MATH 314 - Class Notes

9/26/2017

Scribe: Darian Hegberg

Summary: We recapped Eulers Theorem worked examples and moved to understanding what rings and fields are in addition to examples regarding fields.

Notes: Include detailed notes from the lecture or class activities.

1. Eulers function: $\varphi = n * \prod_{p|n}(\frac{p-1}{p})$
2. Eulers cont. If the GCD(a,n) = 1, then $a^{\varphi(n)} \equiv 1(modn)$
3. Basic principle of exponential arithmetic mod n, If the GCD(a,n) = 1 and $x \equiv y(mod\varphi(n))$, then $a^x \equiv a^y(modn)$
4. When we work (mod n) we can think of the residues as a ring. (We can add,subtract,multiply). In the case that we have a ring where everything is invertible except 0, we have a field.
5. Theorem: For any integer n there is at most one field with exactly n elements in it. $(Field_4)$
6. We call a polynomial irreducible if the only polynomials that evenly divide it are 1 and itself.
7. If p(x) is an irreducible polynomial then the set of polynomials in $(Field_2[x])$ mod p(x) form a field

Examples: If including plaintext or ciphertext or other data it is often helpful to write them using `typewriter text`.

1. Eulers Example 1.
   - Example: Compute last 3 digits of 3^{80403} What is $3^{80403}(mod1000)$?
   - Use Eulers Thrm: Need $\varphi(1000)$ The only primes that divide 1000 are 2 and 5
   - $\varphi(1000) = 1000\prod_{p|1000}(\frac{p-1}{p}) = 1000(\frac{1}{2})(\frac{4}{5}) = 400$
   - Since $80403 \equiv 3(mod1000), 3^{80403} \equiv 3^3(mod1000) \equiv 27(mod1000)$
   - Last 3 digits are (0, 2, 7)
2. What is $(Field_4)$? Look at the ring $Field_2[x]$ This is the set of all polynomials with coefficients in $Field_2$.
   - How do we do arithmetic in $Field_2[x]$?
     - Arithmetic is the same as usual with polynomials except we reduce all the coefficients modulo 2 at the end.
   - $f(x) = x^3 + 0x^2 + x + 1 = x^3 + x + 1$
   - $g(x) = x^2 + x + 0 = x^2 + x$
     - f(x) + g(x) The x's cancel, to get $x^3 + x^2 + 0x + 1$

- f(x) * g(x)
  - $(x^3 + x + 1)(x^2 + x) = x^5 + x^4 + x^3 + 0x^2 + x$

3. How can we divide one polynomial into another with a remainder? Long division with remainder still works for polynomial divide f(x) by g(x) and find the remainder.

- $\frac{x^3+0x^2+x+1}{x^2+x} = x^3 + x + 1 \equiv 1(mod(x^2 + x))$
- Claim $p(x) = x^2 + x + 1$ is irreducible in $(Field_2[x])$
  - The only option for smaller polynomials are f(x) = x and g(x) = x + 1
  - Note: $f(x)f(x) = x*x = x^2, f(x)*g(x) = x^2+x, g(x)*g(x) = x^2+1$ Is Irreducible
- So the polynomials mod x^2+x+1 form a field, What are the possible remainders when dividing $x^2 + x + 1$.

4. This is $(Field_4)$

+	0	1	x	x+1
0	0	1	x	x+1
1	1	0	x+1	x
x	x	x+1	0	1
x+1	x+1	x	1	0

*	0	1	x	x+1
0	0	0	0	0
1	0	1	x	x+1
x	0	x	x+1	1
x+1	0	x+1	1	x