1. Let \( m = n - k \). We want to show that the power of \( p \) dividing \( \binom{m+k}{k} \) is the number of carries when adding \( m \) to \( k \) in base \( p \). Note that each time a carry occurs, \((a_i + p)\) in the \( i \)th place becomes \( a_{i+1} \) in the \((i+1)\)st place, so the number of carries is

\[
\text{(sum of the digits of } k) + \text{(sum of the digits of } m) - \text{(sum of the digits of } m+k)\). \frac{p-1}{p-1}
\]

Since for any integer \( a \) the power of \( p \) dividing \( a! \) is \((a - s)/(p - 1)\), where \( s \) is the sum of the digits of \( a \) in base \( p \), this expression is precisely the power of \( p \) dividing \( \binom{m+k}{k} \).

2. (a) Divide the \( m + n \) objects (from which we need to choose \( k \)) into two subcollections, \( A \) with \( m \) objects and \( B \) with \( n \) objects. Then we need to choose \( i \) objects from \( A \) and \( k - i \) objects from \( B \), where \( i \) may range from 0 to \( k \).

(b) In the equation

\[
(1 + x)^{m+n} = \left(1 + \binom{m}{1}x + \binom{m}{2}x^2 + \cdots + \binom{m}{m}x^m\right) \cdot \left(1 + \binom{n}{1}x + \cdots + \binom{n}{n}x^n\right),
\]

the coefficient of \( x^k \) in the LHS is \( \binom{m+n}{k} \), and the coefficient of \( x^k \) in the RHS is \( \sum \binom{m}{i} \binom{n}{k-i} \).

(c) Setting \( m = n = k \) gives

\[
\binom{2n}{n} = \sum_{i=0}^{n} \binom{n}{i} \binom{n}{n-i} = \sum_{i=0}^{n} \binom{n}{i}^2.
\]

(d) Consider the identity

\[
(1 - x)^{2n} (1 + x)^{2n} = (1 - x^2)^{2n}.
\]

On the RHS, the coefficient of \( x^{2n} \) is the same as the coefficient of \( x^n \) in the polynomial \( (1 - x)^{2n} \), namely \((-1)^n \binom{2n}{n} \). On the LHS, the coefficient of \( x^{2n} \) is

\[
\sum_{k=0}^{2n} (-1)^k \binom{2n}{k} \binom{2n}{n-k} = \sum_{k=0}^{2n} (-1)^k \binom{2n}{k}^2,
\]

as desired.

3. (a) We know that \( p \mid \binom{p}{i} \) for \( i = 1, \ldots, p-1 \). So \((1+x)^p \equiv 1 + x^p \pmod{p} \) is immediate. We now use proof by induction, where we have just proven the base case. Now

\[
(1 + x)^p^k \equiv ((1 + x)^p)^{p^{k-1}}
\]

\[
\equiv (1 + x^p)^{p^{k-1}}
\]

\[
\equiv 1 + x^{p^k} \pmod{p}
\]

by the inductive hypothesis, completing the induction. We could also have used the result from class that \( \binom{p^k}{i} \equiv 0 \pmod{p} \) for \( i = 1, \ldots, p^k - 1 \).
(b) By part (a),

$$(1 + x)^n = (1 + x)^{a_0 + a_1 p + \cdots + a_r p^r}$$

$$= (1 + x)^{a_0} (1 + x)^{a_1 p} \cdots (1 + x)^{a_r p^r}$$

$$\equiv (1 + x)^{a_0} (1 + x)^{a_1 p} \cdots (1 + x)^{a_r p^r} \pmod{p}. $$

The only way to get $x^{b_0 + b_1 p + \cdots + b_r p^r}$ from the expansion is to choose $x^{b_i}$ from $(1 + x)^{a_i}$, $x^{b_i p^i}$ from $(1 + x^p)^{a_i}$, $\ldots$, $x^{b_i p^r}$ from $(1 + x^p)^{a_r}$. So the coefficient is

$$\left( \begin{array}{c} a \\ b \\ \end{array} \right) \equiv \left( \begin{array}{c} a_r \\ b_r \\ p \\ \end{array} \right) (a_r - 1) \cdots \left( \begin{array}{c} a_0 \\ b_0 \\ p \end{array} \right) \pmod{p}.$$ 

4. Suppose $n$ is prime. Then, since the binomial coefficients in the middle vanish mod $p$,

$$(x - a)^n \equiv x^n + (-a)^n \pmod{p}$$

Now for the converse. The polynomial congruence in particular means that $n$ must divide $\binom{n}{k}$ for $i = 1, \ldots, n - 1$. We’ll see first that this implies $n$ must be a power of a prime.

Let $p$ be any prime dividing $n$. If $n$ is not a power of $p$, then the base $p$ expansion of $n$ does not look like $1$ followed by a bunch of zeroes, so it’s either $n, 0 \cdots 0$ with $n \geq 2$, or $n, n_2, \cdots, n_q$ with some $n_i \geq 1$ for $i < r$. In any case, let $k$ have the base $p$ expansion $10 \cdots 0$ (i.e., $k = p^r$). Then subtracting $k$ from $n$ in base $p$ doesn’t involve any carries, so $p \nmid \binom{n}{k}$ and therefore $n \nmid \binom{n}{k}$, contradiction. So $n$ must be a power of $p$.

Let’s assume $n$ is not a prime, so we now have $n = p^r$ with $r \geq 2$. Then it’s clear that subtracting $p^{r-1}$ (whose base $p$ expansion is $010 \cdots 0$ from $n$ in base $p$) will involve only one carry. So $p \mid \binom{n}{p^{r-1}}$, and thus $n = p^r$ cannot divide this binomial coefficient, contradiction. Therefore, $n$ is indeed a prime.

5. We need to show that $11n^7 + 7n^{11} + 59n$ is divisible by 77. It’s enough to show divisibility by 7 and by 11 separately. Mod 7 we get

$$11n^7 + 7n^{11} + 59n \equiv 11n^7 + 3n$$

$$\equiv 11n + 3n$$

$$\equiv 0 \pmod{7},$$

and similarly mod 11.

6. We have

$$p^x | (x^2 - 1) = (x - 1)(x + 1).$$

Suppose $p$ is odd. Then $p$ can’t divide both $x + 1$ and $x - 1$, since their difference 2 isn’t divisible by $p$, so $(p^x, x + 1) = 1$ or $(p^x, x - 1) = 1$. Hence $p^x | x - 1$ or $p^x | x + 1$, and the only two solutions are $x \equiv \pm 1 \pmod{p^x}$.

Now suppose $p = 2$. Then $x^2 \equiv 1 \pmod{2^x}$ means $x$ must be odd, so let $x = 2^y + 1$. We have

$$2^x | (x - 1)(x + 1) = 4y(y + 1).$$

Note that if $p = 2$ then $x = 1$, and if $p = 4$ then $x = 1, 3$. So let’s assume $e \geq 3$. Since $y$ and $y + 1$ are obviously coprime, we have $2^e - 2 | y$ or $2^e - 2 | y + 1$, i.e., $y \equiv 0 \pmod{2^e - 2}$ or $y \equiv -1 \pmod{2^e - 2}$. Then, modulo $2^e - 1$, the possible solutions for $y$ are $0, 2^e - 2, 2^e - 1, -1$, and the corresponding solutions for $x$ are $1, -1, 2^e - 1 + 1, 2^e - 1 - 1$. It’s easy to verify that all of these work and are distinct modulo $2^e$.

7. (a) The binomial coefficient

$$\binom{x}{k} = \frac{x(x - 1) \cdots (x - k + 1)}{k!}$$
obviously has degree $k$ in $x$ and highest coefficient $1/k!$. We show by induction on the degree $n$ of $p(x)$ that there are unique complex numbers $c_0, \ldots, c_n$ such that

$$p(x) = c_n \binom{x}{n} + c_{n-1} \binom{x}{n-1} + \cdots + c_0.$$ 

For $n = 0$, $p(x)$ is constant, so $p(x)$ can be uniquely expressed as $p(0)\binom{x}{0}$. Now suppose we’ve proved the proposition for polynomials of degree less than $n$. Then if $p(x) = p_n x^n + \cdots$ we let $c_n = k! p_n$ and note that $c_n \binom{x}{n}$ is of degree $n$ and leading coefficient $p_n$. So $p(x) - c_n \binom{x}{n}$ has degree less than $n$, and by the inductive hypothesis, equals $c_{n-1} \binom{x}{n-1} + \cdots + c_0$ for some $c_{n-1}, \ldots, c_0$ uniquely determined. (Note that $c_n$ is also uniquely determined from the highest coefficient). This completes the induction.

(b) Note that

$$\Delta \binom{x}{k} = \binom{x+1}{k} - \binom{x}{k} = \frac{(x+1)x(x-1)\cdots(x-k+2) - x(x-1)\cdots(x-k+1)}{k!} = \frac{x(x-1)\cdots(x-k+2)k}{k!} = \frac{x(x-1)\cdots(x-(k-1)+1)}{(k-1)!} = \binom{x}{k-1}.$$ 

By linearity, if $p(x) = \sum_{k=0}^n c_k \binom{x}{k}$ then

$$\Delta p(x) = \sum_{k=0}^n c_k \Delta \binom{x}{k} = \sum_{k=1}^n c_k \binom{x}{k-1}.$$ 

(Note that the $k = 0$ term goes away since $\Delta \binom{x}{0} = 0$.)

(c) One direction is obvious: if $c_k \in \mathbb{Z}$ for all $k$, then since $\binom{m}{k}$ is always an integer, we have $p(m) = \sum_{k=0}^n c_k \binom{m}{k} \in \mathbb{Z}$ for all integers $m$.

Conversely, suppose $p(m) \in \mathbb{Z}$ for all $m$. Then we’ll show by induction on the degree $n$ of $p$ that the coefficients $c_k$ for such a $p$ must be integers.

For $n = 0$ this is obvious, so suppose we’ve proved the proposition for all polynomials with degree less than $n$. Consider the polynomial $q(x) = \Delta p(x)$. It has degree $n-1$ since $q(x) = \sum_{k=1}^n c_k \binom{x}{k-1}$. Also $q(m) = p(m+1) - p(m)$ is an integer for all integers $m$. So we get by the inductive hypothesis that $c_1, \ldots, c_n$ are all integers. Then, evaluating $p$ at $m = 0$,

$$p(0) = c_0 + c_1 \binom{0}{1} + \cdots + c_n \binom{0}{n} = c_0.$$

So $c_0 \in \mathbb{Z}$ as well. This completes the induction.