MATH 433

Applied Algebra

Lecture 6: Congruences (continued). Modular arithmetic.

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

Proposition 1 If $a \equiv b \bmod n$ then for any $c \in \mathbb{Z}$,
(i) $a + cn \equiv b \bmod n$;
(ii) $a + c \equiv b + c \bmod n$;
(iii) $ac \equiv bc \bmod n$.

Proposition 2 If $a \equiv a' \bmod n$ and $b \equiv b' \bmod n$, then
(i) $a + b \equiv a' + b' \bmod n$;
(ii) $a - b \equiv a' - b' \bmod n$;
(iii) $ab \equiv a'b' \bmod n$.

Primes in arithmetic progressions

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

Proof: Let $p_1, p_2, \ldots, p_k$ be any finite collection of primes different from 3 and satisfying $p_i \equiv 3 \bmod 4$. We need to show that it does not include all primes of that form. Consider the number $N = 4p_1p_2\ldots p_k + 3$. Let $N = q_1q_2\ldots q_m$ be its prime factorisation. By construction, N is odd and not divisible by $p_1, p_2, \ldots, p_k$ and 3. Hence each prime factor q_j is odd and different from $p_1, p_2, \ldots, p_k$ and 3. If we assumed that $q_j \equiv 1 \bmod 4$ for $j = 1, 2, \ldots, m$, then it would follow that $N \equiv 1 \bmod 4$. However, $N \equiv 3 \bmod 4$ by construction. We conclude that $q_j \equiv 3 \bmod 4$ for some j, $1 \leq j \leq m$.

Theorem (Dirichlet 1837) Suppose a and d are positive integers such that $\gcd(a, d) = 1$. Then the arithmetic progression $a, a+d, a+2d, \ldots$ 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

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

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 $d_k + \cdots + d_2 + d_1$ 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
$(-1)^{k-1} d_k + \cdots + d_3 - d_2 + d_1$ is divisible by 11.

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

Problem. Determine the last digit of 7^{2024}.

The last digit is the remainder after division by 10. We have $7^1 \equiv 7 \bmod 10$ and $7^2 = 49 \equiv 9 \bmod 10$. 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 $7^{n+4} \equiv 7^n \bmod 10$ for all $n \geq 1$. Therefore the last digits of the numbers $7^1, 7^2, 7^3, \ldots, 7^n, \ldots$ form a periodic sequence with period 4. Since $2024 \equiv 0 \bmod 4$, the last digit of 7^{2024} is the same as the last digit of 7^4, which is 1.

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 $[0]_n, [1]_n, [2]_n, \dots, [n-1]_n$.

Modular arithmetic

Modular arithmetic is an arithmetic on the set $\mathbb{Z}_n$ for some $n \geq 1$. The arithmetic operations on $\mathbb{Z}_n$ are defined as follows. For any integers a and b, we let

$$[a]_n + [b]_n = [a + b]_n,$$
$$[a]_n - [b]_n = [a - b]_n,$$
$$[a]_n \times [b]_n = [ab]_n.$$

Theorem The arithmetic operations on $\mathbb{Z}_n$ are well defined, namely, they do not depend on the choice of representatives a, b for the congruence classes.

Proof: Let a' be another representative of $[a]_n$ and b' be another representative of $[b]_n$. Then $a' \equiv a \bmod n$ and $b' \equiv b \bmod n$. According to a previously proved proposition, this implies $a' + b' \equiv a + b \bmod n$, $a' - b' \equiv a - b \bmod n$ and $a'b' \equiv ab \bmod n$. In other words, $[a' + b']_n = [a + b]_n$, $[a' - b']_n = [a - b]_n$ and $[a'b']_n = [ab]_n$.