Dr. Z.'s Number Theory Lecture 20 Handout:
Quadratic residues and the law of Quadratic Reciprocity

By Doron Zeilberger

Important Definition: a is a **quadratic residue** mod n is there is an integer x, $0 \leq x < n$ such that

$$x^2 \equiv a \pmod{n} \quad .$$

Otherwise it is a **quadratic non-residue**.

Note: every congruence class between 0 and $n-1$ (inclusive) is either a quadratic residue or a quadratic non-reside.

Note: 0 is trivially a quadratic residue, since $0^2 = 0$.

How to find the set of quadratic residues modulo an integer?

Simple! Just compute the set

$$\{x^2 \pmod{n} \,|\, 0 \leq x \leq n-1\}$$

But, since $(-x)^2 = x^2$, you only need to compute

$$\{x^2 \pmod{n} \,|\, 0 \leq x \leq (n-1)/2\}$$

The set of quadratic non-residues is the complement

$$\{x \,|\, 0 \leq x \leq n-1\} \backslash \{x^2 \pmod{n} \,|\, 0 \leq x \leq (n-1)/2\}$$

Problem 20.1: Find the set of quadratic residues of $n = 13$. Also find the set of non-quadratic residues.

Solution to 20.1:

$$QuadraticResiduesMod(13) = \{0^2, 1^2, 2^2, 3^2, 4^2, 5^2, 6^2\} \pmod{13}$$

$$= \{0, 1, 4, 9, 16, 25, 36\} \pmod{13}$$

$$= \{0, 1, 4, 9, 3, 12, 10\} = \{0, 1, 3, 4, 9, 10, 12\} \quad .$$

The set of non-quadratic residues is the complement

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, \} \backslash \{0, 1, 3, 4, 9, 10, 12\} = \{2, 5, 6, 7, 8, 11\} \quad .$$

Ans. to 20.1: The set of quadratic residues modulo 13 is $\{0, 1, 3, 4, 9, 10, 12\}$. The set of quadratic non-residues modulo 13 is $\{2, 5, 6, 7, 8, 11\}$.

Simple but important fact: If p is an odd prime, except for 0, there are as many quadratic residues as quadratic non-residues.

Proof: If $0 < x, y \leq (p-1)/2$, and $x^2 \equiv y^2 \pmod{p}$ then $x^2 - y^2$ is divisible by p. So $(x-y)(x+y)$ must be divisible by p. But $0 < x + y < p$ so $x - y = 0$, so $x = y$, and the $(p-1)/2$ elements

$$1^2 \quad , \quad 2^2 \quad , \quad \ldots \quad , ((p-1)/2)^2$$

are all different. Hence the set

$$\{x^2 \pmod{n} \,|\, 0 \leq x \leq (n-1)/2\}$$

has $(p-1)/2$ elements, and the complemnet has $(p-1) - (p-1)/2 = (p-1)/2$ elements.

Important Notation:

$a\,R\,n$ means that a is a quadratic residue modulo n.

$a\,N\,n$ means that a is **not** a quadratic residue modulo n.

Important Notation (The **Legendre symbol**) .

$$\left(\frac{a}{p}\right) := \begin{cases} 0, & \text{if } a = 0\ ; \\ 1, & \text{if } a\,R\,p\ ; \\ -1, & \text{if } a\,N\,p. \end{cases}$$

If p is very big, and we want to find out whether a certain r, between 1 and $p-1$, is a quadratic residue, of course we can try out all the first $(p-1)/2$ possibilities, but this will take a very long time. Since we know, from Lecture 9 how to to exponentiate (modulo p) very fast, here is a much better way.

Important Test: r is a quadratic residue mod an odd prime iff $r^{(p-1)/2} \equiv 1 \pmod{p}$.

Problem 20.2: Using the important test (no credit for brute force!) find $\left(\frac{5}{17}\right)$.

Sol. of 20.2: Here $r = 5$ and $p = 17$, $(p-1)/2 = 8$. We need

$$5^8 \; mod \; 17 \quad .$$

$$5^2 \equiv 8 \pmod{17} \quad .$$

$$5^4 \equiv 8^2 \pmod{17} \equiv -4 \pmod{17}$$

(since the reaminder of dividing 64 by 17 is 13 and it is more convenient to write it as -4)

$$5^8 \equiv (-4)^2 \pmod{17} \equiv 16 \pmod{17} \equiv -1 \pmod{17} \quad .$$

Since we got -1 (BTW, you **always** get either 1 or -1 , if $r \neq 0$), it is not **not** a quadratic residue.

Ans. to 20.2: $\left(\frac{5}{17}\right) = -1$.

But there is an even quicker way, using some **rules**.

Rule 1: If p is an odd prime and a and b are not multiples of p, then

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$$

Rule 2: If p is an odd prime then

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} \quad .$$

Rule 3: If p is an odd prime then

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} \quad .$$

FINALLY,One of the **MOST FAMOUS** results in Number theory

Rule 4: (**THE QUADRATIC-RECIPROCITY LAW**)

If p and q are distinct odd primes, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} \quad .$$

Problem 20.3: Using the Qudadratic Reciprocity Law (no credit for other methods) and Rules 1-3, find

$$\left(\frac{13}{101}\right)$$

Sol. to 20.3: By QRL

$$\left(\frac{13}{101}\right)\left(\frac{101}{13}\right) = (-1)^{(13-1)(101-1)/4} = 1 \quad .$$

So

$$\left(\frac{13}{101}\right) = \left(\frac{101}{13}\right)$$

But 101 *mod* 13 = 10, so

$$\left(\frac{13}{101}\right) = \left(\frac{10}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{5}{13}\right) \quad .$$

By Rule 3,

$$\left(\frac{2}{13}\right) = (-1)^{(13^2-1)/8} = (-1)^{168)/8} = (-1)^{21} = -1 \quad .$$

Using the QRL once again

$$\left(\frac{5}{13}\right)\left(\frac{13}{5}\right) = (-1)^{(13-1)(5-1)/4} = 1 \quad .$$

So

$$\left(\frac{5}{13}\right) = \left(\frac{13}{5}\right) = \left(\frac{3}{5}\right) \quad .$$

Using QRL one more time:

$$\left(\frac{3}{5}\right)\left(\frac{5}{3}\right) = (-1)^{(3-1)(5-1)/4} = 1 \quad .$$

So

$$\left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) \quad .$$

Now we use Rule 3:

$$\left(\frac{2}{3}\right) = (-1)^{(3^2-1)/8} = -1 \quad .$$

Going **back** we have

$$\left(\frac{3}{5}\right) = -1$$

$$\left(\frac{5}{13}\right) = -1$$

and finally,

$$\left(\frac{13}{101}\right) = (-1)(-1) = 1 \quad .$$

Ans. to 20.3: $\left(\frac{13}{101}\right) = 1 \quad .$

(In words: 13 is a quadratic residue modulo 101).

Note: The Four rules will be given to you on a test or quiz, so you don't have to memorize them, only how to **use** them.