Homework 27 Solutions

1. **Eve listens in on a communication between Bob and Amanda. She knows that Bob transmitted to Amanda $n = 2047$, $k = 125$. Amanda responded with the number 2. What was Amanda's message? (Computational hint: $n = 2047$ is close to a power of 2. Use this to your advantage.)**

   One approach is to "crack the code" by factoring $n = 2047$ and then using our usual method to compute $2^{1/125} \pmod{2047}$ (recall that we decrypt by taking the k-th root of the encoded message $\pmod{n}$). However, the hint encourages us to try a simpler approach which circumvents the process of factoring 2047. In particular, we see that $2^{11} \equiv 2048 \equiv 1 \pmod{2047}$. If we think about how our usual method of taking roots works, we see that this equation makes a nice substitute for Euler's theorem. It's obvious that 11 and 125 are relatively prime, so we can solve $125x + 11y = 1$. Then we can write

   $$2^{125x} \equiv 2^{1-11y} \equiv 2 \pmod{2047},$$

   and taking the 125-th root of both sides gives $2^x \equiv 2^{1/125} \pmod{2047}$. (Those of you who have been paying close attention to the theory might object that, because we're not using the general procedure derived from Euler's theorem, there's no reason to believe that this answer should be unique. While it's true that simply trying to take roots using this sort of lucky coincidence is no guarantee of uniqueness, in this case we know that the answer will be unique because the problem comes from the RSA encryption scheme. That is, as Eve, we assume that Bob and Amanda are correctly using RSA, and thus that they've set things up so that decryption will be unique. Since we know in advance that there will be a unique solution, any method of finding it is fine.)

   At any rate, we want to solve $125x + 11y = 1$. The Euclidean algorithm gives

   $$\begin{aligned} 125 &= 11 \cdot 11 + 4 \\ 11 &= 2 \cdot 4 + 3 \\ 4 &= 3 + 1. \end{aligned}$$

   Running it backwards, we get

   $$\begin{aligned} 1 &= 4 - 3 \\ 1 &= 4 - (11 - 2 \cdot 4) = -11 + 3 \cdot 4 \\ 1 &= -11 + 3(125 - 11 \cdot 11) = 3 \cdot 125 - 34 \cdot 11. \end{aligned}$$

   Thus we can take $x = 3$ and $2^{1/125} \equiv 2^3 \equiv 8 \pmod{2047}$. So Amanda's message was $\boxed{8}$.

   As mentioned you, could chose to factor 2047 and go from there. It turns out that $2047 = 23 \cdot 89$ (both of which are prime), and thus $\phi(2047) = 22 \cdot 88 = 1936$. If you solve $125x + 1936y = 1$ using the Euclidean algorithm, you get $x = 1301,\ y = -84$. Thus $2^{1/125} \equiv 2^{1301} \pmod{2047}$. At this point, it saves a lot of work to realize that $2^{11} \equiv 1 \pmod{2047}$. Using this, we have

   $$2^{1301} \equiv \left(2^{11}\right)^{118} \cdot 2^3 \equiv \boxed{8} \pmod{2047}$$

   which, of course, agrees with our previous answer.

2. **A number b between 1 and $n-1$ is called a *witness* for the fact that n is composite, or simply a witness for n, if $b^{n-1} \not\equiv 1 \pmod{n}$. (As was discussed in today's lecture: 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.**
We wish to compute $3^{90} \pmod{91}$. Successive squaring gives

$$\begin{aligned} 3^2 &\equiv 9 \\ 3^4 &\equiv 81 \equiv -10 \\ 3^8 &\equiv 100 \equiv 9 \\ 3^{16} &\equiv -10 \\ 3^{32} &\equiv 9 \\ 3^{64} &\equiv -10, \end{aligned}$$

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

$$3^{90} \equiv 3^{64} \cdot 3^{16} \cdot 3^8 \cdot 3^2 \equiv -10 \cdot -10 \cdot 9 \cdot 9 \equiv 9 \cdot -10 \equiv -90 \equiv 1 \pmod{91}.$$

So $3^{90} \equiv 1 \pmod{91}$, and thus 3 is not a witness for 91.

(b) **Show that 2 is a witness for 255.**
We wish to compute $2^{254} \pmod{255}$. Successive squaring gives

$$\begin{aligned} 2^2 &\equiv 4 \\ 2^4 &\equiv 16 \\ 2^8 &\equiv 256 \equiv 1, \end{aligned}$$

where all of these congruences are taken $\pmod{255}$. Thus we have

$$2^{254} \equiv \left(2^8\right)^{31} \cdot 2^6 \equiv 64 \pmod{255}.$$

Since 64 is not congruent to 1 or $-1 \pmod{255}$, we see that 2 is a witness to the fact that 255 is composite.

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

We begin by trying 2 to see if it is a witness. Successive squaring gives

$$\begin{aligned} 2^2 &\equiv 4 \\ 2^4 &\equiv 16 \\ 2^8 &\equiv 256 \equiv 14 \\ 2^{16} &\equiv 196 \equiv 75 \equiv -46 \\ 2^{32} &\equiv 2116 \equiv 59 \\ 2^{64} &\equiv 3481 \equiv 93 \equiv -28, \end{aligned}$$

where all of these congruences are taken $\pmod{121}$. Thus we have

$$2^{120} \equiv 2^{64} \cdot 2^{32} \cdot 2^{16} \cdot 2^8 \equiv -28 \cdot 59 \cdot -46 \cdot 14 \equiv 56 \pmod{121}.$$

Thus 2 is a witness. Of course, we could have used the fact that $121 = 11^2$ to compute $\phi(121) = 110$. Then we could use Euler's theorem to see that

$$2^{120} \equiv 2^{10} \equiv 14 \cdot 4 \equiv 56 \pmod{121}.$$

We didn't do this because the point of primality testing is that you don't know whether the modulus is prime, so using its factorization in the computation isn't exactly in the spirit of things.

Next we can try 3. We have

$$\begin{aligned} 3^2 &\equiv 9 \\ 3^4 &\equiv 81 \equiv -40 \\ 3^8 &\equiv 1600 \equiv 27 \\ 3^{16} &\equiv 729 \equiv 3 \\ 3^{32} &\equiv 9 \\ 3^{64} &\equiv -40, \end{aligned}$$

where all of these congruences are taken $\pmod{121}$. Thus we have

$$3^{120} \equiv 3^{64} \cdot 3^{32} \cdot 3^{16} \cdot 3^8 \equiv -40 \cdot 9 \cdot 3 \cdot 27 \equiv -40 \cdot 27^2 \equiv -40 \cdot 3 \equiv 120 \equiv 1 \pmod{121}.$$

So 3 fails to be a witness.

If, as indicated above, we wish to do this problem as in the true spirit of primality testing, we should continue with the next prime, that is, with 5. We have

$$\begin{aligned} 5^2 &\equiv 25 \\ 5^4 &\equiv 625 \equiv 20 \\ 5^8 &\equiv 400 \equiv 37 \\ 5^{16} &\equiv 1369 \equiv 38 \\ 5^{32} &\equiv 1444 \equiv 113 \equiv -8 \\ 5^{64} &\equiv 64, \end{aligned}$$

where all of these congruences are taken $\pmod{121}$. Thus we have

$$5^{120} \equiv 5^{64} \cdot 5^{32} \cdot 5^{16} \cdot 5^8 \equiv 64 \cdot -8 \cdot 38 \cdot 37 \equiv -28 \cdot 75 \equiv 78 \pmod{121}.$$

Thus 5 is witness.

So we've found two witnesses simply by picking primes and using successive squaring. As mentioned above, if we wanted to make our lives easier, we could have taken advantage of some shortcuts. For example, once we found that $2^{120} \equiv 56 \pmod{121}$, we could have tried

$$4^{120} \equiv \left(2^2\right)^{120} \equiv \left(2^{120}\right)^2 \equiv 56^2 \equiv 111 \pmod{121}.$$

Thus 4 is also a witness. Alternatively, once we saw that $2^{120} \equiv 56 \pmod{121}$ and $3^{120} \equiv 1 \pmod{121}$, we find that

$$6^{120} \equiv 2^{120} \cdot 3^{120} \equiv 56 \cdot 1 \equiv 56 \pmod{121},$$

and thus 6 is a witness.

Finally, if we were annoyed at having to find witnesses for a number we already knew how to factor, we could use the factorization to solve the problem right away. In particular, $11^2 \equiv 121 \equiv 0 \pmod{121}$, which shows that $11^{120} \equiv 0 \pmod{121}$. So 11 is a witness. Similarly,

$$22^{120} \equiv 2^{120} \cdot 11^{120} \equiv 2^{120} \cdot 0 \equiv 0 \pmod{121},$$

so 22 is a witness. For that matter, the same idea shows that any multiple of 11 would work.