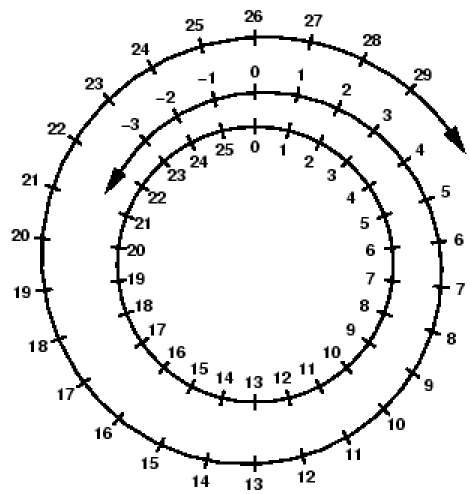
Harold's Modular Arithmetic
Cheat Sheet
22 October 2022

Modular Arithmetic

Property	Condition (if)	Formula (then)
Visualization	**24-Hour Clock** 	**(mod 26)** 
Variables	*m* = modulus (+ int) *r, n* = residue or remainder (+ int)	*a, b* = integers *q, k* = quotient or multiples of (int)
Modulus	$b = qm + r$	$b \bmod m \equiv r$
	$b = km + n$	$b \bmod m \equiv n$
	$\boldsymbol{a \equiv b \pmod{m}}$	$\boldsymbol{a \bmod m \equiv b \bmod m}$
	b MOD *m*	*Integers r* or *n*
	b DIV *m*	*Integers q* or *k*
Congruence	≡ $a \equiv b \pmod{m}$	$a \bmod m = n$ $b \bmod m = n$
	$\dfrac{a-b}{m} = n$ 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:		
Reflexivity	$a \equiv a \pmod{m}$	
Symmetry	$b \equiv a \pmod{m}$ for all a, b, and n	$a \equiv b \pmod{m}$
Transitivity	$a \equiv b \pmod{m}$ $b \equiv c \pmod{m}$	$a \equiv c \pmod{m}$

Identities

<table>
<tr><th>Property</th><th>Condition (if)</th><th>Formula (then)</th></tr>
<tr><td>Addition</td><td>$a + b = c$</td><td>$a \ mod \ m + b \ mod \ m \ \equiv c \ mod \ m$</td></tr>
<tr><td>Computing</td><td colspan="2">$[(a \ mod \ m) + (b \ mod \ m)] \ mod \ m = [a + b] \ mod \ m = c \ mod \ m$</td></tr>
<tr><td>Translation</td><td>$a \equiv b \quad (mod \ m)$</td><td>$a + k \equiv b + k \quad (mod \ m)$
for any integer k</td></tr>
<tr><td>Combining</td><td>$a \equiv b \quad (mod \ m)$
$c \equiv d \quad (mod \ m)$</td><td>$a + c \equiv b + d \quad (mod \ m)$</td></tr>
<tr><td>Subtraction</td><td>$a - b = c$</td><td>$a \ mod \ m - b \ mod \ m \equiv c \ mod \ m$</td></tr>
<tr><td>Negation</td><td>$a \equiv b \quad (mod \ m)$</td><td>$-a \equiv -b \quad (mod \ m)$</td></tr>
<tr><td>Multiplication</td><td>$a \cdot b = c$</td><td>$a \ mod \ m \cdot b \ mod \ m \equiv c \ mod \ m$</td></tr>
<tr><td>Computing</td><td colspan="2">$[(a \ mod \ m)(b \ mod \ m)] \ mod \ m = [ab] \ mod \ m = c \ mod \ m$</td></tr>
<tr><td>Scaling</td><td>$a \equiv b \quad (mod \ m)$</td><td>$ka \equiv kb \quad (mod \ m)$
$ka \equiv kb \quad (mod \ km)$</td></tr>
<tr><td>Combining</td><td>$a \equiv b \quad (mod \ m)$
$c \equiv d \quad (mod \ m)$</td><td>$ac \equiv bd \quad (mod \ m)$</td></tr>
<tr><td rowspan="2">Division</td><td>$gcd \ (k, m) = 1$
(Meaning k and m are coprime)
$ka = kb \quad (mod \ m)$</td><td>$a \equiv b \quad (mod \ m)$</td></tr>
<tr><td>$\frac{a}{e} = \frac{b}{e} \left(mod \ \frac{m}{gcd \ (m, e)} \right)$</td><td>where e is a positive integer that divides a and b</td></tr>
<tr><td rowspan="2">Exponentiation</td><td>$a \equiv b \ (mod \ m)$</td><td>$a^k \equiv b^k \ (mod \ m)$</td></tr>
<tr><td>Example: Find the last digit of 17^{17}
$17^{17} \ (mod \ 10)$
$\equiv \ (7^2)^8 \cdot 7 \ (mod \ 10)$
$\equiv (49)^8 \cdot 7 \ (mod \ 10)$
$\equiv (9)^8 \cdot 7 \ (mod \ 10)$
$\equiv (9^2)^4 \cdot 7 \ (mod \ 10)$
$\equiv (81)^4 \cdot 7 \ (mod \ 10)$
$\equiv (1)^4 \cdot 7 \ (mod \ 10)$
$\equiv 7 \ (mod \ 10)$
Hence, the last digit of $17^{17} = 7$</td><td>The exponentiation property only works on the base.

For powers, use Euler's theorem.</td></tr>
<tr><td rowspan="3">Multiplicative Inverse mod n</td><td>$\boldsymbol{a \cdot a^{-1} \equiv 1 \quad (mod \ m)}$
$gcd \ (a, m) = 1$
(a and m are relatively prime)
$1 \leq a, a^{-1} \leq m + 1$
$m \geq 2$</td><td>a^{-1} is a multiplicative inverse of *a* mod *m*</td></tr>
<tr><td colspan="2">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 $r = a^{-1}$ and $a^{-1}ax \equiv x \ (mod \ m)$, then $(2)(3)x \equiv 6x \equiv x \ (mod \ 5)$.</td></tr>
<tr><td>*p* is prime
$0 < a < p$</td><td>$a^{-1} \equiv a^{p-2} \ (mod \ p)$</td></tr>
</table>

Theorems

Theorem	Condition (if)	Formula (then)
Greatest Common Divisor (GCD)	$gcd(x, y) = p_1^{min\{\alpha_1,\beta_1\}} \cdot p_2^{min\{\alpha_2,\beta_2\}} \cdot p_k^{min\{\alpha_k,\beta_k\}}$ Largest positive integer that is a factor of both x and y. Think Intersection (∩) of α_i, β_i.	
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) = x_i

Example	gcd(675, 210) = 15 y x r 675 210 45 30 15 0	
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** x r = y – **(y div x)** · x 15 = 45 – (45 div 30) · 30 15 = 45 – 1 · 30 Slide [y x r] window left 30 = 210 – (210 div 45) · 45 30 = 210 - 4 · 45 Slide [y x r] window left 45 = 675 - 3 · 210 Back substitute green into red gcd (675, 210) = 15 = **5** · 675 **– 16** · 210 Output Format: sx + ty	Example: gcd (675, 210) = 15 Do 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 y t = y's inverse mod x
Fermat's Little Theorem	p is prime a is an integer not divisible by p	$a^{p-1} \equiv 1 \quad (mod\ p)$ $a^p \equiv a \quad (mod\ p)$
	Example: Find 7^{222} mod 11 Since $7^{10} \equiv 1$ (mod 11) and $(7^{10})^k \equiv 1$ (mod 11) $7^{222} = 7^{22 \bullet 10+2} = (7^{10})^{22} \bullet 7^2$ $\equiv (1)^{22} \bullet 49$ $\equiv 5 \ (mod\ 11)$ Hence, 7^{222} mod 11 = 5	

Euler's Theorem	$c \equiv d \pmod{\varphi(n)}$ where ϕ is Euler's totient function	$a^c \equiv a^d \pmod{n}$ provided that a is coprime with n
	a and m are coprime	$a^{\varphi(n)} \equiv 1 \pmod{m}$ 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 $(p - 1)! \equiv -1 \pmod{p}$	
Linear Congruence	$ax \equiv b \pmod{m}$	Solutions are all integers x that satisfy the congruence
Chinese Remainder Theroem	$m_1, m_2, \ldots, m_n$ are pairwise relatively prime positive integers > 1 $a_1, a_2, \ldots, a_n$ are arbitrary integers	$x \equiv a_1 \pmod{m_1}$ $x \equiv a_2 \pmod{m_2}$ … $x \equiv a_n \pmod{m_n}$ has a unique solution modulo $m = m_1 m_2 \cdots m_n$. (Meaning $0 \leq x < m$ and all other solutions are congruent ($\equiv$) modulo m to this solution.)
Legrange's Theorem	The congruence $f(x) \equiv 0 \pmod{p}$, where p is prime, and $f(x) = a_0 x^n + \ldots + a^n$ is a polynomial with integer coefficients such that $a_0 \not\equiv 0 \pmod{p}$, 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 $g^k \equiv a \pmod{m}$. A primitive root modulo m exists if and only if n is equal to 2, 4, p^k or $2p^k$, where p is an odd prime number and k is a positive integer. If a primitive root modulo m exists, then there are exactly $\varphi(\varphi(m))$ such primitive roots, where ϕ is the Euler's totient function.	

Sources:

- SNHU MAT 260 - Cryptology, Invitation to Cryptology, 1st Edition, Thomas Barr, 2001.
- SNHU MAT 230 - 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