**Harold’s Modular Arithmetic**

**Cheat Sheet**

22 October 2022

**Modular Arithmetic**

|  |  |  |
| --- | --- | --- |
| **Property** | **Condition (if)** | **Formula (then)** |
| **Visualization** | **24-Hour Clock** | **(mod 26)**Shape  Description automatically generated with low confidence |
| **Variables** | *m* = modulus (+ int)*r, n* = residue or remainder (+ int) | *a, b* = integers*q, k* = quotient or multiples of (int) |
| **Modulus** |  |  |
|  |  |
|  |  |
| *b* MOD *m* | *Integers r* or *n* |
| *b* DIV *m* | *Integers q* or *k* |
| **Congruence** | ≡ |  |
| m | (a - b) | *a* and *b* have the same remainder when divided by m. n is an integer.m divides a – b. |
| The congruence relation satisfies all the conditions of an [equivalence relation](https://en.wikipedia.org/wiki/Equivalence_relation): |
| **Reflexivity** |  |  |
| **Symmetry** |  for all a, b, and n |  |
| **Transitivity** |  |  |

**Identities**

|  |  |  |
| --- | --- | --- |
| **Property** | **Condition (if)** | **Formula (then)** |
| **Addition** |  |  |
|  Computing |  |
|  Translation |  | for any integer k |
|  Combining |   |  |
| **Subtraction** |  |  |
|  Negation |  |  |
| **Multiplication** |  |  |
|  Computing |  |
|  Scaling |  |  |
|  Combining |   |  |
| **Division** | (Meaning k and m are coprime) |  |
|  | where e is a positive integer that divides a and b |
| **Exponentiation** |  |  |
| Example: Find the last digit of Hence, the last digit of  | The exponentiation property only works on the base. For powers, use Euler's theorem. |
| **Multiplicative Inverse mod n** | (a and m are relatively prime)*m* ≥ 2 |  is a multiplicative inverse of *a* mod *m* |
| Example: Solve for x in 2x ≡ 3 (mod 5)To find the inverse first solve for r:If 2∙r ≡ 1 (mod 5) then r = 3.So, the multiplicative inverse of 2 is 3 with (mod 5).Since and , then . |
| *p* is prime |  |

**Theorems**

|  |  |  |
| --- | --- | --- |
| **Theorem** | **Condition (if)** | **Formula (then)** |
| **Greatest Common Divisor (GCD)** | Largest positive integer that is a factor of both x and y.Think Intersection (∩) of . |
| **GCD Theorem** | x and y are positive integers where x < y | gcd (x, y) = gcd (y mod x, x) |
| **Euclid’s Algorithm** | if ( y < x ) Swap (x, y);r = y mod x;while ( r ≠ 0 ) { y = x; x = r; r = y mod x;}return (x); | gcd (x, y) = xi |
| Example |  |
| **Extended Euclidean Theorem** | Let x and y be integers, then there are integers s and t such that | gcd (x, y) = sx + ty |
| **Extended Euclidean Algorithm** | r = y **mod** xr = y – **(y div x)** x15 = 45 – (45 div 30) 3015 = 45 – 1 ⋅ 30Slide [y x r] window left30 = 210 – (210 div 45) 4530 = 210 - 4 ⋅ 45Slide [y x r] window left45 = 675 - 3 210Back substitute green into redgcd (675, 210) = 15 = **5 ⋅** 675 **– 16 ⋅** 210Output Format: sx + ty | Example:gcd (675, 210) = 15Do Euclid’s Algorithm first, Saving intermediate results.Start with sliding window on right. << [y x r]675 210 45 30 15 |
| **Multiplicative Inverses** | gcd (x, y) = sx + ty | s = x’s inverse mod yt = y’s inverse mod x |
| **Fermat’s Little Theorem** | p is primea is an integer not divisible by p |  |
| Example: Find 7222 mod 11Since 710 ≡ 1 (mod 11)and (710)k ≡ 1 (mod 11)7222 = 722•10+2 = (710)22 •72 ≡ (1)22 • 49 ≡ 5 (mod 11)Hence, 7222 mod 11 = 5 |  |
| **Euler’s Theorem** | *c ≡ d (mod φ(n))*where φ is Euler's totient function | *ac ≡ ad (mod n)*provided that a is coprime with n |
| a and m are coprime | *aφ(n) ≡* *1 (mod m)*where φ is Euler's totient function |
| Euler’s Totient Function | φ(n) = number of integers ≤ n that do not share any common factors with n |
| **Wilson’s Theorem** | p is prime if and only if (p − 1)! ≡ −1 (mod p) |
| **Linear Congruence** |  | Solutions are all integers x that satisfy the congruence |
| **Chinese Remainder Theroem** | m1, m2, …, mn are pairwise relatively prime positive integers > 1a1, a2, …, an are arbitrary integers | x ≡ a1 (mod m1)x ≡ a2 (mod m2)…x ≡ an (mod mn)has a unique solution modulo m = m1m2∙∙∙mn.(Meaning 0 ≤ x < m and all other solutions are congruent (≡) modulo m to this solution.) |
| **Legrange’s Theorem** | The congruence *f (x) ≡ 0 (mod p)*, where p is prime, and *f (x) = a0 xn + ... + an* is a polynomial with integer coefficients such that a0 ≠ 0 (mod p), has at most n roots. |
| **Primitive Root Modulo m** | A number g is a primitive root modulo m if, for every integer a coprime to m, there is an integer k such that gk ≡ a (mod m). A primitive root modulo m exists if and only if n is equal to 2, 4, pk or 2pk, where p is an odd prime number and k is a positive integer. If a primitive root modulo m exists, then there are exactly *φ(φ(m))* such primitive roots, where φ is the Euler's totient function. |

**Sources:**

* [SNHU MAT 260](https://www.snhu.edu/admission/academic-catalogs/coce-catalog#/courses/NkdqI-8Fe) - Cryptology, I[nvitation to Cryptology](https://www.amazon.com/Invitation-Cryptology-Thomas-H-Barr/dp/0130889768/ref%3Dsr_1_1?crid=9A8O5P2JQ7F&keywords=978-0-13-088976-8&qid=1656057152&sprefix=978-0-13-088976-8%2Caps%2C71&sr=8-1), 1st Edition, Thomas Barr, 2001.
* [SNHU MAT 230](https://www.snhu.edu/admission/academic-catalogs/coce-catalog#/courses/4kVhSZLtg) - Discrete Mathematics, zyBooks.
* <https://brilliant.org/wiki/modular-arithmetic/>
* <https://en.wikipedia.org/wiki/Modular_arithmetic>
* <https://artofproblemsolving.com/wiki/index.php/Modular_arithmetic/Introduction>