Math 152 Notes

Lucas Garron

October 22, 2009

20091022

$(\frac{a}{p}) = {}^{1,QR}_{\substack{0,QNR\\0,GCD(a,p)>1}}$

Read about Dirichlet characters around page 404.
$\chi(a+p) = \chi(a)$ (periodic)
χ multiplicative
$\chi(a) = 0$ if $GCD(a,p) > 1$ (TYPO in book.)

Gauss' Lemma: Assume p odd prime, $GCI(a,p) = 1$, $(\frac{a}{p}) = (-1)^n$, where n is the # of least residues of $a, 2a, \frac{p-1}{2}a$ which are $> \frac{p}{2}$
If m is given, $m = pq + r$ $(q \in \mathbb{Z}, 0 \leq r \leq p)$

$q = [\frac{m}{p}]$, ($[x]$ greatest integer $\leq x$)
Because $\frac{m}{p} = q + \frac{r}{p}$, $q \in Z, o \leq \frac{r}{p} < 1$, so $q = [\frac{m}{p}]$

$r_1, ..., r_n$ least residues of elements of $\{a, 2a, ..., \frac{p-1}{2}a\}$ are $\frac{p}{2} < r < p$
$s_1, ..., s_m$ those least res. of $\{a, 2a, ..., \frac{p-1}{2}a\}$ that are $0 < s_i < \frac{p}{2}$ ($0, \frac{p}{2}$ impossible, so strict ineq.)
$\{a, 2a, ..., \frac{p-1}{2}a\}$ are $\equiv /r_1^n/s_1^m/$ rearranged.
Proved last time: $/r_1^m/, p - /r_1^n/$ are $1, 2, \frac{p-1}{2}$ rearranged.

$ak = qp + r$, $0 \leq r < p$ and $q = [\frac{ak}{p}]$
$ak = p[\frac{ak}{p}] + |^{r_i}_{s_j}$ (when $k \in \{1, ..., \frac{p-1}{2}\}$)
Gauss' Lemma can be reformatted:
$(0 < R_j < p/2, \frac{p}{2<r_i<p})$

Application: If p is odd, $p \neq 3$, $(\frac{3}{p}) = 1$ if $p \equiv 1$ or $11 \bmod 12$, or $= -1$ if $p = 5$ or $7 \bmod 12$
Using Gauss' Lemma.
$3, 6, 9, ..., 3p - 1/2$ are all between 0 and $\frac{3p}{2}$
$3k = [\frac{3k}{p}]p +$ residue; depending on range:
$res = 3k$ if $0 < ak < p$, $3k - 1$ if $p < ak < \frac{3p}{2}$
$n = \#$ of $3k$ in the range $\frac{p}{2}$ to p.
Write $p = 12l + t$, $t = 1, 5, 7,$ or 11.
$3k = p[\frac{3k}{p}] + r$
We are counting r with $\frac{p}{2} < r < p$

$\frac{p}{2} < 3k < p, \frac{p}{6} < k < \frac{p}{3}$.
Therefore, the # of such k is $[\frac{p}{3}] - [\frac{p}{6}]$ ($= n$ from Gauss' Lemma)
(If u, v are not integers, # of k with $u < k < v$ is $[u] - [v]$ because the ineq. is equiv. to $[u] < k \leq [v]$)
$[\frac{p}{3}] - [\frac{p}{6}] = [\frac{12l+t}{3}] - [\frac{12l+t}{6}] = [4 + \frac{t}{3}] + [2 + \frac{t}{6}] = l\,\substack{(4-2)\\ \text{even}} + [\frac{t}{3}] + [\frac{t}{6}]$
n has the same parity as $[\frac{t}{3}] - [\frac{t}{6}] =$
$0 - 0 \equiv 0 \bmod 7$, $t = 1$
$1 - 0 \equiv 1$, $t = 5$
$2 - 1 \equiv 1$, $t = 7$
$3 - 1 \equiv 0$, $t = 11$

$\theta : \mathbb{Z} \to \{\pm 1\}$
$\theta = 0$ if $GCD(n, 12) > 1$
$\theta(n) = 1$ if $n \equiv \pm 1 \bmod 12$, -1 if $s \equiv \pm 5 \bmod 12$.
We've proved if p is an odd prime $p \neq 2$, $(\frac{3}{p}) = \theta(p)$
$(\theta(p + 12) = \theta(p), \theta(ab) = \theta(a)\theta(b))$ Before: $(\frac{a}{p}) = \chi_p(a)$ is a Dirichlet char. (p fixed)
Much deeper: If we fix a there is a product character (modulus depends on a, e.g. if $a = 3, M(a) = 12$), i.e. is a Dirichlet character mod12
Such that if p is prime, $(a, p) = 1 \Rightarrow (\frac{a}{p}) = \theta_a(p)$

Towards proof of
Theorem (Gauss): If p, q odd primes, $(\frac{}{pq})(\frac{q}{p}) = (-1)^{1/2(p-1)\frac{1}{2}(q-1)}$
$\frac{1}{2}(p-1)$ is even if $p \equiv 1 \bmod 4$, odd if $p \equiv 3 \bmod 4$
$(\frac{p}{q}) = (\frac{q}{p})$ if $p \equiv 1 \bmod 4$ or $q \equiv 1 \bmod 4$
$(\frac{p}{q}) = -(\frac{q}{p})$ if $p \equiv q \equiv 3 \bmod 4$

Suppose a is odd. In this case, we can write Gauss' lemma: $(\frac{a}{p}) = (-1)^N$, $N = \displaystyle\sum_{k=1}^{p-1/2} [\frac{kq}{2}]$

Remember $ka = p[\frac{ka}{p}] + \{^{r_i}_{s_i}$

Sum over k. Let $P = \displaystyle\sum_{k=1}^{\frac{p-1}{2}} k = \frac{1}{8}(p^2 - 1)$

$$Pa = p\sum_{k=1}^{\frac{p-1}{2}} [\frac{ka}{p}] + R + S$$

$/s_1^m/, p - /r_1^n/$ are $1, 2, ..., \frac{p-1}{2}$ rearranged.
Summing, $S + p \cdot n - R = 1 + 2 + ... + \frac{p-1}{2} = P = \frac{1}{8}(p^2 - 1)$

$$P(a + 1) = p\sum_{k=1}^{\frac{p-1}{2}} [\frac{ka}{p}] + 2S + p \cdot n$$

$even, k = 1, even \Rightarrow n, \displaystyle\sum_{k=1}^{\frac{p-1}{2}} [\frac{ka}{p}] = N$ have the same parity.

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

Claim: If p, q distinct odd primes, "$\Sigma_1 + \Sigma_2$" $= \sum_{k=1}^{\frac{p-1}{2}} [\frac{kq}{p}] + \sum_{l=1}^{\frac{p-1}{2}} [\frac{lp}{q}] = \frac{1}{2}(p-1) \cdot \frac{1}{2}(q-1)$ for geometric reasons (Gauss, noted by Eisenstein). This implies QR: $(\frac{q}{p})(\frac{p}{q}) = (-1)^{\Sigma_1} \cdot (-1)^{\Sigma_2}$

Example: $p = 5, q = 3$
$(0,0)$ to $(5,3)$ rect. in Cart. plane, line with slope $\frac{q}{p=3/5}$ through origin.
# of lattice points inside rect. $(p-1)/2, (q-1)/2$
Lattice points below line in small rect. $(1,1), (1,2), ..., (1, [\frac{q}{p}])$ $(\frac{y}{x} < \frac{q}{p})$
$(2,1), (2,2), ..., (2, [\frac{2q}{p}])$
Total below line: Σ_1
Similarly, above: Σ_2 (flipped argument).