Quadratic residues and quadratic reciprocity.

We would like to learn how to answer the following question.

Let p be a prime and $a \in \mathbb{F}_p^\times$ some number.
Is a a square modulo p? In other words, is there some number $b \in \mathbb{F}_p^\times$, s.t. $a = b^2$?

__Example.__ Let $p=11$. Is 3 a square modulo 11?

$1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 9, 4^2 \equiv 5, \underline{\underline{5^2 \equiv 3}}$. Ok, it is, $5^2 \equiv 3$.

What about 7?

$1^2 \equiv 10^2 \equiv 1,\ 2^2 \equiv 9^2 \equiv 4, 3^2 \equiv 8^2 \equiv 9, 4^2 \equiv 7^2 \equiv 5, 5^2 \equiv 6^2 \equiv 3$.

So, 7 is not a square modulo 11.

But checking all the possibilities (taking x^2 for all $x \in \mathbb{F}_p^\times$) does not seem to be a lot of fun. Imagine doing it for $p = 5753006209$ ...

__Remark.__ It is enough to check for the first $\frac{p-1}{2}$ numbers, as $a^2 \equiv (-a)^2$, but still way too much...

Legendre symbol.

__Def-n.__ Let p be a prime and $a \in \mathbb{F}_p^\times$. The __Legendre symbol__ $\left(\frac{a}{p}\right) := \begin{cases} 1, & a \text{ is a square mod. } p \\ -1, & a \text{ is not a square mod. } p. \\ 0, & a \equiv 0 \pmod{p}. \end{cases}$

Example. We have observed that $\left(\frac{1}{11}\right)=\left(\frac{3}{11}\right)=\left(\frac{4}{11}\right)=\left(\frac{5}{11}\right)=\left(\frac{9}{11}\right)=1$ and $\left(\frac{2}{11}\right)=\left(\frac{6}{11}\right)=\left(\frac{7}{11}\right)=\left(\frac{8}{11}\right)=\left(\frac{10}{11}\right)=-1$.

Proposition. Let p be an odd prime.

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

Proof. Recall that the group $\mathbb{F}_p^\times$ is cyclic. Let's pick a generator $g\in\mathbb{F}_p^\times$. Then $g^s\equiv p-1\equiv -1$ for some $0<s<p-1$. As $1\equiv(-1)^2\equiv g^{2s}$, we get $2s=p-1$ or $s=\frac{p-1}{2}$.

Claim. Let $0<t<p-1$, then g^t is a square modulo p if and only if t is even (see Problem 6 in Midterm 1 Review).

It follows from the claim that -1 is a square modulo p iff $\frac{p-1}{2}=2l$ (for some $l\in\mathbb{Z}$) $\Leftrightarrow p-1=4l$ $\Leftrightarrow p-1\equiv 0 \pmod 4$ $\Leftrightarrow p\equiv 1 \pmod 4$ $\blacksquare$

Def-n. A number $a\in\mathbb{F}_p^\times$ is called a quadratic residue modulo p if it is a square modulo p and quadratic nonresidue modulo p, otherwise.

Properties of Legendre symbol.

$\forall a,b\in\mathbb{F}_p^\times$ $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ multiplicativity.

Verification: use a generator $g \in \mathbb{F}_p^\times$ and the parities of its powers k and s, where $a = g^k$, $b = g^s$.

Thm (Euler's property).

$$\frac{a}{p} = a^{\frac{p-1}{2}} \pmod{p}.$$

Proof. Let $g \in \mathbb{F}_p^\times$ be a generator, then $a = g^s$ and $\left(\frac{g}{p}\right) = -1$, so $\left(\frac{a}{p}\right) = (-1)^s \equiv \left(g^{\frac{p-1}{2}}\right)^s \equiv (g^s)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}}$.

Now the VIP (very important property): let p and q be two distinct primes, then odd

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

This property is called the law of quadratic reciprocity.

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

<u>Example</u>. Let's compute the Legendre symbol $\left(\frac{96}{37}\right)$.
Notice that $96 = 2^5 \cdot 3$, hence,

$$\left(\frac{96}{37}\right) = \left(\frac{2^5}{37}\right) \cdot \left(\frac{3}{37}\right) = \left(\frac{2}{37}\right)^5 \cdot \left(\frac{3}{37}\right) \quad \text{(multiplicativity)}$$

As $37 \equiv 5 \, (\equiv -3) \pmod 8$, we have $\left(\frac{2}{37}\right) = -1$.
Finally, quadratic reciprocity gives

$$\left(\frac{3}{37}\right) \equiv (-1)^{\frac{(3-1)(37-1)}{4}} \cdot \left(\frac{37}{3}\right) = (-1)^{18} \cdot \left(\frac{1}{3}\right) = 1.$$

We conclude that $\left(\frac{96}{37}\right) = -1 \cdot 1 = -1$.

<u>Jacobi symbol.</u>

<u>Def-n.</u> Let $a, b \in \mathbb{Z}_{\geq 0}$ with b an odd number.
The <u>Jacobi symbol</u> $\left(\frac{a}{b}\right) := \left(\frac{a}{p_1}\right)^{k_1} \cdot \ldots \cdot \left(\frac{a}{p_s}\right)^{k_s}$ where $b = p_1^{k_1} \cdots p_s^{k_s}$ is prime factorization of b and $\left(\frac{a}{p_i}\right)$ the Legendre symbol of a (modulo p_i).

Example. $\left(\frac{131}{399}\right)=\left(\frac{131}{19}\right)\cdot\left(\frac{131}{3}\right)\cdot\left(\frac{131}{7}\right)=\left(\frac{17}{19}\right)\cdot\left(\frac{2}{3}\right)\cdot\left(\frac{5}{7}\right)=$

$=1\cdot(-1)\cdot(-1)=1.$

$(6^2=36\equiv17)$

Rmk. In case b is prime (odd), then $\left(\frac{a}{b}\right)$ is the Legendre symbol.

Properties:

1. $\left(\frac{a_1a_2}{b}\right)=\left(\frac{a_1}{b}\right)\cdot\left(\frac{a_2}{b}\right)$ (multiplicativity in both parameters)

$\left(\frac{a}{b_1b_2}\right)=\left(\frac{a}{b_1}\right)\cdot\left(\frac{a}{b_2}\right)$

2. If $a_1\equiv a_2 \pmod b$, then $\left(\frac{a_1}{b}\right)=\left(\frac{a_2}{b}\right)$.

3. $\left(\frac{-1}{b}\right)=\begin{cases}1, & b\equiv1 \pmod 4\\ -1, & b\equiv3 \pmod 4).\end{cases}$

$\left(\frac{2}{b}\right)=\begin{cases}1, & b\equiv\pm1 \pmod 8\\ -1, & b\equiv\pm3 \pmod 8\end{cases}$

$\left(\frac{a}{b}\right)=\begin{cases}\left(\frac{b}{a}\right), & a\equiv1 \pmod 4 \text{ or } \{b\equiv1\} \pmod 4\\ -\left(\frac{b}{a}\right), & a\equiv3 \pmod 4 \text{ and } b\equiv3 \pmod 4).\end{cases}$

Proof: properties follow from the corresponding analogs for the Legendre symbols.

Here is a natural question.

Does $\left(\frac{a}{b}\right)=1$ imply a is a square modulo b?

Example. Let's take $b=15$ and $a=8$. We compute

$$\left(\frac{8}{15}\right)=\left(\frac{8}{3}\right)\cdot\left(\frac{8}{5}\right)=\left(\frac{2}{3}\right)\cdot\left(\frac{3}{5}\right)=(-1)\cdot(-1)=1.$$

However, the squares modulo 15 are $\{1,4,6,9,10\}$.

Hence, $\left(\frac{a}{b}\right)=1$ does not mean a is a square modulo b.

Rmk. It is straightforward to show (using the CRT) that if $b=p_1^{k_1}p_2^{k_2}\cdots p_s^{k_s}$ and $\left(\frac{a}{p_1}\right)^{k_1}=\left(\frac{a}{p_2}\right)^{k_2}=\dots=\left(\frac{a}{p_s}\right)^{k_s}=1$, then a is a quadratic residue modulo b.

These observations will be useful for cryptographic purposes.

The Goldwasser-Micali cryptosystem.

Step 1. Bob chooses two large primes p and q and a number a, s.t. $\left(\frac{a}{p}\right)=\left(\frac{a}{q}\right)=-1$. He then publishes $N=pq$ and a.

Step 2. Alice chooses a bit of information $m\in\{0,1\}$ and a number $r\in\mathbb{Z}_N$, $r>1$. She then computes

$$c=\begin{cases} r^2 \pmod N, & m=0 \\ ar^2 \pmod N, & m=1 \end{cases}$$ and sends it to Bob.

Step 3. Upon receiving the message, Bob recovers m via computing $\left(\frac{c}{p}\right)$: $m = \begin{cases} 0, & \left(\frac{c}{p}\right) = 1 \\ 1, & \left(\frac{c}{p}\right) = -1. \end{cases}$

Indeed, $\left(\frac{r^2}{p}\right) = 1$ and $\left(\frac{ar^2}{p}\right) = \left(\frac{a}{p}\right) = -1$.

Rmk. Suppose Sherlock intercepted the message c. Since both $\left(\frac{r^2}{N}\right) = 1$ and $\left(\frac{ar^2}{N}\right) = \left(\frac{a}{N}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{a}{q}\right) = (-1)\cdot(-1) = 1$, this gives him no extra info, unless he can factorize N.

Rmk. This cryptosystem is not very practical, since the blocks of information (to be sent) must be separated into tiny portions (bits) and each bit requires some work to encode.

Example. Bob chooses $p = 17$, $q = 19$, $a = 3$.
(Check that $\left(\frac{3}{17}\right) = \left(\frac{3}{19}\right) = -1$!).
He publishes the pair $(N, a) = (323, 3)$
Alice chooses $r = 15$ and finds $r^2 \equiv 225 \pmod{323}$.
She wants to send the message $m = 1$, hence
$c \equiv ar^2 \equiv 3 \cdot 225 \equiv 675 \equiv 29 \pmod{323}$.
Bob decrypts it via finding $\left(\frac{29}{17}\right) = \left(\frac{12}{17}\right) = -1 \rightsquigarrow m = 1$.