

TC-C-04

Evidence:

The screenshot shows the Truffle UI interface. On the left, there's a sidebar titled "DEPLOY & RUN TRANSACTIONS" with a dropdown menu. Below it, a section titled "Deployed Contracts" shows a single contract named "CALCULATOR AT 0xd91...3913". A red box highlights the "transact" button in the "Calculator" interface. To the right, the "Compiler" tab is active, displaying the Solidity code for the "Calculator" contract. The code includes event definitions for addition and subtraction, and external functions for performing these operations. An "Explain contract" button is also visible. At the bottom, a red box highlights the transaction details in the "Output" tab, which shows a pending transaction to the "Calculator.addition" function.

```
// SPDX-License-Identifier: MIT
// File: Calculator.sol
// Solidity version: 0.8.14

// pragma solidity ^0.8.14;

contract Calculator {
    // Events
    event Addition(uint256 number1, uint256 number2, uint256 result);
    event Subtraction(uint256 number1, uint256 number2, uint256 result);

    // External functions
    function addition(uint256 num1_, uint256 num2_) public returns(uint256 result_) {
        result_ = num1_ + num2_;
        emit Addition(num1_, num2_, result_);
    }

    function subtraction(uint256 num1_, uint256 num2_) public returns(uint256 result_) {
        result_ = num1_ - num2_;
        emit Subtraction(num1_, num2_, result_);
    }
}
```

Balance: 0 ETH

ADDITION

num1_: 11579208923731619542357098500
num2_: 0

Calldata Parameters transact

multiply: uint256 num1_
multiply2: uint256 num1_
subtraction: uint256 num1_, uint256 num2_
result:
0: uint256: 10
subtraction2: int256 num1_, int256 num2_

Output

transact to Calculator.addition pending ...

[vm] from: 0x5B3...eddC4 to: Calculator.addition(uint256,uint256) 0xd91...39138 value: 0 wei data: 0x54f...00000 logs: 1 hash: 0x1c6...88183

Debug