CLASS 27, GIVEN ON 11/22/2010, FOR MATH 25

1. Quadratic residues mod p^e

At this point we have a fairly good understanding of quadratic residues mod primes p. We now use earlier ideas from this class to extend this to knowledge of quadratic residues mod prime powers p^e, and then finally to general integers n. Keep in mind that we only call a a quadratic residue/non-residue mod n if $\gcd(a, n) = 1$.

When considering prime powers p^e, we consider the cases $p = 2$ and p odd separately. When p is odd a routine application of Hensel's Lemma proves the following proposition:

Proposition 1. *Let p be an odd prime and let $\gcd(a, p) = 1$. Then a is a quadratic residue mod p^e if and only if a is a quadratic residue mod p.*

Proof. If a is a quadratic residue mod p^e, it must also be a quadratic residue mod p, because if $x^2 \equiv a \mod p^e$ has a solution, then $x^2 \equiv a \mod p$ also has a solution.

Conversely, suppose a is a quadratic residue mod p. Let x_1 be an integer such that $x_1^2 \equiv a \mod p$. Apply Hensel's Lemma to the polynomial $f(x) = x^2 - a$. We know that $f'(x) = 2x$, and because $\gcd(x_1, p) = 1$ (because $\gcd(a, p) = 1$ and $p > 2$), this means that $p \nmid f'(x_1)$. Therefore there is some $x_2 \equiv x_1 \mod p$ such that $x_2^2 \equiv a \mod p^2$; repeatedly applying Hensel's Lemma shows that there is some x_k such that $x_k^2 \equiv a \mod p^k$ for all k; therefore a is a quadratic residue mod p^e. □

Because the derivative of $x^2 - a$ is $2x$, we needed to know that $p > 2$ to apply Hensel's Lemma in the previous proof. When the modulus is a power of 2, we can determine whether an odd integer is a quadratic residue using the following straightforward test:

Proposition 2. *Let a be an odd integer, and let $e \geq 3$. Then a is a quadratic residue mod 2^e if and only if $a \equiv 1 \mod 8$.*

Proof. The proof of this proposition is an application of the fact we proved earlier that every element of U_{2^e} can be represented in the form $\pm 5^i$, for some integer i satisfying $1 \leq i \leq 2^{e-2}$. First, this tells us that given any odd x, we can find i such that $x \equiv \pm 5^i \mod 2^e$. Then $x^2 \equiv 5^{2i} \equiv 25^i \mod 2^e$. In particular, if we consider $25^i \mod 8$, since $25 \equiv 1 \mod 8$, this tells us that $x^2 \equiv 1 \mod 8$. Therefore any odd a which is a quadratic residue mod 2^e must satisfy $a \equiv 1 \mod 8$.

Conversely, suppose $a \equiv 1 \mod 8$. We will show that a is a quadratic residue by showing that the number of elements of U_{2^e} represented by numbers $\equiv 1 \mod 8$ is equal to the number of quadratic residues of U_{2^e}; more specifically, we show that both of these sets have 2^{e-3} elements in them. Since we already know that every quadratic residue of U_{2^e} is $\equiv 1 \mod 8$, if these sets have the same size they must be equal.

Obviously the number of elements of U^{2^e} congruent to 1 mod 8 is 1/4 of the elements of U^{2^e}, since elements in U^{2^e} are represented by odd numbers and the numbers congruent to 1 mod 8 are a quarter of all odd numbers, so that there are 2^{e-3} elements of U^{2^e} congruent to 1 mod 8. On the other hand, we claim that the numbers $5^{2i} \mod 2^e$, where $1 \leq i \leq 2^{e-3}$ are the quadratic residues of U_{2^e}. We already saw that every quadratic residue has the form $5^{2i} \mod 2^e$, and conversely every 5^{2i} is obviously a quadratic residue, being the square of 5^i. There are 2^{e-3} such classes mod 2^e, because there are 2^{e-3} choices of i, and distinct choices yield distinct classes mod 2^{e-3} because the numbers $\pm 5^i, 1 \leq i \leq 2^{e-2}$, are all distinct mod 2^e. This proves the proposition.

An proof in slightly different language can also be given using group theory. We know that $U_{2^e} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{e-2}\mathbb{Z}$, and the set of squares in U_{2^e} corresponds to the set of elements of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{e-2}\mathbb{Z}$ which are in the image of the multiplication by 2 map. Let $[2]G$ be the image of the multiplication by 2 map in the group G; for instance, $[2]\mathbb{Z}/4\mathbb{Z} = \{0 \mod 4, 2 \mod 4\}$. Then one can show that $[2](G_1 \times G_2) = [2]G_1 \times [2]G_2$. In our case, $[2]\mathbb{Z}/2\mathbb{Z} = \{0 \mod 2\}$, and $[2]\mathbb{Z}/2^{e-2}\mathbb{Z} = \{2k \mod 2^{e-2} | k \in \mathbb{Z}\}$, which have size $1, 2^{e-3}$, respectively. Therefore there are 2^{e-3} quadratic residues in U_{2^e}. □

Example. Determine whether 37 is a quadratic residue mod 125 or not. The first proposition tells us that 37 is a quadratic residue mod 125 if and only if 37 is a quadratic residue mod 5, and $\left(\frac{37}{5}\right) = \left(\frac{2}{5}\right) = -1$, so 37 is a quadratic non-residue mod 125.

2. Quadratic residues mod n

We are now in a position to consider the general case of quadratic residues mod n. The following proposition is the key idea:

Proposition 3. *Let $n = p_1^{e_1} \dots p_r^{e_r}$ be the prime factorization of n, and let p^e be any of the prime powers in this factorization. Then a is a quadratic residue mod n if and only if it is a quadratic residue mod each of the p^e.*

Proof. Suppose a is a quadratic residue, so that $x^2 \equiv a \mod n$ has a solution. Since $p^e \mid n$, each of the congruences $x^2 \equiv a \mod p^e$ also have solutions, and $\gcd(a, p^e) = 1$ as well, so a is a quadratic residue mod p^e.

Conversely suppose $\gcd(a, p^e) = 1$ for all p^e, and $x^2 \equiv a \mod p^e$ has a solution, say x_p. Then $\gcd(a, n) = 1$, and we can obtain a solution to $x^2 \equiv a \mod n$ by using the Chinese Remainder Theorem on all the x_p; that is, if $x \equiv x_p \mod p^e$ for all p^e, then $x^2 \equiv x_p^2 \equiv a \mod p^e$ for all p^e, and this implies that $x^2 \equiv a \mod n$, as desired. □

Example. Determine whether 27 and 39 are quadratic residues mod 70 or not. First, we check that $\gcd(27, 70), \gcd(39, 70) = 1$, and that $70 = 2 \cdot 5 \cdot 7$. Next, notice that $27 \equiv 2 \mod 5$, and $\left(\frac{2}{5}\right) = -1$, so that 27 is not a quadratic residue mod 5, and hence not a residue mod 70. On the other hand, $\left(\frac{39}{2}\right) = \left(\frac{1}{2}\right) = 1, \left(\frac{39}{5}\right) = \left(\frac{4}{5}\right) = 1, \left(\frac{39}{7}\right) = \left(\frac{4}{7}\right) = 1$, so 39 is a quadratic residue mod 70.

The method of proof in the previous proposition actually shows a little bit more than what we proved there:

Corollary 1. *Let $n = p_1^{e_1} \dots p_r^{e_r}$ be the prime factorization of n. Then*

$$Q_n \simeq Q_{p_1^{e_1}} \times \dots \times Q_{p_r^{e_r}}.$$

Proof. One checks that the map $x \mod n \mapsto (x \mod p_1^{e_1}, \dots, x \mod p_r^{e_r})$ when restricted to quadratic residues mod n maps to an element whose coordinates are all quadratic residues mod p^e, and that this map is a bijection between Q_n and $Q_{p_1^{e_1}} \times \dots \times Q_{p_r^{e_r}}$. □