Lecture Notes for Introduction to Modern Algebra I: Lecture 3.1

1 Mathematical Induction and modular arithmetic

1.1 Induction

Induction: In order to prove that a property $P = P(n)$ **is true for all natural numbers** $n \geq n_0$, we can prove:

1. $P(n_0)$ is True.
2. For all $k \geq n_0$, $P(k)$ is True $\Rightarrow P(k+1)$ is also True.

In this way for example, if n_0 where to be $n_0 = 10$ and we will have proven steps (1) and (2), then we will have the validity of P for n_0 as well as the chain of implications:

$$P(n_0) \text{ is True} \Rightarrow P(n_0+1) \text{ is True} \Rightarrow P(n_0+2) \text{ is True} \Rightarrow \ldots,$$

that guarantees the validity of P for all natural numbers $n \geq n_0$.

Alternative or strong induction: In order to prove a property $P = P(n)$ for all natural numbers $n \geq n_0$, we can prove:

1. $P(n_0)$ is True.
2. For all $k \geq n_0$, $P(k_0), \ldots, P(k)$ are True $\Rightarrow P(k+1)$ is also True.

Some examples of the use of induction:

Example 1. Prove that $n! > 2^n$ for all $n \in \mathbb{N}$ with $n > 3$.
Beginning or Base case: For $n = 4$, we have $4! = 4(3)(2)(1) = 24$ and $2^4 = 16$, hence it is true for $n = 4$ that $n! > 2^n$.
Induction step: Now for $k \geq 4$, using the fact that the inequality is true for k, we should obtain the inequality or $k+1$. We have:

$$(k+1)! = k!(k+1) > 2^k(k+1) \qquad \text{by Induction hypothesis.}$$

At the same time $k+1 \geq 5 > 2$ because $k \geq 4$. So we can extend the previous inequality to:

$$(k+1)! = k!(k+1) > 2^k(k+1) > 2^k \cdot 2 = 2^{k+1}.$$

In this way we obtained the inequality for $n = k+1$ from $n = k$. Since we have also a base case $n = 4$. We have proved the property for all natural numbers $n \geq 4$.

Example 2. Prove that $6^n - 1$ is divisible by 5, for all natural numbers n.
Beginning or Base case: For $n = 1$ we have $6^1 - 1 = 5$ is certainly divisible by 5.
Induction step: Let $k \geq 1$. Assuming that $6^k - 1$ is divisible by 5, we need to obtain $6^{k+1} - 1$ is also divisible by 5. We have:

$$6^{k+1} - 1 = 6(6^k) - 1 = 6(6^k - 1) + 6 - 1 = 6(6^k - 1) + 5.$$

Since both terms $6^k - 1$ (hypothesis of induction) and 5 are divisible by 5, the sum $6(6^k - 1) + 5 = 6^{k+1} - 1$ is also divisible by 5.

1.2 Modular arithmetic

Given an integer $n > 1$, called a modulus, two integers a, b are said to be congruent modulo n, if n is a divisor of their difference (i.e., if there is an integer k such that $a - b = kn$). Congruence modulo n is an equivalence relation compatible with the operations of addition, subtraction, and multiplication. Congruence modulo n is denoted:

$$a \equiv b (\operatorname{mod} n).$$

Remark 3. Two numbers a, b are congruent $\operatorname{mod} n$, if and only if they have the same remainder when divided by n. For example,

$$144 \equiv 74 (\operatorname{mod} 10), \quad 18 \equiv 103 (\operatorname{mod} 5), \quad -5 \equiv 4 (\operatorname{mod} 9).$$

Any integer $a \operatorname{mod}(\, n)$ can be made congruent to an element in the set $\{0, 1, ..., n-1\}$ by taking the remainder of the division of a by n.

Some properties of modular congruency:

(1) (addition)If $a_1 \equiv b_1 (\operatorname{mod} n)$ and $a_2 \equiv b_2 (\operatorname{mod} n)$, then $a_1 + a_2 \equiv b_1 + b_2 (\operatorname{mod} n)$.

(2) (subtraction) If $a_1 \equiv b_1 (\operatorname{mod} n)$ and $a_2 \equiv b_2 (\operatorname{mod} n)$, then $a_1 - a_2 \equiv b_1 - b_2 (\operatorname{mod} n)$.

(3) (multiplication) If $a_1 \equiv b_1 (\operatorname{mod} n)$ and $a_2 \equiv b_2 (\operatorname{mod} n)$, then $a_1 a_2 \equiv b_1 b_2 (\operatorname{mod} n)$.

(4) (powers) If $a_1 \equiv b_1 (\operatorname{mod} n)$ and r is a natural number, then $a_1^r \equiv b_1^r (\operatorname{mod} n)$.

(5) (inverse) There exists an integer denoted a^{-1} such that $a \cdot a^{-1} \equiv 1 (\operatorname{mod} n)$ if and only if a, n are relatively prime. This integer a^{-1} is called a modular multiplicative inverse of a modulo n. For example:

$$\gcd(16, 9) = 1 \Rightarrow \text{ there is x with } 16x \equiv 1 (\operatorname{mod} 9) \text{ and we try the multiples:}$$

$$16(1) = 16 \equiv 7 (\operatorname{mod} 9), \quad 16(2) = 32 \equiv 5 (\operatorname{mod} 9),$$
$$16(3) = 48 \equiv 3 (\operatorname{mod} 9), \quad \underline{16(4) = 64 \equiv 1 (\operatorname{mod} 9)}$$

and we have found that 4 is an inverse of 16 in modulus 9.

(6) (linear equations) If $ax \equiv b(\text{mod} n)$ and a, n are relatively prime ($\gcd(a, n) = 1$), then the solution to this linear congruence is given by $x \equiv a^{-1}b \pmod n$. For example for the equation $16x \equiv 3 \pmod 9$ we use the inverse of $16 \pmod 9$ which we found to be 4;

$$16x \equiv 3 \pmod 9 \quad \text{and} \quad 16(4)x \equiv 3(4) \equiv 12 \pmod 9 \Rightarrow x \equiv 3 \pmod 9.$$

Example 4. Find the remainder of 4^{2021} when divided by 9.
Answer: $4^3 = 64 \equiv 1 \pmod 9 \Rightarrow 4^{3(673)} \equiv 1 \pmod 9 \Rightarrow 4^{2019} \equiv 1 \pmod 9 \Rightarrow 4^{2021} = 4^{2019}(4^2) \equiv 4^2(1) \pmod 9 \Rightarrow 4^{2021} \equiv 16 \equiv 7 \pmod 9$. The remainder is 7.

Example 5. Find the last two digits in the decimal representation of 7^{2022}.
Answer: The last two digits of a number can be obtained when we work $(\text{mod}\, 100)$. You can check that two numbers are congruent mod 100 if and only if, they end up having the same two digits. First, we observe (using a calculator) $7^8 = 5764801 \equiv 1 \pmod{100}$. As a consequence for any exponent k multiple of 8, we will have $7^k \equiv 1 \pmod{100}$. Now, we see how how close is 2022 to be a multiple of 8:

$$2022 = 8(252) + 6.$$

Hence we can do:

$$7^{2022} = 7^6 7^{252(8)} \equiv 7^6 = 117649 \equiv 49 \pmod{100}.$$

We probably cannot compute the whole number 7^{2022} with a calculator, but we know that the last two digits will be 49.