MATH 415

Modern Algebra I

Lecture 17: 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 $a \equiv b \pmod{n}$.

Examples. $12 \equiv 4 \bmod 8$, $24 \equiv 0 \bmod 6$, $31 \equiv -4 \bmod 35$.

Proposition If $a \equiv b \bmod n$ then for any integer c,
(i) $a + cn \equiv b \bmod n$;
(ii) $a + c \equiv b + c \bmod n$;
(iii) $ac \equiv bc \bmod n$.

Indeed, if $a - b = kn$, where k is an integer, then
$(a + cn) - b = a - b + cn = (k + c)n$,
$(a + c) - (b + c) = a - b = kn$, and
$ac - bc = (a - b)c = (kc)n$.

More properties of congruences

Proposition 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) $ab \equiv a'b' \bmod n$.

Proof: Since $a \equiv a' \bmod n$ and $b \equiv b' \bmod n$, 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

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

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 $(0 \le d_i \le 9)$. Then

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

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

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 $[a]_n = \{a + nk \mid k \in \mathbb{Z}\}$. Also denoted $a \bmod n$.

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 $[a]_n = a + n\mathbb{Z}$ is a coset of the subgroup $n\mathbb{Z}$ of the group $\mathbb{Z}$. Hence the set of all congruence classes modulo n is the factor space $\mathbb{Z}/n\mathbb{Z}$. It is usually identified with $\mathbb{Z}_n$ so that $\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \dots, [n-1]_n\}$.

Modular arithmetic

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

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

Theorem The arithmetic operations on $\mathbb{Z}_n$ are defined uniquely, 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 $[a'b']_n = [ab]_n$.

Invertible congruence classes

The set $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$, with addition and multiplication defined above, forms a commutative ring with unity. The unity is $[1]_n$. We say that a congruence class $[a]_n$ is **invertible** (or the integer a is **invertible modulo** n) if $[a]_n$ has a multiplicative inverse in $\mathbb{Z}_n$, that is, $ab \equiv 1 \bmod n$ for some $b \in \mathbb{Z}$. If this is the case, then b is called a **multiplicative inverse of** a **modulo** n.

The set of all invertible congruence classes in $\mathbb{Z}_n$ is denoted G_n or $\mathbb{Z}_n^*$. It is a multiplicative group (which is true for any ring with unity).

Theorem A nonzero congruence class $[a]_n$ is invertible if and only if $\gcd(a, n) = 1$. Otherwise it is a divisor of zero.

Corollary The ring $\mathbb{Z}_n$ is a field if and only if n is prime.

Theorem A nonzero congruence class $[a]_n$ is invertible if and only if $\gcd(a, n) = 1$. Otherwise $[a]_n$ is a divisor of zero.

Proof: Let $d = \gcd(a, n)$. If $d > 1$ then n/d and a/d are integers, $[n/d]_n \neq [0]_n$, and $[a]_n[n/d]_n = = [an/d]_n = [a/d]_n[n]_n = [a/d]_n[0]_n = [0]_n$. Hence $[a]_n$ is a divisor of zero.

Now consider the case $\gcd(a, n) = 1$. In this case 1 is an integral linear combination of a and n: $ma + kn = 1$ for some $m, k \in \mathbb{Z}$. Then

$$[1]_n = [ma + kn]_n = [ma]_n = [m]_n[a]_n.$$

Thus $[a]_n$ is invertible and $[a]_n^{-1} = [m]_n$.

Linear congruences

Linear congruence is a congruence of the form $ax \equiv b \bmod n$, where x is an integer variable. We can regard it as a linear equation in $\mathbb{Z}_n$: $[a]_n X = [b]_n$.

In the case $b = 1$, solving the linear congruence is equivalent to finding the inverse of the congruence class $[a]_n$. In the case $b = 0$, it is equivalent to determining if $[a]_n$ is a zero-divisor.

Proposition 1 If the congruence class $[a]_n$ is invertible and a' is a multiplicative inverse of a modulo n, then the congruence $ax \equiv b \bmod n$ is equivalent to $x \equiv a'b \bmod n$.

Proposition 2 Let $a, b, c, n \in \mathbb{Z}$ and $c, n \geq 1$. Then the congruence $ac \equiv bc \bmod nc$ is equivalent to $a \equiv b \bmod n$.

Proposition 3 Let $a, b, c, n \in \mathbb{Z}$ and $c, n \geq 1$. If $ac \equiv bc \bmod n$ and $\gcd(c, n) = 1$, then $a \equiv b \bmod n$.

Theorem The linear congruence $ax \equiv b \bmod n$ has a solution if and only if $d = \gcd(a, n)$ divides b. If this is the case then the solution set consists of d congruence classes modulo n that form a single congruence class modulo n/d.

Proof: If the congruence has a solution x, then $ax = b + kn$ for some $k \in \mathbb{Z}$. Hence $b = ax - kn$, which is divisible by $\gcd(a, n)$.

Conversely, assume that d divides b. Then the linear congruence is equivalent to $a'x \equiv b' \bmod m$, where $a' = a/d$, $b' = b/d$ and $m = n/d$. In other words, $[a']_m X = [b']_m$, where $X = [x]_m$.

We have $\gcd(a', m) = \gcd(a/d, n/d) = \gcd(a, n)/d = 1$. Hence the congruence class $[a']_m$ is invertible. It follows that all solutions x of the linear congruence form a single congruence class modulo m, $X = [a']_m^{-1}[b']_m$. This congruence class splits into d distinct congruence classes modulo $n = md$.

Problem. Solve the congruence $12x \equiv 6 \bmod 21$.

$\iff 4x \equiv 2 \bmod 7 \iff 2x \equiv 1 \bmod 7$
$\iff [x]_7 = [2]_7^{-1} = [4]_7$
$\iff [x]_{21} = [4]_{21}$ or $[11]_{21}$ or $[18]_{21}$.

Problem. Find all integer solutions of the equation $12x - 21y = 6$.

For any integer solution of the equation, the number x is a solution of the linear congruence $12x \equiv 6 \bmod 21$. By the above, $x \equiv 4 \bmod 7$, that is, $x = 4 + 7k$ for some $k \in \mathbb{Z}$. Then $y = (12x - 6)/21 = (12(4 + 7k) - 6)/21 = 2 + 4k$, which is also integer. Thus the general integer solution is $x = 4 + 7k$, $y = 2 + 4k$, where $k \in \mathbb{Z}$.

Corollaries of Lagrange's Theorem

Fermat's Little Theorem If p is a prime number then $a^{p-1} \equiv 1 \bmod p$ for any integer a that is not a multiple of p.

Proof: If a is not a multiple of p then $[a]_p$ is in G_p, the multiplicative group of invertible congruence classes modulo p. Lagrange's Theorem implies that the order of $[a]_p$ in G_p divides $|G_p| = p - 1$. It follows that $[a]_p^{p-1} = [1]_p$, which means that $a^{p-1} \equiv 1 \bmod p$.

Euler's Theorem If n is a positive integer and $\phi(n)$ is the number of integers between 1 and n coprime with n, then $a^{\phi(n)} \equiv 1 \bmod n$ for any integer a coprime with n.

Proof: $a^{\phi(n)} \equiv 1 \bmod n$ means that $[a]_n^{\phi(n)} = [1]_n$. The number a is coprime with n, i.e., $\gcd(a, n) = 1$, implies that the congruence class $[a]_n$ is in G_n. It remains to notice that $|G_n| = \phi(n)$ and apply Lagrange's Theorem.

Problem. Determine the last two digits of 3^{2022}.

The last two digits form the remainder after division by 100.

First let us compute $\phi(100)$. Since $100 = 2^2 \cdot 5^2$, an integer k is coprime with 100 if and only if it is not divisible by 2 or 5. Among integers from 1 to 100, there are $50 = 100/2$ even numbers and $20 = 100/5$ numbers divisible by 5. Note that some of them are divisible by both 2 and 5. These are exactly numbers divisible by 10. There are $10 = 100/10$ such numbers. We conclude that $\phi(100) = 100 - 50 - 20 + 10 = 40$.

By Euler's Theorem, $3^{40} \equiv 1 \bmod 100$. Then

$$\begin{aligned}[3^{2022}] &= [3]^{2022} = [3]^{40\cdot 50+22} = ([3]^{40})^{50}\,[3]^{22} = [3]^{22} \\ &= ([3]^5)^4\,[3]^2 = [243]^4\,[9] = [43]^4\,[9] = [(50-7)^2]^2\,[9] \\ &= [7^2]^2\,[9] = [49]^2\,[9] = [(50-1)^2]\,[9] = [1^2]\,[9] = [9].\end{aligned}$$

Thus $3^{2022} = \ldots 09$.