MATH 565: Week 12 Notes

Steven C. White

November 15, 2019

p = 3	q	3	5	7	11	13	17
	$\left(\frac{p}{q}\right)$	0	-1	-1	1	1	-1
	$\left(\frac{q}{p}\right)$	0	-1	1	-1	1	-1

p = 5	q	3	5	7	11	13	17
	$\left(\frac{p}{q}\right)$	-1	0	-1	1	-1	-1
	$\left(\frac{q}{p}\right)$	1	0	-1	1	-1	-1

p = 7	q	3	5	7	11	13	17
	$\left(\frac{p}{q}\right)$	-1	-1	0	1	-1	-1
	$\left(\frac{q}{p}\right)$	1	-1	0	-1	-1	-1

p = 11	q	3	5	7	11	13	17
	$\left(\frac{p}{q}\right)$	1	1	-1	0	-1	-1
	$\left(\frac{q}{p}\right)$	-1	1	1	0	-1	-1

p = 13	q	3	5	7	11	13	17
	$\left(\frac{p}{q}\right)$	1	-1	-1	-1	0	1
	$\left(\frac{q}{p}\right)$	1	-1	-1	-1	0	1

p = 17	q	3	5	7	11	13	17
	$\left(\frac{p}{q}\right)$	-1	-1	-1	-1	1	0
	$\left(\frac{q}{p}\right)$	-1	-1	-1	-1	1	0

Observations: Let $p \in \{5, 13, 17\}$. Then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ and $p \equiv 1 \pmod 4$. Also, let $p, q \in \{3, 7, 11\}$. Then $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ and $p \equiv q \equiv 3 \pmod 4$.

Conjecture: Suppose p and q are both odd primes.
If either $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$, then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$.
If $p \equiv q \equiv 3 \pmod 4$, then $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.
This was observed by Legendre when he defined numbers this way.

Notation. $(\mathbb{Z}/n\mathbb{Z})^{\times}$ = the set of reduced residues (mod n)
$(\mathbb{Z}/pq\mathbb{Z})^{\times} = \{1 \le a < pq \mid p \nmid a,\ q \nmid a\}$ = the set of numbers 1 through $pq - 1$ not divisible by p or q, where p and q are odd primes and $p \neq q$
$(\mathbb{Z}/p\mathbb{Z})^{\times} \times (\mathbb{Z}/q\mathbb{Z})^{\times} = \{(a, b) \mid 1 \le a < p,\ p \nmid a,\ 1 \le b < q,\ q \nmid b\}$

Chinese Remainder Theorem: The map $\sigma : (\mathbb{Z}/pq\mathbb{Z})^{\times} \to (\mathbb{Z}/p\mathbb{Z})^{\times} \times (\mathbb{Z}/q\mathbb{Z})^{\times}$ given by $\sigma(k) = (k(mod\ p)), k(mod\ q))$ is a bijection. So $\mid (\mathbb{Z}/pq\mathbb{Z})^{\times} \mid = \mid (\mathbb{Z}/p\mathbb{Z})^{\times} \times (\mathbb{Z}/q\mathbb{Z})^{\times} \mid = (p-1)(q-1) = \phi(pq)$.
Let $R = \{1 \le a < \frac{pq}{2} \mid p \nmid a,\ q \nmid b\}$. Then, $\mid R \mid = \frac{1}{2}\phi(pq)$.

Let $S = \{(a, b) \mid 1 \le a < p,\ 1 \le b < \frac{q}{2}\} \subseteq (\mathbb{Z}/p\mathbb{Z})^{\times} \times (\mathbb{Z}/q\mathbb{Z})^{\times}$. Then, $\mid S \mid = \frac{1}{2}\phi(pq)$.

Theorem: If $k \in R$, then there exists $(a, b) \in S$ such that $\sigma(k) = \pm 1(a, b)$.

Example: Let $p = 5$ and $q = 3$. Then $R = \{1, 2, 4, 7\}$ and $(\mathbb{Z}/15\mathbb{Z})^{\times}$ and

$S = \{(a,b) \mid 1 \le a < 5,\ 1 \le b < \frac{3}{2}\} = \{(1,1),(2,1),(3,1),(4,1)\}$. Note that

$$\begin{aligned}
\phi(1) &= (1,1)\\
\phi(2) &= (2,2) = -(3,1)\\
\phi(3) &= (4,1)\\
\phi(4) &= (2,1)
\end{aligned}$$

So $\phi\left(\prod_{k\in R} k\right) = \prod_{k\in R} \sigma(k) = \prod_{k\in R} \pm 1\cdot(a,b) = e\prod_{k\in R}(a,b)$, where $e = \pm 1$.

Note that for each $(a,b) \in S$ there is a unique $k \in R$ such that $(a,b) = \pm(k,k)$.

Then $\prod_{(a,b)\in S}(a,b) = e\prod_{k\in R}(k,k)$. Let $P = \frac{p-1}{2}$ and $Q = \frac{q-1}{2}$. Consider the left hand side of the previous equation.

$$\begin{aligned}
\prod_{(a,b)\in S}(a,b) &= \prod_{\substack{1\le a<p\\ 1\le b<\frac{q}{2}}}(a,b)\\
&= \left((p-1)!^{\frac{q-1}{2}}, \left(\left(\frac{q-1}{2}\right)!\right)^{p-1}\right)\\
&= \left((p-1)!^{Q}, Q!^{2P}\right)
\end{aligned}$$

Observe that

$$\begin{aligned}
Q!^2 &= \left(\prod_{1\le k<\frac{q-1}{2}} k\right)\left(\prod_{1\le k<\frac{q-1}{2}} k\right)\\
&= \left(\prod_{1\le k<\frac{q-1}{2}} k\right)\left(\prod_{\frac{q-1}{2}\le m<q} m\right)(-1)^{\frac{q-1}{2}}\\
&= (q-1)!(-1)^{\frac{q-1}{2}}
\end{aligned}$$

Continuing the original equality and applying Wilson's Theorem

$$\begin{aligned}
&= \left((p-1)!^{Q}, \left((q-1)!(-1)^{Q}\right)^{P}\right)\\
&= \left((-1)^{Q}, \left((-1)(-1)^{Q}\right)^{P}\right)\\
&= \left((-1)^{Q}, (-1)^{P}(-1)^{PQ}\right)
\end{aligned}$$

Consider the first (mod p) coordinate of the right hand side

$$\begin{aligned}
\prod_{k\in R} k &= \prod_{\substack{1\le k\le\frac{pq}{2}\\ p\nmid k,\, q\nmid k}} k\\
&= \underbrace{\left(\prod_{1\le k<p} k\right)}_{\text{(p-1)!}}\underbrace{\left(\prod_{p\le k<2p} k\right)}_{\text{(p-1)!}}\cdots\underbrace{\left(\prod_{(Q-1)p\le k<Qp} k\right)}_{\text{(p-1)!}}\left(\prod_{Qp\le k<\frac{pq}{2}} k\right)\underbrace{\left(\prod_{\substack{1\le k<\frac{pq}{2}\\ q\mid k}} k\right)^{-1}}_{\text{divide out q's}}
\end{aligned}$$

Observe that

$$\left(\prod_{\substack{1\le k<\frac{pq}{2}\\ q\mid k}} k\right)^{-1} = \left(\prod_{1\le k\le\frac{p-1}{2}=P} qk\right)^{-1} = \frac{1}{\left(\prod_{1\le k\le P} k\right)q^{P}}$$

and

$$\left(\prod_{Qp\leq k<\frac{pq}{2}=Qp+\frac{p}{2}} k\right) \equiv \left(\prod_{1\leq k\leq P} k\right)$$

Then continuing the equality we have

$$\begin{aligned}
&= \frac{(p-1)!^Q \left(\prod_{1\leq k\leq P} k\right)}{\left(\prod_{1\leq k\leq P} k\right) q^P} \\
&= \frac{(p-1)!^Q}{q^P} \\
&= (-1)^Q (q^{-1})^P \\
&= (-1)^Q (q^{-1})^{\frac{p-1}{2}} (mod\ p) \\
&= (-1)^Q \left(\frac{q^{-1}}{p}\right) \\
&= (-1)^Q \left(\frac{q}{p}\right)
\end{aligned}$$

This is the first coordinate. This side is symmetric in p and q so the second coordinate is $(-1)^P \left(\frac{p}{q}\right)$. Now, plug all of this back into the original equation

$$\prod_{(a,b)\in S} (a,b) = e \prod_{k\in R} (k,k)$$

$$\left((-1)^Q, (-1)^P(-1)^{PQ}\right) = e\left((-1)^Q \left(\frac{q}{p}\right), (-1)^P \left(\frac{p}{q}\right)\right)$$

Then,

$$\begin{aligned}
(-1)^Q &= e(-1)^Q(-1)^P \left(\frac{q}{p}\right) \\
1 &= e\left(\frac{q}{p}\right) \\
e &= \left(\frac{q}{p}\right)
\end{aligned}$$

$$\begin{aligned}
(-1)^P(-1)^{PQ} &= e(-1)^P \left(\frac{p}{q}\right) \\
(-1)^{PQ} &= e\left(\frac{p}{q}\right) \\
(-1)^{PQ} &= \left(\frac{q}{p}\right)\left(\frac{p}{q}\right)
\end{aligned}$$

Then,

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = \begin{cases} -1 & \text{if P and Q odd} \Leftrightarrow \frac{p-1}{2} \text{ and } \frac{q-1}{2} \text{ odd} \Leftrightarrow \text{p and q} \equiv 3(\text{mod } 4) \\ 1 & \text{if P or Q even} \Leftrightarrow \frac{p-1}{2} \text{ or } \frac{q-1}{2} \text{ even} \Leftrightarrow \text{p or q} \equiv 1(\text{mod } 4) \end{cases}$$

End Proof.

Special Rule for 2 on p.

$$\left(\frac{2}{p}\right) = \begin{cases} -1 & \text{if p} \equiv 3{,}5 \pmod{8} \\ 1 & \text{if p} \equiv 1{,}7 \pmod{8} \end{cases}$$