More Congruence mod p

September 20, 2012

1 Reading and Homework for Thursday September 27

1. Read pages 188, 189
2. Do Exercises 6,7,10, 15 and 17-21 on page 37
3. Do Exercises 1,2 on page 76

2 Quadratic equations

2.1 Quadratic polynomials in the field $\mathbf{Z}/p\mathbf{Z} = \mathbf{F}_p$

$$(**)_p \qquad AX^2 \ + \ BX \ + \ C \ \equiv \ 0 \text{ mod p.}$$

Discuss the "moral" of the quadratic formula: reduction to finding *square roots*. Except when $p = 2$.

3 Square roots

Discuss extraction of square roots. Examples. $X^2 - 1 = (X-1)(X+1)$ has only two roots. So ± 1 are the only two congruence classes that are *equal* to their own inverses.

Question: Let $\bar{a} = a + p\mathbf{Z}$ be a congruence class modulo the prime p. How many "square roots" might $\bar{a} \in \mathbf{F}_p$ have?

Answer: $0, 1$, or 2. That's all the possible answers, and $0 \in \mathbf{F}_p$ is the only element that has only one square root. Discuss this!

Now let $p > 2$. So

$$|\mathbf{F}_p^*| = p - 1$$

subsectionA "multiplication table."

- *First naively:* Vocabulary: **residues, nonresidues**. Convention: a **residue** is a *nonzero* residue; i.e., a square in $\mathbf{F}_p^*$.

  A product of residues is again a residue; a product of a residue and a nonresidue is a nonresidue. (It is also true that a product of two nonresidues is a *residue* but that we'll see in a few moments:

  Note that

  $$|\mathbf{F}_p^*| = |\text{Res}| + |\text{Nonres}| = p - 1.$$

  and since every residue r is the square of exactly two elements $\pm\alpha \in \mathbf{F}_p^*$, we have

  $$|\text{Res}| = \frac{p-1}{2},$$

  and therefore

  $$|\text{Nonres}| = \frac{p-1}{2}.$$

  Corollary 1 *Fix $u \in$ Nonres $\subset \mathbf{F}_p^*$ a nonresidue, any one. Then any nonresidue v is (uniquely) expressible as*

  $$v = u \cdot r$$

  where r is a residue.

  Corollary 2 *The product of two nonresidues is a residue.*

- *Then give a group-theoretic description:*

  Think of the kernel and image of the squaring map (which is a homomorphism of groups):

  $$\mathbf{F}_p^* \quad \stackrel{\text{square}}{\longrightarrow} \quad \mathbf{F}_p^*.$$

  The kernel consists in the square roots of 1; that is, the subgroup

  $$\{\pm 1\} \subset \mathbf{F}_p^*.$$

  The subgroup of residues in $\mathbf{F}_p^*$ is the image of this homomorphism so is of index two in $\mathbf{F}_p^*$. It follows that the subset of nonresidues is simple *the* nontrivial coset of this subgroup of residues; i.e.:

  $$\text{Nonres} = u \cdot \text{Res}$$

  for any choice of u a nonresidue.

  This re-says Corollaries 1 and 2.

3.1 The Legendre symbol

Two definitions!

4 Wilson's Theorem

Proposition 1 Wilson's theorem *Let p be prime. Then $(p-1)! \equiv -1$ modulo p*

Corollary 3 *Let p be a prime that is congruent to 1 mod 4. Then $(\frac{p-1}{2})!$ (modulo p) is a root of the polynomial X^2+1. That is, it represents a "square root of minus one" in the field $\mathbf{F}_p$.*