SKETCH OF SOLUTIONS (HOMEWORK VIII)

17.1- $x \equiv 763$

17.2- (a) $x \equiv 37$ (b) $x \equiv 559$

17.4- (a) Let $m = p_1 \cdots p_n$ with p_i distinct primes. We must show that

$$b^{1+v\phi(m)} \equiv b \mod m$$

Notice that for every prime q we have the following congruence for *every* a:

$$a^{1+\phi(q)} \equiv a \mod q$$

(It is **not** true that $a^{\phi(q)} \equiv 1 \mod q$ this fails for $a \equiv 0 \mod q$)

Using the chinese remainder theorem we know there is a unique solution $\mod p_1 \cdots p_n$ to the following system of congruences:

$$\begin{array}{lcll} b^{1+v\phi(m)} & \equiv & x & \mod p_1 \\ \vdots & & & \\ b^{1+v\phi(m)} & \equiv & x & \mod p_n \end{array}$$

since b satisfies all congruences (by the previous remark) we get the result (remember that ϕ is multiplicative).

(b) $6^7 \equiv 0 \mod 9$

18.1 FERMAT

18.2 The proof for (a) and (b) is the same as in 17.4

- Use the quadratic formula to find the roots of the polynomial $x^2 - (p + q)x + pq = 0$ The answer is $p = 1453$ $q = 3019$