Tuesday, October 22

Recall from Thursday:

Quadratic Reciprocity Theorem:

If p and q are distinct odd primes, then

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

So $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ when either p or q is $1 \pmod 4$;

$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ when both $p \equiv q \equiv 3 \pmod 4$.

Notation: • $\alpha = \frac{p-1}{2}$ and $\beta = \frac{q-1}{2}$

• $F = \left\{1 \le k < \frac{pq}{2} : (k, pq) = 1\right\}$ (mod pq)

• $L = \underbrace{\{1 \le a \le p-1\}}_{(\text{mod } p)} \times \underbrace{\left\{1 \le b < \frac{q}{2}\right\}}_{(\text{mod } q)}$

Claims remaining to prove:

• RHS of (1) $\equiv (-1)^r (-1)^\beta \left(\frac{q}{p}\right) \pmod p$

• RHS of (2) $\equiv (-1)^r (-1)^\alpha \left(\frac{p}{q}\right) \pmod q$.

(1) $\displaystyle\prod_{(a,b)\in L} a \equiv (-1)^r \prod_{k\in F} k \pmod p$

(2) $\displaystyle\prod_{(a,b)\in L} b \equiv (-1)^r \prod_{k\in F} k \pmod q$.

Today it suffices to show:

$$\prod_{k\in F} k \equiv (-1)^\beta \left(\frac{q}{p}\right) \pmod p.$$

Proof:

$$\prod_{k\in F} k \equiv \prod_{\substack{1 \le k < \frac{pq}{2} \\ (k,pq)=1}} k$$

$$\equiv \Bigg(\prod_{\substack{1 \le k < \frac{pq}{2} \\ p \nmid k}} k\Bigg)\Bigg(\prod_{\substack{1 \le k < \frac{pq}{2} \\ q \mid k}} k\Bigg)^{-1} \pmod p$$

Today it suffices to show:

$$\prod_{k\in F} k \equiv (-1)^{\beta}\left(\frac{q}{p}\right) \pmod{p}.$$

Proof:

$$\prod_{k\in F} k \equiv \prod_{\substack{1\le k<\frac{pq}{2}\\ (k,pq)=1}} k$$

$$\equiv \Bigg(\prod_{\substack{1\le k<\frac{pq}{2}\\ p\nmid k}} k\Bigg)\Bigg(\prod_{\substack{1\le k<\frac{pq}{2}\\ q\mid k}} k\Bigg)^{-1} \pmod{p}$$

$\qquad$ ① $\qquad\qquad\qquad$ ②

$$① \equiv \prod_{j=1}^{\beta\ \cancel{\alpha}} \prod_{k=(j-1)p+1}^{jp-1} k \cdot \prod_{k=\beta p+1}^{\beta p+\alpha} k$$

$$\equiv (p-1)!^{\beta}\cdot \alpha! \equiv (-1)^{\beta}\alpha! \pmod{p}.$$

② has $\frac{p-1}{2}$ terms, each a multiple of q; so

$$② \equiv q^{\alpha}\,\alpha! \equiv \left(\frac{q}{p}\right)\alpha! \pmod{p}.$$

Euler's criterion.

Therefore

$$①\,②^{-1} \equiv (-1)^{\beta}\alpha!\left(\left(\frac{q}{p}\right)\alpha!\right)^{-1}$$
$$\equiv (-1)^{\beta}\left(\frac{q}{p}\right) \pmod{p}. \quad //$$

(The proof of the other RHS is the same, switching p with q and α with β.)

Example: Does $x^2 \equiv 55 \pmod{367}$ have solutions? Note: $367 \equiv 3 \pmod 4$ is a prime.

Solution: Use Legendre symbols:

$$\left(\frac{55}{367}\right) = \left(\frac{5}{367}\right)\left(\frac{11}{367}\right) = +1.$$

YES!!

- Since $5 \equiv 1 \pmod 4$, $\left(\frac{5}{367}\right) = \left(\frac{367}{5}\right) = \left(\frac{2}{5}\right) = -1.$ ★
- Since $11 \equiv 3 \pmod 4$, $\left(\frac{11}{367}\right) = -\left(\frac{367}{11}\right) = -\left(\frac{4}{11}\right) = -1.$ ★

General algorithm for computing $\left(\frac{a}{p}\right)$: ← assume $|a|<p$

- Factor $a = \pm p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$.
- Then $\left(\frac{a}{p}\right) = \left(\frac{\pm 1}{p}\right)\left(\frac{p_1}{p}\right)^{r_1} \cdots \left(\frac{p_k}{p}\right)^{r_k}$
- We know $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$ ✓
- If p_j is odd, use Quadratic Reciprocity to write $\left(\frac{p_j}{p}\right)$ in terms of $\left(\frac{p}{p_j}\right)$.
- Reduce $p \pmod{p_j}$ and recurse.

Example: Prove there are infinitely many primes of the form $8k+3$.

Proof: Let $p_1, \dots, p_k$ be any primes $\equiv 3 \pmod 8$; we'll find another one. Set

$$N = (p_1 \cdots p_k)^2 + 2.$$

Note $N \equiv 0^2 + 2 \not\equiv 0 \pmod{p_j}$.

Let p be any prime factor of N.

Then $p \mid \left((p_1 \cdots p_k)^2 + 2\right) \Rightarrow$

$(p_1 \cdots p_k)^2 \equiv -2 \pmod p$, so $\left(\frac{-2}{p}\right) = 1$.

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

If every $p \mid N$ were $1 \pmod 8$, then N itself would be $1 \pmod 8$; but $N = (\text{odd})^2 + 2$
$\equiv 1 + 2 \equiv 3 \pmod 8$.

So some prime dividing N is $3 \pmod 8$.