Modular Arithmetic Questions

|  |
| --- |
| How do these these aritmatic based functions improve code/data security? |
| **If we were in a different mod, the 2^k mod 3 ting would change as well, correct? Is there some simple way to tell what the number replacing the three would be aside from pattern recognition?** |
| **Do all mods result in a pattern?** |
| Very familiar with modular arithmetic. Since RSA uses modular arithmetic, does it use a single modulus? How would the modulus(es?) be determined? |
| Is it possible to find the staring position by reversing the formula? |
| is the equation always have a 2 in the ones place or does that change per question as the exponent place does? |
| What did you mean by "the world of mod 7". Did this just mean when you have a circle with 7 people in it? |
| i understand the concept of modular arithmetic, but am wondering how this will help make our lives easier? |
| **Is each of the 'kids' in the circle actually a device/computer in our example? A packet is sent through multiple devices and may or may not end up in the same place it started?** |
| **How does this proccess work for other numbers? Why does knowing that there is a cycle for 2^k help us with RSA?** |
| Are there **other applications of mods used in network protocols, outside of encryption?** |
| Does the 2^(k \* mod(n)) work for different values of k? |
| why mod7? and can we go over/go more in depth about step forward and back with different colors in class? |
| **the 2^kmod3 was a bit confusing I didn't understand how you are counting skips** |
| Why are we using 2 as the base for the power? |
| Everything was clear, but how exactly does modulus relate to RSA? |
| ***Mod7 was 6 = -1 in a previous slide and later in the example it was equal to 1, why is that?*** |
| What would more advanced applications of this look like? |
| ***I was not sure how did you 3=6 in terms of the circle. Any suggestions?*** |
| when you did the 2^n does it repeat every 3 digits up until infinity? |
| What is an applicable use for this topic? |
| How would you find k so that it is not the same every time? |
| No questions. I guess I'm just more interested now how this will factor into RSA. |