

A few thoughts on the combinatorics problems:

1. My usual proof is to first note that the binomial coefficient $\binom{p}{k}$ is a multiple of p if $0 < k < p$ — simply use the “factorial” description of these coefficients. Then from the binomial theorem we conclude $(1 + X)^p \equiv 1 + X^p \pmod{p}$. Then we can expand $(1 + X)^{ap} = ((1 + X)^p)^a \equiv (1 + X^p)^a$ by using the Binomial Theorem in two ways: the coefficient of X^{pb} when expanding the left side is $\binom{pa}{pb}$, and when expanding the right side it's $\binom{a}{b}$.

Actually a little more is true: if $n = ap + c$ then $(1 + X)^n \equiv (1 + X^p)^a(1 + X)^c$ can also be expanded on both sides. If $m = bp + d$ then the coefficient of X^m will be $\binom{n}{m}$ when expanding the left and will be $\binom{a}{b} \binom{c}{d}$ on the right, assuming that both c and d are between 0 and $p - 1$ inclusive. By induction, then, we can compute any binomial coefficient modulo p by using the base- p expansion of the entries:

$$\binom{\dots a_2 a_1 a_0}{\dots b_2 b_1 b_0} \equiv \dots \binom{a_2}{b_2} \binom{a_1}{b_1} \binom{a_0}{b_0}$$

For example, to compute $\binom{69}{31}$ modulo 5, write $69 = 234_5$ and $31 = 111_5$ to get $\binom{69}{31} \equiv \binom{2}{1} \binom{3}{1} \binom{4}{1} = 2 \cdot 3 \cdot 4 \equiv 4$. Indeed, the binomial coefficient is 39789158751476438304, which is congruent to 4 mod 5.

Luis noticed another argument I had not thought of, literally using the definition of the binomial coefficients as counting the number of subsets of a given set with a given cardinality. Suppose we have a set $X = \{x_1, x_2, \dots, x_{pa}\}$ of cardinality pa and we enumerate all the subsets of X having cardinality pb . We will call two such subsets *equivalent* if they contain the same cardinality of elements from among $\{x_1, x_2, \dots, x_p\}$, and the same cardinality of elements from among $\{x_{p+1}, x_{p+2}, \dots, x_{2p}\}$, and so on for the a such blocks of consecutive elements of X . Given any one S subset of cardinality pb , we can itemize all the subsets that are equivalent to it by selecting different subsets within each block, having the same cardinality; so if S contains n_1 elements in the first block, and n_2 elements in the second, and so on, then the number of subsets equivalent to S is

$$\binom{p}{n_1} \binom{p}{n_2} \dots \binom{p}{n_a}$$

Since most binomial coefficients are multiples of p , this number is surely a multiple of p as well unless each n_k is either 0 or p , that is, S must be the union of whole blocks (in which case there is nothing equivalent to S except for S itself). We can list all subsets S of this type simply by deciding which whole blocks are to be included: there are a blocks to choose from and we must choose b to ensure S has cardinality pb .

Then, counting all the subsets of the right cardinality, we get $\binom{a}{b}$ that are alone in their equivalence class, and the remainder are in equivalence class whose number of elements is a multiple of p . Hence $\binom{pa}{pb} \equiv \binom{a}{b}$