Legendre symbol

For a prime p & $a \in \mathbb{Z}$, define

$$\left(\frac{a}{p}\right) := \begin{cases} 0 & \text{if } p \mid a \\ 1 & \text{if } p \nmid a \text{ \& } a \text{ is a quadratic residue modulo } p \\ -1 & \text{if } p \nmid a \text{ \& } a \text{ is not a quadratic residue modulo } p. \end{cases}$$

Eg.: $\left(\frac{0}{p}\right) = 0$, $\left(\frac{6}{3}\right) = 0$

$\left(\frac{2}{3}\right) = -1$ (since $x^2 \equiv 2 \bmod 3$ has no soln)

$\left(\frac{1}{p}\right) = 1$, $\left(\frac{3}{5}\right) = -1$, $\left(\frac{4}{5}\right) = 1$, $\left(\frac{a^2}{p}\right) = 1$

$\left(\frac{2}{7}\right) = 1$ $\quad$ $\left(\frac{3}{7}\right) = -1$

Properties:

(1) $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ if $a \equiv b \bmod p$.

(2) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$. ($p$ is an odd prime)

(Euler's criterion: a is a quadratic residue modulo p $\Leftrightarrow$ $a^{\frac{p-1}{2}} \equiv 1 \bmod p$.)

Observe that $a^{p-1} \equiv 1 \bmod p$

so $a^{\frac{p-1}{2}} \equiv \pm 1 \bmod p$

(3) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

[Carefully observe that when neither of a & b is a quadratic residue mod p, then ab also is a quadratic residue modulo p.]

Gauss's reciprocity law: If p & q are distinct odd primes then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$

$$\left(\frac{-65}{17}\right) = \left(\frac{68-65}{17}\right) = \left(\frac{3}{17}\right)$$

$$= \left(\frac{17}{3}\right) \times (-1)^8$$

$$= \left(\frac{17}{3}\right)$$

$$= \left(\frac{2}{3}\right)$$

$$= -1$$

$68 = 17 \times 4$

$p=3, q=17$

$\frac{3-1}{2} \times \frac{17-1}{2} = 1 \times 8 = 8$

Thm: There are infinitely many primes of the form $4k+1$ where $k = 1, 2, \ldots$

Proof: Proof is by contradiction

Suppose there are finitely many primes of the form $4k+1$

Suppose $p_1, \ldots, p_r$ are the primes of the form $4k+1$

$$N = (2p_1 p_2 \cdots p_r)^2 + 1$$

So $\exists$ a prime $p \neq 2, p_1, \ldots, p_r$ & $p \mid N$.

$$(2p_1 p_2 \cdots p_r)^2 \equiv -1 \mod p.$$

Since $\gcd((2p_1 \cdots p_r), p) = 1$

$$(2p_1 \cdots p_r)^{p-1} \equiv 1 \mod p$$

$$\left[(2p_1 \cdots p_r)^2\right]^{\frac{p-1}{2}} \equiv 1 \mod p$$

$$(-1)^{\frac{p-1}{2}} \equiv 1 \mod p \longrightarrow (1)$$

Let $p = 4k+3$. Then $\frac{p-1}{2} = 2k+1$

So that $(-1)^{\frac{p-1}{2}} = (-1)^{2k+1} \equiv -1 \mod p. \longrightarrow (2)$

Using (1) & (2) $1 \equiv -1 \pmod p$

But $1 \not\equiv -1 \mod p$ (as $p > 2$) $\longrightarrow$

p is true

$\sim P \Rightarrow Q$ & Q is false

P is true $\Leftarrow \sim Q$ is true.

$X \Rightarrow Y$

$\Leftrightarrow \sim Y \Rightarrow \sim X$

So, p must be of the form $4k+3$

Thm: There are infinitely many primes of the form $4k+3$

Proof: Suppose $p_1 < p_2 < \cdots < p_r$ are the first r odd primes. ($p_1 = 3, p_2 = 7, \ldots$)

$$N = 4p_2p_3\cdots p_r + 3$$

Write an argument to show that $\exists$ a prime p of the form $4k+3$ & $p > p_r$ ($p \neq p_i$ $i = 1, \ldots r$.

→ Observe $p_i \nmid N$, $i = 1, 2, \ldots r$, $2 \nmid N$.

Prime factorization $N = q_1^{s_1} q_2^{s_2} \cdots q_\ell^{s_\ell}$

$\ell \geq 1$ $s_1, \ldots, s_\ell \geq 1$

If each $q_i = 4k_i + 1$, then $N \equiv 1 \pmod 4$

or $N = 4\tilde{k} + 1$

not possible

So $\exists$ one prime of the form $4k+3$. ($\neq p_i$ $i = 1 \cdots r$)

Recall RSA (n, e) public key
(p, q) private key
$pq = n$

$\mathcal{E}(m) = m^e$, $\mathcal{D}(c) = c^d$ where

$d = e^{-1}$ in $\mathbb{Z}/\phi(n)$

(Remember that $(e, \phi(n)) = 1$)

~~$U(\mathbb{Z}_n) \longrightarrow \mathbb{Z}_{\varphi(n)}$~~

Attacks on RSA

(without knowing or finding the private key)

~~Small exp.~~ Low exponent attack.

Suppose A sends a message to B, C & D using

$$m \longmapsto m^3 \mod n_B$$

$$m \longmapsto m^3 \mod n_C$$

$$m \longmapsto m^3 \mod n_D$$

supply.

Suppose $\gcd(n_B, n_C, n_D) = 1$

$\neq \gcd(\gcd(n_B, n_C), n_D)$

Then $\exists\ x, y, z \in \mathbb{Z}$ s.t.

$$x n_B + y n_C + z n_D = 1$$