“Around the quadratic reciprocity” Tutorial 4 Report

Jamie Khan, Ciaran Brennan, Kevin Coughlan, Rory Higgins, Michael Reynolds

February 17, 2014

Let n be an odd number, and let $n = p_1 p_2 \ldots p_k$ be its prime decomposition (possibly with repeated factors). Let us define the *Jacobi symbol* $(\frac{a}{n})$ by the formula

$$(\frac{a}{n}) = (\frac{a}{p_1})(\frac{a}{p_2})\ldots(\frac{a}{p_k}).$$

1). Give an example of a and n for which $(\frac{a}{n}) = 1$, but a is not congruent to a square modulo n.

Consider $a = 5$, $n = 9$

$$\begin{aligned} \text{Then} \quad (\frac{5}{9}) &= (\frac{5}{3})(\frac{5}{3}) \\ &= (\frac{2}{3})(\frac{2}{3}) = (\frac{4}{3}) = (\frac{1}{3}) = 1 \end{aligned}$$

But, $0^2 \equiv 0,\ \ 1^2 \equiv 1,\ \ 2^2 \equiv 4,\ \ 3^2 \equiv 0,\ \ 4^2 \equiv 7,\ \ 5^2 \equiv 7,\ \ 6^2 \equiv 0,\ \ 7^2 \equiv 4,\ \ 8^2 \equiv 1$

So $x^2 \not\equiv 5 \pmod 9$

2). Show that for Jacobi symbols we have $(\frac{a}{n})(\frac{b}{n}) = (\frac{ab}{n})$ and $(\frac{a}{n_1})(\frac{a}{n_2}) = (\frac{a}{n_1 n_2})$ whenever n, n_1, n_2 are odd.

Let $n = p_1 p_2 \ldots p_k$ be odd then

$$\begin{aligned}
(\frac{a}{n})(\frac{b}{n}) &= (\frac{a}{p_1})(\frac{a}{p_2})\dots(\frac{a}{p_k})(\frac{b}{p_1})\dots(\frac{b}{p_k}) \\
&= (\frac{a}{p_1})(\frac{b}{p_1})\dots(\frac{a}{p_k})(\frac{b}{p_k}) \\
&= (\frac{ab}{p_1})\dots(\frac{ab}{p_k}) = (\frac{ab}{n})
\end{aligned}$$

Let $n_1 = p_1 \dots p_k$, $n_2 = q_1 \dots q_k$,
then $n_1 n_2 = p_1 \dots p_k q_1 \dots q_k = p_1 q_1 \dots p_k q_k$

$$\begin{aligned}
\text{Then} \quad (\frac{a}{n_1})(\frac{a}{n_2}) &= (\frac{a}{p_1})\dots(\frac{a}{p_k})(\frac{a}{q_1})\dots(\frac{a}{q_k}) \\
&= (\frac{a}{p_1})(\frac{a}{q_1})\dots(\frac{a}{p_k})(\frac{a}{q_k}) \\
&= (\frac{a}{n_1 n_2})
\end{aligned}$$

3). Show that if m and n are odd integers, then $\frac{mn-1}{2} \equiv \frac{m-1}{2} + \frac{n-1}{2} \pmod 2$. Explain why it implies that for each odd n we have $(\frac{-1}{n}) = (-1)^{\frac{n-1}{2}}$

Part 1

$$(\frac{mn-1}{2}) \equiv (\frac{m-1}{2} + \frac{n-1}{2}) \pmod 2 \iff (\frac{mn-1}{2} - \frac{(m+n)-2}{2}) \equiv 0 \pmod 2$$

$$(\frac{mn-1}{2} - \frac{(m+n)-2}{2}) = \frac{mn-1-(m+n)+2}{2} = \frac{mn-(m+n)+1}{2} = \frac{(m-1)(n-1)}{2}$$

If $(m-1), (n-1)$ are even $\Rightarrow \frac{(m-1)(n-1)}{2}$ is even.

So $\frac{(m-1)(n-1)}{2} \equiv 0 \pmod 2 \Rightarrow (\frac{mn-1}{2}) \equiv (\frac{m-1}{2} + \frac{n-1}{2}) \pmod 2$

Part 2

For part 2 we use the fact that for a prime p: $(\frac{-1}{p}) = -1^{(\frac{p-1}{2})}$.

We want $(\frac{-1}{n}) = -1^{(\frac{n-1}{2})}$ for n odd.

$$
\begin{aligned}
(\frac{-1}{n}) &= (\frac{-1}{p_1})(\frac{-1}{p_2})\dots(\frac{-1}{p_k}) \quad \text{where } p_1\dots p_k \text{ is the prime decomposition of } n \text{ and } p_i \text{ is odd} \\
&= -1^{(\frac{p_1-1}{2})}. -1^{(\frac{p_2-1}{2})}\dots -1^{(\frac{p_k-1}{2})} \\
&= -1^{\sum_{i=1}^{k}\frac{p_i-1}{2}}
\end{aligned}
$$

Now we observe that $\sum_{i=1}^{k}\frac{p_i-1}{2} \equiv (\frac{p_1p_2\dots p_k-1}{2}) \pmod 2$ follows from part 1 by induction,

so

$$
-1^{\sum_{i=1}^{k}(\frac{p_i-1}{2})} = -1^{\frac{p_1p_2\dots p_k-1}{2}} = -1^{\frac{n-1}{2}}
$$

4). Show that for any two coprime odd integers m, n we have $(\frac{m}{n})(\frac{n}{m}) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}$.

Let $m = p_1\dots p_k$ and $n = q_1\dots q_l$

m, n coprime $\Rightarrow q_i \neq p_j$ for any i, j.

$$
\begin{aligned}
(\frac{m}{n}) &= (\frac{p_1\dots p_k}{q_1\dots q_l}) \\
&= (\frac{p_1}{q_1\dots q_l})(\frac{p_2}{q_1\dots q_l})\dots(\frac{p_k}{q_1\dots q_l}) = \prod_{i=1}^{k}(\frac{p_i}{q_1\dots q_l}) \\
\prod_{i=1}^{k}(\frac{p_i}{q_1\dots q_l}) &= \prod_{i=1}^{k}(\frac{p_i}{q_1})\prod_{i=1}^{k}(\frac{p_i}{q_2})\dots\prod_{i=1}^{k}(\frac{p_i}{q_l})
\end{aligned}
$$

Similarly, for $(\frac{n}{m})$ we get $(\frac{n}{m}) = (\frac{q_1\dots q_l}{p_1\dots p_k}) = \prod_{j=1}^{l}(\frac{q_j}{p_1\dots p_k}) = \prod_{j=1}^{l}(\frac{q_j}{p_1})\prod_{j=1}^{l}(\frac{q_j}{p_2})\dots\prod_{j=1}^{l}(\frac{q_j}{p_k})$.

$$
\begin{aligned}
\Rightarrow (\frac{m}{n})(\frac{n}{m}) &= \prod_{i=1}^{k}(\frac{p_i}{q_1})\dots\prod_{i=1}^{k}(\frac{p_i}{q_l}).\prod_{j=1}^{l}(\frac{q_j}{p_1})\dots\prod_{j=1}^{l}(\frac{q_j}{p_k}) \\
&= (\prod_{j=1}^{l}\prod_{i=1}^{k}(\frac{p_i}{q_j}).\prod_{i=1}^{k}\prod_{j=1}^{l}(\frac{q_j}{p_i})) \quad \text{by quadratic reciprocity law } (\frac{p_i}{q_j})(\frac{q_j}{p_i}) = -1^{(\frac{p_i-1}{2})(\frac{q_j-1}{2})} \\
&= -1^{\sum_{j=1}^{l}\sum_{i=1}^{k}(\frac{p_i-1}{2})(\frac{q_j-1}{2})} \\
&= -1^{\sum_{i=1}^{k}(\frac{p_i-1}{2})\sum_{j=1}^{l}(\frac{q_j-1}{2})}
\end{aligned}
$$

And by Question 3 $\sum_{i=1}^{k}(\frac{p_i-1}{2}) \equiv \frac{m-1}{2}$.

Similarly for $\sum_{j=1}^{l}(\frac{q_j-1}{2}) \equiv \frac{n-1}{2}$.

$$\Rightarrow -1^{(\frac{m-1}{2})(\frac{n-1}{2})} = (\frac{m}{n})(\frac{n}{m})$$

5). Applying previous problem with $m = n + 2$, show that for each odd n we have $(\frac{2}{n}) = (-1)^{\frac{n^2-1}{8}}$.

$(\frac{n+2}{n})(\frac{n}{n+2}) \Rightarrow$ for odd n, $(\frac{2}{n}) = -1^{\frac{n^2-1}{8}}$
Our argument will rely on induction on n. Take $n = 3$, $(\frac{2}{3}) = -1^1 = -1^{\frac{9-1}{8}}$, true for $n = 3$.
$(\frac{n+2}{n})(\frac{n}{n+2}) = -1^{(\frac{n+2-1}{2}).(\frac{n-1}{2})} = -1^{\frac{n^2-1}{4}}$
Observe that $(\frac{n+2}{n}) = (\frac{2}{n})$ and $(\frac{n}{n+2}) = (\frac{-2}{n+2}) = (\frac{2}{n+2})(\frac{-1}{n+2})$
We have $(\frac{2}{n})(\frac{2}{n+2})(\frac{-1}{n+2}) = -1^{\frac{n^2-1}{4}}$
Assume $(\frac{2}{n}) = -1^{\frac{n^2-1}{8}}$ and $\frac{-1}{n+2} = -1^{(\frac{(n+2)-1}{2})}$ by Question 3.

$$\begin{aligned}
\Rightarrow \quad \frac{2}{n+2} \quad & (-1^{\frac{n^2-1}{8}})(-1^{(\frac{n+1}{2})}) = -1^{\frac{n^2-1}{4}} \\
\frac{2}{n+2} \quad & = -1^{\frac{n^2-1}{4}-(\frac{n^2-1}{8})-(\frac{n+1}{2})} = -1^{\frac{(n+2)^2-1}{8}} \\
\Rightarrow \quad \frac{2}{n} \quad & = -1^{\frac{n^2-1}{8}} \quad \forall \text{ odd } n > 1.
\end{aligned}$$

6). Show that all prime divisors of $9n^2 + 3n + 1$ are of the form $3k + 1$.

Let $\alpha = 9n^2 + 3n + 1 = 3(3n^2 + n) + 1 \Rightarrow \alpha \equiv 1 \pmod 3$.
Let p be a prime divisor of $\alpha, \Rightarrow p \neq 3$ from above, and is clearly not 2.
Want to show that $p \equiv 1 \pmod 3$, $\forall p$ prime divisors.
$4\alpha = 9n^2 + 12n + 4 = (6n^2 + 1)^2 + 3 \equiv 0$ (mod p)
$\Rightarrow (6n^2 + 1)^2 \equiv -3$ (mod p) which implies that
$(\frac{-3}{p}) = 1$

Since p is odd, we know that
$(\frac{3}{p})(\frac{p}{3}) = (-1)^{\frac{3-1}{2}\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} \Rightarrow (\frac{3}{p}) = (-1)^{\frac{p-1}{2}}(\frac{p}{3})$

Since we also know that $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$, then:
$(\frac{-3}{p}) = (\frac{-1}{p})(\frac{3}{p}) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}}(\frac{p}{3}) = (\frac{p}{3})$

Therefore, $(\frac{p}{3}) = 1, \iff p \equiv 1 \pmod 3$, which is what we want.

7). Let p be an odd prime number.
(a) Show that the function $k \mapsto \frac{1-k}{1+k}$ maps the set $(Z/pZ)\backslash\{-1\}$ to itself and is a 1-to-1 correspondence.
(b) Compute the sum $\sum_{k=0}^{p-1}(\frac{k}{p})$.

Part (a)

Consider $\frac{1}{1+k}$ to be the multiplicative inverse $1+k$ in $(Z/pZ)\backslash\{-1\}$, we get

$$(\frac{1}{1+k})(1+k) \equiv 1 \pmod p. \qquad 1+k \not\equiv 0 \pmod p$$

then $-p < \frac{1-k}{1+k} < p \quad \forall k = 0, 1, \ldots, p-1$.

As $-p - p^k \leq -p < -p+1 < 1-k < 1 < p \leq p + pk$ and $\frac{1-k}{1+k} \neq -1$
$1 - k \neq -1 - k \Rightarrow \frac{1-k}{1+k} \in (Z/pZ)\backslash\{-1\}$.

So this is a map $(Z/pZ)\backslash\{-1\} \mapsto (Z/pZ)\backslash\{-1\}$.

For a 1-to-1 correspondence; suppose $\frac{1-a}{1+a} \equiv \frac{1-b}{1+b} \pmod p$.

$(1+b)(1-a) \equiv (1-b)(1+a)$
$1 + b - a - ab \equiv 1 - b + a - ab \pmod p$
$2b \equiv 2a \pmod p$
Hence $k \mapsto \frac{1-k}{1+k}$ is a 1-to-1 map from $(Z/pZ)\backslash\{-1\}$ to itself.

Part (b)

For an odd prime p where we know that exactly $\frac{1}{2}$ of $\{1, 2, \ldots, p-1\}$ are quadratic residues mod p and the other half are not. Let the residues be denoted $R_1, \ldots, R_{\frac{p-1}{2}}$ and the non residues denoted by $n_1, \ldots, n_{\frac{p-1}{2}}$. Then

$$\begin{aligned}\sum_{k=0}^{p-1}(\frac{k}{p}) &= (\frac{0}{p}) + \sum_{i=1}^{\frac{p-1}{2}}(\frac{R_i}{p}) + \sum_{j=1}^{\frac{p-1}{2}}(\frac{n_j}{p}) \\ &= 0 + \frac{p-1}{2} - \frac{p-1}{2} = 0\end{aligned}$$

8).Find the number of solutions to the equation $x^2 + y^2 = 1$ in Z/pZ.

This is equivalent to finding the number of solutions to $x^2 \equiv 1 - y^2$ (mod p).

If for a particular $y \not\equiv 1, \exists x^2$ such that the above equation is satisfied, then the number of solutions for this fixed y is 2 (namely $\pm x$), and $(\frac{1-y^2}{p}) = 1$, that is, number of solutions for this fixed y is $1 + (\frac{1-y^2}{p}) = 2$.

Similarly, if for a particular $y \not\equiv 1$, $\nexists x^2$ such that the above equation is satisfied, then there are no solutions for this fixed y, and $(\frac{1-y^2}{p}) = -1$, that is, number of solutions for this fixed y is $1 + (\frac{1-y^2}{p}) = 0$.

Finally, for $y \equiv 1$, the only solution to the above equation is 0, and $(\frac{1-y^2}{p}) = 0$, as $gcd(1 - y^2, p) \neq 1$, that is, number of solutions for $y = 0$ is $1 + (\frac{1-y^2}{p}) = 1$.

Hence, the number of solutions to $x^2 \equiv 1 - y^2$ (mod p) is the sum of the number of solutions for fixed y, from $y = 0$ to $y = p - 1$, namely;

$\sum_{y=0}^{p-1}(1 + (\frac{1-y^2}{p}))$