Now: HW4 Solutions.

Quadratic Reciprocity

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

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

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

4. ∞ many primes 3 mod 8.

$$\left(\frac{47}{67}\right) = \left(\frac{67}{47}\right)(-1)^{\frac{47-1}{2}\cdot\underbrace{\frac{67-1}{2}}_{\text{odd}}}.$$

$$= -\left(\frac{67}{47}\right) = -\left(\frac{20}{47}\right)$$

$$= -\left(\frac{2^2\cdot 5}{47}\right) = -\cancel{\left(\frac{2}{47}\right)^2}\left(\frac{5}{47}\right)$$

$$= -\left(\frac{5}{47}\right) = -\left(\frac{47}{5}\right)(-1)^{\underbrace{\frac{5-1}{2}\cdot\frac{47-1}{2}}_{\text{even}}}$$

$$= -\left(\frac{47}{5}\right) = -\left(\frac{2}{5}\right)$$

Is 2 square mod 5? NO.

a	1	2	3	4
a^2	1	4	4	1

$$= -(-1) = +1.$$

Conclusion: 47 <u>is square</u> mod 67.

Since 67 is prime, there are exactly two square roots. My computer found them:

$$\sqrt{47} = 28 \text{ or } 39 \mod 67.$$

$$\left(\frac{-1}{p}\right) = \begin{cases} +1 & p = 1 \mod 4 \\ -1 & p = 3 \mod 4 \end{cases}$$

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

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

$$= \begin{cases} +1 & p \equiv 1\ (4)\ \&\ p \equiv 1,7\ (8) \\ +1 & p \equiv 3\ (4)\ \&\ p \equiv 3,5\ (8) \\ -1 & p \equiv 1\ (4)\ \&\ p \equiv 3,5\ (8) \\ -1 & p \equiv 3\ (4)\ \&\ p \equiv 1,7\ (8) \end{cases}$$

$$= \begin{cases} +1 & p \equiv 1 \bmod 8 \\ +1 & p \equiv 3 \bmod 8 \\ -1 & p \equiv 5 \bmod 8 \\ -1 & p \equiv 7 \bmod 8 \end{cases} = \begin{cases} +1 & p \equiv 1,3\ (8) \\ -1 & p \equiv 5,7\ (8) \end{cases}$$

---

4. Let $p_1, \dots, p_k$ be any primes of the form 3 mod 8. We will find <u>another</u> prime $p \equiv 3 \bmod 8$ that is not in the list.

TRICK: $N = (p_1 p_2 \cdots p_k)^2 + 2$.

Since $p_i \equiv 3 \bmod 8$

$p_i^2 \equiv 1 \bmod 8$

we have

$$N = p_1^2 p_2^2 \cdots p_k^2 + 2$$
$$= 1 \cdot 1 \cdots 1 + 2 = 3 \mod 8.$$

(In particular, N is odd.)

For any prime $p | N$ we have

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

$$\Rightarrow \left(\frac{-2}{p}\right) = +1$$

$$\Rightarrow p = 1 \text{ or } 3 \mod 8.$$

Now factor N into primes:

$$N = q_1 q_2 \cdots q_\ell$$

we know $q_i = 1$ or $3 \mod 8$ $\forall i$.

Suppose $q_i = 1 \mod 8$ $\forall i$. Then

$N \equiv 1 \cdot 1 \cdots 1 \equiv 1 \mod 8.$

Contradicts the fact $N \equiv 3 \mod 8$.

Therefore $\exists$ some factor $q_i \equiv 3 \mod 8$.

We have shown $\exists$ prime p such that $p \mid N$ (i.e. $N \equiv 0 \mod p$) and $p \equiv 3 \mod 8$. I claim that this p is not in the list $p_1, p_2, \dots, p_k$.

Indeed, for any i we have

$$N = p_i(\text{something}) + 2$$
$$\equiv 2 \mod p_i$$

If $p = p_i$ then this contradicts the fact that $N \equiv 0 \mod p$.

(Because $p \neq 2$ hence $0 \not\equiv 2 \mod p$.)

Q.E.D.

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

Q.R.: $$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)(-1)^{\cancel{\frac{3-1}{2}}\,\frac{p-1}{2}}$$

$$= \left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}}$$

$$\left(\frac{p}{3}\right) = \begin{cases} +1 & p \equiv 1 \bmod 3 \\ -1 & p \equiv 2 \bmod 3. \end{cases}$$

$$(-1)^{\frac{p-1}{2}} = \begin{cases} +1 & p \equiv 1 \bmod 4 \\ -1 & p \equiv 3 \bmod 4. \end{cases}$$

Hence:

$$\left(\frac{3}{p}\right) = \begin{cases} +1 & p \equiv 1\,(3) \;\&\; p \equiv 1\,(4) & p \equiv 1\,(12) \\ +1 & p \equiv 2\,(3) \;\&\; p \equiv 3\,(4) & p \equiv 11\,(12) \\ -1 & p \equiv 1\,(3) \;\&\; p \equiv 3\,(4) & p \equiv 7\,(12) \\ -1 & p \equiv 2\,(3) \;\&\; p \equiv 1\,(4) & p \equiv 5\,(12) \end{cases}$$

Recall the CRT bijection

$$(\mathbb{Z}/12\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/4\mathbb{Z})^\times$$

$x \bmod 12$	$(x \bmod 3, x \bmod 4)$
1	(1, 1)
5	(2, 1)
7	(1, 3)
11	(2, 3)

Summary:

$$\left(\frac{3}{p}\right) = \begin{cases} +1 & p \equiv 1, 11 \bmod 12 \\ -1 & p \equiv 5, 7 \bmod 12 \end{cases}$$

Does this simplify any further?

Actually there is a pattern.

For odd primes $p \neq q$ it is true that

$$\boxed{\left(\frac{q}{p}\right) = +1 \iff p \equiv \pm \beta^2 \bmod 4q, \text{ for an odd integer } 1 \leq \beta < \sqrt{4q}.}$$

Example:

$$\left(\frac{7}{p}\right) = +1 \iff p \equiv \pm 1, \pm 9, \pm 25 \bmod 28.$$

It turns out this is hard to prove.
Actually, it is equivalent to Q.R.

The end of Q.R. (for us).

What Next?

Solve the equation $x^2 + y^2 = z$ by studying prime factorization in the ring of "Gaussian integers"

$$\mathbb{Z}[\sqrt{-1}] = \{ a + b\sqrt{-1} : a, b \in \mathbb{Z} \}.$$

It turns out this ring has the "unique prime factorization" property.

We will prove a more general result that also applies to the rings

$$\mathbb{Z}, \ \mathbb{Z}[\sqrt{-2}], \ \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right], \text{ and others} \ldots$$

First let's just think about $\mathbb{Z}$.

Def: Say $p \in \mathbb{Z}$ is <u>prime</u> if for all $a \in \mathbb{Z}$,

$$a \mid p \Rightarrow a = 1 \text{ or } a = p.$$

This implies that 1 is prime.
Do we want that?

Fancier Definition: First note that

$$ab = 1 \Longrightarrow a = +1 \text{ or } -1.$$

We say that ± 1 are the <u>units</u> of the ring $\mathbb{Z}$, i.e., the elements that have "multiplicative inverse."

Say $p \in \mathbb{Z}$ is <u>prime</u> if $\forall a, b \in \mathbb{Z}$,

$$p = ab \Longrightarrow a = \pm 1 \text{ or } b = \pm 1$$

(a or b is a unit).

$$(|a| = 1 \text{ or } |b| = 1)$$

Note: This definition allows negative

numbers to be prime.

$\pm 2, \pm 3, \pm 5, \pm 7, \ldots$ are prime.

What about ± 1 ?

Rephrase: p is prime if

- p not a unit
- $p = ab \Rightarrow a$ or b is a unit.

Same idea works in the ring of polynomials $\mathbb{F}[x]$ over a field $\mathbb{F}$.

What are the units ?

When is $\frac{1}{f(x)}$ a polynomial ?

Answer : When $f(x)$ is a nonzero constant.

Def: Polynomial $f(x) \in \mathbb{F}[x]$ is prime (a.k.a. "irreducible") when

- $f(x)$ not a unit
- $f(x) = g(x)h(x) \Rightarrow g(x)$ or $h(x)$ is a unit.

Example: $x^2+1 \in \mathbb{Q}[x]$ is prime.

So is $2x^2+2$. For any $0 \neq a \in \mathbb{Q}$,

the polynomial $ax^2+a \in \mathbb{Q}[x]$ is prime

What about Gaussian integers?

What are the units?

$i = \sqrt{-1}$

$(a+bi)(c+di) = 1 + 0i$.

TRICK: Consider the squared absolute value.

$|a+bi|^2 |c+di|^2 = |1+0i|^2$

$(a^2+b^2)(c^2+d^2) = 1$

$\Rightarrow \quad a^2+b^2 = \pm 1$

$a^2+b^2 = +1$ (positive).

Since $a, b \in \mathbb{Z}$ this implies that

$(a,b) = (1,0), (-1,0), (0,1), (0,-1)$

$a+bi = 1, -1, i, -i$.

The ring $\mathbb{Z}[i]$ has <u>4 units</u>

For the purpose of factorization we should just ignore the units.

Def: Say $a+bi \in \mathbb{Z}[i]$ is prime if

- $a+bi \notin \{\pm 1, \pm i\}$
- for all $\alpha, \beta \in \mathbb{Z}[i]$,

$$a+bi = \alpha\beta \implies \alpha \in \{\pm 1, \pm i\} \text{ or } \beta \in \{\pm 1, \pm i\}.$$

Sounds complicated, but need to define it this way if we want unique factorization.

Examples:

$$5 = 2^2 + 1^2 = (2+i)(2-i)$$

So $5 \in \mathbb{Z}$ is prime but $5 \in \mathbb{Z}[i]$ is <u>not</u> prime.

More generally, if a prime $p \in \mathbb{Z}$ can be written as $p = a^2+b^2$ for some $a, b \in \mathbb{Z}$, Then p is not a "Gaussian prime" because

$$p = a^2 + b^2 = (a+bi)(a-bi)$$

It will turn out that odd prime $p \in \mathbb{Z}$ is a Gaussian prime $\Longleftrightarrow$ $p \equiv 3 \bmod 4$.

To prove uniqueness there are two steps.

(1) Show that every number is a product of primes.

(2) Show that for a, b, p with p prime we have $\boxed{p \mid ab \Rightarrow p \mid a \text{ or } p \mid b.}$
"Euclid's Lemma"

Quick Example: Suppose

$$p_1 p_2 = q_1 q_2 \quad (p_1, p_2, q_1, q_2 \text{ prime})$$

$$p_1 \mid q_1 q_2 \Rightarrow p_1 \mid q_1 \text{ or } p_1 \mid q_2.$$

Say $p_1 | q_1$. Say $q_1 = p_1 k$.

Since q_1 is prime this means

~~p_1 unit~~ or k unit. ✓

Conclude $p_1 = q_1$ (some unit).

$p_1 \sim q_1$ "basically the same".

Then it also follows that

$p_2 \sim q_2$.

Hence $p_1 p_2 = q_1 q_2$ "uniqueness"

$\Longrightarrow$ $p_1 \sim q_1$ & $p_2 \sim q_2$