

MATH 433

Applied Algebra

Lecture 6:

Congruences (continued).

Congruence classes.

Congruences

Let n be a positive integer. The integers a and b are called **congruent modulo n** if they have the same remainder when divided by n . An equivalent condition is that n divides the difference $a - b$.

Notation. $a \equiv b \pmod{n}$ or $a \equiv b \pmod{n}$.

Proposition If $a \equiv b \pmod{n}$ then for any $c \in \mathbb{Z}$,

- (i) $a + cn \equiv b \pmod{n}$;
- (ii) $a + c \equiv b + c \pmod{n}$;
- (iii) $ac \equiv bc \pmod{n}$.

More properties of congruences

Proposition If $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, then

- (i) $a + b \equiv a' + b' \pmod{n}$;
- (ii) $a - b \equiv a' - b' \pmod{n}$;
- (iii) $ab \equiv a'b' \pmod{n}$.

Proof: Since $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, the number n divides $a - a'$ and $b - b'$, i.e., $a - a' = kn$ and $b - b' = \ell n$, where $k, \ell \in \mathbb{Z}$. Then n also divides

$$(a + b) - (a' + b') = (a - a') + (b - b') = kn + \ell n = (k + \ell)n,$$

$$(a - b) - (a' - b') = (a - a') - (b - b') = kn - \ell n = (k - \ell)n,$$

$$\begin{aligned} ab - a'b' &= ab - ab' + ab' - a'b' = a(b - b') + (a - a')b' \\ &= a(\ell n) + (kn)b' = (a\ell + kb')n. \end{aligned}$$

Primes in arithmetic progressions

Theorem There are infinitely many prime numbers of the form $4k + 3$, $k \in \mathbb{Z}$.

Idea of the proof: Let p_1, p_2, \dots, p_n be primes different from 3 and satisfying $p_i \equiv 3 \pmod{4}$.

Consider the number $N = 4p_1p_2 \cdots p_n + 3$. This number must have a prime divisor $p \equiv 3 \pmod{4}$.

Note that p is different from p_1, p_2, \dots, p_n and 3.

Theorem (Dirichlet) Suppose a and d are positive integers such that $\gcd(a, d) = 1$. Then the arithmetic progression $a, a + d, a + 2d, \dots$ contains infinitely many prime numbers.

Divisibility of decimal integers

Let $\overline{d_k d_{k-1} \dots d_3 d_2 d_1}$ be the decimal notation of a positive integer n ($0 \leq d_i \leq 9$). Then

$$n = d_1 + 10d_2 + 10^2d_3 + \dots + 10^{k-2}d_{k-1} + 10^{k-1}d_k.$$

Proposition 1 The integer n is divisible by 2, 5 or 10 if and only if the last digit d_1 is divisible by the same number.

Proposition 2 The integer n is divisible by 4, 20, 25, 50 or 100 if and only if $\overline{d_2 d_1}$ is divisible by the same number.

Proposition 3 The integer n is divisible by 3 or 9 if and only if the sum of its digits $d_k + \dots + d_2 + d_1$ is divisible by the same number.

Proposition 4 The integer n is divisible by 11 if and only if the alternating sum of its digits $(-1)^{k-1}d_k + \dots + d_3 - d_2 + d_1$ is divisible by 11.

Hint: $10^m \equiv 1 \pmod{9}$, $10^m \equiv 1 \pmod{3}$, $10^m \equiv (-1)^m \pmod{11}$.

Problem. Determine the last digit of 7^{2015} .

The last digit is the remainder under division by 10.

We have $7^1 \equiv 7 \pmod{10}$ and $7^2 = 49 \equiv 9 \pmod{10}$.

Then

$$7^3 = 7^2 \cdot 7 \equiv 9 \cdot 7 = 63 \equiv 3 \pmod{10}.$$

Further,

$$7^4 = 7^3 \cdot 7 \equiv 3 \cdot 7 = 21 \equiv 1 \pmod{10}.$$

Now it follows that $7^{n+4} \equiv 7^n \pmod{10}$ for all $n \geq 1$.

Therefore the last digits of the numbers

$7^1, 7^2, 7^3, \dots, 7^n, \dots$ form a periodic sequence with period 4. Since $2015 \equiv 3 \pmod{4}$, the last digit of 7^{2015} is the same as the last digit of 7^3 , which is 3.

Problem. When the number $14^7 \cdot 25^{30} \cdot 40^{12}$ is written out, how many consecutive zeroes are there at the right-hand end?

The number of consecutive zeroes at the right-hand end is the exponent of the largest power of 10 that divides our number.

As follows from the Unique Factorisation Theorem, a positive integer A divides another positive integer B if and only if the prime factorisation of A is part of the prime factorisation of B .

The prime factorisation of the given number is

$$14^7 \cdot 25^{30} \cdot 40^{12} = (2 \cdot 7)^7 \cdot (5^2)^{30} \cdot (2^3 \cdot 5)^{12} = 2^{43} \cdot 5^{72} \cdot 7^7.$$

For any integer $n \geq 1$ the prime factorisation of 10^n is $2^n \cdot 5^n$.

Hence 10^n divides the given number if $n \leq 43$ and $n \leq 72$.

The largest number with this property is 43. Thus there are 43 zeroes at the right-hand end.

Congruence classes

Given an integer a , the **congruence class of a modulo n** is the set of all integers congruent to a modulo n .

Notation. $[a]_n$ or simply $[a]$. Also denoted $a + n\mathbb{Z}$ as $[a]_n = \{a + nk : k \in \mathbb{Z}\}$.

Examples. $[0]_2$ is the set of even integers, $[1]_2$ is the set of odd integers, $[2]_4$ is the set of even integers not divisible by 4.

If n divides a positive integer m , then every congruence class modulo n is the union of m/n congruence classes modulo m . For example, $[2]_4 = [2]_8 \cup [6]_8$.

The congruence class $[0]_n$ is called the **zero congruence class**. It consists of the integers divisible by n .

The set of all congruence classes modulo n is denoted \mathbb{Z}_n . It consists of n elements $[0]_n, [1]_n, [2]_n, \dots, [n-1]_n$.