MATH 115, SUMMER 2012
LECTURE 15

JAMES MCIVOR

Today we gather more results about the Legendre symbol.
Recall: last time we
- defined QRs and QNRs
- defined the Legendre symbol
- proved Euler's criterion, and its corollary, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$.
- gathered a few other properties

1. Gauss' Lemma

- Tomorrow we'll prove the famous and enormously useful Quadratic Reciprocity Law, which deals with the Legendre symbol for odd primes.
- Our goal today is to understand it for the prime 2.
- Namely, what is $\left(\frac{2}{p}\right)$? This takes a little more work than you think.

Theorem 1. *(Gauss' Lemma) Let p be an odd prime and a an integer with $(a, p) = 1$. Consider the least positive residues of the integers $a, 2a, \ldots, \frac{p-1}{2}a$. Let n be the number of these residues which are greater than $\frac{p}{2}$. Then*

$$\left(\frac{a}{p}\right) = (-1)^n$$

We'll deduce this as a corollary of the following more general result. I think this proof is nicer than the textbook's.

Theorem 2. *Let S be any subset of $(\mathbb{Z}/p)^\times$ with the following property: for each $x \in (\mathbb{Z}/p)^\times$, either $x \in S$ or $-x \in S$ (but not both). For each $a \in (\mathbb{Z}/p)^\times$, define $\mu(a)$ to be the number of elements t of S such that (at) is not in S. Then*

$$\left(\frac{a}{p}\right) = (-1)^{\mu(a)}$$

- For example, if $p = 5$, then $(\mathbb{Z}/p)^\times = \{1, 2, 3, 4\}$.
- Take S to be the subset $\{1, 3\}$.
- Check this S satisfies the stated property.
- Take $a = 3$. We check for each $t = 1, 3$, whether $3t \in S$. (note we have to multiply our *a only by things in S!*)
- $1 \cdot 3 \in S$. $3 \cdot 3 = 9 \equiv 4 \notin S$.
- Thus $\mu(3) = 1$, so the theorem says that

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

- so 3 is a QNR mod 5. True - we already saw that the only QRs mod 5 are 1 and 4.

Proof of Theorem 2. - in this proof, we consider all elements as being in the ring $\mathbb{Z}/p$, so "=" means congruent mod p

- Let $S = \{a_1, \ldots, a_r\} \subset (\mathbb{Z}/p)^\times$ have the stated property.
- for each a_i, we look at the elements $a_i n$ and $-a_i n$.
- exactly one of them is in S, for each i.
- Moreover, if $i \neq j$, then $a_i n \neq a_j n$ or $-a_j n$.
- Reason: if $a_i n = a_j n$, then since $n \in (\mathbb{Z}/p)^\times$, it's a unit. cancel it to get $a_i = a_j$. No good!
- similarly, if $a_i n = -a_j n$, get $a_i = -a_j \notin S$ - contradiction.
- so one list of elements of S is the one we started with, $\{a_1, \ldots, a_r\}$
- another way is $\{\pm a_1 n, \pm a_2 n, \ldots, \pm a_r n\}$, where it's negative for each i that makes $a_i n \notin S$ (write out lists side by side for clarity)
- there are $\mu(n)$ negative signs in the second list, by def of μ.
- the products must be equal, since they're just two ways of listing S. It gives

$$\prod_{a \in S} an = (-1)^{\mu(n)} \prod_{a \in S} a$$

- cancel the products, leaving

$$n^{\frac{p-1}{2}} = (-1)^{\mu(n)},$$

since there are $\frac{p-1}{2}$ elements in S.

□

Proof of Gauss' Lemma. We just have to check that $S = \{1, 2, \ldots, \frac{p-1}{2}\}$ has the stated property. This is clear.

□

2. Computing $\left(\frac{2}{p}\right)$

Theorem 3. *Let p be an odd prime. Then*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \mod 8 \\ -1 & \text{if } p \equiv \pm 3 \mod 8 \end{cases}.$$

Proof. We use Theorem 2 with $S = \{1, 2, \ldots, \frac{p-1}{2}\}$. According to this, we look at the set

$$2S = \{2s \mid s \in S\} = \{2, 4, 6, \ldots, p-1\}$$

and we ask: how many of these integers are greater than $p/2$?

- Say the answer is m. Then by Gauss' Lemma, $\left(\frac{2}{p}\right) = (-1)^m$.
- equivalently: how many even numbers $2s$ are there such that

$$\frac{p+1}{2} \leq 2s \leq p - 1?$$

- equivalently, how many integers s are in the interval $[\frac{p+1}{4}, \frac{p-1}{2}]$?
- every odd number is congruent to one of ± 1 or ± 3 mod 8,
- write $p = 8k + \alpha$, where $\alpha = \pm 1$ or ± 3.
- note: if $a < b \in \mathbb{Z}$, number of integers in interval $[a, b] = b - a + 1$.
- case 1: $\alpha = 1$
- then want number of integers s in the range $[2k + \frac{1}{2}, 4k]$ = number of integers in $[2k + 1, 4k] = 4k - (2k + 1) + 1 = 2k$.

- case 2: $\alpha = -1$
- want number of integers s in the range $[2k, 4k-1] = 4k - 1 - 2k + 1 = 2k$.
- So in both of these cases, the number of elements we want is even, and $\left(\frac{2}{p}\right) = (-1)^{2k} = 1$.
- case 3: $\alpha = 3$
- want number of integers in the range $[2k+1, 4k+1] = 4k+1-(2k+1)+1 = 2k+1$, which is odd, so $\left(\frac{2}{p}\right) = (-1)^{2k+1} = -1$
- case 4: $\alpha = -3$
- want: number of integers in range $[2k-\frac{1}{2}, 4k-2]$ = number of integers in range $[2k, 4k-2] = 4k - 2 - 2k + 1 = 2k - 1$, which is odd, so $\left(\frac{2}{p}\right) = (-1)^{2k-1} = -1$

$\square$

Problem Session

[first go over back of WS from yesterday]

(1) Fun problem (not related to quadratic residues): find the positive integer x such that

$$x^9 = 760231058654565217 = 7.6023... \times 10^{17}$$

[Hint: apply Euler's Theorem with the modulus 20]

(2) Check that, mod 11, the set $S = \{2, 4, 6, 8, 10\}$ satisfies the conditions of Theorem 2. Use that Theorem to compute $\left(\frac{3}{11}\right)$. Answer = 1 (5 and 6 are square roots of 3 mod 11). Check it "by hand".

(3) Useful rephrase of the $\left(\frac{2}{p}\right)$ calculation: Show that

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

(4) (NZM 3.1.16) Show that if a is a QR mod m and $ab \equiv 1 \mod m$, then b is also a QR mod m. Then prove that the product of all the QRs mod m is congruent to 1 if $p \equiv 3 \mod 4$ and congruent to -1 if $p \equiv 1 \mod 4$.

(5) Let p be prime and $(a, p) = 1$. Prove that if $a^{2^n} \equiv -1 \mod p$ then a has order 2^{n+1} mod p.

(6) Let $F_n = 2^{2^n} + 1$ (this is called the nth Fermat number). Let $n \geq 2$, and pick a prime divisor q of F_n. Prove that 2 has order $2^{n+1} \mod q$, using the previous exercise.

(7) (notation as above) Prove that $q \equiv 1 \mod 2^{n+1}$.

(8) (notation as above) Prove that there exists an integer a such that $a^{2^{n+1}} \equiv -1 \mod q$, using the value of $\left(\frac{2}{q}\right)$.