Counting solutions to the Welch equation: $g^{x-1+c} \equiv x \pmod{p^e}$

MOUNT HOLYOKE

Abigail Mann

ROSE-HULMAN INSTITUTE OF TECHNOLOGY

SONAR and RADAR Performance

To optimize SONAR and RADAR performance, we can use Costas arrays (see example at right) to determine the best time-frequency transmission pattern. These matrices have the property that no two vectors between points are equal. The Welch equation,

$$g^{x-1+c} \equiv x \pmod{p} \tag{1}$$

can generate such arrays. This equation where $c = 1$ also reduces to a congruence used in the El Gamal digital signature scheme in cryptography.

We wish to know more about this equation by studying the number of solutions modulo p^e.

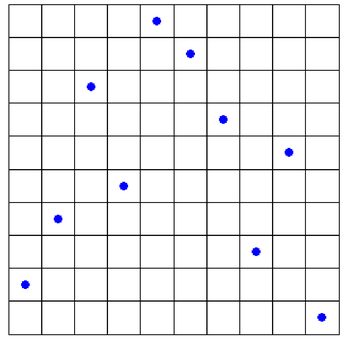

Figure 1: An example of a Costas array

Counting solutions modulo p^e for odd p

To analyze the number of solutions to $g^{x-1+c} \equiv x \pmod{p^e}$, we fix g and c. Letting x range from 1 to mp, where $m = ord_p(g)$, we get the following result, as exemplified by the table to the right.

Table 1: Observations for $g^{x-1+c} - x \pmod 7$ for $x \in \{1, 2, \ldots, 7ord_7(g)\}$

g	$ord_7(g)$	c	# of 0's
3	6	0	6
3	6	1	6
3	6	2	6
3	6	3	6
3	6	4	6
3	6	5	6
4	3	0	3
4	3	1	3
4	3	2	3
6	2	0	2
6	2	1	2

Theorem 1. *For odd prime p, let $g \in \mathbb{Z}$ be fixed where $p \nmid g$ and let m be the multiplicative order of g modulo p. Then there are exactly m solutions to the congruence*

$$g^{x-1+c} \equiv x \pmod{p^e}$$

for $x \in \{1, 2, \ldots, p^e m\}$. These solutions are also all distinct modulo m.

Proving Theorem 1

- Factor g into $\omega(g)\langle g\rangle$, where $\omega(g)$ is a $p-1^{\text{th}}$ root of unity and $\langle g\rangle \in 1 + p\mathbb{Z}_p$.
- Take m functions, $f_{x_0}(x) = \omega(g)^{x_0}\langle g\rangle^{x-1+c}$ and interpolate each function from $x \in \mathbb{Z}$ to $x \in \mathbb{Z}_p$. Note $f_{x_0}(x) = g^{x-1+c}$ when $x - 1 + c \equiv x_0 \pmod{m}$.
- Each $f_{x_0}(x) \equiv x \pmod{p}$ has one solution
- Write $f_{x_0}(x)$ as $\omega(g)^{x_0}(\exp(x\log(\langle g\rangle)))$ and find its Taylor expansion
- Use Hensel's lemma on the solution modulo p for each $f_{x_0}(x) - x$ since the function satisfies the conditions. We now have a solution x modulo every positive power of p.
- Piece together solutions to

$$x \equiv x_0 + 1 - c \pmod{m}, \text{ and}$$
$$x \equiv \omega(g)^{x_0}\langle x - 1 + c\rangle \pmod{p^e},$$

using the Chinese Remainder Theorem to get exactly m solutions modulo $p^e m$.

Counting solutions modulo 2^e

For the case when $p = 2$, we get a similar result as we do for odd primes. Because the order of any g where $p \nmid g$ is 1 modulo 2, we are able to look at a simpler range of x. The proof is similar, but interpolation is simpler.

Theorem 2. *For $p = 2$, let $g, c \in \mathbb{Z}$ be fixed. Then there is exactly one solution to the congruence*

$$g^{x-1+c} \equiv x \pmod{2^e}$$

for $x \in \{1, 2, \ldots, 2^e\}$.