a little math problem - 13 August 2013

Consider the polynomial equation in N variables $x_j, j = 1 \dots N$ with degree $D < N$

$$f(\mathbf{x}) = a_0 + \sum_{i=1}^{M} a_i X_i = 0 \text{ mod } p \tag{1}$$

with

$$X_i = \prod_{j=1}^{N} x_j^{r_{ij}} \tag{2}$$

and

$$1 \leq \sum_{j=1}^{N} r_{ij} \leq D, \quad i = 1 \dots M \tag{3}$$

where the coefficients $\mathbf{a}$ and the values of the variables $\mathbf{x}$ are in the prime field Z_p, the set of integers modulo prime p, and the powers r_{ij} are non-negative integers.

The number of terms in the summation of (1) is

$$M = \sum_{d=1}^{D} \binom{N+d-1}{d} = \binom{N+D}{D} - 1 \tag{4}$$

Proposition 1:

The number of solutions to (1) is congruent to 0, mod p.

If $f(\mathbf{x})$ is homogeneous there is at least one solution with all $\mathbf{x}$ values equal to zero, so according to proposition 1 there must always be some multiple of p solutions in this case.

Aside: $f(\mathbf{x})$ is homogeneous with degree D if $a_0 = 0$ and $\sum_{j=1}^{N} r_{ij} = D,\ i = 1 \dots M$. If $f(\mathbf{x})$ is not homogeneous it can be made so by introducing another variable, say x_0, replacing x_j with $x_j/x_0, j = 1 \dots N$, and multiplying the equation by x_0^D. The original equation is obtained by letting $x_0 = 1$.

Example with $N = 1$

In this case $D = 0$, so x_1 does not appear in the equation, and (1) becomes

$$a_0 = 0 \tag{5}$$

If a_0 is non-zero there are 0 solutions.

If a_0 is zero there are p solutions, $x_1 \in \{0, 1, \ldots, p-1\}$.

Example with $N = 2$

If $D = 0$ then (5) applies, and if a_0 is zero there are p^2 solutions, $(x_1, x_2) \in \{0, 1, \ldots, p-1\}$.

If $D = 1$ then $f(\mathbf{x})$ can be written in general as

$$a_0 + a_1 x_1 + a_2 x_2 = 0 \tag{6}$$

If a_1 and a_2 are both zero, that is the same as $D = 0$.

If a_1 is not zero then $x_1 = a_1^{-1}(-a_0 - a_2 x_2)$ where a_1^{-1} is the modular inverse of a_1, i.e. $a_1^{-1} a_1 = 1 \bmod p$. In general, for each of the p possible values of x_2, there is a solution for x_1, so there are p total solutions.

Similarly, if a_2 is not zero, (6) can be solved for x_2 in terms of x_1, again yielding p total solutions.

Example with $N = 3$

In this case the general form of $f(\mathbf{x})$ is

$$a_0 + a_1 x_1 + a_2 x_2 + a_3 x_3 + a_4 x_1^2 + a_5 x_2^2 + a_6 x_3^2 + a_7 x_1 x_2 + a_8 x_1 x_3 + a_9 x_2 x_3 = 0 \tag{7}$$

If $a_4 \ldots a_9$ are all zero, then $D \leq 1$. If $a_1 \ldots a_3$ are also all zero, then $D = 0$ and if a_0 is non-zero there are 0 solutions, otherwise there are p^3 solutions, $(x_1, x_2, x_3) \in \{0, 1, \ldots, p-1\}$. But if at least one of $a_1 \ldots a_3$ is non-zero, say a_1, then the solution is $x_1 = a_1^{-1}(-a_0 - a_2 x_2 - a_3 x_3)$ and for each of the p^2 possible values of (x_2, x_3), there is a solution for x_1, so there are p^2 total solutions.

If at least one of $a_4 \ldots a_9$ is not zero, then $D = 2$, and there may be no solutions. For example, with $p = 5$

$$2 + x_1^2 = 0 \bmod 5 \tag{8}$$

has no solutions, since for $x_1 = (0, 1, 2, 3, 4)$, $x_1^2 \bmod 5 = (0, 1, 4, 4, 1)$ and $2 + x_1^2 \bmod 5 = (2, 3, 1, 1, 3)$.

Proof of proposition 1

The characteristic function $g(\mathbf{x})$ which is 1 when $f(\mathbf{x}) = 0$ and 0 otherwise, may be written as

$$g(\mathbf{x}) = 1 - f(\mathbf{x})^{p-1} \bmod p \tag{9}$$

The characteristic function $h(\mathbf{x}, \mathbf{b})$ of a point $\mathbf{b}$ which is 1 when $\mathbf{x} = \mathbf{b}$ and 0 otherwise, may be written as

$$h(\mathbf{x}, \mathbf{b}) = \prod_{i=1}^{N} 1 - (x_i - b_i)^{p-1} \bmod p \tag{10}$$

The characteristic function $g(\mathbf{x})$ may also be written as a summation over $h(\mathbf{x}, \mathbf{b})$

$$g(\mathbf{x}) = \sum_{\mathbf{b}|f(\mathbf{b})=0} h(\mathbf{x}, \mathbf{b}) \tag{11}$$

Since (9) and (11) are equal for all values of $\mathbf{x}$, they must represent the same polynomial. However (11) has degree $N(p-1)$ and (9) has degree $D(p-1)$, with $D < N$. Therefore the coefficient of $x_1^{p-1} x_2^{p-1} \ldots x_N^{p-1}$ in (11) must be zero, mod p, i.e.

$$\sum_{\mathbf{b}|f(\mathbf{b})=0} (-1)^N = 0 \bmod p \tag{12}$$

So the number of terms in the summation, that is the number of values of $\mathbf{b}$ such that $f(\mathbf{b}) = 0$, must be a multiple of p.

Questions

Is proposition 1 still true if p is not prime? What if the modulus is a power of a prime? What if the modulus is an arbitrary composite number (product of powers of primes)?

Is proposition 1 still true under some conditions if $D \geq N$?

Proposition 2:

The number of solutions to the polynomial equation $f(\mathbf{x}) = 0 \bmod p^e$ is a multiple of p^{N-1}, where p is prime and $e > 1$, with no restriction on the degree of the polynomial.

Proof of Proposition 2 for $e = 2$:

If $f(\mathbf{b}) = 0 \bmod p^2$ for $\mathbf{x} = \mathbf{b}$, then $f(\hat{\mathbf{b}}) = 0 \bmod p$ for $\hat{\mathbf{b}} = \mathbf{b} \bmod p$.

Each $\hat{\mathbf{b}}$ corresponds to a set $\mathbf{x} = \mathbf{b} + \mathbf{c}$, where $c_i = k_i p$ for some integers $k_i, i = 1 \ldots N$.

$f(\mathbf{b} + \mathbf{c})$ may be written as

$$\begin{aligned} f(\mathbf{b}+\mathbf{c}) &= f(\mathbf{b}) + c_1 \frac{\partial f}{\partial x_1}(\mathbf{b}) + \cdots + c_N \frac{\partial f}{\partial x_N}(\mathbf{b}) \bmod p^2 && (13) \\ &= f(\mathbf{b}) + p \left(k_1 \frac{\partial f}{\partial x_1}(\mathbf{b}) + \cdots + k_N \frac{\partial f}{\partial x_N}(\mathbf{b}) \right) \bmod p^2 && (14) \end{aligned}$$

where the 2nd and higher order derivatives are all zero, mod p^2, since the coefficients of those terms are of the form $c_i\ c_j \ldots = k_i p\ k_j p \ldots$

Since $f(\mathbf{b}) = 0$, the cases of interest where $f(\mathbf{b} + \mathbf{c}) = 0$ satisfy

$$k_1 \frac{\partial f}{\partial x_1}(\hat{\mathbf{b}}) + \cdots + k_N \frac{\partial f}{\partial x_N}(\hat{\mathbf{b}}) = 0 \quad \bmod p \qquad (15)$$

If at least one of the derivatives is non–zero, say $\frac{\partial f}{\partial x_N}(\hat{\mathbf{b}})$, then $k_1 \ldots k_{N-1}$ may be chosen arbitrarily from $\{0, 1, \ldots, p-1\}$ and k_N is determined using the inverse of $\frac{\partial f}{\partial x_N}(\hat{\mathbf{b}})$, mod p. So there are p^{N-1} solutions in this case.

If all of the derivatives are zero, then $k_1 \ldots k_N$ may be chosen arbitrarily from $\{0, 1, \ldots, p-1\}$ and there are p^N solutions.