HW4 Problems:

1. Compute $\left(\frac{47}{67}\right)$.

2. Compute $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$

3. Compute $\left(\frac{3}{p}\right)$.

uses QR & CRT.

4. Prove $\exists\ \infty$ many primes $\equiv 3 \bmod 8$.

Recall from last time:

$\exists\ \infty$ many primes $\equiv 7 \bmod 8$.

Proof: Let $p_1, \ldots, p_k$ be primes $\equiv 7 \bmod 8$, and define

$$N = (p_1 p_2 \cdots p_k)^2 - 2.$$

- Observe that $7^2 \equiv 1 \mod 8$.

$$\Rightarrow (p_1 p_2 \cdots p_k)^2 = p_1^2 p_2^2 \cdots p_k^2$$
$$\equiv 1 \cdot 1 \cdot \cdots \cdot 1 \equiv 1 \mod 8.$$

$$\Rightarrow \quad N = (p_1 \cdots p_k)^2 - 2$$
$$\equiv 1 - 2 \equiv -1 \mod 8.$$

- Every prime $p \mid N$ satisfies
$p \equiv 1$ or $7 \mod 8$. Why?
Reduce mod p:

$$N = (p_1 \cdots p_k)^2 - 2$$
$$0 \equiv (p_1 \cdots p_k)^2 - 2 \mod p$$
$$2 \equiv (p_1 \cdots p_k)^2 \mod p$$
2 is square mod p.

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

$$\Rightarrow p \equiv 1, 7 \mod 8 \qquad \checkmark$$

- There must exist *some* $p \mid N$ with $p \equiv 7 \bmod 8$.

  Otherwise, every prime divisor of N is $\equiv 1 \bmod 8$, hence $N \equiv 1 \bmod 8$.

  Contradicts the fact that

  $$N \equiv -1 \bmod 8. \quad \checkmark$$

- Finally, this $p \mid N$, $p \equiv 7 \bmod 8$ is not in the list $p_1, \ldots, p_k$ because

  $$\begin{aligned} N &= (p_1 \cdots p_k)^2 - 2 \\ &\equiv 0 - 2 \mod p_i \ \forall i. \end{aligned}$$

  But $N \equiv 0 \bmod p$. $\checkmark$

This is a "Euclidean" style proof. My professor M. Ram Murty from Queen's University (Canada) wrote a paper in 1988, proving that

$$\exists \text{ "Euclidean" proof of } \infty \text{ many primes } \equiv a \bmod n$$

$$\Updownarrow$$

$$a^2 \equiv 1 \bmod n.$$

Luckily, <u>every</u> element of $(\mathbb{Z}/8\mathbb{Z})^\times$ squares to 1.

Today, as promised, we will prove Quadratic Reciprocity: For odd primes $p \neq q$ we have

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

Example: Compute $\left(\frac{29}{37}\right)$.

$$\left(\frac{29}{37}\right) = \left(\frac{37}{29}\right) \overset{+1}{\cancel{(-1)^{\frac{36}{2}\cdot\frac{28}{2}}}}$$

$$= \left(\frac{37}{29}\right)$$ reduce top mod 29.

$$= \left(\frac{8}{29}\right)$$ 8 <u>not prime</u>

$$= \left(\frac{2\cdot 2\cdot 2}{29}\right)$$

$$= \left(\frac{2}{29}\right)\left(\frac{2}{29}\right)\left(\frac{2}{29}\right)$$

$$= \left(\frac{2}{29}\right)^3 \qquad \left(\frac{2}{p}\right) = \begin{cases} +1 & p \equiv 1,7 \bmod 8 \\ -1 & p \equiv 3,5 \bmod 8 \end{cases}$$

$29 \equiv 5 \bmod 8$.

$$= (-1)^3$$

$$= -1$$ 29 <u>not</u> square mod 37.

Of course, we can also compute

$$\left(\frac{29}{37}\right) \doteq 29^{36/2} \mod 37.$$

$$= \underbrace{29^{18} \mod 37.}_{\text{this is also not so hard by "repeated squaring"}}$$

<u>Proof Time</u> :

We will follow a proof by Rousseau from 1991.

Only uses Wilson's Theorem & Chinese Remainder Theorem, and the tricks are fairly mild.

Given odd primes $p \neq q$, the idea is to multiply all elements of $(\mathbb{Z}/pq\mathbb{Z})^\times$ together, in two ways.

Example: $p, q = 3, 5$

$$\overset{p}{(\mathbb{Z}/3\mathbb{Z})^\times} \times \overset{q}{(\mathbb{Z}/5\mathbb{Z})^\times} \cong (\mathbb{Z}/15\mathbb{Z})^\times$$

1	1		1	1
2	1		2	2
1	2		4	4
2	2		7	7
1	3		8	8
2	3		11	11
1	4		13	13
2	4		14	14

prod: $2!^4 \bmod 3$ $\quad$ $4!^2 \bmod 5$

$(p-1)!^{q-1}$ $\quad$ $(q-1)!^{p-1}$

$(-1)^{q-1}$ $\quad$ $(-1)^{p-1}$

$\bmod p.$ $\quad$ $\bmod q.$

$1\cdot 2\cdot 4\cdot 7\cdot 8\cdot 11\cdot 13\cdot 14 \bmod 3$

$= (-1)^4$

$= 1$

& $1\cdot 2\cdot 4 \cdots 13\cdot 14 \bmod 5$

$= (-1)^2 = 1.$

Conclusion:

Let $$M = \prod_{\substack{1 \le k \le pq \\ \gcd(k, pq) = 1}} k.$$

Then, as above,

$$M = (-1)^{q-1} = 1 \mod p$$
$$M = (-1)^{p-1} = 1 \mod q.$$

Chinese Remainder Theorem:

$$\begin{cases} M = 1 \mod p \\ M = 1 \mod q \end{cases} \Rightarrow M = 1 \mod pq.$$

$$1 = px + qy \qquad 1qy + 1px$$

Is this interesting?

Theorem: For p, q prime

$$\prod_{\substack{1 \le k \le pq \\ \gcd(k, pq) = 1}} k = 1 \mod pq.$$

For quadratic reciprocity, we don't multiply all the elements together, just half of them.

How to choose the half ?

The group $(\mathbb{Z}/pq\mathbb{Z})^\times$ breaks into pairs $\{x, -x\}$. We never have $x = -x$ because then $x x^{-1} = -x x^{-1}$

$$1 = -1 \mod pq.$$

contradiction because $pq \geq 3$.

Pick one element from each pair and compute the product mod p & mod q. In other words, use the isomorphism

$$(\mathbb{Z}/pq\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$$

$$x \bmod pq \longmapsto (x \bmod p, x \bmod q).$$

Compute

$$\prod_{\substack{\text{half of} \\ \text{the } x\text{'s}}} (x \bmod p, x \bmod q) =: M$$

Easiest way to choose half:

Take $1 \leq x \leq \frac{pq-1}{2}$ & coprime to pq.

Example: $p, q = 3, 5$

$(\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times$

1	1
2	2
4	4
7	7
8 (−7)	8 (−7)
11 (−4)	11 (−4)
13 (−2)	13 (−2)
14 (−1)	14 (−1)

choose the 1st half.

What happens when we multiply them all?

$1 \le x \le \frac{pq-1}{2}$ & ~~coprime to~~ pq.
$p \nmid x$ & $q \nmid x$

$$p \nmid x \Rightarrow x = \frac{q-1}{2}\left\{\begin{array}{l} 1, 2, \dots, p-1, \cancel{p} \\ 1, 2, \dots, p-1, \cancel{p} \\ \\ 1, 2, \dots, p-1, \cancel{p} \end{array}\right. \mod p$$

$$1, 2, \dots, \frac{p-1}{2}$$

Then we have to throw out the multiples of q.

$$\prod \text{these } x = \frac{(p-1)!^{\frac{q-1}{2}} \left(\frac{p-1}{2}\right)!}{\text{product of multiples of } q \text{ in the range } 1, \ldots, \frac{pq-1}{2}.} \mod p$$

Note: $q(2q)(3q)\cdots\left(\frac{p-1}{2}q\right) \leq \frac{pq-1}{2}$

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

$$\prod \text{these } x = \frac{(p-1)!^{\frac{q-1}{2}} \cancel{\left(\frac{p-1}{2}\right)!}}{q^{\frac{p-1}{2}} \cancel{\left(\frac{p-1}{2}\right)!}} \mod p$$

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

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

By symmetry:

$$\prod \text{these } x = (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) \mod q.$$

Summary:

$$M = \prod_{\substack{\gcd(x,pq)=1 \\ 1 \le x \le \frac{pq-1}{2}}} (x \bmod p,\ x \bmod q)$$

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

Whew!

Now we will compute M in a completely different way.

Elements of $(\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$ come in negative pairs

$\{(a,b), (-a,-b)\}$

How can we get <u>one</u> element from each pair?

It suffices to take <u>all</u> $1 \le a \le p-1$ and half of the b's: $1 \le b \le \frac{q-1}{2}$.

$$S = \left\{ (a,b) : \begin{array}{l} 1 \le a \le p-1 \\ 1 \le b \le \frac{q-1}{2} \end{array} \right\}$$

$$(a,b) \in S \iff (a,-b) \notin S.$$

$$\iff (-a,-b) \notin S.$$

Since we have chosen one from each negative pair we get

$$\prod_{\text{before}} (x,x) = \pm \prod_{(a,b)\in S} (a,b)$$

each product has one from each negative pair, but not necessarily the same ones!

Compute:

$$\prod_{(a,b)\in S} (a,b) = \left(\underset{\bmod p}{(p-1)!^{\frac{q-1}{2}}} , \underset{\bmod q}{\left(\frac{q-1}{2}\right)!^{\,p-1}} \right)$$

$$= \left(\underset{\text{mod } p}{(-1)^{\frac{q-1}{2}}}, ? \right)$$

We have $-1 \equiv (q-1)! \mod q$

$$-1 \equiv 1 \cdot 2 \cdots \tfrac{q-1}{2} \left(-\tfrac{q-1}{2}\right) \cdots (-2)(-1) \mod q.$$

$$-1 \equiv (-1)^{\frac{q-1}{2}} \left(\tfrac{q-1}{2}\right)!^{2}$$

$$(-1)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\tfrac{q-1}{2}\right)!^{p-1}$$

In other words:

$$\left(\tfrac{q-1}{2}\right)!^{p-1} \equiv (-1)^{\frac{p-1}{2}} (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Whew!

In summary, we have shown

$$\left(\cancel{(-1)^{\frac{q-1}{2}}} \left(\frac{q}{p}\right), \cancel{(-1)^{\frac{p-1}{2}}} \left(\frac{p}{q}\right) \right)$$

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

$$\Longrightarrow \left(\underset{\text{mod } p}{\left(\frac{q}{p}\right)}, \underset{\text{mod } q}{\left(\frac{p}{q}\right)} \right) \underset{\substack{\text{in the group}\\ (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times}}{=} \pm \left(\underset{\text{mod } p}{1}, \underset{\text{mod } q}{(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}} \right).$$

Since $p, q \neq 2$ these equations are also true as integers:

$$\left(\left(\frac{q}{p}\right), \left(\frac{p}{q}\right) \right) \underset{\text{in } \mathbb{Z}^2}{=} \pm \left(1, (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \right)$$

Thus we have $\left(\frac{q}{p}\right) = 1$ & $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

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

In either case,

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

QED.