Homework 28 Solutions

1. **For each number in arithmetic** $\pmod{15}$**, compute its square.**

   We need only compute them up to 7, since $8 = -7$, $9 = -6$, and so on, and thus the table repeats itself in reverse order starting at 8. Doing so gives

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
x^2	0	1	4	9	1	10	6	4	4	6	10	1	9	4	1

   (a) **Which numbers are squares?**

   The numbers which are squares are precisely those that appear on the bottom line of the above chart. Hence the squares are $\boxed{0,\ 1,\ 4,\ 6,\ 9,\ \text{and } 10}$.

   (b) **How many square roots does each number have?**

   For each number from the last problem, we simply need to count how many times it appears in the bottom row of the chart. So 0 has one square root, 1 and 4 each have four square roots, and 6, 9, and 10 each have two square roots.

2. **Suppose you know that 341 is a pseudoprime to base 2; that is,** $2^{340} \equiv 1 \pmod{341}$ **(this is, in fact, true).**

   (a) **Compute** $2^{170} \pmod{341}$**. Hint: what is** $2^{10} \pmod{341}$**?**

   Taking the hint, we compute $2^{10} \equiv 1024 \equiv 1 \pmod{341}$. Thus

$$2^{170} \equiv \left(2^{10}\right)^{17} \equiv 1^{17} \equiv \boxed{1} \pmod{341}.$$

   (b) **Keeping in mind that** $2^{340} = \left(2^{170}\right)^2$**, what does this tell you about the primality of 341?**

   The previous part shows that $1^2 \equiv \pmod{341}$, which we know is consistent with 341 being prime. Thus, at this stage of the Miller-Rabin test, we can only conclude that $\boxed{\text{341 may or may not be prime.}}$

   (c) **Compute** $2^{85} \pmod{341}$**.**

   Using that $2^{10} \equiv 1 \pmod{341}$, we see that

$$2^{85} \equiv 2^5 \equiv \boxed{32} \pmod{341}.$$

   (d) **Keeping in mind that** $2^{170} = \left(2^{85}\right)^2$**, what does this tell you about the primality of 341?**

   The previous part shows that $32^2 \equiv 1 \pmod{341}$. Since 32 is not congruent to either 1 or $-1 \pmod{341}$, this proves that $\boxed{\text{341 is not prime.}}$

3. **On the last homework, we saw that** $3^{90} \equiv 1 \pmod{91}$**. Thus the Fermat test didn't unmask 91 as a composite. Starting from** $3^{90} \equiv 1 \pmod{91}$**, apply the Miller-Rabin test and report what it reveals about the primality of 91.**

   We wish to compute $3^{45} \pmod{91}$. Successive squaring gives

$$\begin{aligned} 3^2 &\equiv 9 \\ 3^4 &\equiv 81 \equiv -10 \\ 3^8 &\equiv 100 \equiv 9 \\ 3^{16} &\equiv -10 \\ 3^{32} &\equiv 9 \end{aligned}$$

where all of these congruences are taken $\pmod{91}$. Thus

$$3^{45} \equiv 3^{32} \cdot 3^8 \cdot 3^4 \cdot 3 \equiv 9 \cdot 9 \cdot -10 \cdot 3 \equiv -10 \cdot -10 \cdot 3 \equiv 9 \cdot 3 \equiv 27 \pmod{91}.$$

This shows that $27^2 \equiv 1 \pmod{91}$. Since 27 is not congruent to either 1 or $-1 \pmod{91}$, this proves that $\boxed{\text{91 is not prime.}}$