Math 580: Quiz 9

Show ALL Work Name **Solutions**

1. Do the following problem without using the Chinese Remainder Theorem or any ideas that even resemble the Chinese Remainder Theorem. Use some other important theorem from class that you should know the name of and say what the theorem is (either by name or, if you don't know the name, just state what the theorem is). Note that $1270 = 2 \cdot 5 \cdot 127$, where each of the three factors shown are primes. Find $x \in \{0, 1, \ldots 1269\}$ satisfying

$$2^{2019} \equiv x \pmod{1270}.$$

In other words, what is the remainder when 2^{2019} is divided by 1270? Justify your answer with appropriate work.

Answer: $\boxed{8}$

Solution. Since $\phi(5 \cdot 127) = 4 \cdot 126 = 504$, Euler's Theorem implies that $2^{504} \equiv 1$ modulo $5 \cdot 127$. Raising both sides to the fourth power, we get $2^{2016} \equiv 1 \pmod{5 \cdot 127}$. Multiplying both sides by 2^3, we obtain $2^{2019} \equiv 8 \pmod{5 \cdot 127}$. We want an integer x such $2^{2019} - x$ is divisible by $2 \cdot 5 \cdot 127$. We have shown $2^{2019} - 8$ is divisible by $5 \cdot 127$. Since $2^{2019} - 8$ is clearly even and, hence, divisible by 2, the answer is 8. ■

2. You should use the Chinese Remainder Theorem on this problem. You know (in theory) how to compute the inverse of 8 modulo 125, but your nice teacher has decided to tell you that $8 \cdot 47 \equiv 1 \pmod{125}$. What are the last three digits (the three right-most digits) of the number 2^{402}? Justify your answer with appropriate work and put all three digits in the correct order as they appear from left to right. At the end, you will have to do a little arithmetic.

Answer: $\boxed{504}$

Solution. We want to work modulo $1000 = 2^3 \cdot 5^3$. Since $\phi(5^3) = 5^2 \cdot 4 = 100$, we get $2^{402} \equiv (2^{100})^4 2^2 \equiv 4 \pmod{125}$. Also, $2^{402} \equiv 0 \pmod{8}$. So we want to solve $x \equiv 4 \pmod{125}$ and $x \equiv 0 \pmod{8}$. The solutions are given by

$$x \equiv 4 \cdot 8 \cdot 47 + 0 \cdot (\text{something}) \equiv 1504 \equiv 504 \pmod{1000}.$$

So the answer is 504. ■