SKETCH OF SOLUTIONS (HOMEWORK V)

9.1 a) $9^{794} \equiv 9^{11*72+2} \equiv 9^2 \equiv 8 \mod 73$

b) $x = 8, 21$

c) $x^{39} \equiv x^{3*13}$ which is either 0 or 1, therefore there are no solutions.

9.4 a) yes, b) yes, c) no.

10.1 a) First let us deal with the hard case: $m = 2$. In this case $b_1 = 1 = B$. Now let us deal with the easy case: $m > 2$. Notice that if $b_i \in \{b_1, \ldots, b_{\phi(m)}\}$ then there is some representative of $b_i^{-1} \mod m \in \{b_1, \ldots, b_{\phi(m)}\}$ (*why?*) also, if $b_i \in \{b_1, \ldots, b_{\phi(m)}\}$ then there is some representative of $-b_i \mod m \in \{b_1, \ldots, b_{\phi(m)}\}$ (*why?*). Using these two remarks we will pair the factors in the product in order to get $B \equiv \pm 1 \mod m$.

Start with b_1: If $b_1 \neq b_1^{-1}$ pair b_1 with b_1^{-1}.That is, factor

$$B \equiv (b_1 b_1^{-1})(b_{i_1} b_{i_2} \cdots b_{i_{\phi(m)-2}}) \equiv (1)(b_{i_1} b_{i_2} \cdots b_{i_{\phi(m)-2}})$$

If $b_1 \equiv b_1^{-1}$ pair b_1 with $-b_1 \mod m$.That is, factor

$$B \equiv (b_1(-b_1))(b_{i_1} b_{i_2} \cdots b_{i_{\phi(m)-2}}) \equiv (-1)(b_{i_1} b_{i_2} \cdots b_{i_{\phi(m)-2}})$$

Notice that if $b_1 \equiv -b_1 \mod m$ then $2b_1 \equiv 0 \mod m$, multiplying times $b_1^{-1} \mod m$ we get $2 \equiv 0 \mod m$ therefore $m = 2$, i.e. we are in the hard case, which we already solved. Pairing $b_2, b_3, \ldots$ in the same way we get recursively the result (*why?*).

b) It turns out that $B = b_1 \cdot b_2 \cdot \ldots \cdot b_{\phi(m)} \equiv 1 \bmod m$, unless $m = 4, p^r$, or $2p^r$, where p is and odd prime and r is a positive integer, in which cases it is $\equiv -1 \bmod m$. This follows from an analysis similar to the proof of Wilson's theorem we discussed in class.

10.2 Notice that $\phi(7) = 6, \phi(7^2) = 42, \phi(7^3) = 294$, and $\phi(7^4) > 1000$ therefore $\gcd(7, m) = 1$ (*why?*). Now we can use Euler's formula: $7^{3003} \equiv 7^{3*\phi(m)+3} \equiv 7^3 \mod m$

10.3 a) We have the following three congruences:

$$a^{560} \equiv a^{2*280} \equiv 1 \mod 3$$
$$a^{560} \equiv a^{10*56} \equiv 1 \mod 11$$
$$a^{560} \equiv a^{16*35} \equiv 1 \mod 17$$

by the chinese remainder theorem $a^{560} \equiv 1 \mod 561$ (*why?*)

11.1 $\phi(97) = 96$, $\phi(8800) = \phi(2^5 \cdot 5^2 \cdot 11) = 3200$

11.2 If $m \geq 3$ then m has an odd prime factor p or it is a power of 2 with exponent greater than 1. In the first case, $m = p^s k$ with $s \geq 1$ and $\gcd(p, k) = 1$ Therefore $\phi(m) = \phi(p^s)\phi(k)$ but $\phi(p^s) = p^{s-1}(p-1)$ which is even. In the second case $m = 2^s$ with $s > 1$ therefore $\phi(m) = \phi(2^s) = 2^{s-1}$ which is even since $s > 1$

b) m should be of the form $2^s p^t$ where $s = 0, 1$ and p is an odd prime of the form $4n + 3$