**Solidity Assignment**

**1)Hello World using solidity**

// SPDX-License-Identifier: GPL-3.0

pragma solidity ^0.8.10;

contract hello{

    string public print = "Hello World";

}

**2)Program to find Factorial of number via pure functions**

// SPDX-License-Identifier: GPL-3.0

pragma solidity ^0.8.10;

contract fact{

    function factorial(uint a) public pure returns(uint){

        if (a == 0){

            return 1;

        }

        else{

            uint b = a\*factorial(a-1);

            return b;

        }

    }

}

**3)Implementing decentralised voting system for 3 candidates, each voter can vote twice (Doubt)**

// SPDX-License-Identifier: GPL-3.0

pragma solidity ^0.8.7;

struct Candidate {

    uint id;

    string name;

    uint votercount;

}

contract Election{

    mapping (address => bool)voter;

    mapping (uint => Candidate) public candidates;

    uint public candidatesCount;

    function addCandidate(string memory name) private

    {

        candidatesCount++;

        candidates[candidatesCount] = Candidate(candidatesCount,name,0);

    }

    constructor() public {

        addCandidate("Bijan Roy");

        addCandidate("Sagnik");

        addCandidate("Bipin");

    }

    function vote(uint candidateID) public

    {

        require(!voter[msg.sender]);

        require(candidateID > 0 && candidateID <= candidatesCount);

        voter[msg.sender] = true;

        candidates[candidateID].votercount++;

    }

}

**4)Palindrome Program : to write a code to return palindrome of a string, if it is palindrome transfer 50 ETH from one account to manager account.**

// SPDX-License-Identifier: GPL-3.0

pragma solidity ^0.8.10;

contract Palindrome{

    address payable Manager = payable(0x617F2E2fD72FD9D5503197092aC168c91465E7f2);

    function payEther() public payable{

    }

    function sendEther(string memory word) public returns(string memory){

        bytes memory new\_word = bytes(word);

        string memory len = new string(new\_word.length);

        bytes memory nw1 = bytes(len);

        for(uint i = 0; i<new\_word.length; i++){

            nw1[new\_word.length-i-1] = new\_word[i];

        }

        string memory s;

        if(keccak256(abi.encodePacked(word)) == keccak256(abi.encodePacked(nw1))){

            Manager.transfer(50 ether);

            s = "SendingDone";

        }

        else{

            s = "false";

        }

        return s;

    }

}

**5)Write a contract 'Time' which implements a function named getTime. (Doubt)**

getTime() accepts a Unix timestamp (number of seconds since 1970-01-01 00:00:00 GMT). Method will check if this timestamp exists after the current time. If yes, it will return a timestamp after 1 hour, 20 minutes and 30 seconds from passed time else return 0.

Informational Hint

Time Units

Suffixes like seconds, minutes, hours, days and weeks after literal numbers can be used to specify units of time where seconds are the base unit and units are considered naively in the following way:

1 == 1 seconds

1 minutes == 60 seconds

1 hours == 60 minutes

1 days == 24 hours

1 weeks == 7 days

To get current time, now can be used being aware about the fact that it can be influenced by miners to some degree. It retuns uint

// SPDX-License-Identifier: GPL-3.0

pragma solidity ^0.8.10;

contract Time{

    uint public currentTime = block.timestamp;

    function getTime(uint time) public view returns(bool)

    {

        bool a;

        uint t = time - currentTime;

        if(t < currentTime){

            return true;

        }

        else{

            a = false;

            return a;

        }

    }

}

**6)Problem Statement**

Write a contract 'ThreeAndSeven' which implements a function named check.

check() accepts a number and return true if number is fully divided by 3 or 7 and greater than 10 else false. This function should not consume any gas.

Informational Hint

Boolean Value Type

bool: The possible values are constants true and false.

Operators:

! (logical negation)

&& (logical conjunction, “and”)

|| (logical disjunction, “or”)

== (equality)

!= (inequality)

The operators || and && apply the common short-circuiting rules. This means that in the expression f(x) || g(y), if f(x) evaluates to true, g(y) will not be evaluated even if it may have side-effects.

// SPDX-License-Identifier: GPL-3.0

pragma solidity ^0.8.10;

contract ThreeAndSeven{

    function check(uint n) public pure returns(bool){

        if((n%3==0 || n%7==0) && n>10){

            return true;

        }

        else{

            return false;

        }

    }

}

**7)EvenOdd**

Problem Statement

Write a contract 'EvenOdd' to which implements a function named check.

check() accepts a number and return whether the passed number is odd or even without consuming gas. (Ignore various checks on passed parameters for now)

Informational Hint

Any integer that can be divided exactly (i.e. remainder = 0) by 2 is an even number.

Modulo: The modulo operation a % n yields the remainder r after the division of the operand a by the operand n

// SPDX-License-Identifier: GPL-3.0

pragma solidity ^0.8.10;

contract EvenOdd{

    function check(uint n) public pure returns(string memory){

        string memory num;

        if (n % 2 == 0){

            num = "Even";

        }

        else{

            num = "Odd";

        }

        return num;

    }

}

**8)Problem Statement**

Write a contract 'Calculator' to which returns addition, subtraction, multiplication and division of two passed integers without consuming gas. (Ignore various checks on passed parameters for now)

Informational Hint

To define a function which should not consume any gas and return the response immediatly, we should use view or pure function.

Operators

Comparisons: <=, <, ==, !=, >=, > (evaluate to bool)

Bit operators: &, |, ^ (bitwise exclusive or), ~ (bitwise negation)

Arithmetic operators: +, -, unary -, unary +, \*, /, % (remainder), \*\* (exponentiation)

Division by zero and modulus with zero throws an exception.

// SPDX-License-Identifier: GPL-3.0

pragma solidity ^0.8.10;

contract calculator{

    function add(int a , int b) public pure returns(int){

        return a+b;

    }

    function sub(int a, int b) public pure returns(int){

        return a-b;

    }

    function div(int a, int b) public pure returns(int){

        return a/b;

    }

    function multi(int a, int b) public pure returns(int){

        return a\*b;

    }

    /\*function returnAll(uint a, uint b) public pure returns(uint,uint,uint,uint){

        return (a\*\*b,a+b,a\*b,a/b);

}\*/

}

**9)Program to find Sum of Digits**

// SPDX-License-Identifier: GPL-3.0

pragma solidity ^0.8.10;

contract sum\_of\_digit{

    function sum(uint n) public pure returns(uint){

        uint sum = 0;

        while(n>=1){

            uint r = n%10;

            n = n/10;

            sum = sum + r;

        }

        return sum;

    }

}

**10)Problem Statement**

Write a contract named "AttendanceRegister" which will be deployed by teacher. There will be a function add which will take student name, class & joiningDate and will store it where:

name: String to store student name

class: Number from 1 to 12

joiningDate: Date timestamp of student joining day Each student will be stored corresponding to a unique serial number called roll number.

Only teacher can add the data of student. An event will be emitted on success.

Use struct, modifier & mapping wherever applicable.

Informational Hint

Structs

Solidity provides a way to define new types in the form of structs. Struct types can be used inside mappings and arrays and they can itself contain mappings and arrays.

It is not possible for a struct to contain a member of its own type, although the struct itself can be the value type of a mapping member or it can contain a dynamically-sized array of its type. This restriction is necessary, as the size of the struct has to be finite.

Modifiers

Modifiers can be used to easily change the behaviour of functions. For example, they can automatically check a condition prior to executing the function. Modifiers are inheritable properties of contracts and may be overridden by derived contracts.

Multiple modifiers are applied to a function by specifying them in a whitespace-separated list and are evaluated in the order presented.

Explicit returns from a modifier or function body only leave the current modifier or function body. Return variables are assigned and control flow continues after the “\_” in the preceding modifier.

Arbitrary expressions are allowed for modifier arguments and in this context, all symbols visible from the function are visible in the modifier. Symbols introduced in the modifier are not visible in the function (as they might change by overriding).

// SPDX-License-Identifier: GPL-3.0

pragma solidity ^0.8.10;

struct student{

        string Name;

        uint Class;

        string JoiningDate;

    }

contract AttendanceRegister{

    address public Teacher = msg.sender;

    mapping (uint => student) public data;

    event Register(address Teacher, student Data);

    modifier onlyTeacher() {

        require(Teacher == msg.sender, "You are not a teacher");

        \_;

    }

    function add(uint roll, string memory name, uint class, string memory date) public onlyTeacher {

        data[roll] = student(name,class,date);

        emit Register(msg.sender, data[roll]);

    }

}