# Interesting arguments, ideas

Victor Wang

October 23, 2013

1. Hmm this is pretty tricky and I wish I actually knew what it meant but here is an application anyway. (Adapted from Gabriel Dospinescu, 2010 MR U160). Let $p$ be a prime and let $n, s$ be positive integers. Prove that

$$v_p\left(\sum_{p|k,0\le k\le n}(-1)^k k^s\binom{n}{k}\right)\ge v_p(n!).$$

$$hfdkal;f$$

**Solution:** Let the sum be $S$. Then by a roots of unity filter and the Stirling number representation of $k^s$ (define $0^0=\binom{0}{0}=1$),

$$\begin{aligned}
pS&=\sum_{j=0}^{p-1}\sum_{k=0}^{n}\binom{n}{k}k^s(-\omega^j)^k\\
&=\sum_{j=0}^{p-1}\sum_{k=0}^{n}\binom{n}{k}(-\omega^j)^k\sum_{\ell=0}^{s}S(s,\ell)\binom{k}{\ell}\ell!\\
&=\sum_{j=0}^{p-1}\sum_{\ell=0}^{\min(s,n)}S(s,\ell)\ell!\sum_{k=0}^{n}\binom{k}{\ell}\binom{n}{k}(-\omega^j)^k\\
&=\sum_{j=0}^{p-1}\sum_{\ell=0}^{\min(s,n)}S(s,\ell)\ell!\binom{n}{\ell}\sum_{k=\ell}^{n}\binom{n-\ell}{k-\ell}(-\omega^j)^k\\
&=\sum_{j=0}^{p-1}\sum_{\ell=0}^{\min(s,n)}S(s,\ell)\ell!\binom{n}{\ell}(-\omega^j)^\ell(1-\omega^j)^{n-\ell}.
\end{aligned}$$

If $j=0$ and $\ell<n$, then we get a zero term. Also, if $s\ge n$, then from the $\ell=n$ terms we get

$$n!\sum_{j=0}^{p-1}(-\omega^j)^n=pn!(-1)^n[p|n],$$

which is a multiple of $p^{1+v_p(n!)}$. Thus it suffices to show that for $1\le j\le p-1$,

$$v_p\left(\ell!\binom{n}{\ell}(1-\omega^j)^{n-\ell}\right)>v_p(n!)$$

for all $0\le\ell\le\min(s,n-1)$. But using the extension of $v_p$ to the ring of algebraic numbers $\bar{\mathbb{Q}}$ (i.e. $v_p(x)=\frac{1}{d}v_p(f(0))$, where $f$ is the minimal polynomial of $x$), the LHS is just

$$v_p(n!)-\frac{n-\ell-s_p(n-\ell)}{p-1}+\frac{n-\ell}{p-1}>v_p(n!),$$

so we're done (note that $n-\ell \geq 1 \implies s_p(n-\ell) > 0$ in this case).[/hide]

**Edit:** Two more applications (also from PFTB)!

(Gabriel Dospinescu). Let $p > 2$ be a prime number and let $m$ and $n$ be multiples of $p$, with $n$ odd. For any function $f : \{1, 2, \ldots, m\} \to \{1, 2, \ldots, n\}$ satisfying $\sum_{k=1}^{m} f(k) \equiv 0 \pmod{p}$, consider the product $\prod_{k=1}^{m} f(k)$. Prove that the sum of these products is divisible by $\left(\frac{n}{p}\right)^m$. (Yes, we can strengthen it easily.)

(St. Petersburg 2003). Let $p$ be a prime and let $n \geq p$ and $a_1, a_2, \ldots, a_n$ be integers. Define $f_0 = 1$ and $f_k$ the number of subsets $B \subseteq \{1, 2, \ldots, n\}$ having $k$ elements and such that $p$ divides $\sum_{i \in B} a_i$. Show that $f_0 - f_1 + f_2 - \cdots + (-1)^n f_n$ is a multiple of $p$.

2. (MathOverflow, July 2012) By Newton interpolation (or other standard methods), one can easily determine the number and structure (the latter to a lesser extent) of sequences $(a_1, a_2, \ldots, a_n) \pmod{n}$ represented by integer polynomials given the prime factorization of $n$ (note that we can reduce to the prime power case by the Chinese remainder theorem). For instance, see this AoPS thread. However, for such $f \in \mathbb{Z}[x]$ we have strong restrictions like $u - v \mid f(u) - f(v)$ for integers $u, v$.

   IMO it's then natural to wonder about (e.g. the new structure of valid $f$) for rational polynomials in general, where standard interpolation methods (in certain mods) aren't as clean. (Mostly copied from my comment below.)

   To this end, consider a pair of positive integers $(n, m)$ with $n, m > 1$ such that for every sequence $(a_1, a_2, \ldots, a_n) \in (\mathbb{Z}/m\mathbb{Z})^n$, there exists an integer-valued polynomial $f \in \mathbb{Q}[x]$ satisifying $f(x) \equiv a_i \pmod{m}$ whenever $x \equiv i \pmod{n}$.

   First, it is easy to show that $n, m$ must be powers of the same prime. Indeed, if there exist distinct primes $p, q$ such that $p \mid n$ and $q \mid m$, then for some sufficiently large integer $\ell$, we have $q \mid f(x+n) - f(x)$ and $q \mid f(x + q^\ell) - f(x)$ for every $x$. But $\gcd(n, q^\ell) \mid n/p$, so by Bzout's identity, $q \mid f(x + n/p) - f(x)$ for all $x$ and thus the $a_{i(n/p)}$ must all be congruent $\pmod{q}$ in order for $f$ to exist.

   On the other hand, if $n = p^i$ and $m = p^j$ for some prime $p$ and positive integers $i, j$, then given a sequence $(a_1, a_2, \ldots, a_n)$, consider the polynomial $g(x) = \sum_{k=1}^{n} a_k x^k$. By a simple induction on $d \geq 0$, we can show (using finite differences) that a degree $d$ polynomial $f$ (for convenience, say $\deg 0 = -1$) satisfying the desired properties exists iff $d$ is the smallest number such that the division of $(x-1)^{d+1} g(x)$ by $x^n - 1$ gives a remainder $r(x)$ with coefficients all divisible by $m$ (call $d+1$ the *order* of the sequence $(a_1, a_2, \ldots, a_n)$, so the all-zero sequence has order 0). Since $(x-1)^n = x^n - 1$ in $\mathbb{F}_p$, we have $(x-1)^{jn} = (x^n - 1)u(x) + p^j v(x)$ for some polynomials $u, v$ with integer coefficients, so the order of any sequence is finite and at most $jn$.

   However, this leads to the following two questions:

   ¿ 1. For fixed $p, i, j$, what is the maximum possible order $M$ of a sequence $(a_1, a_2, \ldots, a_n) \in (\mathbb{Z}/m\mathbb{Z})^n$? (Resolved in the update.) ¿ 2. How many sequences are there of order $r$, where $r \in [0, M]$ is a fixed integer? ¿ 3. Is there a reasonably nice way to describe the sequences of a fixed order $r$ (possibly in terms of one of the corresponding polynomials $f, g$)?

   Looking at small cases, it seems that the answer to 1 should be $p^i + (j-1)\phi(p^i)$, where $\phi$ denotes Euler's totient function.

   **Update:** OK, I think I have a (messy) proof that the answer to question 1 is indeed $p^i + (j-1)\phi(p^i)$, but it doesn't seem to lend itself to 2 or 3 in any way.

   Fix $p, i$. First note that since $(x-1)^{p^k} = x^{p^k} - 1$ (in $\mathbb{F}_p$) for $k = i$ and $k = i-1$, we have $(x-1)^{\phi(p^i)} = \Phi_{p^i}(x)$ in $\mathbb{F}_p$ as well, so $(x-1)^{\phi(p^i)} = \Phi_{p^i}(x) + pT(x)$ for some integer polynomial $T$ of degree at most $\phi(p^i) - 1$, where $\Phi_t$ denotes the $t^{th}$ cyclotomic polynomial. Observe that $T(1) = -1$, so 1 is not a root of $T$ in $\mathbb{F}_p$.

   Using this key fact, we will induct on $j \geq 1$ to construct a sequence of integer polynomials $P_j, Q_j$ such that

$$(x-1)^{p^i + (j-1)\phi(p^i)} = (x^{p^i} - 1)P_j(x) + p^j(x-1)Q_j(x),$$

$v_p(Q_j(1)) = i-1$, and in $\mathbb{F}_p$, $(x-1)^{p^{i-1}-1} \| Q_j(x)$ (i.e. 1 is a root of multiplicity $p^{i-1}-1$).

For $j=1$, we simply take $P_1(x)=1$ and $Q_1(x) = \frac{(x-1)^{p^i}-(x^{p^i}-1)}{p(x-1)}$, where clearly $Q_1(1) = -p^{i-1} \implies v_p(Q_1(1)) = i-1$. Showing $(x-1)^{p^{i-1}-1} \| Q_j(x)$ is slightly harder, but not too bad. It's easy to show by counting prime factors that $\binom{p^i}{k}$ is divisible by $p$ for all $1 \le k \le p^i-1$ and not divisible by $p^2$ iff $p^{i-1} \mid k$. Furthermore, by Babbage's theorem we have $\binom{p^i}{kp^{i-1}} \equiv \binom{p}{k} \pmod{p^2}$ for $1 \le k \le p-1$. Hence for $p=2$, we just need to show that $(x-1)^{p^{i-1}} \| x^{p^{i-1}} - 1$ in $F_2$, which is obvious; for $p>2$ odd, we need to show

$$(x-1)^{p^{i-1}} \| \sum_{k=1}^{p-1} \frac{x^{kp^{i-1}}}{k} = \left( \sum_{k=1}^{p-1} \frac{x^k}{k} \right)^{p^{i-1}}$$

in $\mathbb{F}_p$ (note that $k^p = k$ by Fermat's little theorem). But if $h(x) = \sum_{k=1}^{p-1} \frac{x^k}{k}$, then $h(1) \equiv 0 \pmod{p}$ while $h'(1) \equiv p-1 \pmod{p}$, so 1 is a simple root of $h$ and we're done with the base case.

Now assuming the result for some $j \ge 1$ (so that $\frac{x^{p^{i-1}}-1}{x-1} \mid Q_j(x)$ in $\mathbb{F}_p$), we can write $Q_j(x) = \frac{x^{p^{i-1}}-1}{x-1} R(x) + pS(x)$ for two integer polynomials $R, S$ with $\deg S < p^{i-1}-1$. (*) Then

$$(x-1)^{p^i + j\phi(p^i)} = (x-1)^{p^i + (j-1)\phi(p^i)} (x-1)^{\phi(p^i)}$$

can be written as

$$(x^{p^i}-1)P_j(x)(x-1)^{\phi(p^i)} + p^{j+1}(x-1)T(x)Q_j(x) + p^j \Phi_{p^i}(x)(x-1)Q_j(x)$$

or equivalently after substitution,

$$(x^{p^i}-1)(P_j(x)(x-1)^{\phi(p^i)} + p^j R(x)) + p^{j+1}(S(x)\Phi_{p^i}(x) + T(x)Q_j(x)),$$

so we can take

$$P_{j+1}(x) = P_j(x)(x-1)^{\phi(p^i)} + p^j R(x)$$

and

$$Q_{j+1}(x) = S(x)\Phi_{p^i}(x) + T(x)Q_j(x).$$

As

$$(x-1)^{p^{i-1}} \mid (x-1)^{\phi(p^i)} = \Phi_{p^i}(x)$$

in $\mathbb{F}_p$ and $T(1) = -1$, we see that $(x-1)^{p^{i-1}-1} \| Q_{j+1}(x)$.

It remains to show that $v_p(Q_{j+1}(1)) = i-1$. By (*) and the definition of $Q_{j+1}$, we find $Q_{j+1}(1) = \Phi_{p^i}(1)S(1) + T(1)Q_j(1) = pS(1) - Q_j(1) = -p^{i-1}R(1)$, so $v_p(Q_{j+1}(1)) \ge i-1$. However, if $p^i \mid Q_{j+1}(1)$, then $p \mid R(1)$, so writing (*) in $\mathbb{F}_p$ we have $Q_j(x) = (x-1)^{p^{i-1}-1} R(x)$. But then $(x-1)^{p^{i-1}} \mid Q_j(x)$, contradicting our inductive hypothesis.

Thus our induction is complete.

Clearly this construction shows that the order of any sequence is at most $M = p^i + (j-1)\phi(p^i)$. On the other hand, it is easy to show that the order of $(1, 0, \ldots, 0)$ is $M$. Indeed, note that $g(x) = x$ for this sequence, and suppose $x(x-1)^{M-1}/(x^{p^i}-1)$ leaves a remainder with coefficients all divisible by $p^j$. From the induction statement, we have

$$(x-1)^{M-1} = \frac{x^{p^i}-1}{x-1} P_j(x) + p^j Q_j(x),$$

so writing $P_j(x) = (x-1)U(x) + V$ for an integer $V$, we get $p^j \mid V$. But then plugging in 1 to this equation, $0 = (0)U(1) + (p^i)V + p^j Q_j(1)$, whence $p^i \mid Q_j(1)$, contradiction.

3. (Classical umbral calculus) Using linear operators, one can deal with recurrences more easily. This is a powerful idea, for instance, when computing recurrences mod prime powers. For instance, we can apply this to the Touchard polynomials $T_n(x) = \sum_{k=1}^{n} S(n,k)x^k$, using the identity $T_{n+1}(x) = x\sum_{k=0}^{n}\binom{n}{k}T_k(x)$ and defining the linear operator $L(x^n) = T_n(x)$. We can, of course, set particular values of $x$, e.g. $\pm 1$ for the Bell and Uppuluri-Carpenter numbers, respectively. Then using the Frobenius endomorphism we can get some nice recurrences.

   This also applies to linear recurrences, e.g. for any starting values, $a_n = a_{n-1} + a_{n-p}$ has period dividing $p^2 - 1$. However, this can also be done with generating functions, noting that the sequence must be purely periodic.

4. Solve

$$x^n - 1 = (3 + 3x + \cdots + 3x^9 + 2x^{10} + 2x^{11} + \cdots + 2x^{1209} + x^{1210} + x^{1211} + \cdots + x^{146409})f(x) + 11 \cdot g(x).$$