Homework 27 Solutions

Problems

1. **A number b between 1 and $n-1$ is called a *witness* for the fact that n is composite if $b^{n-1} \not\equiv 1 \pmod{n}$. (remember: if n were prime, Fermat's little theorem would say that $b^{n-1} \equiv 1 \pmod{n}$. So n has to be composite if it has any witness).**

   (a) **Show that 3 fails to be a witness for 91 to be composite.**
   We compute (using doubling) that $3^{90} \equiv 1 \pmod{91}$, hence 3 is not a witness to the fact that 91 is composite.

   (b) **Show that 2 is a witness for 255 to be composite.**
   We compute (using doubling) that $2^{254} \equiv 64 \pmod{255}$ hence 2 is not a witness to the fact that 255 is composite.

2. **Find two witnesses to the fact that 121 is composite.**

   One might notice that $11^{120} \equiv 0 \pmod{121}$, though we only call w a witness if $\gcd(w, 121) = 1$.

   However, we can just try several small values:

$$2^{120} \equiv 56 \pmod{121},$$

$$3^{120} \equiv 1 \pmod{121},$$

$$5^{120} \equiv 78 \pmod{121}.$$

   So 2 and 5 (among many others) are witnesses to 121 being composite.