MATH 135 - Linear Diophantine & Modular Equations Review

Based on *Language and Proofs in Algebra: An Introduction Version 1.3* by *University of Waterloo Faculty of Mathematics*. Sheet created in 2023 by *wkennedy* under fair use for education.

7.1 Linear Diophantine Equation Theorem, Part 1 (LDET 1)

For all integers a, b and c, with a and b both not zero,
the linear Diophantine equation $ax + by = c$ (in variables x and y)
has an integer solution if and only if $d \mid c$, where $d = \gcd(a, b)$.

7.2 Linear Diophantine Equation Theorem, Part 2 (LDET 2)

Let a, b and c be integers with a and b both not zero, and define $d = \gcd(a, b)$.
If $x = x_0$ and $y = y_0$ is one particular integer solution to
the linear Diophantine equation $ax + by = c$,
then the set of all solutions is given by $\{(x, y) : x = x_0 + \frac{b}{d}n, y = y_0 - \frac{a}{d}n, n \in \mathbb{Z}\}$.

8.1 Definition of Congruence

Let m be a fixed positive integer.
For integers a and b, we say that a is congruent to b modulo m, and write
$a \equiv b \pmod{m}$, when $m \mid (a - b)$.

For integers a and b such that $m \nmid (a - b)$, we write $a \not\equiv b \pmod{m}$.
We refer to $\equiv$ as congruence, and m as its modulus.

8.2 Congruence is an Equivalence Relation (CER)

For all integers a, b and c, we have

1. Reflexivity: $a \equiv a \pmod{m}$
2. Symmetry: If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$
3. Transitivity: If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$

8.2 Congruence Add and Multiply (CAM)

For all positive integers n, for all integers $a_1, a_2, \cdots, a_n$ and $b_1, b_2, \cdots, b_n$,
if $a_i \equiv b_i \pmod{m}$ for all $1 \le i \le n$ then

1. $a_1 + a_2 + \cdots a_n \equiv b_1 + b_2 + \cdots b_n \pmod{m}$
2. $a_1 a_2 \cdots a_n \equiv b_1 b_2 \cdots b_n \pmod{m}$

8.2 Congruence Power (CP)

For all positive integers n and integers a and b,
if $a \equiv b \pmod{m}$, then $a^n \equiv b^n \pmod{m}$.

8.2 Congruence Divide (CD)

For all integers a, b and c,
if $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$.

8.3 Congruence Iff Same Remainder (CISR)

For all integers a and b,
$a \equiv b \pmod{m}$ if and only if a and b have the same remainder when divided by m.

8.3 Congruent to Remainder (CTR)

For all integers a and b with $0 \le b < m$,
$a \equiv b \pmod{m}$ if and only if a has remainder b when divided by m.

8.4 Linear Congruence Theorem (LCT)

For all integers a and c, with a non-zero,
the linear congruence $ax \equiv c \pmod{m}$ has a solution if and only if $d \mid c$, where $d = \gcd(a, m)$.

Moreover, if $x = x_0$ is one particular solution to this congruence,
then the set of all solutions is given by $\{x \in \mathbb{Z} : x \equiv x_0 \pmod{\frac{m}{d}}\}$,
or, equivalently, $\{x \in \mathbb{Z} : x \equiv x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \ldots, x_0 + (d-1)\frac{m}{d} \pmod{m}\}$.

8.5 Non-Linear Congruences

table go brrr

Test 2

8.6.1 Definition of a Congruence Class

The congruence class modulo m of the integer a is the set of integers
$[a] = \{x \in \mathbb{Z} : x \equiv a \pmod{m}\}$.

8.6.2 Definition of $\mathbb{Z}_m$

We define $\mathbb{Z}_m$ to be the set of m congruence classes
$\mathbb{Z}_m = \{[0], [1], [2], \ldots, [m-1]\}$

We define two operations on $\mathbb{Z}_m$ as follows:
Addition: $[a] + [b] = [a + b]$
Multiplication: $[a][b] = [ab]$

Applying these operations on the set $\mathbb{Z}_m$ is known as Modular Arithmetic.

8.6 Properties of Modular Arithmetic (Example 13)

In Modular Arithmetic, the following properties hold for all $[a] \in \mathbb{Z}_m$.

1) $[a] + [0] = [a] = [0] + [a]$ We say that $[0]$ is the additive identity.
2) $[a][0] = [0] = [0][a]$
3) $[a] + [-a] = [0] = [-a] + [a]$ We say that $[-a]$ is the additive inverse of $[a]$.
4) $[a][1] = [a] = [1][a]$ We say that $[1]$ is the multiplicative identity.

For any $[a] \in \mathbb{Z}$, if there exists $[b] \in \mathbb{Z}$ such that $[a][b] = [b][a] = 1$,
we say that $[b]$ is the multiplicative inverse of $[a]$, and use the notation $[b] = [a]^-1$.

8.6 Modular Arithmetic Theorem (MAT)

For all integers a and c, with a non-zero,
the equation $[a][x] = [c]$ in $\mathbb{Z}_m$ has a solution if and only if $d \mid c$, where $d = \gcd(a, m)$.

Moreover, when $d \mid c$, there are d solutions, given by
$[x_0], [x_0 + \frac{m}{d}], [x_0 + 2\frac{m}{d}], \ldots, [x_0 + (d-1)\frac{m}{d}]$
where $[x] = [x_0]$ is one particular solution.

8.6 Inverses in $\mathbb{Z}_m$ (INV $\mathbb{Z}_m$)

Let a be an integer with $1 \leq a \leq m - 1$.
The element $[a]$ in $\mathbb{Z}_m$ has a multiplicative inverse if and only if $\gcd(a, m) = 1$.
Moreover, when $\gcd(a, m) = 1$, the multiplicative inverse is unique.

8.6 Inverses in $\mathbb{Z}_p$ (INV $\mathbb{Z}_p$)

For all prime numbers p and non-zero elements $[a]$ in $\mathbb{Z}_p$,
the multiplicative inverse $[a]^{-1}$ exists and is unique.

8.7 Fermat's Little Theorem (FℓT)

For all prime numbers p and integers a not divisible by p, we have
$a^{p-1} \equiv 1 \pmod{p}$

8.7 (Corollary 15)

For all prime numbers p and integers a, we have
$a^p \equiv a \pmod{p}$

8.8 Chinese Remainder Theorem (CRT)

For all integers a_1 and a_2, and positive integers m_1 and m_2, if $\gcd(m_1, m_2) = 1$, then the simultaneous linear congruences $n \equiv a_1 \pmod{m_1}$ and $n \equiv a_2 \pmod{m_2}$ has a unique solution modulo $m_1 m_2$.

Moreover, if $n = n_0$ is one particular solution,
then the solutions are given by the set of all integers n such that
$n = n_0 \pmod{m_1 m_2}$

8.8 Generalized Chinese Remainder Theorem (GCRT)

For all positive integers k and $m_1, m_2, \ldots, m_k$, and integers $a_1, a_2, \ldots, a_k$,
if $\gcd(m_i, m_j) = 1$ for all $i \neq j$, then the simultaneous congruences
$n \equiv a_1 \pmod{m_1}, \quad n \equiv a_2 \pmod{m_2}, \quad \cdots, \quad n \equiv a_k \pmod{m_k}$
have a unique solution modulo $m_1 m_2 \cdots m_k$

Moreover, if $n = n_0$ is one particular solution,
then the solutions are given by the set of all integers n such that
$n \equiv n_0 \pmod{m_1 m_2 \cdots m_k}$

8.9 Splitting Modulus Theorem (SMT)

For all integers a and positive integers m_1 and m_2, if $\gcd(m_1, m_2) = 1$,
then the simultaneous congruences $n \equiv a \pmod{m_1}$ and $n \equiv a \pmod{m_2}$
have exactly the same solutions as the single congruence $n \equiv a \pmod{m_1 m_2}$