SUBORDERS OF QUADRATIC POLYNOMIALS MODULO PRIMES

LARRY LEHMAN
UNIVERSITY OF MARY WASHINGTON
Let \( r_n = sr_{n-1} + tr_{n-2} \) for some \( s, t \) in \( Z \), with \( r_0 = 0 \) and \( r_1 = 1 \).

If \( p \) is a prime number, consider \( r_n \) in \( Z_p \), a field with \( p \) elements.

What is the smallest positive integer \( m \) for which \( r_m = 0 \) in \( Z_p \)?
EXAMPLE

\[ r_n = r_{n-1} - 3r_{n-2} : 0, 1, 1, -2, -5, 1, 16, 13, -35, -74, 31, 253, 160, \ldots \]

\[ r_n \mod 5 : 0, 1, 1, -2, 0, 1, 1, -2, 0, \ldots \quad m = 4 \]

\[ r_n \mod 7 : 0, 1, 1, -2, 2, 1, 2, -1, 0, 3, 3, \ldots \quad m = 8 \]

\[ r_n \mod 11 : 0, 1, 1, -2, -5, 1, 5, 2, -2, -3, -2, 0, -5, \ldots \quad m = 11 \]
Let \( f(x) = x^2 - sx - t = x^2 + bx + c \) be a polynomial with integer coefficients.

If \( p \) is prime, what is the smallest positive integer \( m \) so that \( f(x) \) divides some polynomial of the form \( x^m - d \) in \( \mathbb{Z}_p[x] \)?

Such an \( m \) exists if \( p \) does not divide \( c \).

We call \( m \) the suborder of \( f(x) \) modulo \( p \): \( \text{sub}_p(f) = m \).
If \( f(x) = x^2 + bx + c \) with \( c \) not zero in \( \mathbb{Z}_p \), define the subnumber of \( f(x) \) in \( \mathbb{Z}_p \) to be:

\[
a = a_p(f) = b^2 c^{-1} - 2
\]

If \( f(x) \) and \( g(x) \) have the same subnumber in \( \mathbb{Z}_p \), then they have the same suborder modulo \( p \).
Let $f(x) = x^2 + bx + c$ and $g(x) = x^2 + rx + s$ with $c$ and $s$ not zero in $\mathbb{Z}_p$.

Suppose that $b^2c^{-1} - 2 = r^2s^{-1} - 2$ in $\mathbb{Z}_p$, so $b^2s = r^2c$.

Here $b = 0 \iff r = 0 \iff \text{sub}_p(f) = 2 = \text{sub}_p(g)$.

If $b$ and $r$ are not zero, then $g(x) = x^2 + btx + ct^2$ where $t = b^{-1}r$.

In that case, $f(x)$ divides $x^m - d \iff g(x)$ divides $x^m - t^md$ in $\mathbb{Z}_p[x]$. 
For all $a$ in $\mathbb{Z}_p$, write $\text{sub}_p(a) = m$ if there is a quadratic polynomial $f(x)$ with subnumber $a$ for which $\text{sub}_p(f) = m$.

So for all primes $p$, the suborder is a well-defined function from $\mathbb{Z}_p$ to $\mathbb{Z}$.

What can we say about this suborder function on $\mathbb{Z}_p$?
PROPERTIES OF THE SUBORDER FUNCTION

\[ \text{sub}_p(-2) = 2 \quad \text{and} \quad \text{sub}_p(2) = p. \]

If \( a \neq \pm 2 \) in \( \mathbb{Z}_p \), then \( \text{sub}_p(a) = m \) is a divisor of \( p-1 \) or \( p+1 \).

For each divisor \( m > 2 \) of \( p-1 \) or \( p+1 \), there are precisely \( \varphi(m)/2 \) elements \( a \) in \( \mathbb{Z}_p \) with \( \text{sub}_p(a) = m \).

If \( \text{sub}_p(a) = m \), then \( \text{sub}_p(-a) = \begin{cases} 2m & \text{if } m \text{ is odd,} \\ m/2 & \text{if } m \equiv 2 \pmod{4}, \\ m & \text{if } m \equiv 0 \pmod{4}. \end{cases} \)

If \( \text{sub}_p(a) = m \), then \( \text{sub}_p(a^2-2) = \begin{cases} m & \text{if } m \text{ is odd,} \\ m/2 & \text{if } m \text{ is even.} \end{cases} \)
For each $a$ in $\mathbb{Z}_p$, define a sequence $a_n$ in $\mathbb{Z}_p$ by $a_0 = 2$, $a_1 = a$, and $a_n = a a_{n-1} - a_{n-2}$, if $n > 1$.

If $a \neq 2$, then $m = sub_p(a)$ is the smallest positive integer for which $a_m = 2$.

Furthermore, for $1 \leq k \leq m/2$, the elements $a_k$ are distinct, and

$$ sub_p(a_k) = m / \gcd(k, m). $$
EXAMPLE

\[ p = 19, \quad a = 6. \]

\[ a_n = 6a_{n-1} - a_{n-2}, \text{ with } a_0 = 2 \text{ and } a_1 = 6 \]

2, 6, -4, 8, -5, 0, 5, -8, 4, -6, -2, -6, 4, -8, 5, 0, -5, 8, -4, 6, 2, \ldots

\[ \text{sub}_{19}(6) = 20 \]

\[ \text{sub}_{19}(a) = 20 \quad \leftrightarrow \quad a = 6, 8, -8, 6 \]
\[ \text{sub}_{19}(a) = 10 \quad \leftrightarrow \quad a = -4, 5 \]
\[ \text{sub}_{19}(a) = 5 \quad \leftrightarrow \quad a = -5, 4 \]
\[ \text{sub}_{19}(a) = 4 \quad \leftrightarrow \quad a = 0 \]
\[ \text{sub}_{19}(a) = 2 \quad \leftrightarrow \quad a = -2 \]
Let $E$ be a quadratic extension field of $Z_p$, that is, a field with $p^2$ elements.

A quadratic polynomial must factor in $E[x]$:
$$f(x) = x^2 + bx + c = (x-u)(x-v) = x^2 - (u+v)x + uv.$$  

The subnumber of $f(x)$ is
$$a_p(f) = b^2c^{-1} - 2 = (u+v)^2(uv)^{-1} - 2 = uv^{-1} + u^{-1}v.$$  

If $u \neq v$, the suborder of $f(x)$ modulo $p$ is the order of $z = uv^{-1}$ in the group of units in $E$.

(If $f(x)$ divides $x^m - d$, then $u^m = d = v^m$, so $(uv^{-1})^m = 1.$)
For each $a$ in $\mathbb{Z}_p$, there is a unique pair of inverse elements $z$ and $z^{-1}$ in $E$ so that $a = z + z^{-1}$. (z and $z^{-1}$ are roots of $x^2 - ax + 1$ in $E$.)

For each integer $k$, let $a_k = z^k + z^{-k}$, an element of $\mathbb{Z}_p$.

Note that $a_0 = 2$ and $a_1 = a$.

Since $aa_k = (z+z^{-1})(z^k+z^{-k}) = z^{k+1} + z^{k-1} + z^{k+1} + z^{k-1} = a_{k+1} + a_{k-1}$
we find that $a_n = a a_{n-1} - a_{n-2}$ for $n > 1$.

$a_m = 2$ if and only if $z^m = 1$.
The smallest positive $m$ is $ord(z) = sub_p(a)$.

Likewise, $sub_p(a_k) = ord(z^k)$, which is $m/gcd(k,m)$. 
QUESTIONS?