^3\}$, so this is a cyclic group of order 4.

TWO WORKSHEET PROBLEMS

Divide into groups. Calculators are ok, but not necessary.

1. Determine $g = gcd(30, 72)$ and find integers r, s so that $g = 30r + 72s$.

2. Recall that $((\mathbb{Z}/7\mathbb{Z})^*, \odot)$ is the multiplicative group mod 7 of relatively prime classes. Since 7 is prime,

$$(\mathbb{Z}/7\mathbb{Z})^* = \{[1]_7, [2]_7, [3]_7, [4]_7, [5]_7, [6]_7\}$$

For each a, determine $\langle [a]_7 \rangle$. Which a have the property that $\langle [a]_7 \rangle = (\mathbb{Z}/7\mathbb{Z})^*$?

SOLUTION to 1:

$$\underline{72} = 2 \cdot \underline{30} + \underline{12}$$

SOLUTION to 1:

$$\underline{72} = 2 \cdot \underline{30} + \underline{12}$$
$$\underline{30} = 2 \cdot \underline{12} + \underline{6}$$

SOLUTION to 1:

$$\underline{72} = 2 \cdot \underline{30} + \underline{12}$$
$$\underline{30} = 2 \cdot \underline{12} + \underline{6}$$
$$\underline{12} = 2 \cdot \underline{6}.$$

SOLUTION to 1:

$$\underline{72} = 2 \cdot \underline{30} + \underline{12}$$
$$\underline{30} = 2 \cdot \underline{12} + \underline{6}$$
$$\underline{12} = 2 \cdot \underline{6}.$$

$gcd(30, 72) = 6.$

SOLUTION to 1:

$$\underline{72} = 2 \cdot \underline{30} + \underline{12}$$
$$\underline{30} = 2 \cdot \underline{12} + \underline{6}$$
$$\underline{12} = 2 \cdot \underline{6}.$$

$gcd(30, 72) = 6.$

$$6 = 30 - 2 \cdot 12; 12 = 72 - 2 \cdot 30 \implies 6 = 30 - 2(72 - 2 \cdot 30)$$
$$= (1 + 2 \cdot 2)30 - 2 * 72 = 5 \cdot 30 - 2 \cdot 72 = 150 - 144$$

SOLUTION to 1:

$$\underline{72} = 2 \cdot \underline{30} + \underline{12}$$
$$\underline{30} = 2 \cdot \underline{12} + \underline{6}$$
$$\underline{12} = 2 \cdot \underline{6}.$$

$gcd(30, 72) = 6.$

$$6 = 30 - 2 \cdot 12; 12 = 72 - 2 \cdot 30 \implies 6 = 30 - 2(72 - 2 \cdot 30)$$
$$= (1 + 2 \cdot 2)30 - 2 * 72 = 5 \cdot 30 - 2 \cdot 72 = 150 - 144 \qquad \checkmark$$

Note that $gcd(\frac{30}{6}, \frac{72}{6}) = gcd(5, 12) = 1.$

SOLUTION to 2

I'll just write a for $[a]_7$ a lot of the time.

SOLUTION to 2

I'll just write a for $[a]_7$ a lot of the time.

As always, $\langle 1 \rangle = 1$. Since $2^2 = 4$, $2^3 = 8 \equiv 1 \mod 7$, $[2]_7$ has order 3, and $[2]_7^{-1} = [2]_7^2 = 4$, so

SOLUTION to 2

I'll just write a for $[a]_7$ a lot of the time.

As always, $\langle 1 \rangle = 1$. Since $2^2 = 4$, $2^3 = 8 \equiv 1 \mod 7$, $[2]_7$ has order 3, and $[2]_7^{-1} = [2]_7^2 = 4$, so

$$\langle 2 \rangle = \{1, 2, 4\} = \{1, 4, 2\} = \langle 4 \rangle$$

SOLUTION to 2

I'll just write a for $[a]_7$ a lot of the time.

As always, $\langle 1 \rangle = 1$. Since $2^2 = 4$, $2^3 = 8 \equiv 1 \mod 7$, $[2]_7$ has order 3, and $[2]_7^{-1} = [2]_7^2 = 4$, so

$$\langle 2 \rangle = \{1, 2, 4\} = \{1, 4, 2\} = \langle 4 \rangle$$

The powers of 3 are 1, 3, $3^2 = 9 \equiv 2 \mod 7$, $3^3 = 27 \equiv 6 \mod 7$, $3^4 = 81 \equiv 4 \mod 7$, $3^5 = 243 \equiv 5 \mod 7$, $3^6 = 729 \equiv 1 \mod 7$,

SOLUTION to 2

I'll just write a for $[a]_7$ a lot of the time.

As always, $\langle 1 \rangle = 1$. Since $2^2 = 4$, $2^3 = 8 \equiv 1 \mod 7$, $[2]_7$ has order 3, and $[2]_7^{-1} = [2]_7^2 = 4$, so

$$\langle 2 \rangle = \{1, 2, 4\} = \{1, 4, 2\} = \langle 4 \rangle$$

The powers of 3 are 1, 3, $3^2 = 9 \equiv 2 \mod 7$, $3^3 = 27 \equiv 6 \mod 7$, $3^4 = 81 \equiv 4 \mod 7$, $3^5 = 243 \equiv 5 \mod 7$, $3^6 = 729 \equiv 1 \mod 7$,

$$\langle 3 \rangle = \{1, 3, 2, 6, 4, 5\} = (\mathbb{Z}/7\mathbb{Z})^* = \langle 5 \rangle$$

Note that $[3]_7^{-1} = [3]_7^5 = 5$. Also, $3 * 5 = 15 \equiv 1 \mod 7$. You can simplify powers by working mod 7 all along, so $3^2 \equiv 2 \mod 7$ implies that $3^4 = (3^2)^2 \equiv 2^2 = 4 \mod 7$, etc.

SOLUTION to 2

I'll just write a for $[a]_7$ a lot of the time.

As always, $\langle 1 \rangle = 1$. Since $2^2 = 4$, $2^3 = 8 \equiv 1 \mod 7$, $[2]_7$ has order 3, and $[2]_7^{-1} = [2]_7^2 = 4$, so

$$\langle 2 \rangle = \{1, 2, 4\} = \{1, 4, 2\} = \langle 4 \rangle$$

The powers of 3 are 1, 3, $3^2 = 9 \equiv 2 \mod 7$, $3^3 = 27 \equiv 6 \mod 7$, $3^4 = 81 \equiv 4 \mod 7$, $3^5 = 243 \equiv 5 \mod 7$, $3^6 = 729 \equiv 1 \mod 7$,

$$\langle 3 \rangle = \{1, 3, 2, 6, 4, 5\} = (\mathbb{Z}/7\mathbb{Z})^* = \langle 5 \rangle$$

Note that $[3]_7^{-1} = [3]_7^5 = 5$. Also, $3 * 5 = 15 \equiv 1 \mod 7$. You can simplify powers by working mod 7 all along, so $3^2 \equiv 2 \mod 7$ implies that $3^4 = (3^2)^2 \equiv 2^2 = 4 \mod 7$, etc.

Finally, $6^2 = 36 \equiv 1 \mod 7$, so $\langle 6 \rangle = \{1, 6\}$. This always happens: $(m-1)^2 = m^2 - 2m + 1 = m(m-2) + 1 \equiv 1 = (-1)^2 \mod m$.