Now that we have studied primitive roots we return to studying quadratic congruences. Recall we were interested in determining for which values of a the congruence

$$x^2 \equiv a \pmod{p}$$

has a solution. Also recall the following definition:

Def: Let p be prime and $a \in \mathbb{Z}$ w/ $\gcd(a,p)=1$. If there is a solution to $x^2 \equiv a \pmod{p}$ we say a is a quadratic residue of p; if there is no solution we say a is a quadratic nonresidue of p.

The first result we prove is Euler's criterion. It basically finishes the problem theoretically. It is very useful for proving theorems and computing with small values of p. However, it is not something to use for large p. The quadratic reciprocity law will give us an effective way to work with large primes.

Thm (Euler's criterion): Let p be an odd prime, $a \in \mathbb{Z}$ w/ $\gcd(a,p)=1$. Then a is a quadratic residue of p iff $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Proof: "$\Rightarrow$" Let a be a quadratic residue modulo p. So $\exists y$ s.t. $y^2 \equiv a \pmod{p}$. Raising both sides to $\frac{p-1}{2}$ we have

$y^{p-1} \equiv a^{\frac{p-1}{2}} \pmod{p}$. However, $y^{p-1} \equiv 1 \pmod{p}$ by Euler's theorem, then $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

"$\Leftarrow$" Suppose $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Let r be a primitive root modulo p. There exists $k \in \mathbb{Z}$ s.t. $r^k = a$. We have

$$(r^k)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Thus, $r^{\frac{k(p-1)}{2}} \equiv 1 \pmod{p} \Rightarrow \frac{k(p-1)}{2} \mid (p-1)$

$\Rightarrow 2 \mid k$. So $\exists j \in \mathbb{Z}$ s.t. $k = 2j$. Thus,

$$(r^j)^2 \equiv a \pmod{p}.$$

And so a is a quadratic residue. ∎

One should note that since $(a^{\frac{p-1}{2}})^2 = a^{p-1} \equiv 1 \pmod{p}$, we must have $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$. (We saw before the only x w/ $x^2 \equiv 1 \pmod{p}$ is $x = \pm 1$). So we could write Euler's criterion as "a is quadratic nonresidue iff $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.",

Example: Consider the prime 137. (Use SAGE here).

Observe that $3^{\frac{137-1}{2}} \equiv -1 \pmod{137}$, so 3 is a quadratic nonresidue. 5 is the same.

Observe that $7^{\frac{137-1}{2}} \equiv 1 \pmod{137}$, so 7 is a quadratic residue modulo 137.

We now introduce the Legendre symbol. It is a useful shorthand for talking about quadratic residues.

Def: Let p be an odd prime and $a \in \mathbb{Z}$. The <u>Legendre symbol</u> $\left(\frac{a}{p}\right)$ is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue of } p \\ -1 & \text{if } a \text{ is a quadratic nonresidue of } p \\ 0 & \text{if } p \mid a. \end{cases}$$

Example: $p = 137$

$\left(\frac{3}{137}\right) = -1$

$\left(\frac{5}{137}\right) = -1$

$\left(\frac{7}{137}\right) = 1.$

In SAGE the command is

legendre_symbol(a,p)

(didn't work for me..., use

kronecker(a,p) instead!)

Thm: Let p be an odd prime and $a, b \in \mathbb{Z}$.

1. If $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
2. If $\gcd(a,p) = 1$, then $\left(\frac{a^2}{p}\right) = 1$
3. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$
4. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
5. $\left(\frac{1}{p}\right) = 1$, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Proof: Most of these are very easy. We prove property 4 as it

is the only one that really requires any work. Using ③ we have

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}.$$

Then, $\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}$. If $p \mid a$ or $p \mid b$, then the statement is clear that $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. Assume $p \nmid a$, $p \nmid b$. Then $\left(\frac{ab}{p}\right) = \pm 1$, $\left(\frac{a}{p}\right), \left(\frac{b}{p}\right) = \pm 1$. Since p is odd, we have that $\left(\frac{ab}{p}\right) \equiv \pm 1 \pmod{p}$ iff $\left(\frac{ab}{p}\right) = \pm 1$. Thus, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. ∎

<u>Cor:</u> If p is an odd prime, then

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4} \end{cases}$$

<u>Example:</u> Determine if $X^2 \equiv 12 \pmod{37}$ has any solutions. If it does, find them.

We are asking if 12 is a quadratic residue of 37. This is the same as asking to determine $\left(\frac{12}{37}\right)$.

$$\left(\frac{12}{37}\right) = \left(\frac{2^2 \cdot 3}{37}\right) = \left(\frac{2^2}{37}\right)\left(\frac{3}{37}\right)$$

$$= \left(\frac{3}{37}\right)$$

$$\equiv 3^{\frac{36}{2}} \equiv 3^{18}$$

$$\equiv 1 \pmod{37}.$$

Thus, there is a solution! Now we just check the elements to

see which is a solution.

$$7^2 \equiv 12 \pmod{37}$$

Thus, 7 and $37-7=30$ are the two solutions!

Thm: Let p be an odd prime. Then

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0.$$

Proof: Let r be a primitive root modulo p. Then for each $1 \le a \le p-1$, there exists a unique k $1 \le k \le p-1$ so that $a = r^k$. Thus,

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv \left(r^k\right)^{\frac{p-1}{2}} = \left(r^{\frac{p-1}{2}}\right)^k$$

$$\equiv (-1)^k \pmod{p}.$$

Here we have used that for a primitive root r, $r^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

This is in fact a homework problem!

Thus, for each a we have

$$\left(\frac{a}{p}\right) \equiv (-1)^k \pmod{p}.$$

Since $(-1)^k = \pm 1$, we have $\left(\frac{a}{p}\right) = (-1)^k$. The pigeonhole principle applied to associating the a's with the k's gives

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = \sum_{k=1}^{p-1} (-1)^k = 0.$$

∎

Cor: There are the same number of quadratic residues as nonresidues.

Proof: If there were more quadratic residues, then

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) > 0.$$

Similarly for more quadratic nonresidues. ∎

Cor: Let r be a primitive root modulo p. All of the quadratic residues modulo p occur as $r^2, r^4, \ldots, r^{p-1}$ and all the nonresidues occur as $r, r^3, r^5, \ldots, r^{p-2}$.

Proof: We know $r, r^2, \ldots, r^{p-1}$ are all of the distinct elements modulo p since r is primitive. Half of these must be quadratic residues by the previous corollary. It is easy to see the even powers are quadratic residues:

$$(r^n)^2 \equiv r^{2n} \pmod{p}.$$

Since this accounts for half of the elements, it must be the other half are nonresidues. ∎

The following lemma will be fundamental in our proof of the quadratic reciprocity law:

Gauss' Lemma: Let p be an odd prime and let $a \in \mathbb{Z}$ s.t $\gcd(a,p)=1$. Let n be the ~~con~~ number of element in the set

$$S = \{a, 2a, 3a, \ldots, \left(\tfrac{p-1}{2}\right)a\}.$$

whose remainder upon division by p exceed $p/2$. Then

$$\left(\frac{a}{p}\right) = (-1)^n.$$

Before we prove this lemma, we state the quadratic reciprocity law as it is our ultimate goal here.

Quadratic Reciprocity Law: Let p and q be distinct odd primes. Then

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

Let us compute an example using this law to see its power.

Example: Determine if the equation

$$X^2 \equiv 5 \pmod{123479}$$

has any solutions.

So we want to determine

$$\left(\frac{5}{123479}\right).$$

Quadratic reciprocity shows:

$$\left(\frac{5}{123479}\right)\left(\frac{123479}{5}\right) = (-1)^{\frac{123479}{2}\cdot\frac{4}{2}} = 1.$$

Thus, $\left(\frac{5}{123479}\right) = \left(\frac{123479}{5}\right)$ since each is ± 1.

We now apply the fact that if $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Since $123479 \equiv 4 \pmod{5}$, we have

$$\left(\frac{5}{123479}\right) = \left(\frac{4}{5}\right) = \left(\frac{2^2}{5}\right) = 1.$$

So there are solutions! This is much easier than computing

$$5^{\frac{123479-1}{2}} \pmod{123479}.$$

We will see many more applications of quadratic reciprocity after we have proven it. Before we prove Gauss' lemma we illustrate it with an example.

Example: Let $p = 17$, $a = 3$. Then $\frac{p-1}{2} = 8$, so

$$S = \{3, 6, 9, 12, 15, 18, 21, 24\}$$

Modulo p,

$$S = \{3, 1, 3, 4, 6, 7, 9, 12, 15\}.$$

Thus, only $9, 12, 15$ are larger than $\frac{p}{2} = 8.5$, so

$$\left(\frac{3}{17}\right) = (-1)^3 = -1.$$

One can check this by computing

$$3^8 \equiv -1 \pmod{17}$$

Proof (Gauss' lemma): We begin by observing that since $\gcd(a,p)=1$, none of the elements in S are congruent to $0 \bmod p$ and none are congruent to each other. (Check this!). Let $r_1, \dots, r_m$ be the elements that are between 0 and $p/2$ when reduced modulo p and $s_1, \dots, s_n$ the ones that reduce to between $p/2$ and p. Note that $m+n = \frac{p-1}{2}$.

Claim: $p - s_i \neq r_j$ for all $1 \le i \le n$, $1 \le j \le m$.

Pf: Suppose $\exists\, i,j$ s.t. $p - s_i = r_j$. Then we know $\exists$ u, v s.t. $1 \le u, v \le \frac{p-1}{2}$,

$$s_i \equiv ua \pmod{p}$$

$$r_j \equiv va \pmod{p}.$$

Thus,

$$(u+v)a \equiv s_i + r_j \equiv 0 \pmod{p}.$$

$\Rightarrow u+v \equiv 0 \pmod{p}$ # because $u+v \le \frac{p-1}{2} + \frac{p-1}{2} = p-1$. □

So we have $\frac{p-1}{2}$ distinct numbers $r_1, \dots, r_m, p-s_1, \dots, p-s_n$ between 1 and $\frac{p-1}{2}$, all lying in S. The pigeonhole principle gives that these must be exactly the integers $1, 2, \dots, \frac{p-1}{2}$ in some order.

Thus,

$$r_1 r_2 \cdots r_m (p-s_1) \cdots (p-s_n) \equiv \left(\tfrac{p-1}{2}\right)! \pmod{p}$$

$$\Vert$$

$$r_1 r_2 \cdots r_m (-s_1) \cdots (-s_n)$$

$$\Vert$$

$$(-1)^n r_1 \cdots r_m s_1 \cdots s_n$$

However, we also know that $r_1, \dots, r_m, s_1, \dots, s_n$ are precisely the elements of S in some order. Then,

$$r_1 r_2 \cdots r_m s_1 s_2 \cdots s_n \equiv a \cdot 2a \cdots \left(\tfrac{p-1}{2}\right)a \pmod{p}$$

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

Combining these equations we have:

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

Since $\frac{p-1}{2} < p$, we have $\gcd(p, \frac{p-1}{2}) = 1$ and thus we can cancel the $\frac{p-1}{2}$ to obtain

$$(-1)\, a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

I.e.,

$$a^{\frac{p-1}{2}} \equiv (-1)^n \pmod{p}.$$

Now just use that $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$. ∎

We need one more lemma before quadratic reciprocity. This lemma will allow us to rephrase what Gauss' lemma says in a way that can be applied to quadratic reciprocity.

<u>Lemma:</u> Let p be an odd prime and a an odd integer s.t. $\gcd(a, p) = 1$.

Then

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor}.$$

Proof: As in the previous proof, set

$$S = \{ a, 2a, \ldots, \left(\tfrac{p-1}{2}\right)a \}.$$

Write

$$ka = q_k p + t_k$$

for $q_k \in \mathbb{Z}_{\geq 0}$, $1 \leq t_k \leq p-1$ by the division algorithm.

Then we have $\frac{ka}{p} = q_k + \frac{t_k}{p} \Rightarrow \left\lfloor \frac{ka}{p} \right\rfloor = q_k$.

Thus, given $ka \in S$, we have

$$(*) \qquad ka = \left\lfloor \frac{ka}{p} \right\rfloor p + t_k .$$

Recall that if $t_k < p/2$ it is among what we denoted as

$r_1, \ldots, r_m$ and if $t_k > p/2$ it is among $s_1, \ldots, s_n$.

Sum over all the equations $(*)$ for $ka \in S$:

$$\sum_{k=1}^{\frac{p-1}{2}} ka = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor p + \sum_{k=1}^{m} r_k + \sum_{k=1}^{n} s_k . \qquad (**)$$

We use again that $r_1, \ldots, r_m, p-s_1, \ldots, p-s_n$ are just the integers $1, \ldots, \frac{p-1}{2}$ in a get:

$$\sum_{k=1}^{\frac{p-1}{2}} k = \sum_{k=1}^{m} r_k + \sum_{k=1}^{n} (p - s_k) = pn + \sum_{k=1}^{m} r_k - \sum_{k=1}^{n} s_k .$$

Subtracting this from $(**)$ we have

$$(a-1) \sum_{k=1}^{\frac{p-1}{2}} ka = p\left(\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor - n \right) + 2 \sum_{k=1}^{n} s_k$$

Looking at this modulo 2 we have: (since we are interested in a power of (-1) this is enough!)

$$0 \cdot \sum_{k=1}^{\frac{p-1}{2}} k \equiv 1 \left(\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor - n \right) \pmod 2$$

i.e,

$$n \equiv \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor \pmod 2.$$

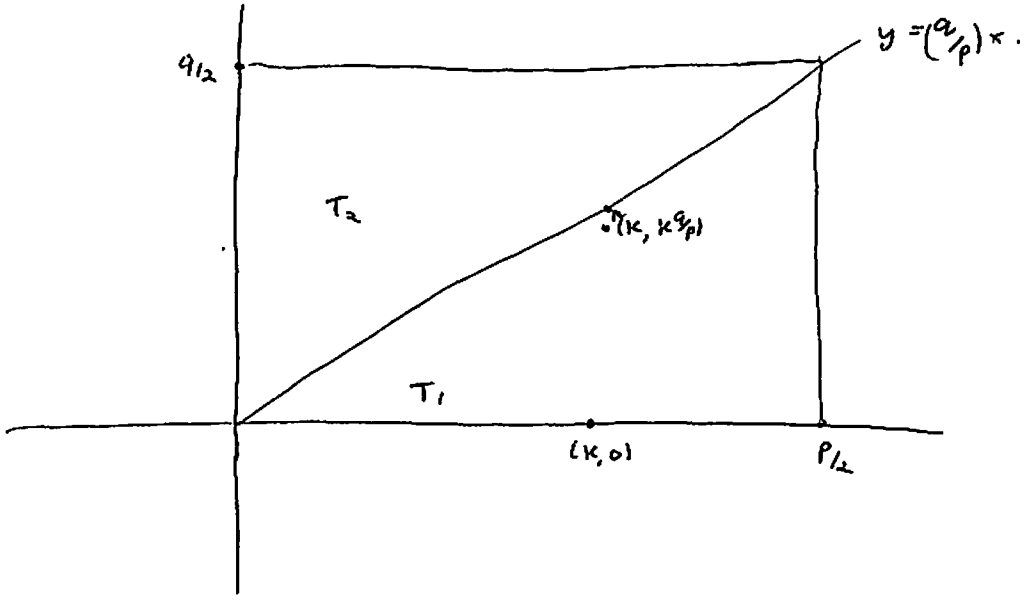
Now we apply Gauss' lemma:

$$\left(\frac{a}{p}\right) = (-1)^n = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor}.$$

∎

The proof of quadratic reciprocity will use some geometry, as was encountered in a previous proof.

Proof (quadratic reciprocity): Consider the following rectangle



What we will do is count the number of lattice points in this rectangle in two different ways to arrive at the result.

↑ not counting the edges!

Since p and q are odd, there are precisely

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

lattice points in the rectangle. This is the first way. Now consider the diagonal across the rectangle. It is a line w/ equation $y = \frac{qx}{p}$. Since $gcd(p,q) = 2$, none of the lattice points can be on the diagonal. We now count the lattice points in T_1 and in T_2.

We begin with T_1. Consider a point $(k,0)$ on the x-axis. The number of integers in the interval $0 < y < k\frac{q}{p}$ is precisely $\left\lfloor \frac{kq}{p} \right\rfloor$. So for any k w/ $0 < k < p/2$, we have precisely $\left\lfloor \frac{kq}{p} \right\rfloor$ lattice points on the line above $(k,0)$ below the diagonal. Thus, there are $\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor$ lattice points in T_1. Similarly, there are $\sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor$ lattice points in T_2. Thus,

$$\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right) = \sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor.$$

Applying the previous lemma we have

$$(-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)} = (-1)^{\sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor}$$

$$= \left(\frac{q}{p}\right)\left(\frac{p}{q}\right)$$

as desired. □

Thm: Let p be an odd prime. Then

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

Proof: Since 2 is clearly not an odd prime, we cannot use quadratic reciprocity here. Instead we apply Gauss' lemma with $a = 2$. The set S is then:

$$\{2, 4, 6, \ldots, p-1\}.$$

Since these are all less than p, reducing modulo p does not change anything.

Let $p = 8k+1$. Then $\frac{p}{2} = 4k + \frac{1}{2}$ and so our $s_1, \ldots, s_n$ are $\{4k+2, 4k+4, \ldots, 8k\}$. There are $2k$ elements in this set so $\left(\frac{2}{p}\right) = (-1)^{2k} = 1$ in this case.

Let $p = 8k-1$. Then $p/2 = 4k - \frac{1}{2}$ and so the $s_1, \ldots, s_n$ are $\{4k, 4k+2, \ldots, 8k-2\}$. Again there are $2k$ elements in this set so $\left(\frac{2}{p}\right) = (-1)^{2k} = 1$.

Let $p = 8k+3$ so $\frac{p}{2} = 4k + \frac{3}{2}$. Then $s_1, \ldots, s_n$ are $\{4k+2, 4k+4, \ldots, 8k+2\}$. There are $2k+1$ elements in this set so $\left(\frac{2}{p}\right) = (-1)$ in this case.

Finally, let $p = 8k+5$. Then $p/2 = 4k + \frac{5}{2}$ and $s_1, \ldots, s_n$ are $\{4k+4, 4k+6, \ldots, 8k+4\}$. Again there are $2k+1$ elements and so $\left(\frac{2}{p}\right) = -1$ in the case. ∎

Example: Determine if $x^2 \equiv 60 \pmod{83}$ has any solutions.

First note that 83 is prime, so we really just want to determine if $\left(\frac{60}{83}\right) = 1$ or not.

$60 = 2^2 \cdot 3 \cdot 5$, so $\left(\frac{60}{83}\right) = \left(\frac{2^2}{83}\right)\left(\frac{3}{83}\right)\left(\frac{5}{83}\right)$

$= \left(\frac{3}{83}\right)\left(\frac{5}{83}\right)$

$\left(\frac{3}{83}\right)\left(\frac{83}{3}\right) = (-1)^{\left(\frac{3-1}{2}\right)\left(\frac{83-1}{2}\right)} = (-1)$

$83 \equiv 2 \pmod{3}$, so $\left(\frac{83}{3}\right) = \left(\frac{2}{3}\right) = 2^{\frac{3-1}{2}} \pmod{3}$

$= 2 \equiv -1 \pmod{3}$

Thus, $\left(\frac{83}{3}\right) = -1 \Rightarrow \left(\frac{3}{83}\right) = 1$

$\left(\frac{5}{83}\right)\left(\frac{83}{5}\right) = (-1)^{\left(\frac{5-1}{2}\right)\left(\frac{83-1}{2}\right)} = 1.$

$83 \equiv 3 \pmod{5}$, so $\left(\frac{83}{5}\right) = \left(\frac{3}{5}\right)$ Thus,

$\left(\frac{3}{5}\right)\left(\frac{5}{3}\right) = (-1)^{\left(\frac{3-1}{2}\right)\left(\frac{5-1}{2}\right)} = 1.$

$\left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1.$

Thus, $\left(\frac{3}{5}\right) = -1 \Rightarrow \left(\frac{5}{83}\right) = -1.$

Combining all of the we have

$$\left(\frac{60}{83}\right) = -1$$

So there are no solutions to the congruence.

Thm: Let $p > 3$ be an odd prime. Then

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{12} \\ -1 & \text{if } p \equiv \pm 5 \pmod{12} \end{cases}$$

Proof: The q.r. law gives that

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

Now $\left(\frac{p}{3}\right) = \left(\frac{r}{3}\right)$ when $p \equiv r \pmod 3$. There are only two possible choices here, $r = 1, 2$. If $r = 1$, then $\left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1$.

Thus, if $p \equiv 1 \pmod 3$ then $\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}$.

If $r \equiv 2 \pmod 3$, then $\left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1$. Thus,

if $p \equiv 2 \pmod 3$, then $\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot (-1)$.

We know that $(-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$

Thus, if $p \equiv 1 \pmod 4$ and $p \equiv 1 \pmod 3$, then $\left(\frac{3}{p}\right) = 1$.

i.e. if $p \equiv 1 \pmod{12}$ then $\left(\frac{3}{p}\right) = 1$.

Similarly, if $p \equiv 3 \pmod 4$ and $p \equiv 1 \pmod 3$, then $\left(\frac{3}{p}\right) = -1$.

$\Leftrightarrow$ if $p \equiv 7 \pmod{12} \equiv -5 \pmod{12}$ (CRT!)

If $p \equiv 1 \pmod 4$ and $p \equiv 2 \pmod 3$, then $\left(\frac{3}{p}\right) = -1$.

$\Leftrightarrow p \equiv 5 \pmod{12}$.

If $p \equiv 3 \pmod 4$ and $p \equiv 2 \pmod 3$, then $\left(\frac{3}{p}\right) = 1$.

$\Leftrightarrow p \equiv -1 \pmod{12}$. ∎

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

Proof: Suppose there are only finitely many, say $p_1, \dots, p_n$. Consider $N = (8p_1 \cdots p_n)^2 + 2$. There is at least one prime p that divides N. Thus,

$$(8p_1 \cdots p_n)^2 \equiv -2 \pmod{p}$$

$\Rightarrow \left(\frac{-2}{p}\right) = 1$. So we need to calculate when this happens.

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

We know $\left(\frac{-1}{p}\right) = \begin{cases} 1 & p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$ and

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

We need either $\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = 1$ or $\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = -1$.

Observe that if $p \equiv 1 \pmod 4$, then $p \not\equiv -1 \pmod 8$ and if $p \equiv 3 \pmod 4$, then $p \not\equiv -3 \pmod 8$. Then our two possibilities are $p \equiv 1 \pmod 8$ or $p \equiv 3 \pmod 8$. If all primes $p \mid N$ are $\equiv 1 \pmod 8$, then $N \equiv 1 \pmod 8$. But $N \equiv 2 \pmod 8$. Thus there is at least one $p \mid N$ s.t. $p \equiv 3 \pmod 8$. But then $p \mid N$ and $p \mid (8p_1 \cdots p_n)^2 \Rightarrow p \mid 2$. $\#$ since $p \equiv 3 \pmod 8$. Thus there must be ∞'ly many primes of the form $8k+3$. ∎

We have now completely solved the problem of determining when

$$X^2 \equiv a \pmod{p}$$

has a solution for p a prime number. We would now like to deal with the equation

$$X^2 \equiv a \pmod{n} \qquad (*)$$

for n composite. First observe that if $a \equiv 0 \pmod{n}$ then $x = 0$ is clearly a solution so we restrict ourselves to the case that $a > 0$. Write $n = p_1^{e_1} \cdots p_r^{e_r}$ with $p_i \neq p_j$ if $i \neq j$. First suppose there is a solution to $(*)$. Then clearly we have solutions to

$$\begin{aligned} X^2 &\equiv a \pmod{p_1^{e_1}} \\ &\vdots \\ X^2 &\equiv a \pmod{p_r^{e_r}}, \end{aligned} \qquad (**)$$

namely just reduce our original solution modulo $p_i^{e_i}$ for each i. Conversely, suppose we have a solutions to the equations $(**)$. Then we have $X \equiv c_i \pmod{p_i^{e_i}}$ for some c_i. Using the CRT we obtain an X mod n so that $X \equiv c_i \pmod{p_i^{e_i}}$, so this X gives a solution to $(*)$. Thus, solving $(*)$ is equivalent to solving

$$X^2 \equiv a \pmod{p^k}$$

for prime powers. We now study this problem.

We begin with the case that we have an odd prime p and $\gcd(a,p)=1$.

Recall the theorem we proved before dealing with solutions to congruences of the form

$$f(x) \equiv 0 \pmod{p^n}.$$

<u>Thm (from early this term)</u>: Let $f(x) \in \mathbb{Z}[x]$ w/ $\deg f \geq 1$. Let p be a prime and $n \geq 1$. Let x_1 be a solution to the congruence

$$f(x) \equiv 0 \pmod{p^n}.$$

Then x_1 lifts to a solution to the congruence

$$f(x) \equiv 0 \pmod{p^{n+1}}$$

iff there is a solution t to the congruence

$$t f'(x_1) \equiv \frac{-f(x_1)}{p^n} \pmod{p}. \qquad (1)$$

In particular, if we let h be the number of solutions to (1), then

$$h = \begin{cases} 1 & \text{if } p \nmid f'(x_1) \\ 0 & \text{if } p \mid f'(x_1) \text{ and } p^{n+1} \nmid f(x_1) \\ p & \text{if } p \mid f'(x_1) \text{ and } p^{n+1} \mid f(x_1). \end{cases}$$

Note that if none of the solutions to

$$f(x) \equiv 0 \pmod{p^n}$$

lift to a solution modulo p^{n+1}, then there are no solutions!

We use this to give an easy proof of the following theorem:

Thm: Let p be an odd prime and $a \in \mathbb{Z}$ w/ $\gcd(a,p)=1$. Then

$$X^2 \equiv a \pmod{p^k}$$

has a solution iff $\left(\frac{a}{p}\right)=1$.

Proof: First observe that if $X^2 \equiv a \pmod{p^k}$ has a solution, so does

$$X^2 \equiv a \pmod{p}$$

and so $\left(\frac{a}{p}\right)=1$.

Suppose now that $\left(\frac{a}{p}\right)=1$. Observe that solving

$$X^2 \equiv a \pmod{p^k}$$

is the same as solving

$$f(x) \equiv 0 \pmod{p^k}$$

where $f(x) = x^2 - a$. Now $p \nmid a$ since $\gcd(a,p)=1$

and so $p \nmid f'(x)$ for x a solution to $X^2 \equiv a \pmod{p}$.

Thus, this solution lifts to a unique solution modulo p^2,

call it x_2. The same argument shows $p \nmid f'(x_2)$, so

x_2 lifts to x_3 modulo p^3. Thus, we have inductively

solutions for all $k \geq 1$. ∎

We now deal with the case $p=2$. Note that for $k=1$, we

know

$$X^2 \equiv 1 \pmod{2}$$

definitely has a solution. $k=2$ can be handled by agreeing everything odd

modulo 4:

$$1^2 \equiv 1 \pmod{4}$$

$$3^2 \equiv 1 \pmod{4}$$

Thus,

$$X^2 \equiv a \pmod{4}$$

has a solution iff $a \equiv 1 \pmod 4$. We now deal with the general case.

Thm: Let a be an odd integer. The congruence $(k \geq 1)$

$$x^2 \equiv a \pmod{2^k} \qquad (*')$$

has a solution iff $a \equiv 1 \pmod 8$.

Proof: First note that the squares of odd integers modulo 8 are all congruent to 1, thus for $(*')$ to have a solution, there is a solution to

$$x^2 \equiv a \pmod 8$$

$\Rightarrow a \equiv 1 \pmod 8$. (We use here $k \geq 3$ since we have already dealt with $k = 1, 2$). Now we need to show that if $a \equiv 1 \pmod 8$, then

$$x^2 \equiv a \pmod{2^k}$$

always has a solution for $k \geq 3$. We proceed by induction on k. The base case of

$$x^2 \equiv 1 \pmod 8$$

is clear. Assume that

$$x^2 \equiv a \pmod{2^n}$$

has a solution x_0. We produce a solution to

$$x^2 \equiv a \pmod{2^{n+1}}$$

And so have the result by induction.

We know $\exists\, t \in \mathbb{Z}$ s.t

$$x_0^2 = a + 2^n t.$$

Since a is odd, x_0^2 must also be odd, and so x_0 is odd.

Thus there is a $y \in \mathbb{Z}$ s.t

$$X_0 y \equiv -t \pmod 2.$$

Namely, write

$$X_0 \text{ as } \alpha + 2\beta = 1$$

$$\Rightarrow \quad X_0 \alpha(-t) + 2\beta(-t) = -t$$

so $y = \alpha(-t)$.

Consider $X_1 = X_0 + y 2^{n-1}$. Then

$$X_1^2 = (X_0 + y 2^{n-1})^2$$

$$= X_0^2 + y X_0 2^n + y^2 2^{2n-2}$$

$$\equiv a + (t + 2s) 2^n$$

$$\equiv a + 2^n t + y X_0 2^n + 0 \pmod{2^{n+1}} \qquad (2n-2 \geq n+1 \text{ since } n \geq 3)$$

$$\equiv a + 2^n t + (-t + 2s) 2^n \pmod{2^{n+1}} \qquad (\text{some } s \in \mathbb{Z})$$

$$\equiv a + 2^{n+1} s \pmod{2^{n+1}}$$

$$\equiv a \pmod{2^{n+1}}.$$

Thus, $X_0 + y 2^{n-1}$ is a solution mod 2^{n+1} and so we have the result by induction. ∎

We now drop the assumption that $\gcd(a,p)=1$ where we now include $p=2$ as well. Write $a = p^r b$ with $\gcd(p,b)=1$, $r \geq 1$. We split into two cases: r even and r odd.

Suppose r is even, so $\exists s \in \mathbb{Z}$ with $r=2s$. Then our goal is to solve

$$X^2 \equiv p^{2s} b \pmod{p^k}. \qquad (1)$$

If there is a solution y to the congruence

$$X^2 \equiv b \pmod{p^k}, \qquad (2)$$

then we have

$$(y p^s)^2 \equiv p^{2s} b \pmod{p^k}$$

so we have a solution. Since $\gcd(b,p)=1$, a solution to (2) exists iff $\left(\frac{b}{p}\right)=1$ (p odd), $b \equiv 1 \pmod 8$ iff $p=2$. Thus, we are able to reduce this case to the ones already dealt with.

Suppose now that $a = p^r b$ with r odd. Note that if there is a solution to (1), then

$$X^2 \equiv p^r b \pmod{p^k},$$

then $p^r \mid X^2 \Rightarrow p^{\lceil \frac{r}{2} \rceil} \mid X$. Thus we obtain the equation

$$p^{r+1} y^2 = p^r b + p^k t$$

for some $t \in \mathbb{Z}$. Thus, what we want is a solution to the congruence

$$py^2 \equiv b \pmod{p^{k-r}}.$$

However,

$$p^{k-r} \mid (py^2 - b)$$

$$\Rightarrow \quad p \mid (py^2 - b)$$

$$\Rightarrow \quad p \mid b. \qquad \#.$$

Thus there are no solutions if r is odd.

Back to the general case, recall that if we have a solution

$$x^2 \equiv a \pmod{n}, \qquad (*)$$

we obtain a solution

$$x^2 \equiv a \pmod{p^k}$$

for every prime p w/ $p^k \| n$. Thus, if $p^e \| a$ with e odd for some prime $p \mid n$, p odd, or if $a = 2^r b$ w/ $b \not\equiv 1 \pmod{4}$, then there are no solutions to $(*)$. We summarize with the following theorem.

Thm: Let $n = 2^{e_0} p_1^{e_1} \cdots p_r^{e_r}$ w/ p_i odd. The congruence

$$x^2 \equiv a \pmod{n}$$

has a solution iff for each prime p_i, $p_i^{f_i} \| a$ w/ f_i even and $\left(\frac{a/p^{f_i}}{p}\right) = 1$ and

$p_1^{e_1} \cdots p_r^{e_r} \equiv 1 \pmod{8}$ if $e_0 > 0$.