Arithmetic Algorithms 2014: HW3

Taylor Lee

March 26, 2014

Problem 1

Part A:

Euler

Part B:

I believe he could. If he knew how to represent $F_5/641$ in binary form, then he could see that, many of the bits in the less significant end of the representation were already back to zero.

Part C:

Since their are 10 different ways to multiply a number by a single-digit number, if each multiple occurs uniformily, then we can estimate the expected number of times we expected to record a randomly occuring multiple before having them all. We have compensated our estimate for the chances that we catch.

$$1 + 10/9 + 10/8 + 10/7 + 10/6 + 10/5 + 10/4 + 10/3 + 10/2 + 10 = 29.2896825396825$$

In a sense, however, this is not an accurate prediction of the expected number of multiples we will have to generate before cataloging all ten multiples of d. If we were to select 2 through 9 before 0 and 1, then we would have acheived our goal, because the results of multiplying these two numbers to our divisor d is trivial. Since there are 10 choose 8 ways of selecting the first 8 numbers, and sense only one of these 45 leaves both 0 and 1 until the end, we can make a small correction to our second to last term,

as there is a $1/45$ chance we will not have to attempt it. Likewise, with our final term, if we happen to have selected all but one of our two trivial multiples in the prior iterations, then we can skip this final step as well. Since this is also subject to the early-abort scenario of the second to last term, we will also include $44/45$ in this term, to compliment the $4/5$ correction for arriving the end with only a trivial multiple outstanding. Hence, our expected number of iterations prior to recording all single digit multiples of d is:

$$1+10/9+10/8+10/7+10/6+10/5+10/4+10/3+(10/2)*(44/45)+10*(44/45)*(8/10) = 27.00079365079365$$

Problem 2

Part A:

Since we know that we are operating over the Ring of integers $\mathbb{Z}/p^k\mathbb{Z}$, we know that the multiplicative Group of this Ring, $\left(\mathbb{Z}/p^k\mathbb{Z}\right)*$, is isomorphic to $\mathbb{Z}/p^{k-1}\mathbb{Z} \times \mathbb{Z}/p-1/zz$. Hence, for any $a \in \left(\mathbb{Z}/p^k\mathbb{Z}\right)*$, we know the order of a must divide either p^{k-1} or $p-1$, if not both.

Now, by squaring both sides of the given congruence, we can quickly see the size of $L(p^k)$.

$$a^{(p^k-1)/2} \equiv \pm 1 \pmod{p^k} \Rightarrow a^{(p^k-1)} \equiv 1 \pmod{p^k}.$$

Hence, if a is to be counted in $L(p^k)$, then not only must it be invertible, but it's order must divide p^k-1. Now, we can see that

$$(p-1)*(p^{k-1}+p^{k-2}+\ldots+p+1) = p^k-1$$

So a can divide $(p-1)$. But since $p^{k-1} \nmid p^{k-1}+p^{k-2}+\ldots+p+1$, a must divide $(p-1)$ and $(p-1)$ alone. Since there are $p-1$ elements of this type, which satisfy both our congruence condition and our requirements for element order, we can see that $|L(p^k)| = p-1$.

Part B: