Equivalence Classes

Let $R$ be a relation on $\mathcal{P}([m])$ defined by $(A, B) \in R$ if and only if $A \cap [m] = B \cap [m]$. You proved as part of the practice problems for midterm 3 that $R$ is an equivalence relation.

How many equivalence classes are there? Describe the equivalence classes in the simplest possible way.

For each $X \subseteq [m]$, the set $C_X = \{ A \subseteq [2m] | A \cap [m] = X \}$ is an equivalence class. Indeed, for any $A, B \in C_X$,

$$A \cap [m] = B \cap [m] = X.$$

Conversely, any equivalence class $C$ of $R$ may be written as $C_X$ for some $X \subseteq [m]$. Indeed, let $C$ be an equivalence class of $R$ and let $A \in C$. Define $X = A \cap [m]$. Then $A \in C_X$.

$X \subseteq [m]$ and $C = C_X$.

The equivalence classes of $R$ are thus precisely

$$\{ C_X | X \subseteq [m] \},$$

and there are thus $|\mathcal{P}([m])| = 2^m$ of them.
Number Theory

Important Identities

For every \( a, b \in \mathbb{R} \) and every natural number \( n > 1 \):

(a) \( a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \ldots + b^{n-1}) \)

\[ = (a-b) \sum_{i=0}^{n-1} a^{n-1-i}b^i \]

(b) \( a^{2n+1} + b^{2n+1} = (a+b)(a^{2n} - a^{2n-1}b + a^{2n-2}b^2 - \ldots + b^{2n}) \)

\[ = (a+b) \sum_{i=0}^{2n} (-1)^i a^{2n-i}b^i \]

Proof

(a) We induct on \( n > 1 \). The base case is trivial since \( a^2 - b^2 = (a-b)(a+b) \). Now let us assume that \( a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \ldots + b^{n-1}) \) for some \( n > 1 \). Then:

\[ a^{n+1} - b^{n+1} = a \cdot a^n - b \cdot b^n \]

\[ = a \cdot a^{n-1} - b \cdot a^{n-1} + b \cdot a^{n-1} - b \cdot b^n \]

\[ = (a-b) a^{n-1} + b (a^{n-1} - b^{n-1}) \]

\[ = (a-b) a^{n-1} + b (a^{n-1} + a^{n-2}b + \ldots + b^{n-1}) \]

\[ = (a-b) (a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \ldots + b^{n-1}) \]
(b) We induct on \( m \geq 1 \). The base case is trivial since

\[
(a+b)(a^2-ab+b^2) = a^3 - a^2b + ab^2 + a^2b - ab^2 + b^3 = a^3 + b^3
\]

Now let us assume that \( a^n + b^n = (a+b)(a^{n-1} - a^{n-2}b + \ldots + b^{n-1}) \) for some \( n \geq 1 \). Then:

\[
(a+b)(a^{2n+2} - a^{2n+1}b + \ldots - a^2b^n + b^n) = a^{2n+3} - a^{2n+2}b + \ldots + ab^{2n+1} + b^{2n+3}
\]

\[
= a^3 + b^3
\]

Applications

21 Show that \( 2^{6+1} + 1 \) and \( 2^{10+1} + 1 \) are not prime.

By (b) above with \( a = 4, \ b = 1, \) and \( n = 1 \) we see that

\[
2^{6+1} + 1 = 4^3 + 1 = 4^{2+1} + 1 = (4+1)(4^2 - 4 + 1)
\]

so indeed \( 2^{6+1} \) is not prime.

Similarly, by (b) above with \( a = 2^4 = 16, \ b = 1, \) and \( n = 12 \):

\[
2^{10+1} + 1 = 2^{12+1} + 1 = 16^{2+1} + 1 = (16+1)(16^{2} - 16^{1} + 16^{0} - 16^-1)
\]

\[
\ldots = (16+1)(16^{2} - 16^{1} + 16^{0} - 16^{-1} - 16+1)
\]
i.e. $2^{100} + 1$ is divisible by 17 and thus not prime.

Congruence equations

General recipe

To solve $ax \equiv b \pmod{m}$ ($\exists b \in \mathbb{Z} \quad ax - bl = km$)

First: compute $\gcd(a, m)$.

If $b$ is not divisible

by $\gcd(a, m)$

Then there are no solutions.

If $b$ is divisible by $\gcd(a, m)$

If $\gcd(a, m) = 1$

There is a unique solution

(abstract class of solutions)

If $\gcd(a, m) > 1$

There are $d$ (congruence classes of) solutions.

\* This is because $a$ has a "multiplicative inverse modulo $m$"
when $\gcd(a, m) = 1$, e.g. $3$ is the multiplicative inverse
of $2$ modulo $5$ since $2 \cdot 3 = 6 \equiv 1 \pmod{5}$, and therefore
$2x \equiv b \pmod{5}$ has a unique solution $x \equiv 3b \pmod{5}$. 
This is because \( a \) does not have a multiplicative inverse modulo \( n \) when \( \gcd(a, n) > 1 \), e.g., 2 does not have a multiplicative inverse modulo 4 (which means there is no \( x \) such that \( 2x \equiv 1 \pmod{4} \)), and therefore \( 2x \equiv 0 \pmod{4} \) has two solutions: \( x \equiv 0 \pmod{4} \) and \( x \equiv 2 \pmod{4} \).

3. Solve \( 54x \equiv 3 \pmod{35} \)

We compute \( \gcd(54, 35) \) via the Euclidean Algorithm:

\[
54 = 1 \cdot 35 + 19
\]
\[
35 = 1 \cdot 19 + 16
\]
\[
19 = 1 \cdot 16 + 3
\]
\[
16 = 5 \cdot 3 + 1
\]

Therefore \( \gcd(54, 35) = 1 \).

Note that solving \( 54x \equiv 3 \pmod{35} \) for \( x \) is equivalent to solving \( 54x + 35y = 3 \) for \( x \) and \( y \).

This is a linear Diophantine equation with two unknowns. It suffices to find a particular solution so we reverse-engineer the Euclidean Algorithm:
\[ 1 = 16 - 5 \cdot 3 \]
\[ = 16 - 5 \cdot (19 - 16) \]
\[ = 6 \cdot 16 - 5 \cdot 19 \]
\[ = 6 \cdot (35 - 19) - 5 \cdot 19 \]
\[ = 6 \cdot 35 - 11 \cdot 19 \]
\[ = 6 \cdot 35 - 11 \cdot (54 - 35) \]
\[ = 17 \cdot 35 - 11 \cdot 54 \]

*This tells us that \((-11) \cdot 54 \equiv 1 \pmod{35}, i.e. -11 is the multiplicative inverse of 54 modulo 35.*

So we have that \((x, y) = (-11, 17)\) solves \(54x + 35y = 1\), and therefore \(x \equiv -33 \pmod{35}\) solves \(54x \equiv 3 \pmod{35}\), or equivalently: \(x \equiv 2 \pmod{35}\).

4] Solve \(18x \equiv 2 \pmod{15}\)

We compute \(\gcd(18, 15)\): \(18 = 1 \cdot 15 + 3\)
\(15 = 5 \cdot 3\)

i.e. \(\gcd(18, 15) = 3\). Since 2 is not divisible by 3, this congruence equation does not have any solutions.
Systems of Congruence Equations

5] Solve \[ \begin{align*}
2x + 3y &\equiv 1 \pmod{6} \quad (1) \\
x + 3y &\equiv 4 \pmod{6} \quad (2)
\end{align*} \]

\[(1) + (2) \Rightarrow 3x + 6y \equiv 5 \pmod{6} \]
\[\Rightarrow 3x \equiv 5 \pmod{6} \]

Since \( \gcd(3, 6) = 3 \) and 5 is not divisible by 3, there are no solutions.

6] Solve \[ \begin{align*}
2x + 3y &\equiv 1 \pmod{6} \quad (1) \\
x + 3y &\equiv 5 \pmod{6} \quad (2)
\end{align*} \]

\[(1) - (2) \Rightarrow x \equiv -4 \pmod{6} \]
\[\Rightarrow x \equiv 2 \pmod{6} \quad (1') \]

Substitute (1') into (2): \[ 2 + 3y \equiv 5 \pmod{6} \]
\[\Rightarrow 3y \equiv 3 \pmod{6} \]

Since \( \gcd(3, 6) = 3 \), which divides 3, there are 3 solutions:
\[ \begin{align*}
y &\equiv 1 \pmod{6}, \\
y &\equiv 3 \pmod{6}, \text{ and} \\
y &\equiv 5 \pmod{6}.
\end{align*} \]