

Due: February 21, 2008

1 Lists of exponents

Take any a, b in \mathbb{Z}_n^* (remember this means that a and b are coprime to n). Consider the set:

$$S_a = \{1, a, a^2, a^3, \dots\}$$

(This is just the set containing all powers of a modulo n that we saw in lecture.)

Now, let's create a second set by multiplying the first set by b :

$$S_b = \{b, ba, ba^2, ba^3, \dots\}$$

1.1 Case 1 (20 points)

Prove that if b is an element of S_a , then $S_a = S_b$. (Hint: Remember from lecture that powers of a must loop after at most $(n - 1)$ steps.)

1.2 Case 2 (20 points)

Prove that if b is not an element of S_a , then S_a and S_b have no elements in common. (Hint: If there is some element in common, you should be able to work backwards to show that b is in S_a after all, giving a contradiction.)

1.3 Common factors (10 points)

Why is it important that we started with a coprime to n ? Which step in your proofs from this problem breaks without that assumption? (You don't need to prove anything for this part, just explain why.)

2 Extended Euclid (25 points)

Find x and y such that $6883x + 808y = 1$. Show your work, but feel free to use shorthand, and don't prove anything.

3 Broken Chinese Remainder (25 points)

John Smith is a bad student. He tried to use Chinese Remainder form modulo the values $a = 12, b = 14$, even though he knows perfectly well that we only proved the Chinese Remainder Theorem for coprime values. Show him the error of his ways by giving a pair of values that have the same Chinese Remainders even though they aren't the same modulo $12 \times 14 = 168$.

4 Fixed Chinese Remainder (20 points extra credit)

In the last problem, show that John's representation does uniquely determine the value of a number mod $168/2 = 84$: Start by showing that we can determine the value of a number mod 7 from its value mod 14, then apply the Chinese Remainder Theorem.