FIT3155: Tute+Lab sheet for week 9

Objectives: Concepts from weeks 8

Tute questions:

1. Revise the fast divide-and-conquer approach for large integer multiplication.
2. Prove that the above divide-and-conquer-approach for integer multiplication has a time-complexity of $O(d^{\log_2(3)})$, when multiplying two $2d$ bit integers. This requires you to solve the following time recurrence relationship:
$$T(2d) = 3T(d) + cd$$
where c is a constant.
3. Compute 7^{330} mod 13 by hand using the repeated squaring method.
4. Revise Miller-Rabin's randomized algorithm for primality testing.

Lab questions:

1. Implement the divide-conquer approach for multiplication of two integers.
2. Implement modular exponentiation using the method of repeated squaring.
3. Implement Miller-Rabin's randomized method of primality testing. Generate the the first 10,000 primes using this method.

```
-=0=-
 END
-=0=-
```