Homework 1

This problem set is due January 23rd.

Problem 0 Download Sage and install it on your computer. Use it to factor a 30 digit number.

Problem 1 Prove that if a and b are integers, then $(a+b)^p \equiv a^p + b^p \pmod{p}$.

Problem 2 Prove that an integer is divisible by 3 iff the sum of its decimal digits is. Formulate and prove a similar rule for divisibility by 11.

Problem 3 The British postal system at one time was notoriously corrupt. Any letter, package or box that was open or easily openable would be opened in the sorting office and anything inside would be removed whether or not it had any value. However, since the pickings were so rich, the sorters never bothered to open anything that was locked, even if they suspected it held something of great value.

Now Jack in London had bought a beautiful gem for his girlfriend Natasha, who lived in Bristol, and he wanted to get it to her as quickly as possible. Neither he nor Natasha could travel to the other place, so what was he to do? He had a strongbox with a hasp to which a number of padlocks could be attached. If he bought a padlock and key, he could put the gem in the box, lock the padlock and send the box through the postal system knowing that it would be safe but then Natasha wouldn't be able to open it. He couldn't send the key by letter because it would be opened. Jack called Natasha on the phone and together they came up with a great plan. What did they do?

Now, do this mathematically for a message K encoded as a number. Natasha publishes a large prime $p >> K$and Jack downloads it. They do the following

- Natasha selects a random number a with $gcd(a, p-1) = 1$. and Jack randomly selects a b so that $gcd(b, p-1) = 1$.
- Natasha sends $K_1 \equiv K^a \pmod{p}$ to Jack.
- Jack sends $K_2 \equiv K_1^b \pmod{p}$ to Natasha.
- Natasha sends $K_3 \equiv K_2^{a^{-1}} \pmod{p}$ to Jack.
- Jack computes $K_4 \equiv K_3^{b^{-1}} \pmod{p}$.

Show that $K_4 = K$. You might prove the following lemma along the way:

Lemma 0.1. *Let a, n, x, y be integers with $n \geq 1$, $gcd(a, n) = 1$. If $x \equiv y \pmod{\phi(n)}$, then $a^x \equiv a^y \pmod{n}$.*

Problem 4 Using CRT, prove that the ϕ function is multiplicative; i.e., if $gcd(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$. Find and prove a formula for $\phi(n)$ in terms of the prime factorization of n. Finally, for what values of n is $\phi(n)$ odd? Solve for x in $\phi(x) = 24$.

Problem 5 Find the last three digits of 7^{803}.

Problem 6 Use Wilson's Theorem to prove that -1 is square mod a prime p if $p \equiv 1 \pmod{4}$.

Problem 7 Make a conjecture as to when $(n-1)! \equiv 0 \pmod{n}$. Prove your conjecture.

Problem 8 Seven competitive math students try to share a huge hoard of stolen math books equally between themselves. Unfortunately, six books are left over, and in the fight over them, one math student is expelled. The remaining six math students, still unable to share the math books equally since two are left over, again fight, and another is expelled. When the remaining five share the books, one book is left over, and it is only after yet another math student is expelled that an equal sharing is possible. What is the minimum number of books that allows this to happen?

Problem 9 Here's how to construct the x guaranteed by the generalized CRT. Suppose $m_1, \ldots, m_k$ are integers with $gcd(m_i, m_j) = 1$ whenever $i \neq j$. Perform the following procedure:

- For $i = 1, \ldots, k$, let $z_i = m_1 m_2 \cdots m_{i-1} m_{i+1} \cdots m_k$

- Let $i = 1, \ldots, k$ and let $y_i \equiv z_i^{-1} \pmod{m_i}$
- Let $z = a_1 y_1 z_1 + \cdots + a_k y_k z_k$

Show $x \equiv a_i \pmod{m_i}$ for all i.

Problem 10 Find all positive integers n such that the set $\{n, n+1, n+2, n+3, n+4, n+5\}$ can be partitioned into two subsets so that the product of the numbers in each subset is equal.

Problem 11 How long did it take you to do this assignment? Did you use any of the books on reserve? Any other online resources? Was lecture useful for completing this assignment?