Applications of Congruence to Divisibility Theory

Mulatu Lemma and Dustin Allard

Department of Mathematics

Savanah State University

USA

Abstract. **The concept of congruence plays a big role in the theory of divisibility.** In our study we master different properties of congruence and deeply investigate its applications to the divisibility theory. We will observe that the concept of congruence is such a power technique in dealing with the concept of divisibility. Fermat's and Wilson's Theorems will be studied and applied in the theory of divisibility. Several impressive results and applications will be discussed with different mathematical techniques applied.

Key Words/Phrases: Congruence, Divisibility, Fermat's Theorem, Wilson's Theorem

I. Introduction and History

It is believed to be that Karl Friedrich Gauss is the father of the "Theory of Congruences." Gauss was born in Brunswick, Germany in 1777. At the very young age of 3 Gauss was said to be a mathematician genius. By the time Gauss was 7 years old there was nothing more that his math teachers could teach him. Karl F. Gauss studied mathematics at the University of Göttingen from 1795 to 1798. Gauss first introduced the concept of the "Theory of Congruence," in his Disquisitiones Arithmeticae in 1801 at 24 years old.

In the book "Disquisitiones Arithmeticae," it explains the concept of congruence and the notation that makes it a powerful technique in mathematics. The congruent symbol used in number theory ($\equiv$) was introduced as well. It is said that Gauss choose to use this symbol because of the close analogy with algebraic equality. Gauss systematized the study of number theory (properties of the integers). He proved that every number is the sum of at most three triangular numbers and developed the algebra of congruences.

Modular arithmetic can be handled mathematically be introducing a congruence relation on the integers that is compatible with the operations of the ring of integers: addition, subtraction, and multiplication. For a fixed modulus *n*, it is defined as follows.

Two integers *a* and *b* are said to be congruent modulo *n*, if their difference (a-b) is an integer multiple of *n*. If this is the case, it is expressed as:

$a \equiv b$ (**mod** n).

The above mathematical statement is read. “a is congruent to b **modulo** n.”

For example,

38 ≡ 14 (**mod** 12)

Because 38 – 14 = 24, which is a multiple of 12. For positive n and non-negative a and b, congruence of a and b can also be thought of as asserting that these two numbers have the same remainder after dividing by the modulus n. So,

38 ≡ 14 (**mod** 12)

because, when divided by 12 numbers give 2 as remainder.

If $b - c$ is not integrally divisible by m, then it is said that “b is not congruent to c (modulo m),” which is written

$$b \not\equiv c (\bmod m)$$

I. Properties of Congruence

The properties that make this relation a congruence relation are the following:

1. Equivalence: $a \equiv b(\bmod 0) \Rightarrow a = b$ (which can be regarded as a definition)
2. Determination: either $a \equiv b(\bmod m)$ or $a \equiv b(\bmod m)$
3. Reflexivity: $a \equiv a(\bmod m)$
4. Symmetry: $a \equiv b(\bmod m) \Rightarrow b \equiv c(\bmod m) \Rightarrow a \equiv c(\bmod m)$
5. Transitivity: $a \equiv b(\bmod m)$ and $b \equiv c(\bmod m) \Rightarrow a \equiv c(\bmod m)$
6. $a + b \equiv a^1 + b^1 (\bmod m)$
7. $a - b \equiv a^1 - b^1 (\bmod m)$
8. $ab \equiv a^1 b^1 (\bmod m)$
9. $a \equiv b(\bmod m) \Rightarrow ka \equiv kb(\bmod m)$
10. $a \equiv b(\bmod m) \Rightarrow a^n \equiv b^n (\bmod n)$
11. Least Common Multiple (LCM)

    $a \equiv b(\bmod m_1)$ and $a \equiv b(\bmod m_2) \Rightarrow a \equiv b(\bmod [m_1, m_2]$,

    where $[m_1, m_2]$
12. Greatest Common Divisor

    $ak \equiv bk(\bmod m) \Rightarrow a \equiv b(\bmod \frac{m}{(k,m)})$

II. Some Notations

1. a/b means a divides b or b divisible by a

Example: 3/6 6 is divisible by 3

2. a/b implies that there exists an integer m such that b = ma

III Main Results:

Theorem 1: If p is prime and n > p > 2n, prove that $p/\binom{2n}{n}$

Proof : Note That

$$\binom{2n}{n}=\frac{(2n)!}{n!n!}=\frac{2n(2n-1)\ldots(n+1)}{n!}$$

$$\Rightarrow n!\binom{2n}{n}=2n(2n-1)\ldots(n+1)$$

Since n<p<n+1, it follows that

$\Rightarrow$n / 2n(2n-1) …(n+1)

$$\Rightarrow p/n!\binom{2n}{n}$$

$\Rightarrow p/\binom{2n}{n}$ as p does not divide $n!$ QED

Theorem 2: If a is odd prove that a^{2^n} -1 is divisible by 2^{n+2}

Proof we proceed by induction

1.) Let n=1 then a^2 -1= $(2k+1)^2$ -1

= $4k^2$ + 4k+1-1

= $4k^2$ + 4k

= 4(k (k+1)

= 4(2m) m=k (k+1)

= 8m

$\Rightarrow a^2$ -1= 0(mod 8)

Assume the hypothesis is true for n = k and show that it holds true for n =k+1

$\Rightarrow 2^{k+2}/(2^{2k}-1)$ for n = k

$\Rightarrow a^{2^k}-1=r(2^{k+2})$ for some integer

$$\Rightarrow a^{2^k}=1+r(2^{k+2})$$

$$\Rightarrow (a^{2^k})^2=(1+r2^{k+2})^2$$

$\Rightarrow a^{2^{k+1}}$ = 1+ 2r 2^{k+2} + r^2 2^{2k+4}

$$= 1+r(2^{k+3})+r^2(2^{k+1})2^{k+3}\equiv 1(\bmod 2^{k+3})$$

So by induction, $2^{n+2} / a^{2^n} - 1$

Theorem 3: Let a be any integer and p be any prime, prove that $a^p + (p-1)!$ a is divisible by p.

Proof: $a^p \equiv a(\bmod p)$ (by Fermat's Theorem)

(p-1)! $\equiv -1(\bmod p)$ (by Wilson's Theorem)

(p-1)!a $\equiv -a(\bmod p)$

Now, we have $a^p + (p-1)! \equiv a + (-a)(\bmod p)$

$\equiv 0(\bmod p)$

Fermat's Theorem

Let p be prime and support $p \nmid q$ (p doesn't divides q)

Then $a^p \equiv a(\bmod p)$ (see 1)

Lemma: If p and q are distinct primes with

$$a^p \equiv a(\bmod q) and$$

$$a^q \equiv a(\bmod p), then$$

$$a^{pq} \equiv a(\bmod pq)$$

Wilson's Theorem

An integer p is prime $\Leftrightarrow$ (p-1)! ≡ -1(mod p) (see 1)

IV. Application of Congruence to Divisibility

Here we consider different type of deep problems and study how congruence plays a big role in divisibility.

Application 1: Find the remainder when 2^{402} is divided by 41

Solution: $2^5 \equiv -9$ (mod 41)

$\Rightarrow (2^5)^2 \equiv 81$ (mod 41)

$\Rightarrow 2^{10} \equiv 81$(mod 41)

$$\Rightarrow 2^{10} \equiv -1 (\bmod 41)$$
$$\Rightarrow (2^{10})^4 \equiv 1 (\bmod 41)$$
$$\Rightarrow 2^{40} \equiv 1 (\bmod 41)$$
$$\Rightarrow 2^{400} \equiv 1 (\bmod 41)$$
$$\Rightarrow 2^{400} \cdot 2^2 \equiv 2^2 (\bmod 41)$$
$$\Rightarrow 2^{402} \equiv 4 (\bmod 41)$$
$$\Rightarrow R = 4$$

Application 2: Find the remainder when 2^{354} is divided by 31

Solution: Note that $2^5 \equiv 1 (\bmod 31)$

$$\Rightarrow (2^5)^{70} \equiv 1 (\bmod 31)$$
$$\Rightarrow 2^{350} \equiv 1 (\bmod 31)$$
$$\Rightarrow 2^4 \cdot 2^{350} \equiv 16 (\bmod 31)$$
$$\Rightarrow 2^{354} \equiv 16 (\bmod 31)$$
$$\Rightarrow R = 16$$

Application 3: Show that $89 / 2^{440} - 1$

Solution: $2^6 \equiv -25 (\bmod 89)$

$$\Rightarrow 2^{12} \equiv 625 (\bmod 89)$$
$$\Rightarrow 2^{12} \equiv 2 (\bmod 89)$$
$$\Rightarrow 2^{48} \equiv 16 (\bmod 89)$$
$$\Rightarrow 2^{44} \equiv 1 (\bmod 89)$$
$$\Rightarrow 2^{440} \equiv 1 (\bmod 89)$$
$$\Rightarrow 2^{440} - 1 \equiv 0 (\bmod 89)$$
$$\Rightarrow R = 0$$
$$\therefore 89 / 2^{440} - 1$$

Application 4: Show that $97 / 2^{2400} - 1$

Solution: $2^6 \equiv -33 (\bmod 97)$

$$\Rightarrow 2^{12} \equiv 1089(\bmod 97)$$
$$\Rightarrow 2^{12} \equiv 22(\bmod 97)$$
$$\Rightarrow 2^{24} \equiv 484(\bmod 97)$$
$$\Rightarrow 2^{24} \equiv 96(\bmod 97)$$
$$\Rightarrow 2^{24} \equiv -1(\bmod 97)$$
$$\Rightarrow \left(2^{24}\right)^{100} \equiv 1(\bmod 97)$$
$$\Rightarrow 2^{2400} \equiv 1(\bmod 97)$$
$$\Rightarrow 2^{2400} - 1 \equiv 0(\bmod 97)$$
$$\Rightarrow R = 0$$
$$\therefore 97 / 2^{2400} - 1$$

Application 5: Find the remainder when 5^{10204} is divided by 7

Solution: $5 \equiv -2(\bmod 7)$

$$\Rightarrow 5^{3} \equiv -1(\bmod 7)$$
$$\Rightarrow (5^{3})^{17} \equiv -1(\bmod 7)$$
$$\Rightarrow 5^{51} \equiv -1(\bmod 7)$$
$$\Rightarrow (5^{51})^{200} \equiv 2(\bmod 7)$$
$$\Rightarrow 5^{10200} \equiv 1(\bmod 7)$$
$$\Rightarrow 5^{10200} \cdot 5^{4} \equiv 625(\bmod 7)$$
$$\Rightarrow 5^{10204} \equiv 2(\bmod 7)$$
$$\Rightarrow R = 2$$

Application 6: Using congruence show that $7 / 5^{2n} + 3 \cdot 2^{5n-2}$

Solution: $5^{2} \equiv 4(\bmod 7)$

$$\Rightarrow 5^{2n} \equiv 4^{n}(\bmod 7)$$

Also we have, $2^{5} \equiv 4(\bmod 7)$

$$\Rightarrow 2^{5n} \equiv 4^{n} (\bmod 7)$$
$$\Rightarrow 2^{5n} \cdot 2^{-2} \equiv 4^{n} \cdot 2^{-2} (\bmod 7)$$
$$\Rightarrow 2^{5n-2} \equiv 4^{n-1} (\bmod 7)$$
$$\Rightarrow 3 \cdot 2^{5n-2} \equiv 3 \cdot 4^{n-1} (\bmod 7)$$

Hence, $5^{2n} + 3 \cdot 2^{5n-2} \equiv 4^{n} + 3 \cdot 4^{n-1} (\bmod 7)$

$$\Rightarrow 5^{2n} + 3 \cdot 2^{5n-2} \equiv 4^{n-1}(4+3) (\bmod 7)$$
$$\Rightarrow 5^{2n} + 3 \cdot 2^{5n-2} \equiv 4^{n-1}(7) (\bmod 7)$$
$$\Rightarrow 5^{2n} + 3 \cdot 2^{5n-2} \equiv 4^{n-1}(0) (\bmod 7)$$
$$\Rightarrow 5^{2n} + 3 \cdot 2^{5n-2} \equiv 0 (\bmod 7)$$
$$\therefore 7 / 5^{2n} + 3 \cdot 2^{5n-2}$$

Application 7: Show that $39/53^{103} + 103^{53}$

Solution: $39/53^{103} + 103^{53}$

$$\Rightarrow 53 \equiv 14 (\bmod 39)$$
$$\Rightarrow 53^{2} \equiv 196 (\bmod 39)$$
$$\Rightarrow 53^{2} \equiv 1 (\bmod 39)$$
$$\Rightarrow (53^{2})^{51} \equiv 1 (\bmod 39)$$
$$\Rightarrow 53^{102} \equiv 1 (\bmod 39)$$
$$\Rightarrow 53^{102} \cdot 53 \equiv 53 (\bmod 39)$$
$$\Rightarrow 53^{103} \equiv 14 (\bmod 39)$$
$$\Rightarrow R = 14$$

Also, $\Rightarrow 103 \equiv 64 (\bmod 39)$

$$\Rightarrow 103^{2} \equiv 4096 (\bmod 39)$$
$$\Rightarrow 103^{2} \equiv 1 (\bmod 39)$$
$$\Rightarrow (103^{2})^{26} \equiv 1 (\bmod 39)$$
$$\Rightarrow 103^{52} \equiv 1 (\bmod 39)$$
$$\Rightarrow 103^{52} \cdot 103 \equiv 103 (\bmod 39)$$
$$\Rightarrow 103^{53} \equiv 103 (\bmod 39)$$
$$\Rightarrow 103^{53} \equiv 25 (\bmod 39)$$
$$\Rightarrow R = 25$$

So, we have $53^{103} + 103^{53} \equiv 14 + 25 (\bmod 39)$

$$\Rightarrow 53^{103} + 103^{53} \equiv 39 (\mathrm{mod}\, 39)$$
$$\Rightarrow 53^{103} + 103^{53} \equiv 0 (\mathrm{mod}\, 39)$$
$$\therefore 39 / 53^{103} + 103^{53}$$

Application 8: Show that $7/111^{333} + 333^{111}$

Solution: $111 \equiv 104 (\mathrm{mod}\, 7)$

$$\Rightarrow 111 \equiv -1 (\mathrm{mod}\, 7)$$
$$\Rightarrow 111^2 \equiv 1 (\mathrm{mod}\, 7)$$
$$\Rightarrow (111^2)^{166} \equiv 1 (\mathrm{mod}\, 7)$$
$$\Rightarrow 111^{332} \equiv 1 (\mathrm{mod}\, 7)$$
$$\Rightarrow 111^{332} \cdot 111 \equiv 1 \cdot 111 (\mathrm{mod}\, 7)$$
$$\Rightarrow 111^{333} \equiv 111 (\mathrm{mod}\, 7)$$
$$\Rightarrow 111^{333} \equiv 6 (\mathrm{mod}\, 7)$$

Also, $\Rightarrow 333 \equiv 326 (\mathrm{mod}\, 7)$

$$\Rightarrow 333 \equiv 4 (\mathrm{mod}\, 7)$$
$$\Rightarrow 333^2 \equiv 2 (\mathrm{mod}\, 7)$$
$$\Rightarrow (333^2)^3 \equiv 8 (\mathrm{mod}\, 7)$$
$$\Rightarrow 333^6 \equiv 1 (\mathrm{mod}\, 7)$$
$$\Rightarrow (333^6)^{18} \equiv 1 (\mathrm{mod}\, 7)$$
$$\Rightarrow 333^{108} \equiv 1 (\mathrm{mod}\, 7)$$
$$\Rightarrow 333^{108} \cdot 333^2 \equiv 2 (\mathrm{mod}\, 7)$$
$$\Rightarrow 333^{110} \cdot 333 \equiv 1 (\mathrm{mod}\, 7)$$
$$\Rightarrow 333^{111} \equiv 1 (\mathrm{mod}\, 7)$$

So we have, $111^{333} + 333^{111} \equiv 6 + 1 (\mathrm{mod}\, 7)$

$$\Rightarrow 111^{333} + 333^{111} \equiv 7 (\mathrm{mod}\, 7)$$
$$\Rightarrow 111^{333} + 333^{111} \equiv 0 (\mathrm{mod}\, 7)$$
$$\therefore 7 / 111^{333} + 333^{111}$$

Application 9: Find the remainder when 1!+2!+3!+4!+5!+…..+n! is divided by 24 $(n \geq 4)$

Solution: $1! \equiv 1 (\mathrm{mod}\, 24)$

$$\Rightarrow 2! \equiv 2 (\bmod 24)$$
$$\Rightarrow 3! \equiv 6 (\bmod 24)$$
$$\Rightarrow 4! \equiv 0 (\bmod 24)$$
$$\Rightarrow 5! \equiv 0 (\bmod 24)$$
$$\Rightarrow \cdot$$
$$\Rightarrow \cdot$$
$$\Rightarrow \cdot$$
$$\Rightarrow n! \equiv 0 (\bmod 24)$$
$$\Rightarrow 1!+2!+3!+4!+5!+\ldots+n! \equiv 1+2+6+0 (\bmod 24)$$
$$\Rightarrow 1!+2!+3!+4!+5!+\ldots+n! \equiv 9 (\bmod 24)$$
$$\therefore R = 9$$

Application 10: Using Fermat's Theorem show that $17/(11^{104}+1)$

Solution: $11^{17} \equiv 11 (\bmod 17)$

$$\Rightarrow 11^{17} \equiv 11 (\bmod 17)$$
$$\Rightarrow 11^{17} \equiv -6 (\bmod 17)$$
$$\Rightarrow (11^{17})^2 \equiv (-6)^2 (\bmod 17)$$
$$\Rightarrow 11^{34} \equiv 36 (\bmod 17)$$
$$\Rightarrow 11^{34} \equiv 2 (\bmod 17)$$
$$\Rightarrow (11^{34})^3 \equiv 2^3 (\bmod 17)$$
$$\Rightarrow 11^{102} \equiv 8 (\bmod 17)$$
$$\Rightarrow 11^{102} \cdot 11 \equiv 8 \cdot 11 (\bmod 17)$$
$$\Rightarrow 11^{103} \equiv 88 (\bmod 17)$$
$$\Rightarrow 11^{103} \equiv 3 (\bmod 17)$$
$$\Rightarrow 11^{103} \cdot 11 \equiv 3 \cdot 11 (\bmod 17)$$
$$\Rightarrow 11^{104} \equiv 33 (\bmod 17)$$
$$\Rightarrow 11^{104} \equiv -1 (\bmod 17)$$
$$\Rightarrow 11^{104} + 1 \equiv 0 (\bmod 17)$$
$$\therefore 17/(11^{104}+1)$$

Aplication 11: Using the above Lemma, prove that

$$341 \big/ \left(2^{2040}-1\right)$$

Solution: Note that (1) $$2^5 \equiv 1(\bmod 31)$$
$$\Rightarrow 2^{11} \equiv 2(\bmod 31)$$

Also, we have (2) $$2^5 \equiv -1(\bmod 31)$$
$$\Rightarrow 2^{30} \equiv 1(\bmod 11)$$
$$\Rightarrow 2^{31} \equiv 2(\bmod 11)$$

(1) and (2) $$\Rightarrow 2^{11*31} \equiv 2(\bmod 11*31)$$
$$\Rightarrow 2^{341} \equiv 2(\bmod 341)$$
$$\Rightarrow 2^{340} \equiv 1(\bmod 341)$$
$$\Rightarrow \left(2^{340}\right)^6 \equiv 1(\bmod 341)$$
$$\Rightarrow 2^{2040} \equiv 1(\bmod 341)$$
$$\Rightarrow 341 / \left(2^{2040} - 1\right)$$

Remark: Observe that 341 = 11*31

Application 12: Find the remainder when 2(26!) is divided by 29

Solution: $$(29-1)! \equiv -1(\bmod 29)$$
$$\Rightarrow 28! \equiv -1(\bmod 29)$$
$$\Rightarrow 28 \cdot (27)! \equiv 28(\bmod 29)$$
$$\Rightarrow 27! \equiv 1(\bmod 29)$$
$$\Rightarrow 2 \cdot 27! \equiv 2(\bmod 29)$$
$$\Rightarrow 2 \cdot 27! \equiv -27(\bmod 29)$$
$$\Rightarrow 2 \cdot 27 \cdot 26! \equiv -27(\bmod 29)$$
$$\Rightarrow 2 \cdot 26! \equiv -1(\bmod 29)$$
$$\Rightarrow 2 \cdot 26! \equiv 28(\bmod 29)$$
$$\Rightarrow R = 28$$

.

References

Burton, D. M. (1998). *Elementary number theory*. New York City, New York: McGraw-Hill.

Dodge, C. W. (1975). *Numbers and mathematics*. Boston, Massachusetts: Prindle, Weber & Schmidt Inc..

Dudley, Underwood (1969). *Elementary number theory*. San Francisco: W. H. Freeman and Company.

Jackson, T. H. (1975). *Number theory*. Boston, Massachusetts: Rouledge & Kegan Paul Ltd..