**Congruences (Part 1)**

Original Notes adopted from September 25, 2001 (Week 3)

© P. Rosenthal, MAT246Y1, University of Toronto, Department of Mathematics typed by A. Ku Ong

---

**Modular Arithmetic**

\[ a, b \in \mathbb{Z}, m > 1 \]

"a is congruent to b modulo m" means \( m | (a-b) \).
Equivalently, a & b leave the same remainder by division by m (for \( a, b \geq 0 \))

---

1) **If \( a \equiv b \pmod{m} \), then \( (a+c) \equiv (b+d) \pmod{m} \) & \( c \equiv \pmod{m} \)**

**Proof:**

\[ a \equiv b \pmod{m} \] means \( a - b = mq \), some \( q \in \mathbb{Z} \)
Also \( c - d = mr \), some \( r \in \mathbb{Z} \).

We Want: \( (a-b) - (b+d) \) is a multiple of \( m \)

\[ a = b + mq \]
\[ c = d + mr \]

\[ (a+c) - (b+d) = (b + nq + (d + mr)) - b = b + d + mq + mr - b - d = mq + mr = m(q + r), \text{ a multiple} \]
\[ \therefore \ (a + c) \equiv (b+d) \pmod{m} \]

Eg. \( 7 \equiv 3 \pmod{4} \)
\( -2 \equiv 6 \pmod{4} \)
\( 5 \equiv 9 \pmod{4} \)

2) **If \( a \equiv b \pmod{m} \) & \( c \equiv d \pmod{n} \), then \( ac \equiv bd \pmod{m} \)**

**Proof:**

\[ a = b + qm \]
\[ c = d + rm, \text{ some } r,q \]

\[ ac - bd = (b + qm) (d + rm) - bd = bd + brm + qmd + qrm^2 - bd = m(br + qd + qrm) \]

Divisible by \( m \), so \( ac \equiv bd \pmod{m} \)

**Corollary: If \( a \equiv b \pmod{m} \), then \( a^n \equiv b^n \pmod{m} \)**

**Proof:** Case where \( a = c \) & \( b = d \)

3) **If \( a \equiv b \pmod{m} \) and \( n \in \mathbb{N} \) then \( an \equiv bn \pmod{m} \)**

**Proof:** Use Mathematical Induction.
Case \( n = 1 \) True
Assume true for \( n = k \).
Induction Hypothesis: \( a^k \equiv b^k \pmod{m} \)
Given \( a \equiv b \pmod{m} \), By \( 2 \) \( a^k \equiv b^k \pmod{m} \) or \( a^{k+1} \equiv b^{k+1} \pmod{m} \).

**Does 7/ (229 + 3)?**

\[
2^3 \equiv 1 \pmod{7} \quad (2^3)^8 \equiv 1^8 \pmod{7} \\
2^{24} \equiv 1 \pmod{7} \quad 2^3 \equiv 1 \pmod{7} \\
2^{29} \equiv 1 \pmod{7} \quad 2^3 \equiv 1 \pmod{7} \\
2^{29} \equiv 4 \* 1 \pmod{7} \\
2^{29} \equiv 4 \pmod{7} \\
2^{29} + 3 \equiv (4+3) \pmod{7} \\
2^{29} + 3 \equiv 0 \pmod{7} \\
\]

229 + 3 is divisible by 7.

**Eg. What is the remainder when 3^{202} + 5^9 is divided by 8?**

\[
3^2 \equiv 1 \pmod{8} \quad 5^2 \equiv 1 \pmod{8} \\
(3^3)^{101} \equiv 1101 \pmod{8} \quad (5^3)^{1} \equiv 1 \pmod{8} \\
3^{202} \equiv 1 \pmod{8} \quad 5^4 \equiv 5 \pmod{8} \\
\]

\( 3^{202} + 5^9 \equiv 6 \pmod{8} \). The remainder when \( 3^{202} + 5^9 \) is divisible by 8 is 6.

**Eg. \( 5^2 \equiv 3^2 \pmod{8} \)**

\[
5^2 \equiv 1 \pmod{8} \quad 3^2 \equiv 1 \pmod{8} \quad \text{But } 5 \neq 3 \pmod{8} \\
\]

**Eg. To tell if 3, 974, 279 is divisible by 3, see if 3+ 9 + 7 + 4 + 2 + 7+ 9 is divisible by 3.**

3, 974, 279 = 9 + 7 \* 10 + 2 \* 10^2 + 4 \* 10^3 + 7 \* 10^4 + 9 \* 10^5 + 3 \* 10^6

\[
10 \equiv 1 \pmod{3} \quad : \ a \times 10^k \equiv a \pmod{3} \text{ for all } k \\
10^2 \equiv 1 \pmod{3} \\
10^k \equiv 1 \pmod{3} \text{ for all } k \in \mathbb{N} \\
7 \times 10 \equiv 7 \pmod{3} \\
2 \times 10^3 \equiv 2 \pmod{3} \text{ etc.} \\
9 + 7*10 + 2*10^2 + 4*10^3 + 7*10^4 + 9*10^5 + 3*10^6 \\
= 9 + 7 + 2 + 4 + 7 + 9 + 3 \\
\]

**Thm:** The natural number \( a_n10^n + a_{n-1}10^{n-1} + a_{n-2}10^{n-2} + \ldots + a_110 + a_0 \) whose each \( a_i \) is a number from \{ 0, 1, 2, 3... 9 \} is congruent to \( a_n + a_{n-1} + \ldots + a_1 + a_0 \pmod{3} \)

**Proof:** \( 10^m \equiv 1 \pmod{3} \) for all \( m \)

\[ : a_n10^m \equiv a_n \pmod{3} \text{ for all } a_n \text{ for all } m. \]

\[ : a_n10^m + a_{n-1}10^{n-1} + \ldots + a_110 + a_0 \equiv a_n + a_{n-1} + \ldots + a_1 + a_0. \]

**Eg. 7,230, 591, 006 leaves remainder 0 upon division by 3 (its divisible by 3)**
The natural number $a_n10^n + a_{n-1}10^{n-1} + a_{n-2}10^{n-2} + ... + a_110 + a_0$ whose each $a_i$ is a number from \{0,1,2,...,9\} is congruent to $a_n + a_{n-1} + ... + a_1 + a_0$ (mod 9).

**Proof**: As in case mod 3; $10^m ≡ 1$ (mod 9) for all $m$.

**What about mod 11?**

$10 ≡ (-1)(mod 11)$

$10^2 ≡ (-1)^2(mod 11) ≡ 1 (mod 11)$

$10^3 ≡ -1(mod 11)$

$10^m ≡ 1 (mod 11)$ if $m$ even

$10^m ≡ -1 (mod 11)$ if $m$ odd.

**Eg. What is the remainder when 7, 224, 689 is divisible by 11?**

$7224689 = 9 + 8 *10 + 6*10^2 + 4*10^3 + 2*10^4 + 7-10^6$

$= 9 – 8(odd) + 6(even) – 4 + 2 – 2 + 7 (mod 11)$

$= 10 (mod 11)$

**Question**: Is $3^{729} = 7^{104}$ ?

**Recall**: We proved that every natural number other than 1 is a product of prime numbers.

**Thm: The Fundamental Thm of Arithmetic**

Every natural number $≠ 1$ is a product of primes & the primes in the product are unique (including multiplicity) except for the order in which they occur.

**Proof**: We know that every natural number $≠ 1$ is a product of primes. We must show the uniqueness of the factorization into primes. (Using contradiction)

If there are natural numbers with two distinct factorizations into primes, then there is a smallest one, say $k$. We’ll show that this is impossible. We have $k = p_1, p_2, p_3... p_m = q_1, q_2, ..., q_n$ where all $p_i$ of all $q_i$ are primes and a difference in the occurrence of primes in $p_1, ..., p_m$ to $q$ other than order.

Since $k$ is the smallest, the factorization have no primes in common for if since $p_i$ were a $q_i$, dividing both sides by it, getting a smaller number than $k$ that has distinct prime factorizations.

Either $p > q$ or $p < q$.

Suppose $p_i < q_i$ (Etc. if $p > q$)

Consider $L = k - p_i q_j q_{jn} = 1/p_1 p_2... p_m - p_i q_j... q_n$

$\text{(I) } = p_1 (p_2... p_m q_j... q_n)$

But also $L = q_i q_j... q_n - p_i q_j... q_n$

$\text{(II) } = (q_i-p_i) (q_j... q_n)$

$L < k$, so it has unique factorization $\text{(I) } \Rightarrow p_i$ occurs in factorization of $L$

$\text{(II) } \Rightarrow p_i$ divides into $(q_i - p_i)$
\[ q_1 - p_1 = t p_1 \]
\[ \therefore q_1 = p_1 (1 + t) q_1 \neq p, p, q \text{ primes, impossible.} \]