Class Notes: 9/26:
Number Theory (Continued)

Alex Poniatowski

September 30, 2018

Fields (Continued from last class):

- Integers $\mathbb{Z}$: don't form a field but instead make up a **ring**
  - a **ring** is similar to a field except that you can't always divide in rings
  - by extension, every **ring** is a field
  - Other examples of **rings** include:
    - Square Matrices
    - Polynomials

- Define $\mathbb{F}_2$ [x] the ring of polynomials with coefficients that are 0 and 1; using (mod 2) arithmetic
  - Ex.:
    - $f(x) = x^2 + x + 1$
    - $g(x) = x^3 + x$
    - $f(x) + g(x) = x^3 + x^2 + 0 + 1 = x^3 + x^2 + 1$
  - In $\mathbb{F}_2$ [x], addition and subtraction are the same operation
    - $f(x) + g(x) = f(x) - g(x)$
    - $f(x) + f(x) = 0$
    - $f(x)g(x) = (x^2 + x + 1)(x^3 + x) = x^5 + x^3 + x^4 + x^2 + x^3 + x = x^5 + x^4 + x^2 + x$
  - We can add, subtract and multiply polynomials in $\mathbb{F}_2$[x], but usually we can't divide
  - We can however, perform division with remainders
    - Ex.: divide $g(x)$ into $f(x)$ and find remainder
      $x^3 + 0x + x + 0/x^2 + x + 1 = x + 1$ with remainder $x + 1$

- If a polynomial of degree at least two doesn't have any factors of a degree smaller than itself, we say it is an **irreducible polynomial**
  - Ex.: say $F(x)$ is **irreducible** in $\mathbb{F}_2$[x] and has degree d.
    How many possibilities in $\mathbb{F}_2$[x] have smaller degrees?
    - $C_0 x^{d-1} + C_1 x^{d-2} ... C(d)^1$
  - So 2^d possibilities, resulting in the field $\mathbb{F}_2$[d]
  - Let's find $\mathbb{F}_4 = \mathbb{F}_2^2$; we need an **irreducible polynomial** of degree 2
    - Claim: $p(x) = x^2 + x + 1$ is irreducible
    - So what polynomials have a smaller degree?
      - $(x+0)$ and $(x+1)$ Verify that $p(x)$ is irreducible by dividing these into $p(x)$. If there are remainders then it is irreducible.

+	**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	0

  - Ex.: $\mathbb{F}_4 = x, 1, x+1, 0$; nothing with degree greater than 2; using mod $(x^2 + x + 1)$ (see tables above)
  - Everything in tables have inverses
    - $x(x+1) \equiv 1 (mod x^2 + x + 1)$
    - $x^{-1} \equiv (x+1)(mod x^2 + x + 1)$
    - $(x+1)^{-1} \equiv x(mod x^2 + x + 1)$
- If $a^m (modp)$ produces all of the residues (mod p) for different values of m, then a is called a **primitive root**
  - If a is a **primitive root**, then $a^k \equiv 1$ where $k < p - 1$
- When does $x^2 \equiv b(modp)$ have a solution?
  - If it has a solution, it is called a **quadratic residue**