Recall from last time: Let p be an odd prime number.

Def: $\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } p \mid a \\ 1, & \text{if } a \text{ is a quadratic residue modulo } p \\ -1, & \text{if } a \text{ is a quadratic non-residue modulo } p. \end{cases}$

$\left(\frac{a}{p}\right)$ is called the Legendre's symbol.

Properties: ① If $a \equiv b \pmod p$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

② $\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$

③ Euler's criterion: $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$

④ $\left(\frac{a^2}{p}\right) = 1$ for all a s.t. $p \nmid a$.

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

② $\left(\frac{2}{p}\right) = (-1)^{\frac{(p^2-1)}{8}}$

Gauss's Lemma: Let a be an integer, $p \nmid a$.
For any $i \in \{1, 2, \dots, \frac{p-1}{2}\} = S$ we have $ai \equiv \varepsilon_i \cdot f(i) \pmod p$ for unique $\varepsilon_i \in \{\pm 1\}$ and $f(i) \in S$. Then

a) $S = \{f(1), f(2), \dots, f(\frac{p-1}{2})\}$

b) $\left(\frac{a}{p}\right) = (-1)^k$, where k = the number of $i \in S$ s.t. $\varepsilon_i = -1$.

Theorem: $a \in \mathbb{Z}$, $p \nmid a$. Then

$$\left(\frac{a}{p}\right) = \begin{cases} (-1)^{\sum_{i=1}^{(p-1)/2} \left\lfloor \frac{ai}{p} \right\rfloor}, & \text{if } a \text{ is odd} \\ (-1)^{\sum_{i=1}^{(p-1)/2} \left\lfloor \frac{ai}{p} \right\rfloor + \frac{(p^2-1)}{8}}, & \text{if } a \text{ is even.} \end{cases}$$

Theorem B: Let $p \neq q$ be odd prime numbers. Then

$$\sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{qi}{p} \right\rfloor + \sum_{j=1}^{\frac{q-1}{2}} \left\lfloor \frac{pi}{q} \right\rfloor = \frac{(p-1)(q-1)}{4}$$

Theorems A and B imply

Gauss's Quadratic Reciprocity: Let $p \neq q$ be odd primes.

Then $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$.

Jacobi Symbol: Let m be an odd positive integer.

We factor m as a product of primes: $m = p_1 \cdot \ldots \cdot p_k$ (repetition allowed) and define

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right) \cdot \ldots \cdot \left(\frac{a}{p_k}\right)$$

Example: $m = 45 = 3 \cdot 3 \cdot 5$ so

$$\left(\frac{a}{45}\right) = \left(\frac{a}{3}\right) \cdot \left(\frac{a}{3}\right) \cdot \left(\frac{a}{5}\right)$$

The following properties follow easily from the analogous properties of the Legendre's symbol:

a) If $a \equiv b \pmod m$ then $\left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$

b) $\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$ and $\left(\frac{a}{m_1 m_2}\right) = \left(\frac{a}{m_1}\right)\left(\frac{a}{m_2}\right)$

c) If $\gcd(a,m) = 1$ then $\left(\frac{a^2}{m}\right) = 1$

d) $\left(\frac{a}{m}\right) = 0$ if and only if $\gcd(a,m) > 1$.

Warning: If m is not a prime then $\left(\frac{a}{m}\right) = 1$ DOES NOT imply that a is a quadratic residue modulo m.

We are now going to prove the following key properties of the Jacobi symbol.

Theorem (Jacobi's Reciprocity): Let m, n be odd positive integers, $m>1$, $n>1$.

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

(2) $\left(\frac{2}{m}\right)=(-1)^{\frac{m^2-1}{8}}$

(3) $\left(\frac{m}{n}\right)=(-1)^{\frac{(m-1)}{2}\cdot\frac{(n-1)}{2}}\left(\frac{n}{m}\right)$

We first prove the following lemma.

Lemma: Let m, n be odd integers. Then

a) $\frac{mn-1}{2} \equiv \frac{m-1}{2}+\frac{n-1}{2} \pmod 2$

b) $\frac{m^2n^2-1}{8} \equiv \frac{m^2-1}{8}+\frac{n^2-1}{8} \pmod 2$.

Pf: $mn-1=(m-1)(n-1)+(m-1)+(n-1)$

Dividing by 2: $\frac{mn-1}{2}=\frac{(m-1)(n-1)}{2}+\frac{m-1}{2}+\frac{n-1}{2}$.

Since $\frac{(m-1)(n-1)}{2}$ is even, we get a).

We have $m^2n^2-1=(m^2-1)(n^2-1)+(m^2-1)+(n^2-1)$.

Dividing by 8: $\frac{m^2n^2-1}{8}=\frac{(m^2-1)(n^2-1)}{8}+\frac{m^2-1}{8}+\frac{n^2-1}{8}$

Since $\frac{(m^2-1)(n^2-1)}{8}=\frac{(m-1)}{2}\frac{m+1}{2}\frac{n-1}{2}(n+1)$ is even, we get b).

Proof of ①: Let T be the set of all odd integers $m>1$ such that $\left(\frac{-1}{m}\right)=(-1)^{\frac{m-1}{2}}$. T contains all odd prime numbers by the properties of Legendre's symbol.

Suppose $m, n \in T$. Then

$$\left(\frac{-1}{mn}\right)=\left(\frac{-1}{m}\right)\left(\frac{-1}{n}\right)=(-1)^{\frac{m-1}{2}}(-1)^{\frac{n-1}{2}}=(-1)^{\frac{m-1}{2}+\frac{n-1}{2}}=(-1)^{\frac{mn-1}{2}}$$

(The last equality follows from part a) of the Lemma).

Thus $mn \in T$. We see that T contains all odd primes and is closed under multiplication, so T contains all odd integers >1.

Proof of ②. We follow the same idea. Let T be the set of all odd integers $m>1$ s.t. $\left(\frac{2}{m}\right)=(-1)^{\frac{m^2-1}{8}}$. T contains all odd primes by the properties of Legendre's symbol.

If $m, n \in T$ then

$$\left(\frac{2}{mn}\right)=\left(\frac{2}{m}\right)\left(\frac{2}{n}\right)=(-1)^{\frac{m^2-1}{8}}(-1)^{\frac{n^2-1}{8}}=(-1)^{\frac{m^2-1}{8}+\frac{n^2-1}{8}}=(-1)^{\frac{m^2n^2-1}{8}}$$

(The last equality follows from part b) of the Lemma).

Thus $mn \in T$. As before, this implies that T contains all odd integers >1.

Proof of ③. When both m, n are odd primes, ③ follows from Gauss's Quadratic reciprocity.

Suppose now that n is an odd prime and let T be the set of all odd integers $m>1$ such that ③ holds.

If $m_1, m_2 \in T$ then

$$\left(\frac{m_1 m_2}{n}\right)=\left(\frac{m_1}{n}\right)\left(\frac{m_2}{n}\right)=(-1)^{\frac{m_1-1}{2}\frac{n-1}{2}}\left(\frac{n}{m_1}\right)(-1)^{\frac{m_2-1}{2}\frac{n-1}{2}}\left(\frac{n}{m_2}\right)=$$

$$(*)=(-1)^{\left(\frac{m_1-1}{2}+\frac{m_2-1}{2}\right)\left(\frac{n-1}{2}\right)}\left(\frac{n}{m_1}\right)\left(\frac{n}{m_2}\right)=(-1)^{\frac{m_1m_2-1}{2}\frac{n-1}{2}}\left(\frac{n}{m_1m_2}\right)$$

(last equality follows from part a) of the Lemma)

Thus $m_1m_2 \in T$. We see that T contains all odd primes and is closed under multiplication. It follows that T contains all odd integers >1.

So far we proved (3) if one of m, n is prime.

Now fix n and consider the set S of all odd integers $m>1$ for which (3) holds. We proved in the first step that S contains all odd primes. Now if $m_1, m_2 \in S$ then the same calculation as in (*) above shows that $m_1m_2 \in S$. Thus S contains all odd numbers >1. Since n was an arbitrary odd integer >1, (3) is true.

Example: 1013 is a prime number. Is 874 a quadratic residue modulo 1013? We compute $\left(\frac{874}{1013}\right)$ using properties of the Jacobi symbol.

$$\left(\frac{874}{1013}\right)=\left(\frac{2}{1013}\right)\left(\frac{437}{1013}\right)=\underbrace{(-1)^{\frac{1013^2-1}{8}}}_{-1}\underbrace{(-1)^{\frac{437-1}{2}\frac{1013-1}{2}}}_{1}\left(\frac{1013}{437}\right)=$$

$$=(-1)\left(\frac{2\cdot 437+139}{437}\right)=-\left(\frac{139}{437}\right)=-\underbrace{(-1)^{\frac{139-1}{2}\frac{437-1}{2}}}_{1}\left(\frac{437}{139}\right)=$$

$$=-\left(\frac{3\cdot 139+20}{139}\right)=-\left(\frac{20}{139}\right)=-\left(\frac{4}{139}\right)\left(\frac{5}{139}\right)=-(-1)^{\frac{5-1}{2}\frac{139-1}{2}}\left(\frac{139}{5}\right)$$

$$=-\left(\frac{4}{5}\right)=-1$$

Since $\left(\frac{874}{1013}\right) = -1$, 874 is not a square modulo 1013.

We now move to a new topic: Diophantine equations.

Definition: A Pythagorean triple is a triple (a,b,c) of positive integers such that $a^2+b^2=c^2$.

Let (a,b,c) be a Pythagorean triple. Let $k=\gcd(a,b)$. Then $a=ka_1$, $b=kb_1$, $\gcd(a_1,b_1)=1$ and $k^2(a_1^2+b_1^2)=c^2$. Thus $k^2 \mid c^2$ and therefore $k \mid c$, i.e. $c=kc_1$. We have $a_1^2+b_1^2=c_1^2$ and $\gcd(a_1,b_1)=1$.

Claim: $\gcd(c_1,b_1)=1=\gcd(c_1,a_1)$.

In fact, if a prime p divides c_1 and b_1 then $p \mid c_1^2-b_1^2=a_1^2$, so $p \mid a_1$, which is not possible as $\gcd(a_1,b_1)=1$. Thus $\gcd(a_1,b_1)=1$. Similarly $\gcd(a_1,c_1)=1$.

Definition: A Pythagorean triple (a,b,c) is called primitive if $\gcd(a,b)=\gcd(a,c)=\gcd(b,c)=1$.

We see that every Pythagorean triple is of the form (ka,kb,kc) for unique $k \geq 1$ and unique primitive Pythagorean triple (a,b,c).

Suppose now that (a,b,c) is a primitive Pythagorean triple

Claim: c is odd.

Proof: If c is even then $c^2 \equiv 0 \pmod 4$. Since $\gcd(a,c) = 1 = \gcd(b,c)$, a and b must be odd. Then $a^2 \equiv 1 \equiv b^2 \pmod 4$ so $a^2 + b^2 \equiv 2 \pmod 4$. We get $2 \equiv a^2 + b^2 = c^2 \equiv 0 \pmod 4$, which is false. Thus c can not be even.

Now $a^2 + b^2 = c^2$ implies that one of a, b is odd and the other is even. Assume b is even. Then $c-b$, $c+b$ are odd and $a^2 = (c-b)(c+b)$.

Claim: $c-b$, $c+b$ are relatively prime.

In fact if $d \mid c-b$ and $d \mid c+b$ then d is odd (as $c-b$, $c+b$ are odd) and $d \mid (c-b)+(c+b) = 2c$, and $d \mid (c+b)+(c-b) = 2b$. Thus $d \mid 2c$, d odd $\Rightarrow d \mid c$. Similarly, $d \mid 2b$, d odd $\Rightarrow d \mid b$. Since $\gcd(b,c) = 1$ we have $d = 1$. Thus proves $\gcd(c-b, c+b) = 1$.

General fact: If $\gcd(k,l) = 1$ and $kl = m^2$ then both k, l are squares (think about prime factorization of k, l, m).

Thus we conclude that $c-b = a_1^2$, $c+b = a_2^2$ for some odd integers a_1, a_2. Thus:

$$2c = a_1^2 + a_2^2 = \left[(a_1+a_2)^2 + (a_2-a_1)^2\right]/2, \text{ i.e. } c = \left(\frac{a_1+a_2}{2}\right)^2 + \left(\frac{a_2-a_1}{2}\right)^2.$$

$$2b = a_2^2 - a_1^2 = (a_2-a_1)(a_2+a_1), \text{ i.e. } b = 2 \cdot \frac{a_1+a_2}{2} \cdot \frac{a_2-a_1}{2}$$

$$a = a_1 a_2 = \left(\frac{a_1+a_2}{2}\right)^2 - \left(\frac{a_2-a_1}{2}\right)^2.$$

Set $m = \frac{a_1+a_2}{2}$, $n = \frac{a_2-a_1}{2}$. Then $m > n$ and $c = m^2 + n^2$, $b = 2mn$, $a = m^2 - n^2$. Since c is odd, one of m, n is odd and one is even. Also $\gcd(m,n) = 1$ (since $\gcd(a,c) = 1$).

We see that if (a,b,c) is a primitive Pythagorean triple with b even then there exists integers m,n such that: $\gcd(m,n)=1$, $m>n$, m,n have different parity and $a=m^2-n^2$, $b=2mn$, $c=m^2+n^2$.

Conversely, suppose $m>n$, $\gcd(m,n)=1$, m,n have different parity. Let $a=m^2-n^2$, $b=2mn$, $c=m^2+n^2$. Then

$$a^2+b^2=(m^2-n^2)^2+4m^2n^2=m^4-2m^2n^2+n^4+4m^2n^2=m^4+2m^2n^2+n^4=(m^2+n^2)^2=c^2$$

so (a,b,c) is a Pythagorean triple. Also a and c are odd. If $p\mid a$ and $p\mid c$ for some prime p then $p\mid a+c=2m^2$ and $p\mid c-a=2n^2$ so $p\mid m$ and $p\mid n$ (as p is odd) which contradicts $\gcd(m,n)=1$. This means that $\gcd(a,c)=1$ and therefore (a,b,c) is primitive.

<u>Theorem</u>: There is a bijection between primitive Pythagorean triples (a,b,c) with b even and pairs (m,n) of positive integers s.t. $m>n$, $\gcd(m,n)=1$ and m,n of different parity given by:

$$(m,n)\longleftrightarrow(m^2-n^2,2mn,m^2+n^2).$$