18.781
PROBLEM SET 2

JOHN WANG

1. Problem 1

Problem 1.1. *Let p be prime and $n, k \in \mathrm{N}$. Show that the power of p dividing $\binom{n}{k}$ is the number of carries when adding k to $n-k$ in base p.*

Solution First, we will restate a proposition that was proven in class:

Proposition 1.1. *Write n in base p as $n = a_0 + a_1 p + \ldots + a_k p^k$ with $a_i \in \{0, \ldots, p-1\}$. Then $e(n,p) = \frac{n-(a_1+\ldots+a_k)}{p-1}$ where $e(n,p)$ is defined as a function such that $p^e || n!$ holds, where $e \in \mathrm{Z}$.*

First, we shall define $r = n - k$. Let us say that there are a maximum of s digits in n, k, or r in base p. Then we can write these in base p as:

$$n = n_0 + n_1 p + \ldots + n_s p^s \tag{1.2}$$

$$k = k_0 + k_1 p + \ldots + k_s p^s \tag{1.3}$$

$$r = r_0 + r_1 p + \ldots + r_s p^s \tag{1.4}$$

Where $n_i, k_i, r_i \in \{0, \ldots, p-1\}$ for all i. Next, we know that $\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{(k+r)!}{r!k!}$. The power of p that divides $\binom{n}{k}$ is then $e(k+r,p) - e(r,p) - e(k,p)$. We can write this using the proposition as:

$$e(k+r,p) - e(r,p) - e(k,p) \tag{1.5}$$

$$= \frac{(k+r) - (n_0 + \ldots + n_s) - (k - (k_0 + \ldots + k_s)) - (r - (r_0 + \ldots + r_s))}{p-1} \tag{1.6}$$

$$= \frac{(k_0 + \ldots + k_s) + (r_0 + \ldots + r_s) - (n_0 + \ldots + n_s)}{p-1} \tag{1.7}$$

This is exactly the number of carries when adding k to $n-k$ in base p because $r = n - k$. Thus, the number of carries is the sum of the digits of n subtracted from the digits of k and $n-k$ in base p, divided by the total number of digits possible in base p, which is $p-1$. This completes the proof. □

2. Problem 2

Problem 2.1. *Let m, n, k be positive integers. Use combinatorial reasoning to show that*

$$\binom{m+n}{k} = \sum_{i=0}^{m} \binom{m}{i}\binom{n}{k-i} \tag{2.1}$$

Solution We want to choose k elements from $m+n$. Split the $m+n$ elements into two groups, call them M and N. The group M contains m elements and the group N contains n elements. In order to choose k elements, we must choose i elements from M and $k-i$ elements from N. The number of ways to choose this for any i where $0 \leq i \leq m$ is simply $\binom{m}{i}\binom{n}{k-i}$. We take the sum of the total number of ways to do this for all possible i, which clearly range from $0 \leq i \leq m$. This becomes $\sum_{i=0}^{m} \binom{m}{i}\binom{n}{k-i}$, which is what we wanted. □

Problem 2.2. *Prove this identity by considering the coefficient of x^k in $(1+x)^m(1+x)^n$.*

Solution We see that $(1+x)^{m+n} = (1+x)^m(1+x)^n$. Moreover, the coefficient of x^k in the binomial expansion of $(1+x)^{m+n}$ is $\binom{m+n}{k}1^{m+n} = \binom{m+n}{k}$ by the binomial theorem. The coefficient of x^k in the binomial expansion of $(1+x)^m(1+x)^n$ must then be equal to $\binom{m+n}{k}$. If we compute the binomial expansion, we find:

$$(1+x)^m(1+x)^n = \left(\sum_{i=0}^{m} \binom{m}{i} x^i\right)\left(\sum_{i=0}^{n} \binom{n}{i} x^i\right) \tag{2.2}$$

The x^k term in this expansion is given by:

$$\sum_{k=0}^{m} \binom{m}{i} x^i \binom{n}{k-i} x^{k-i} = \sum_{k=0}^{m} \binom{m}{i}\binom{n}{k-i} x^k \tag{2.3}$$

Therefore, we see that the coefficients on the x^k term must be equal, so that $\binom{m+n}{k} = \sum_{i=0}^{m} \binom{m}{i}\binom{n}{k-i}$ must hold. □

Problem 2.3. *Show that* $\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$.

Solution We see that the following is true by the binomial theorem:

$$(1+x)^{2n} = (1+x)^n(1+x)^n \tag{2.4}$$

$$= \left(\sum_{i=0}^{n} \binom{n}{i} x^i\right)\left(\sum_{i=0}^{n} \binom{n}{i} x^i\right) \tag{2.5}$$

We see that the terms containing x^n can be written as:

$$\sum_{i=0}^{n} \binom{n}{i}\binom{n}{n-i} x^i x^{n-i} = \sum_{k=0}^{n} \binom{n}{i}^2 x^n \tag{2.6}$$

Because we know that $\binom{n}{i}\binom{n}{n-i} = \frac{n!}{i!(n-i)!}\frac{n!}{(n-i)!i!} = \binom{n}{i}^2$. Moreover, by the binomial expanion of $(1+x)^{2n}$, we know that the terms containing x^n can also be expressed as $\binom{2n}{n}x^n$. This shows that the coefficients on these two terms are equal, namely that:

$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n} \tag{2.7}$$

□

Problem 2.4. *Show that* $\sum_{k=0}^{2n} (-1)^k \binom{2n}{k}^2 = (-1)^n \binom{2n}{n}$.

Solution We know that $(x^2-1)^{2n} = ((x+1)(x-1))^{2n} = (x+1)^{2n}(x-1)^{2n}$. Moreover, we can use binomial expansions:

$$(x+1)^{2n}(x-1)^{2n} = \left(\sum_{i=0}^{2n} \binom{2n}{i} x^i\right)\left(\sum_{i=0}^{2n} \binom{2n}{i} x^i (-1)^{2n-i}\right) \tag{2.8}$$

If we collect the terms with x^{2n}, we obtain:

$$\sum_{i=0}^{2n} \binom{2n}{i} x^i \binom{2n}{2n-i} x^{2n-i}(-1)^i = \sum_{k=0}^{2n} \binom{2n}{k}^2 x^{2n}(-1)^k \tag{2.9}$$

Moreover, the term with x^{2n} in the original expression of $(x^2-1)^{2n}$ using the binomial theorem is:

$$\binom{2n}{n}(x^2)^n(-1)^n \tag{2.10}$$

Equating the coefficients on these terms together, we obtain:

$$\sum_{k=0}^{2n} (-1)^k \binom{2n}{k}^2 = (-1)^n \binom{2n}{n} \tag{2.11}$$

□

3. Problem 3

Problem 3.1. *Let p be a prime. Show the polynomial identity* $(1+x)^p \equiv 1 + x^p \mod p$ *and more generally that* $(1+x)^{p^k} \equiv 1 + x^{p^k} \mod p$.

Solution It is sufficient to prove this for $(1+x)^{p^k} \equiv 1 + x^{p^k} \mod p$ since the previous identity follows if we choose $k = 1$. We will use the binomial theorem to prove this. First, we see that

$$(1+x)^{p^k} = 1^{p^k} + x^{p^k} + \sum_{i=1}^{p^k-1} \binom{p^k}{i} x^i \tag{3.1}$$

However, we know that $\binom{p^k}{i} = \frac{p^k!}{i!(p^k-i)!} = \frac{(p^k)(p^k-1)\ldots(p^k-i+1)}{i!}$. Thus, for $i = 1, \ldots, p-1$, it is clear that $p|\binom{p^k}{i}$. Thus, we see that $\binom{p^k}{i} \equiv 0 \mod p$, which means we can write the congruence:

$$(1+x)^{p^k} \equiv 1 + x^{p^k} \mod p \tag{3.2}$$

□

Problem 3.2. *Let $a = a_r p^r + \cdots + a_0$ and $b = b_r p^r + \cdots + b_0$ be the base p expressions of two positive integers. Show that*

$$\binom{a}{b} \equiv \binom{a_r}{b_r}\binom{a_{r-1}}{b_{r-1}}\cdots\binom{a_0}{b_0} \mod p \tag{3.3}$$

Solution First, we note that the x^b term in the binomial expansion of $(1+x)^a$ is simply $\binom{a}{b}x^b$. Moreover, by using the lemma that we have just proven, we see that:

$$(1+x)^a \equiv \prod_{m=0}^{r}(1+x^{a_m p^m}) \mod p \tag{3.4}$$

$$\equiv \prod_{m=0}^{r}(1+x^{p^m})^{a_m} \mod p \tag{3.5}$$

$$\equiv \prod_{m=0}^{r}\sum_{i=0}^{a_m}\binom{a_m}{i}x^{ip^m} \mod p \tag{3.6}$$

We see that the $x^b = x^{b_r p^r + \cdots + b_0}$ terms can be written as:

$$\prod_{m=0}^{r}\binom{a_m}{b_m} \tag{3.7}$$

Since the coefficients on these two terms are equal, we see that:

$$\binom{a}{b} \equiv \binom{a_r}{b_r}\binom{a_{r-1}}{b_{r-1}}\cdots\binom{a_0}{b_0} \mod p \tag{3.8}$$

Which is what we wanted to prove. □

4. Problem 4

Problem 4.1. *Let n be a positive integer. Show that the polynomial identity $(x-a)^n \equiv x^n - a \pmod n$ holds for every integer a if and only if n is prime.*

Solution First, assume that n is prime. Then we must show that $(x-a)^n - (x^n - a) \equiv 0 \pmod n$. First, we know that we can expand this expression to the following:

$$(x-a)^n - (x^n - a) = a - x^n + \sum_{i=0}^{n}\binom{n}{i}x^i(-a)^{n-i} \tag{4.1}$$

$$= a + \sum_{i=0}^{n-1}\binom{n}{i}x^i(-a)^{n-i} \tag{4.2}$$

The coefficient on each x^i term (0 ¡ i ¡ n) is therefore $\binom{n}{i}a^{n-i}(-1)^i$. Moreover, since n is a prime, we see that for all i such that $0 < i < n$, we have $n|\binom{n}{i}$. This means that $\binom{n}{i}a^{n-i}(-1)^i \equiv 0 \pmod n$. For $i = 0$, we see that the coefficient on x^0 is $(-a)^n$. We can group the extra a term with this and we have $a(1-a^{n-1})$ as the coefficient on the x^0 term. Since n is prime, we see by Fermat's Little Theorem that $1 - a^{n-1} \equiv 0 \pmod n$. This shows that all terms are congruent to $0 \pmod n$, which shows that $(x-a)^n \equiv x^n - a \pmod n$.

Now to prove the converse, we assume that $(x-a)^n \equiv (x^n - a) \pmod n$. Now suppose by contradiction that n is composite. Then n has some smallest prime factor p and let $k = n/p$. Then $0 < p < n$ and

$$\binom{n}{p} = \frac{n(n-1)\ldots(n-p+1)}{p!} \tag{4.3}$$

$$= \frac{kp(n-1)\ldots(n-p+1)}{p!} \tag{4.4}$$

$$= \frac{k(n-1)\ldots(n-p+1)}{(p-1)!} \tag{4.5}$$

However, we know that $p|n$ so that $p \nmid n-1, n-2, \ldots, n-p+1$. Therefore, since p is prime, we see that $p \nmid (n-1)(n-2)\ldots(n-p+1)$. Since $n = kp$, we clearly must have $n \nmid (n-1)\ldots(n-p+1)$. Moreover, we clearly see that $n \nmid k = n/p$, since $p > 1$ and we know that $1/p$ is not an integer. Therefore, we see that $\binom{n}{p} \not\equiv 0 \pmod{n}$. This means that the coefficient on x^p is not $0 \pmod{n}$. This is a contradiction, so n must be prime.

□

5. Problem 5

Problem 5.1. *Show that $\frac{n^7}{7} + \frac{n^{11}}{11} + \frac{59n}{77}$ is an integer for all $n \in \mathrm{Z}$.*

Solution First, we will call the above expression N and note that the following is true:

$$N = \frac{n^7}{7} + \frac{n^{11}}{11} + \frac{59n}{77} = \frac{n^7}{7} + \frac{n^{11}}{11} + n - \frac{n}{7} - \frac{n}{11} \tag{5.1}$$

$$= \frac{n}{7}\left(n^6 - 1\right) + \frac{n}{11}\left(n^{10} - 1\right) + n \tag{5.2}$$

Clearly if $7|n$, then $\frac{n}{7}\left(n^6 - 1\right)$ is an integer. If $11|n$, then $\frac{n}{11}\left(n^{10} - 1\right)$ is an integer. Thus if both hold, then N is an integer because all three of its terms are integers.

Now suppose that $7 \nmid n$. By Fermat's Little Theorem, we can write $n^7 \equiv n \mod 7$ for any $n \in \mathrm{Z}$ so that $n^6 \equiv 1 \mod 7$. Thus, we see that $7|(n^6 - 1)$, which means that $\frac{(n^6-1)}{7}$ is an integer, so that $\frac{n}{7}(n^6 - 1)$ is also an integer.

Now suppose that $11 \nmid n$. We use the same logic of Fermat's Little Theorem to find that $n^{11} \equiv n \mod 11$ and so $n^{10} \equiv 1 \mod 11$ since 11 is a prime. This implies that $\frac{n}{11}(n^1 0 - 1)$ is an integer.

Thus, in all cases of $n \in \mathrm{Z}$, we see that all three terms in N are integers, which means N must also be an integer. □

6. Problem 6

Problem 6.1. *Let p be a prime and $e \geq 1$. Find all the solutions of $x^2 \equiv 1 \bmod p^e$.*

Solution Let us first consider the case of $p = 2$. We must find the solutions to $x^2 \equiv 1 \pmod{2^e}$ for $e \geq 1$. This is equivalent to $(x+1)(x-1) \equiv 0 \bmod 2^e$. It is clear that $x \equiv 1$ is always a solution regardless of e. Moreover, $(x-1)$ and $(x+1)$ can both be divisible by 2, but they can't both be divisible by 4. Therefore, the solutions when $p = 2$ are $\{1, 2^{e-1} - 1, 2^{e-1} + 1, 2^e - 1\}$.

Now, when $p > 2$, we have the following congruence to solve: $(x-1)(x+1) \equiv 0 \bmod p^e$. Since $p > 2$, then p^e must divide either $(x-1)$ or $(x+1)$ but not both. Therefore, we have $p^e|(x-1)$ or $p^e|(x+1)$. Then we see that $x \equiv \pm 1 \bmod p^e$. □

7. Problem 7

Problem 7.1. *Show that $\binom{x}{k}$ is a polynomial in x of degree k with leading coefficient $1/k!$. Now let $p(x)$ be an arbitrary polynomial with complex coefficients and degree at most n. Show that there exist complex numbers $c_0, \ldots, c_n$ such that $p(x) = \sum_{k=0}^{n} c_k \binom{x}{k}$ and that the c_k are uniquely determined.*

Solution We can write $\binom{x}{k}$ in terms of factorials and find $\binom{x}{k} = (x(x-1)\ldots(x-k+1))/k!$. Clearly, the largest term in this expansion is x^k, and since each $(x-i)$ has no coefficient on x, we see that the coefficient of x^k is given by $1/k!$.

Let us say the coefficients on $p(x)$ are given by $d_n, d_{n-1}, \ldots, d_0$ so that $p(x) = d_n x^n + \ldots + d_0$. Then one can construct the term $d_n x^n$, since $\binom{x}{n}$ is a polynomial of degree n with leading coefficient $1/k!$. We can choose $c_n = d_n k!$, and the leading term of the polynomial will then be $d_n x^n$. We will now have a new coefficient on the x^{n-1} term that we must construct d'_{n-1}. However, we can choose $c_{n-1} = d'_{n-1} k!$ to exactly match this. Thus, we see that there exist $c_n, c_{n-1}, \ldots, c_0$ such that $p(x) = \sum_{k=0}^{n} c_k \binom{x}{k}$.

Now we must show that each c_k is unique. Suppose there exist two coefficients c_{i1} and c_{i2} which both satisfy the equation $p(x) = \sum_{k=0}^{n} c_k \binom{x}{k}$ for some i. Then the x^i term has coefficients $c_{i1}\binom{x}{i}$ or $c_{i2}\binom{x}{i}$. This means that we have:

$$p_1(x) = c_{i1}\binom{x}{i} + \sum_{k=0, k\neq i}^{n} c_k \binom{x}{k} \tag{7.1}$$

$$p_2(x) = c_{i2}\binom{x}{i} + \sum_{k=0, k\neq i}^{n} c_k \binom{x}{k} \tag{7.2}$$

However, we see that $c_{i1} \neq c_{i2}$, which means that $p_1(x) - p_2(x) = (c_{i1} - c_{i2})\binom{x}{i} \neq 0$. This is a contradiction between we must have $p(x) = p_1(x) = p_2(x)$. Therefore, each c_k is unique. □

Problem 7.2. *For any function $f : \mathrm{N} \to \mathrm{C}$ of the natural numbers, we can define another function Δf by $\Delta f(n) = f(n+1) - f(n)$. Show that $\Delta\binom{x}{k} = \binom{x}{k-1}$. Show that if $p(x)$ is as above then*

$$\Delta p(x) = \sum_{k=1}^{n} c_k \binom{x}{k-1} \tag{7.3}$$

Solution First, we show that $\Delta\binom{x}{k} = \binom{x}{k-1}$. For, this we recall the following identity that we proved combinatorially in class:

Lemma 7.4.

$$\binom{m+1}{l+1} = \binom{m}{l} + \binom{m}{l+1} \tag{7.5}$$

Now let $m = x$ and $l + 1 = k$. Then we see the identity can be rearranged into:

$$\binom{x+1}{k} = \binom{x}{k-1} + \binom{x}{k} \tag{7.6}$$

$$\binom{x+1}{k} - \binom{x}{k} = \binom{x}{k-1} \tag{7.7}$$

$$\Delta\binom{x}{k} = \binom{x}{k-1} \tag{7.8}$$

Now, we would like to see what $\Delta p(x)$ is equal to. In order to do this, we simply write out the definition of the difference operator and rearrange the terms in each of the sums. Then we group together terms to obtain $\Delta\binom{x}{k}$ and use the identity we have just shown to obtain our result.

$$\Delta p(x) = p(x+1) - p(x) \tag{7.9}$$

$$= \sum_{k=0}^{n} c_k \binom{x+1}{k} - \sum_{k=0}^{n} c_k \binom{x}{k} \tag{7.10}$$

$$= \sum_{k=0}^{n} c_k \left(\binom{x+1}{k} - \binom{x}{k} \right) \tag{7.11}$$

$$= \sum_{k=0}^{n} c_k \Delta \binom{x}{k} \tag{7.12}$$

$$= \sum_{k=1}^{n} c_k \binom{x}{k-1} \tag{7.13}$$

This completes the proof. □

Problem 7.3. *Show that $p(x)$ is an integer $\forall x \in \mathrm{Z}$ if and only if all the c_k are integers.*

Solution First, if all the c_k are integers, then $p(x)$ is clearly also an integer. This is because $\binom{x}{i} \in \mathrm{Z}$ for any $x, i \in \mathrm{Z}$ since any binomial coefficient expresses how many possible ways there are to count something, which is an integer. Thus, we see that an integer c_k multiplied by another integer $\binom{x}{k}$ is also an integer. Moreover, the sum of integers is an integer, so $\sum_{k=0}^{n} c_k\binom{x}{k} = p(x)$ is therefore an integer.

Now let us assume that $p(x)$ is an integer for all $x \in \mathrm{Z}$. We will proceed by induction to show that all c_k are integers. Let us say $p(x)$ is a polynomial of degree n and denote it thus $p_n(x)$. We can express $p_n(x)$ in the form $p_n(x) = c_n\binom{x}{n} + \ldots + c_0\binom{x}{0}$. First, we will start our induction with a base case of $n = 0$. We see that if $p_0(x) = c_0$ is an integer, then c_0 must be an integer. Thus, the hypothesis holds in the base case.

Now assume that the hypothesis holds for polynomials up to degree n. Then $p_n(x) = c_n\binom{x}{n} + \ldots + c_0\binom{x}{0}$ being an integer for all $x \in \mathrm{Z}$ implies that $c_n, \ldots, c_0$ are integers. Now we can write $p_{n+1}(x)$ as $p_{n+1}(x) = c_{n+1}\binom{x}{n+1} + \ldots + c_0\binom{x}{0}$. Since $p_{n+1}(x+1)$ and $p_{n+1}(x)$ are integers, then $\Delta p_{n+1}(x)$ must also be an integer.

However, we know the following from our previous exercise:

$$\Delta p_{n+1}(x) = p_{n+1}(x+1) - p_{n+1}(x) \tag{7.14}$$

$$= c_{n+1}\binom{x}{n} + c_n\binom{x}{n-1} + \ldots + c_1\binom{x}{0} \tag{7.15}$$

$$= c_{n+1}\binom{x}{n} + \left[c_n\binom{x}{n-1} + \ldots + c_1\binom{x}{0}\right] \tag{7.16}$$

But we know that $c_n, \ldots, c_1$ are integers so that $c_n\binom{x}{n-1} + \ldots c_1\binom{x}{0}$ is an integer as well. Moreover, we know that $\binom{x}{n}$ is an integer. Since $\Delta p_{n+1}(x)$ is an integer, c_{n+1} must be an integer. This finishes the proof by induction.

□