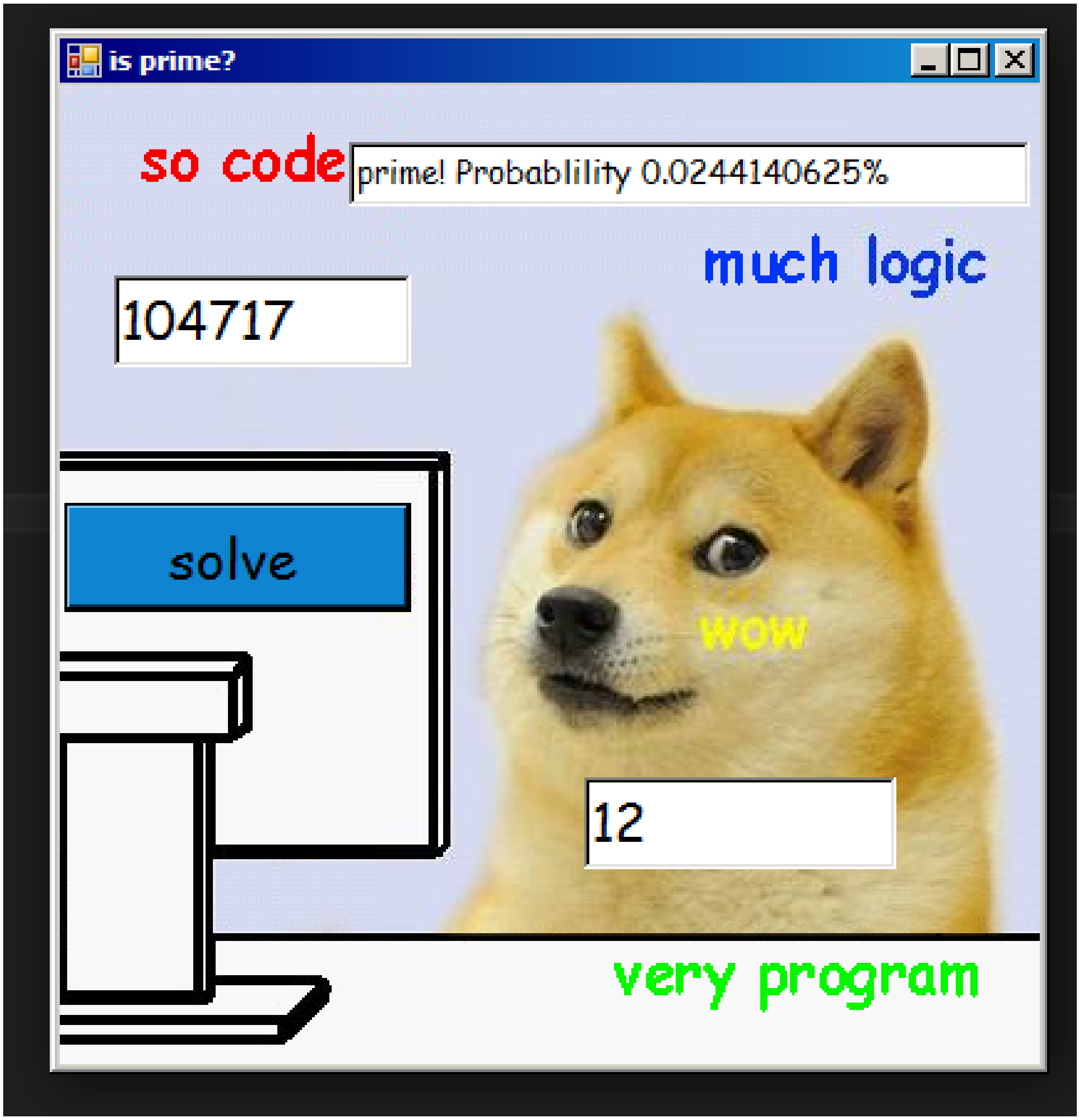
Taylor Cowley

CS 312 Lab 1 Fermat Project September 13, 2016



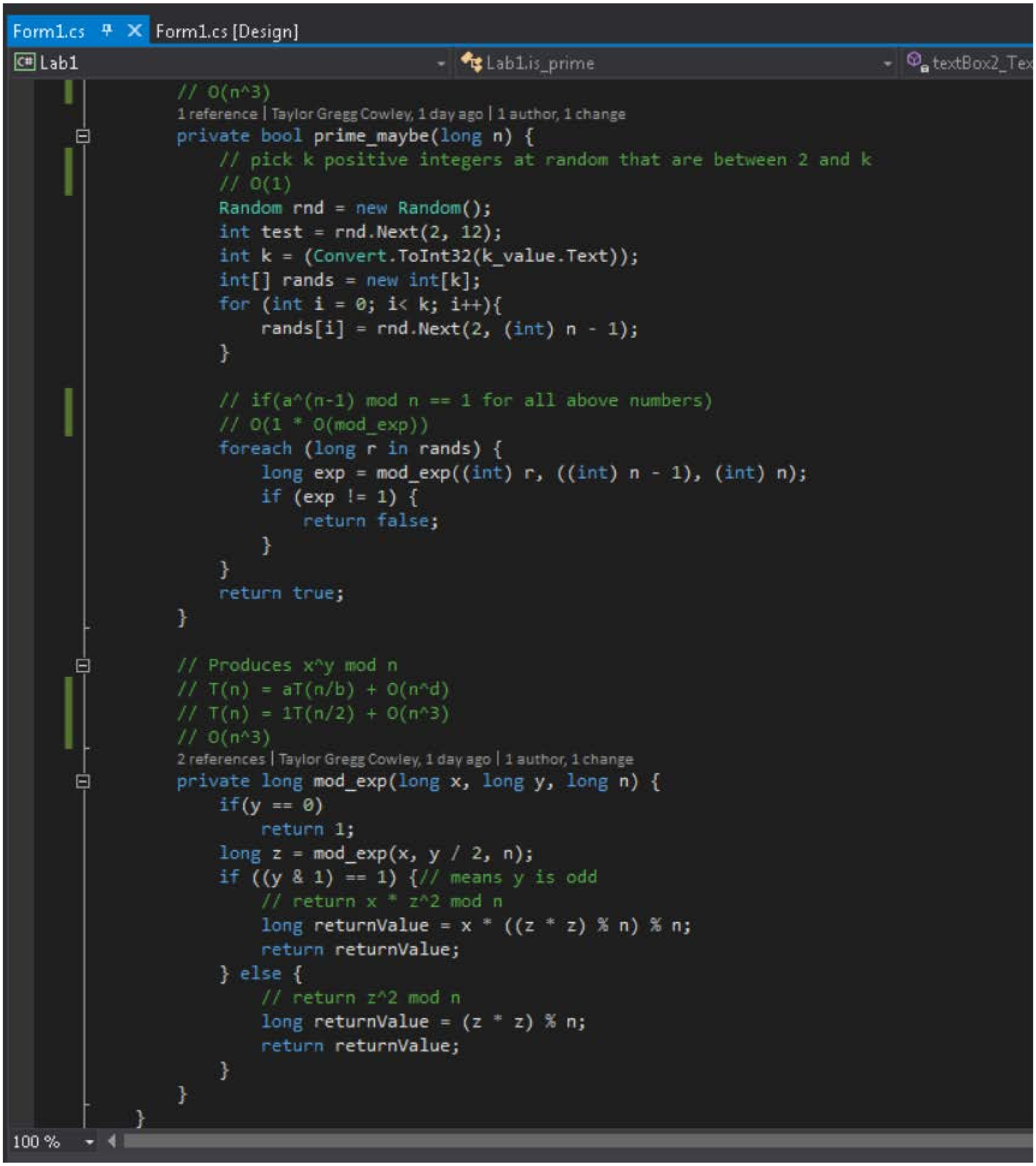
prime! Probablility 0.0244140625%

104717

12

Working example!

Notice the 3 text boxes and the solve button


Form1.cs
Form1.cs [Design]
Lab1
Lab1.is_prime
textBox2_Tex
1 reference | Taylor Gregg Cowley, 1 day ago | 1 author, 1 change
2 references | Taylor Gregg Cowley, 1 day ago | 1 author, 1 change
100 %

```
        // O(n^3)
        private bool prime_maybe(long n) {
            // pick k positive integers at random that are between 2 and k
            // O(1)
            Random rnd = new Random();
            int test = rnd.Next(2, 12);
            int k = (Convert.ToInt32(k_value.Text));
            int[] rands = new int[k];
            for (int i = 0; i< k; i++){
                rands[i] = rnd.Next(2, (int) n - 1);
            }

            // if(a^(n-1) mod n == 1 for all above numbers)
            // O(1 * O(mod_exp))
            foreach (long r in rands) {
                long exp = mod_exp((int) r, ((int) n - 1), (int) n);
                if (exp != 1) {
                    return false;
                }
            }
            return true;
        }

        // Produces x^y mod n
        // T(n) = aT(n/b) + O(n^d)
        // T(n) = 1T(n/2) + O(n^3)
        // O(n^3)
        private long mod_exp(long x, long y, long n) {
            if(y == 0)
                return 1;
            long z = mod_exp(x, y / 2, n);
            if ((y & 1) == 1) {// means y is odd
                // return x * z^2 mod n
                long returnValue = x * ((z * z) % n) % n;
                return returnValue;
            } else {
                // return z^2 mod n
                long returnValue = (z * z) % n;
                return returnValue;
            }
        }
    }
```

Beautiful code ☺

Time and space complexity-

For the random number creation and cycling through them – O(n)

For the modular exponent – O(n^3)

Making the overall O(n^3)

The probability of error is 1/(2^k) where k is the number of random numbers that we use with the modular exponent algorithm.