# Polynomials in many variables

Let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ denote the field of integers modulo $p$. We are interested in polynomials $f(x) \in \mathbb{F}_p[x]$, and in the maps $f : \mathbb{F}_p \to \mathbb{F}_p$ that they define. In Corollary 2.27 we found that distinct polynomials of degree $< p$ define distinct maps, and also in Theorem 2.28 that any map from $\mathbb{F}_p$ to $\mathbb{F}_p$ can be obtained by constructing an appropriate polynomial. Indeed, by Fermat's congruence we see that

$$1 - a^{p-1} \equiv \begin{cases} 1 & \text{if } a \equiv 0 \pmod p \\ 0 & \text{otherwise.} \end{cases} \tag{1}$$

Hence if $c_1, c_2, \ldots, c_p$ are given residue classes, and we want $f(i) \equiv c_i \pmod p$ for $1 \le i \le p$, then it suffices to take

$$f(x) = \sum_{i=1}^{p} c_i \bigl(1 - (x-i)^{p-1}\bigr).$$

Our first object is to generalize these observations to several variables. To facilitate our discussion, we make the following

**Definition.** *A polynomial $f(\boldsymbol{x}) \in \mathbb{F}_p[x_1, \ldots, x_n]$ is said to be* reduced *if $\deg_{x_i} f < p$ for $1 \le i \le n$. Two polynomials $f(\boldsymbol{x})$ and $g(\boldsymbol{x})$ in $\mathbb{F}_p[x_1, \ldots, x_n]$ are said to be* equivalent, *and we write $f \sim g$, if $f(\boldsymbol{x}) \equiv g(\boldsymbol{x}) \pmod p$ for all $\boldsymbol{x} \in \mathbb{F}_p^n$.*

**Theorem 1.** *Every polynomial $f \in \mathbb{F}_p[x_1, \ldots, x_n]$ is equivalent to exactly one reduced polynomial.*

**Proof.** Let $f \in \mathbb{F}_p[x_1, \ldots, x_n]$ be given. We show that there is a reduced polynomial equivalent to $f$. If $f$ is not reduced, then in $f$ there is a monomial term $cx_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$ and an $i$ such that $k_i \ge p$. Replace $x_i^{k_i}$ by $x_i^{k_i-p+1}$. Since $x^{k_i} \equiv x^{k_i-p+1} \pmod p$ for all $x$, it follows that the new polynomial is equivalent to $f$. Repeat this operation until a reduced polynomial is obtained.

If two reduced polynomials are equivalent, then their difference, call it $f$, is a reduced polynomial with the property that $f(\boldsymbol{x}) \equiv 0 \pmod p$ for all $\boldsymbol{x} \in \mathbb{F}_p^n$. We show that in this case every coefficient of $f$ is 0 (mod $p$). To do this, we argue by induction on $n$. The basis of the induction is the case $n = 1$ which has already been treated. Write

$$f(\boldsymbol{x}) = \sum_{i=0}^{p-1} f_i(x_1, \ldots, x_{n-1})x_n^i.$$

If we think of $x_1, \ldots, x_{n-1}$ as being fixed residue classes (mod $p$), then the above is a polynomial in the single variable $x_n$. Since the above is 0 (mod $p$) for every choice of $x_n$, it follows by the case of one variable that all the coefficients are 0 (mod $p$). That is,

$f_i(x_1, \dots, x_{n-1}) \equiv 0 \pmod p$. By the inductive hypothesis, it follows that each coefficient of $f_i$ is 0 (mod $p$). Hence all coefficients of $f$ are 0 (mod $p$).

To appreciate the above from an algebraic standpoint, in $\mathbb{F}_p[x_1, \dots, x_n]$ let $\mathcal{I}_1$ denote the ideal consisting of those polynomials $f$ such that $f(\boldsymbol{x}) \equiv 0 \pmod p$ for all $\boldsymbol{x} \in \mathbb{F}_p^n$, and let $\mathcal{I}_2 = (x_1^p - x_1, x_2^p - x_2, \dots, x_n^p - x_n)$, which is to say that $\mathcal{I}_2$ is the ideal consisting of all polynomials that can be expressed in the form

$$\sum_{i=1}^{n} f_i(\boldsymbol{x})(x_i^p - x_i)$$

where $f_i \in \mathbb{F}_p[x_1, \dots, x_n]$. Clearly $\mathcal{I}_2 \subseteq \mathcal{I}_1$. What Theorem 1 expresses is that $\mathcal{I}_1 = \mathcal{I}_2$.

We note that there are exactly $p^{(p^n)}$ maps from $\mathbb{F}_p^n$ to $\mathbb{F}_p$, and also that there are exactly $p^{(p^n)}$ reduced polynomials in $\mathbb{F}_p[x_1, \dots, x_n]$. Since distinct reduced polynomials define distinct maps, it follows by the pigeonhole principle that each map is defined by a unique reduced polynomial. More explicitly, if for each $\boldsymbol{a} \in \mathbb{F}_p^n$ a residue class $c(\boldsymbol{a}) \in \mathbb{F}_p$ is given, then we put

$$f(\boldsymbol{x}) = \sum_{\boldsymbol{a} \in \mathbb{F}_p^n} c(\boldsymbol{a}) \prod_{i=1}^{n} \big(1 - (x_i - a_i)^{p-1}\big). \tag{2}$$

Thus $f$ is a reduced polynomial with the property that $f(\boldsymbol{a}) \equiv c(\boldsymbol{a}) \pmod p$ for all $\boldsymbol{a}$.

**Theorem 2.** (Chevalley) *Suppose that $P(\boldsymbol{x})$ is a polynomial of degree $d$ in $n$ variables, with integral coefficients. If $n > d$, and if $P(\mathbf{0}) \equiv 0 \pmod p$, then there is an $\boldsymbol{x}$, not all of whose coordinates are divisible by $p$, such that $P(\boldsymbol{x}) \equiv 0 \pmod p$.*

By applying the above to the polynomial $P(\boldsymbol{x} + \boldsymbol{a}) - P(\boldsymbol{a})$ we see that any value (mod $p$) taken by $P(\boldsymbol{x})$ is taken at least twice, if $n > d$.

**Proof.** From (1) we see that if $P(\boldsymbol{x}) \equiv 0 \pmod p$ precisely when $x_i \equiv 0 \pmod p$ for all $i$, then

$$1 - P(\boldsymbol{x})^{p-1} \equiv \begin{cases} 1 & (x_i \equiv 0 \pmod p \text{ for all } i), \\ 0 & (\text{otherwise.}) \end{cases}$$

By taking $c(0) = 1$ and all other $c(\boldsymbol{a}) = 0$ in (2), we deduce that

$$1 - P(\boldsymbol{x})^{p-1} \equiv \prod_{i=1}^{n} \big(1 - x_i^{p-1}\big) \pmod p$$

for all choices of the variables $x_i$. The polynomial on the right hand side above is reduced, but the left hand side is not necessarily reduced. Let $Q(\boldsymbol{x})$ be a reduced polynomial equivalent to the left hand side above. Hence

$$Q(\boldsymbol{x}) \equiv \prod_{i=1}^{n} \big(1 - x_i^{p-1}\big) \pmod p$$

for all choices of the variables $x_i$. By Theorem 1, it follows that all coefficients of

$$\prod_{i=1}^{n} \left(1 - x_i^{p-1}\right) - Q(\boldsymbol{x})$$

are divisible by $p$. But the monomial $x_1^{p-1} \cdots x_n^{p-1}$ has coefficient $(-1)^n$ in the product, and coefficient 0 in $Q$, since $\deg Q \le d(p-1) < n(p-1)$. This is a contradiction, so the proof is complete.

We now lay the foundation for a stronger result.

**Lemma 1.** *For non-negative integers $k$, let $S_k(p) = \sum_{a=1}^{p} a^k$. Then*

$$S_k(p) \equiv \begin{cases} -1 \pmod p & \text{if } k \equiv 0 \pmod{p-1} \text{ and } k > 0, \\ 0 \pmod p & \text{otherwise.} \end{cases}$$

Note: We take $a^0 = 1$ for all $a$, including $a = 0$.

**Proof.** Clearly $S_0(p) = p \equiv 0 \pmod p$. $S(0) = p \equiv 0 \pmod p$. Also, if $k > 0$ and $(p-1)|k$, then by Fermat's congruence

$$S_k(p) \equiv \sum_{a=1}^{p-1} 1 \equiv -1 \pmod p.$$

Finally, suppose that $k > 0$ and that $k \not\equiv 0 \pmod{p-1}$. Recall that if $(c, p) = 1$, then the numbers $ca$ form a complete residue system as $a$ runs through a complete residue system (Theorem 2.6). Hence $c^k S_k(p) \equiv S_k(p) \pmod p$. That is, $S_k(p)(c^k - 1) \equiv 0 \pmod p$. But since $k \not\equiv 0 \pmod{p-1}$, there is a $c$ such that $c^k \not\equiv 1 \pmod p$. Indeed, a primitive root will do. Hence $S_k(p) \equiv 0 \pmod p$, and the proof is complete.

**Theorem 3.** (Warning) *Suppose that $P(\boldsymbol{x})$ is a polynomial of degree $d$ in $n$ variables, with integral coefficients. If $n > d$, then the number of solutions of the congruence $P(\boldsymbol{x}) \equiv 0 \pmod p$ is divisible by $p$.*

**Proof.** By (1) we see that the number of solutions of this congruence is congruent (mod $p$) to

$$\sum_{x_1=1}^{p} \sum_{x_2=1}^{p} \cdots \sum_{x_n=1}^{p} 1 - P(\boldsymbol{x})^{p-1}.$$

Let $cx_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$ be one of the monomial terms that make up the polynomial $1 - P(\boldsymbol{x})^{p-1}$. The contribution made to the above sum by this monomial term is

$$c \prod_{i=1}^{n} \left( \sum_{x_i=1}^{p} x_i^{k_i} \right).$$

Since $P$ has degree $d$, we know that $\sum_{i=1}^n k_i \le d(p-1)$. But $n > d$, so the inequality $k_i < p-1$ holds for at least one $i$. By Lemma 1, this value of $i$ contributes a factor $\equiv 0 \pmod p$ to the above product.

If $P(\boldsymbol{x})$ is a form (i.e., a homogeneous polynomial) of degree $d > 0$, then $P(\mathbf{0}) = 0$, so it follows from either Theorem 2 or Theorem 3 that the congruence $P(\boldsymbol{x}) \equiv 0 \pmod p$ must also have at least one non-trivial solution. For example, the congruence $x^2 + y^2 + z^2 \equiv 0 \pmod p$ always has a solution with not all variables divisible by $p$.

## Exercises

**1.** Let $f \in \mathbb{F}_p[x_1, \dots, x_n]$ have degree $d < n$. Show that

$$\sum_{\substack{\boldsymbol{x} \in \mathbb{F}_p^n \\ f(\boldsymbol{x}) \equiv 0 \pmod p}} x_i^k \equiv 0 \pmod p$$

for $1 \le i \le n$, $0 \le k < p-1$.

**2.** For $1 \le j \le m$ let $f_j \in \mathbb{F}_p[x_1, \dots, x_n]$, and put $d_j = \deg f_j$. Show that if $\sum d_j < n$, then the system of simultaneous congruences

$$f_j() \equiv 0 \pmod p \qquad (1 \le j \le m)$$

has at least two solutions, if it has one.

**3.** Show that in the situation of the preceding exercise, that the number of solutions is a multiple of $p$.

**4.** (a) Let $S_k(p)$ be defined as in Lemma 1. Use the binomial theorem to show that

$$\sum_{k=0}^{n-1} \binom{n}{k} S_k(p) \equiv 0 \pmod p\,.$$

(b) Deduce that

$$\sum_{\substack{0<k<n \\ (p-1)|k}} \binom{n}{k} \equiv 0 \pmod p\,.$$