1. A polynomial \( f \) over a field \( K \) is powerful if every irreducible factor of \( f \) (in \( K[x] \)) occurs with multiplicity at least two. Let \( P(n) \) be the number of powerful monic polynomials of degree \( n \) over \( GF(q) \). Show that \( P(n) = q^{\lfloor \frac{n}{2} \rfloor} + q^{\lfloor \frac{n}{2} \rfloor} - 1 - q^{\lfloor \frac{n-1}{2} \rfloor} \) for all \( n \geq 2 \).

**Proof.** Number all the monic irreducible polynomials of degree at least one over \( GF(q) \): \( f_1(x), f_2(x), f_3(x), \ldots \), with, say, respective degrees \( d_1, d_2, \ldots \). Let \( N_d \) denote the number of degree \( d \), \( d = 1, 2, 3, \ldots \).

Now for any sequence \( i_1, i_2, i_3, \ldots \) of non-negative integers (all but finitely many of which are nonzero), we get a monic polynomial

\[
   f(x) = (f_1(x))^{i_1} (f_2(x))^{i_2} (f_3(x))^{i_3} \ldots , \text{ whose degree is } n = i_1d_1 + i_2d_2 + \ldots .
\]

By unique factorization, every monic polynomial of degree \( n \) arises exactly once in this way. That is to say there is a one-to-one correspondence between monic polynomials of degree \( n \) and sequences \( i_1, i_2, \ldots \) of non-negative integers satisfying \( n = i_1d_1 + i_2d_2 + \ldots \). From this, we see that

\[
   \frac{1}{1-qx} = (1+x+x^2 + \cdots) (1+x+x^2 + \cdots) (1+x+x^2 + \cdots) \cdots
\]

Recall that \( N_d \) is the number of irreducible monic poly of degree \( d \). We have

\[
   \frac{1}{1-qx} = \prod_{d=1}^{\infty} \frac{1}{1-x^d} = \prod_{d=1}^{\infty} \left( \frac{1}{1-x^d} \right)^{N_d}
\]

Now consider powerful monic polynomials of degree \( n \) over \( GF(q) \). Any powerful monic poly \( f(x) \) of degree \( n \) can be factorized in
a unique way as
\[ f(x) = f_1(x) f_2(x) f_3(x) \ldots \]
where \( i_1 d_1 + i_2 d_2 + \ldots = n \) and \( i_1 \geq 0, i_2 \geq 0, i_3 \geq 0, \ldots \)
\( i_1 \neq 1, i_2 \neq 1, i_3 \neq 1, \ldots \)

Therefore we have
\[ \sum_{n=0}^{\infty} P(n) x^n = (1 + x^{2d_1} + x^{3d_1}) (1 + x^{2d_2} + x^{3d_2}) \ldots \]
\[ = \prod_{d=1}^{\infty} \left( \frac{1}{1 - x^{d}} - x^{d} \right)^{N_d} \]
\[ = \prod_{d=1}^{\infty} \left( \frac{1 - x^{d} - x^{2d}}{1 - x^{d}} \right)^{N_d} \]
\[ = \prod_{d=1}^{\infty} \left( \frac{1 + x^{3d}}{1 - x^{3d}} \right)^{N_d} \]
\[ = \prod_{d=1}^{\infty} \left( \frac{(1 - x^{6d})}{(1 - x^{3d})} \right)^{N_d} \]

Now using \( \frac{1}{1-qx} = \prod_{d=1}^{\infty} \left( \frac{1}{1-x^d} \right)^{N_d} \), we obtain
\[ \sum_{n=0}^{\infty} P(n) x^n = \frac{1 - 9x^6}{(1-9x^2)(1-9x^3)} = -\frac{x}{q} + \frac{(1+q)(1+q^3)}{q(1-9x^3)} - \frac{1+9x+9x^2}{9(1-9x^3)} \]

It follows that \( P(n) = q^{\left\lceil \frac{n}{6} \right\rceil} + q^{\left\lceil \frac{n}{3} \right\rceil - 1} - q^{\left\lceil \frac{n-1}{3} \right\rceil} \) if \( n \geq 2 \). This problem is due to Richard Stanley.

2. Let \( c \in GF(q) \setminus \{0, 1\} \), where \( q = 2^t \), \( t \) is odd. Prove that the polynomial \( f(x) = x^5 + cx^2 + x + c^2 + c \) has exactly one root in \( GF(q) \).

One solution can be found in my paper with Jiyou Li and David Chandler,
"Permutation polynomials of degree 6 or 7 over finite fields of characteristic 2."

See Lemma 3.6 of the above paper.

Below is another proof given by Tao Feng. It is short but it uses the fact that the polynomial $x^2 + x^3 + x^5 \in \mathbb{F}_{2^t}[x]$ is a permutation polynomial of $\mathbb{F}_{2^t}$, where $t$ is odd. (Note that $x + x^2 + x^5 \in \mathbb{F}_{2^t}[x]$ is a Dickson polynomial, see page 355-356 of "Finite Fields", by Lidl and Niederreiter.)

**Proof:** Let $c \in \mathbb{F}_{2^t} \setminus \{0, 1\}$. Since $x^2 + x^3 + x^5 \in \mathbb{F}_{2^t}[x]$ is a permutation poly of $\mathbb{F}_{2^t}$, $c \neq 0$ and $c \neq 1$. We see that there is a unique $\alpha \in \mathbb{F}_{2^t}$ s.t. $c = \alpha + \alpha^2 + \alpha^5$.

Let $\beta = \alpha + \alpha^2$. Then $\alpha = \frac{c}{1 + \beta^2}$. Hence $\beta + \frac{c}{1 + \beta^2} + \frac{c^2}{1 + \beta^4} = 0$

\[ \Rightarrow \beta + \beta^5 + c(1 + \beta^2) + \frac{c^2}{1 + \beta^4} = 0 \]

\[ \Rightarrow \beta^5 + \beta + c + \frac{c^2}{1 + \beta^2} = 0. \]

That is, $\beta$ is a solution of $f(x) = x^5 + cx^3 + x + c + c^2$.

The uniqueness of such a solution follows from the fact that $x + x^2 + x^5 \in \mathbb{F}_{2^t}[x]$ is a permutation polynomial of $\mathbb{F}_{2^t}$. Details are as follows:

Let $x \in \mathbb{F}_{2^t}$ be a solution of $f(x) = 0$. Then $x^5 + cx^3 + x + c + c^2 = 0$

\[ \Rightarrow x + x^5 + c(1 + x^3) + c^2 = 0 \]

\[ \Rightarrow x + \frac{c}{1 + x^2} + \left(\frac{c}{1 + x^2}\right)^2 = 0, \quad \text{Hence} \quad x = \frac{z + z^2}{1 + x^2}, \quad z = \frac{c}{1 + x^2} \in \mathbb{F}_{2^t}. \]

It follows that $x = (1 + x^3) = x + x^2 + x^5$.

Now since $x + x^2 + x^5 \in \mathbb{F}_{2^t}[x]$ is a permutation poly of $\mathbb{F}_{2^t}$, we have from $c = x + x^2 + x^5 = \alpha + \alpha^2 + \alpha^5 \Rightarrow \beta = \alpha$. \[ \Rightarrow \quad x = \alpha + \alpha^2 = \beta. \]

That is, $\beta$ is the unique solution of $f(x) = 0$ in $\mathbb{F}_{2^t}$. 

\[ \square \]
3. If \( p \equiv 1 \pmod{3} \), we have seen that \( 4p = A^2 + 27B^2 \) with \( A, B \in \mathbb{Z} \). If we require that \( A \equiv 1 \pmod{3} \), show that \( A \) is uniquely determined.

**Proof:** If \( \exists A, A' \equiv 1 \pmod{3} \) s.t. \( 4p = A^2 + 27B^2 = A'^2 + 27B^2 \), we set \( A = 2a-b, \ b = 3B, \) then

\[
\begin{align*}
A &= (a + b \omega)(a + b \overline{\omega}) \\
A' &= (a' + b \omega)(a' + b \overline{\omega}),
\end{align*}
\]

where \( A \equiv a' \equiv 2 \pmod{3} \)

and \( b \equiv 0 \pmod{3} \).

Now \( a + b \omega, a + b \overline{\omega}, a' + b \omega, a' + b \overline{\omega} \) are all primes in \( \mathbb{Z}[\omega] \) and \( \mathbb{Z}[\omega] \) is a UFD, we have \( a + b \omega \) is either an associate of \( a' + b \omega \)
or an associate of \( a' + b \overline{\omega} \). There are exactly six units in \( \mathbb{Z}[\omega] \), namely \( \pm 1, \pm \omega, \pm \omega^2 \). Using the above facts, one can easily show that

\[
a + b \omega = a' + b \omega \Rightarrow (a = a' \Rightarrow A = A')\]
or

\[
a + b \omega = a' + b \overline{\omega} \ (\text{in the case } b = 0).
\]

But \( b = 0 \) can't happen; otherwise \( 4p = A^2 = A'^2 \), impossible. So we must have \( a + b \omega = a' + b \omega \Rightarrow A = A' \)

\( \Box \)

4. Suppose that \( p \equiv 1 \pmod{6} \) and let \( \chi \) and \( \rho \) be characters of order 3 and 2, respectively. Show that the number of solutions to \( y^2 = x^3 + D \) in \( \mathbb{F}_p \) is \( p + \pi + \pi^2 \), where \( \pi = \chi(\rho(D)) \chi(\rho) \). If \( \chi(2) = 1 \), show that the number of solutions to \( y^2 = x^3 + 1 \) is \( p + A \), where \( 4p = A^2 + 27B^2 \) and \( A \equiv 1 \pmod{3} \).
proof: If $D = 0$, then the equation becomes $y^2 = x^3$.

If $x = 0$, then $y^2 = 0 \Rightarrow y = 0$.

If $x$ is a nonzero square, then $y^2 = x^3$ has exactly two solutions for $y$.

If $x$ is a nonsquare, then so is $x^3 \Rightarrow y^2 = x^3$ has no solutions.

$\Rightarrow N(y^2 = x^3) = p$.

If $D \neq 0$, 

$N(y^2 = x^3 + D) = N(y^2 - x^3 = D)$

$= \sum_{a + b = D} N(y^2 = a) N(x^3 = -b)$

$= \sum_{a + b = 1} N(y^2 = aD) N(x^3 = bD)$

$= \sum_{a + b = 1} \left( \sum_{i = 0}^{1} \chi^i(D) \left( \sum_{j = 0}^{2} \chi^j(-bD) \right) \right)$

$= \sum_{i = 0}^{2} \chi^i(D) J(\chi_i, p)$

$= p + \chi(D) J(\chi, p) + \chi(D) \overline{J(\chi, p)}$.

So $N(y^2 = x^3 + D) = p + \pi + \overline{\pi}$, where $\pi = \chi(D) J(\chi, p)$.

Now set $D = 1$. We have

$N(y^2 = x^3 + 1) = p + J(\chi, p) + \overline{J(\chi, p)}$

$= p + 2 \text{Re} J(\chi, p)$.

Since $\sigma(\chi) = 3$ & $\sigma(p) = 2$, we have $\chi(s) \in \{1, \omega, \omega^2\} \& p(t) \in \{-1, 1\}$, $s, t \in F_p^x$.

$\Rightarrow J(\chi, p) = a + b \omega, \ a, b \in \mathbb{Z}$. 

$N(y^2 = x^3 + 1) = p + 2a - b$.

$p = J(\chi, p) \overline{J(\chi, p)} = a^2 - ab + b^2 \Rightarrow 4p = (2a-b)^2 + 3b^2 = A^2 + 27B^2$

$N(y^2 = x^3 + 1) = p + A$, where $A \equiv 1(3)$ is uniquely determined by $4p = A^2 + 27B^2$. 

5. Let \( p \) be a prime, \( p \equiv 1 (4) \), \( \chi \) a multiplicative char. of order 4 on \( \mathbb{F}_p \), and \( \rho \) the Legendre symbol. Put \( J(\chi, \rho) = a + bi \), \( a, b \in \mathbb{Z} \).

Show (a) \( N(y^2 + x^4 = 1) = p - 1 + 2a \),

\[
N(y^2 + x^4 = 1) = \sum_{a+b=1} N(x^2 = a) \cdot N(y^2 = b)
\]
\[
= \sum_{a+b=1} \left( \frac{3}{\chi^{i}(a)} \right) \left( \frac{4}{\chi^{j}(b)} \right)
\]
\[
= \sum_{i=0}^{3} \sum_{j=0}^{4} J(\chi, \rho) = p + J(\chi, \rho) + J(\chi^2, \rho) + J(\chi^3, \rho)
\]
\[
= p + (a + bi) + J(\chi^2, \rho) + a - bi
\]
\[
= p + 2a + J(\rho, \rho^1)
\]
\[
= p + 2a - \left( \frac{-1}{p} \right) = p + 2a - 1.
\]

(b) \( N(y^2 = 1 - x^4) = \sum_{x \in \mathbb{F}_p} (1 + p(1 - x^4)) \), since

if \( 1 - x^4 = 0 \), then \( y = 0 \) is the only sol. to \( y^2 = 1 - x^4 \);
if \( 1 - x^4 \) is a nonzero square, then there are two solutions to \( y^2 = 1 - x^4 \);
if \( 1 - x^4 \) is a nonsquare, then there are no solutions to \( y^2 = 1 - x^4 \).

Hence

\[
N(y^2 = 1 - x^4) = p + \sum_{x \in \mathbb{F}_p} p(1 - x^4)
\]

(c) \( N(y^2 + x^4 = 1) = N(y^2 = 1 - x^4) \). Hence

\[
p - 1 + 2a = p + \sum_{x \in \mathbb{F}_p} p(1 - x^4)
\]
\[
\Rightarrow 2a \equiv 1 + \sum_{x \in \mathbb{F}_p} (1 - x^4)^{\frac{p-1}{2}} \pmod{p} \quad \text{or more precisely,} \quad 2a = 1 + \sum_{x \in \mathbb{F}_p} (1 - x^4)^{\frac{p-1}{2}}
\]
\[ \sum_{x \in \mathbb{F}_p} (1 - x^i)^{\frac{p-1}{2}} = \sum_{x \in \mathbb{F}_p} \sum_{i=0}^{2m} \binom{2m}{i} (-1)^i x^{4i} \]

\[ = \sum_{i=0}^{2m} \binom{2m}{i} (-1)^i \sum_{x \in \mathbb{F}_p} x^{4i} \]

Now we evaluate \( \sum_{x \in \mathbb{F}_p} x^{4i} \).

If \( i = 0 \), then \( \sum_{x \in \mathbb{F}_p} x^{4i} = p \) (here \( \delta = 1 \)).

If \( 1 \leq i \leq 2m \), then \( \sum_{x \in \mathbb{F}_p} x^{4i} = \sum_{x \in \mathbb{F}_p^*} x^{4i} = \sum_{i=0}^{p-2} (g^{4i})^\frac{i}{2} \) (where \( g \) is a primitive element of \( \mathbb{F}_p^* \))

\[ = \begin{cases} 0, & \text{if } g^{4i} \neq 1 \\ \frac{p-1}{2}, & \text{if } g^{4i} = 1 \iff (p-1) \mid 4i \iff i = m \text{ or } 2m \end{cases} \]

Therefore

\[ \sum_{x \in \mathbb{F}_p} (1 - x^i)^{\frac{p-1}{2}} = p + \binom{2m}{m} (-1)^m (p-1) + (p-1) \]

\[ \overset{\text{in } \mathbb{F}_p, p \neq 0}{\Rightarrow} (-1)^{m+1} \binom{2m}{m} - 1 \]

Hence we have shown that \( 2a \equiv (-1)^{m+1} \binom{2m}{m} \pmod{p} \).

i.e., \( 2a \equiv (-1)^{ \frac{p-1}{4} } \binom{2m}{m} \pmod{p} \).

\[ \square \]

Question:
Can you figure out \( \binom{\frac{p-1}{2}}{\frac{p-1}{4}} \pmod{p^2} \)?