Homework 1: Problem 5

Andrew Tseng

September 2016

1.14

part a: We know that a and b have an unique quotient meaning there is a unique set (q, r) for a and b.

From the Euclidean algorithm, we know that $a = a - bq$ where $q \in Z$, since $b > 0$ we know that $r \geq 0$ since it is a remainder of $a|b$.

part b: Since $b > 0$ and $r \in a - bq : q \in Z$, we know that the remainder is r since $a - bq$ where q is the unique quotient $a - bq > 0$.
Because (q, r) is a unique quotient, $a - bq > 0$, this means that r is a remainder.

part c: We know tha $r = a - bq$. Through the Euclidean algorithm, we can say that r is a remainder since $a = bq + r$ where $b > 0$.

part d: Because a and b have a unique quotient, $a = bq + r_1$, we know that $q_1 = q_2$ which means that $r_1 = r_2$.

1.23

Looking the two cases of n:
Case 0 (n is even): $n = 2Z$ s.t. $z \in Z$.

$$n^2 = (2z)^2 = 4z^2$$

We know that:

$$0 \equiv 4z^2 \mod 4$$

Case 1 (n is odd): $n = 2Z + 1$ s.t. $z \in Z$.

$$n^2 = (2z + 1)^2 = 4z^2 + 4z + 1$$

This means that:

$$1 \equiv 4z^2 + 4z + 1 \mod 4$$

This means in order for n to be a perfect square: $n \mod 4 = 1$ or $n \mod 4 = 0$.
By the definition of modular arithmetic:

$$2m + a^2 \mod 4 = (2m \mod 4) + (a^2 \mod 4)$$

We know a^2 is a perfect square because $a \in Z$. Thus $a^2 \mod 4 = 0$ or 1.
Since m is an odd integer, we can know that $2 \equiv 2m \mod 4$. This is because:

$$2m \mod 4 = (2 \mod 4) * (m \mod 4) = 2$$

This indicates that $2 \equiv 2m + a^2 \mod 4$ or $3 \equiv 2m + a^2 \mod 4$.

In conclusion: $2m + a^2$ cannot be a perfect square.

1.25

Condition in the while loop: The while loop checks all bits of the binary expansion of A. When it is in the loop, we check the least-significant-bit in order to see if we multiply the b by $g^(2^i)$. i is the position of the bit. We then shift the bit to the left by executing the A/2 where it result in a integer.

Setting $a \equiv a^2 \mod m$ is the squaring portion of the algorithm. Such as when $g^2 = g * g \mod m$.