MO-ARML

Name ______________________________

Modular Mathematics
Properties & Examples

TOPIC 1: Modular Basics

In ***base conversions***, the units digit represents the number remaining after all positive multiples of the base have been found.

Example 1: When converting 27 from base 10 to base 4, have $27_{10} = 123_4$, or $1 \cdot 4^2 + 2 \cdot 4 + 3$. The 3 remaining can also be represented in modular form as $27 \equiv 3 \pmod 4$. [parentheses optional]

> Integer division and modules: An integer, a, can be divided up into k equal positive parts of a given size, m, or ***modulus***, with a remainder, r, resulting from this modular division. This relationship is $a = r + km$. When using the ***modulo function***, the result r is an integer between 0 and $m - 1$, inclusive.

Modular notation can be used in 2 ways: as a function which produces a nonnegative integer less than the modulus; or as a relation describing two or more equivalent, or ***congruent***, numbers under that modulus.

Example 2: Find an x for: **a]** $x = 203 \bmod 11$ **b]** $x \equiv 203 \pmod{11}$
Solutions: **a]** $x = 5$ **b]** $x \equiv 5$, or 16, or 27, or … all under modulo 11. In fact, x is any ***Z*** in the set $\{\ldots, -17, -6, 5, 16, \ldots\}$ or $\{x: x = 5 + 11k, k \in \mathbf{Z}\}$, called the ***congruence class*** of 203 mod 11.

Example 3: Convert 495 to base 7, then find 495 mod 7.

TOPIC 2: Properties of Modular Congruences

If $a \equiv b \pmod m$ and $c > 0$, then:

1) $a + c \equiv b + c \pmod m$
2) $a - c \equiv b - c \pmod m$
3) $a\,c \equiv b\,c \pmod m$
4) $a^c \equiv b^c \pmod m$
5) $(a + b) \bmod m \equiv a \bmod m + b \bmod m$
6) $(a\,b) \bmod m \equiv a \bmod m \cdot b \bmod m$
7) If $a \equiv b \pmod m$ and $c \equiv d \pmod m$ then $a + c \equiv b + d \pmod m$
8) The ***modular inverse*** of a, a^{-1}, produces $a \bmod m$ → $a\,a^{-1} \equiv 1 \pmod m$
9) **About division**: When $a\,c \equiv b\,c \pmod m$, then $a \equiv b \pmod m$ **iff** $(m, c) = 1$ (the GCD). In other words, m and c must be *relatively prime*. Otherwise, if $a\,c \equiv b\,c \pmod m$, then $a \equiv b \pmod{[m]/(m, c)]}$, where m is divided by the GCD of m and c. These solutions should be checked in the original congruence.

TOPIC 3: Modular Congruence Theorems

Theorem 1 (Fermat's Little Theorem): If p is *prime*, then $a^{p-1} \equiv 1 \pmod p$ for all a in **Z**
(or $a^p \equiv a \pmod p$).

Theorem 2 (Wilson's Theorem): If p is *prime*, then $(p - 1)! \equiv -1 \pmod p$.

Theorem 3 ('Binomial Modulation' Theorem): If p is *prime*, then $(a + b)^p \equiv a^p + b^p \pmod p$.

Theorem 4: If $(m, a) = 1$, then $a\,c \equiv b \pmod{m}$ can be solved for c, for any value of b.

Theorem 5: If p is *prime* and $p \equiv 1 \pmod{4}$, then the square root of $-1 \bmod p$ has an integral solution. But if $p \equiv 3 \pmod{4}$, then there is no square root of $-1 \bmod p$.

Example 4: For $-1 \bmod 13$, $12 \equiv -1 \pmod{13}$, but not a square; however, $25 = 5^2 \equiv -1 \pmod{13}$, so 5 is a square root of $-1 \bmod 13$.

Theorem 6: For the form $x^2 + y^2 = n$, if n is prime and $n \equiv 1 \pmod{4}$, then there exists an integral solution (x, y). [If $n \equiv 3 \pmod{4}$, then there is generally no solution.]

Example 5: Find positive integers x and y so that $x^2 + y^2 = 29$.

Solution: 29 is prime and $29 \equiv 1 \pmod{4}$; since $12^2 = 144 \equiv -1 \pmod{29}$, then 12 is a square root of $-1 \bmod 29$ [and so are 17, 41, 46, 70, 75, …]; hence, $x^2 + y^2 = (x + 12y)(x - 12y) \equiv 0 \pmod{29}$ $\rightarrow$ $x \equiv \pm 12y \pmod{29}$; trying cases: **if $y = 1$**, then $[x \equiv 12$ or $x \equiv -12 \equiv 17] \pmod{29}$ – no good; **if $y = 2$**, then $[x \equiv 24$ or $x \equiv -24 \equiv 5] \pmod{29}$ – really good, since $5^2 + 2^2 = 29$; so, $x = 5$ and $y = 2$.

Theorem 7 (Chinese Remainder Theorem): Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime integers; then the system of linear congruences: $x \equiv b_1 \pmod{m_1}$, $x \equiv b_2 \pmod{m_2}$, …, $x \equiv b_n \pmod{m_n}$ has a unique solution for x in $\bmod(m_1 \cdot m_2 \cdot \ldots \cdot m_n)$.

Example 6: Solve for x, if $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$, and $x \equiv 2 \pmod{7}$.

Solution: Find $\text{LCM}(3, 5, 7) = 105$; then find a multiple of the excluded modulos for each equation that satisfies x: for eq1, have $5 \cdot 7 = 35$, and $x \equiv 35 \equiv 2 \pmod{3}$ works; for eq2, have $3 \cdot 7 = 21$, and $x \equiv 63 \equiv 3 \pmod{5}$ works; for eq3, have $3 \cdot 5 = 15$, and $x \equiv 30 \equiv 2 \pmod{7}$ works; finally, add the selected multiples: $21 + 63 + 30 = 128$, and the solutions are $x = 128 + 105k$, $k \in \boldsymbol{Z}$.

Theorem 8 (Gauss' Easter Formula - ***corrected*****):** While Easter always falls on the first Sunday after the first full moon in the spring, it was left to Gauss to find a formula to calculate the date:

$a = \textit{year} \bmod 19$ $\qquad b = \textit{year} \bmod 4$ $\qquad c = \textit{year} \bmod 7$

$d = (19a + 24) \bmod 30$ $\qquad e = (2b + 4c + 6d + 5) \bmod 7$

This indicates that Easter will fall on March $(22 + d + e)$ or April $(d + e - 9)$. [Don't blame Gauss; this was all the Catholic church's doing.]

Example 7: Find GCD(91, 287).

Solution: We can apply the *Euclidean algorithm*, which uses a repeated modular reduction until zero is reached, as follows: $287 \bmod 91 = 14 \rightarrow 91 \bmod 14 = 7 \rightarrow 14 \bmod 7 = 0$; since 7 is the last non-zero remainder, GCD(91, 287) = 7.

Theorem 9 (Bezout's Theorem): For a and b in $\boldsymbol{Z}^+$, there exist s and t in $\boldsymbol{Z}$ such that $(a, b) = s\,a + t\,b$.

Example 8: Find a linear combination for GCD(648, 198).

Solution: by reduction: $648 = 3 \cdot 198 + 54 \rightarrow 198 = 3 \cdot 54 + 36 \rightarrow 54 = 1 \cdot 36 + 18 \rightarrow 36 = 2 \cdot \boxed{\mathbf{18}} + 0$; then working backwards through the first three equations above: $18 = 54 - 1 \cdot 36 = 54 - 1(198 - 3 \cdot 54) = -1 \cdot 198 + 4 \cdot 54 = -1 \cdot 198 + 4(648 - 3 \cdot 198) = 4 \cdot 648 - 13 \cdot 198$; so, one possible combination is $18 = \mathbf{4} \cdot 648 - \mathbf{13} \cdot 198$. [another is $18 = \mathbf{15} \cdot 648 - \mathbf{49} \cdot 198$.]

APPLICATIONS: Checking accuracy of ISBN book #s and bank account #s; public key systems in cryptography; proper and efficient apportionment in law, economics, and other social sciences; in music, for efficient distribution of sound in closed spaces, as in concert halls; in computer science, for efficient polynomial calculations to speed up programs; etc.