Gromow-Witten Invariants and Elliptic Genera

Grünberg, D.B.

Citation for published version (APA):
Appendix E

Binomial Congruences

We now prove a lemma from number theory, involving congruences of binomial coefficients (warm thanks to Matthijs Coster):

Lemma E.0.1. For $p$ prime and $n, k \in \mathbb{N}$ we have

$$\binom{np}{kp} \equiv \binom{np-1}{kp-1} \mod p^{3l} \quad \text{for } p > 3, \text{(and } \mod p^{3l-1} \forall p)$$

Proof. We use the notation $\prod', \Sigma'$ for a product or a sum skipping multiples of $p$, and we define $S(n) := \sum_{i=1}^{n} \frac{1}{i}$ and $S_2(n) := \sum_{i=1}^{n} \frac{1}{i^2}$. Note also that all non-multiples of $p$ have an inverse, i.e. that $(\mathbb{Z}/p\mathbb{Z})^*$ is a multiplicative group. We have

$$\prod_{i=1}^{\nu} \left(1 + \frac{kp}{i}\right) = \prod' \frac{kp}{i} + \frac{i}{i} \frac{kp}{i} - \frac{i}{i} = \prod' \left(1 - \frac{k^2p^{2l}}{i^2}\right) \equiv 1 + k^2p^{2l}S_2(kp) \mod p^{3l}$$

except for an extra minus sign for the second line if $p = 2$, $l = 1$, $k$ odd. The l.h.s. is $1 + S(kp)kp - \frac{S_2(kp)}{2}kp^2 \mod p^{3l}$. Comparing both sides $\mod p^{2l}$, we find that $S(kp) \equiv 0 \mod p$. Comparing $\mod p^{2l}$ yields $kS(kp) + \frac{k^2}{2}S_2(kp)p \equiv 0 \mod p^{2l}$; and using $S_2(kp) \equiv 0 \mod p$ ($p > 3$) from Lemma E.0.3, we obtain

$$S(kp) \equiv 0 \mod p^{2l} \quad \text{for } p > 3,$$

while only $\mod p^{2l-1}$ for $p = 3$, and $\mod p^{2l-2}$ for $p = 2$ (as the coefficient $\frac{1}{2}$ takes away one power of $p$).

We now turn to the binomial coefficients: Note first that they both have the same number of multiples of $p$, namely the number of multiples of $p$ lying in the interval $[n-k, n]$ or $[k, n]$ – whichever interval is smaller. We assume that they
actually do not contain multiples of $p$, so that we can consider their quotient. If they do, their difference will contain even more powers of $p$ than $p^{3l}$, so that we could strengthen our result.

\[
\left(\frac{n!}{k!p^l}\right) / \left(\frac{n!}{k!p^{l-1}}\right) = \frac{n! \ldots ((n-k)p^l+1)}{n! \ldots ((n-k)p^{l-1}+1)} \frac{(kp^l-1)!}{(kp^l)!}
\]

\[
= \prod_{i=1}^{kp^l} \frac{(n-k)p^l+i}{p^{kp^l-1}} \frac{p^{-kp^l-1}}{kp^l-i}
\]

\[
= \prod_{i=1}^{kp^l} \left(1 + \frac{(n-k)p^l}{i}\right) = \prod_{i=1}^{kp^l} \left(1 + \frac{(n-k)p^l}{i}\right)
\]

\[
\equiv 1 + p^l(n-k)S(kp^l) + p^{2l}(n-k)^2 \frac{S_2(kp^l) - S_2(kp^l)}{2} \mod p^{3l}
\]

\[
\equiv 1 \mod p^{3l}
\]

by the above. \hfill \Box

As a special case of the lemma, for $n = 2, k, l = 1$, we obtain $(\binom{2p}{p}) \equiv 2 \mod p^3$, or Wolstenholme's theorem:

**Corollary E.0.2.** $(\binom{2p-1}{p-1}) \equiv 1 \mod p^3$ for $p > 3$, (and mod $p^2$ \forall p).

**Lemma E.0.3.** For $l, n \in \mathbb{N}$ and $p$ prime we have

\[
S_n(p^l) := \sum_{i=1}^{p^l} i^n \equiv 0 \mod p \quad \text{if} \ (p-1) \nmid n,
\]

and $0 \mod p^{l-1}$ for any $p, n$.

**Proof.** Note that the same is true of $S_n(kp^l)$ for $k \in \mathbb{N}$, as this is merely $k$ copies (mod $p^l$) of $S_n(p^l)$. Similarly, $S_n(p^{l+1})$ is just $p$ equal copies (mod $p^l$) of $S_n(p^l)$, so by induction, we only need to prove the result for $S_n(p)$.

Let $\zeta$ be a primitive root mod $p$, i.e. a number such that the set $\{1, \zeta, \zeta^2, \ldots, \zeta^{p-1}\}$ covers all elements of the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$ of order $\phi(p) = p-1$. That is, the set is equal (mod $p$) to $\{1, 2, \ldots, p-1\}$; and similarly the set $\{1, 1/2, \ldots, 1/(p-1)^n\}$ is equal (mod $p^l$) to $\{1, \zeta^n, \zeta^{2n}, \ldots, \zeta^{n(p-2)}\}$. Hence

\[
S_n(p) \equiv 1 + \zeta^n + \cdots + \zeta^{n(p-2)} = \frac{1 - \zeta^{n(p-1)}}{1 - \zeta^n} \equiv 0 \mod p
\]

since $\zeta^{p-1} \equiv 1 \mod p$. For the denominator $1 - \zeta^n$ to be invertible mod $p$, we must exclude the case where $\zeta^n \equiv 1 \mod p$, i.e. where $n$ is a multiple of $p-1$. In this case, it still is true that $S_n(p) \equiv 0 \mod p^0$, i.e. 0 mod 1.

For $\sum i^n$, the proof runs similarly. Note that in this case we could drop the dash from the sum to include multiples of $p$, as their contribution would be $p(1 + 2 + \cdots + p^{l-1}) = p^l(p^{l-1} + 1)/2$. \hfill \Box
One could have tackled the proof of Lemma E.0.1 in other ways, in particular by writing out the binomial coefficients as factorials and using properties of factorials. For the sake of completeness, we include a useful property of residues of factorials (Wilson’s theorem):

**Proposition E.0.4.** For $p$ prime we have

$$(p - 1)! \equiv -1 \mod p \quad (p > 2),$$

and $1 \mod p$ for $p = 2$.

**Proof.** In the product $1 \ldots (p - 1)$, the numbers occur in pairs $j$ and $1/j \mod p$, except for 1 and $p - 1$ which are their own inverses, since these are the only solutions of $j^2 - 1 \equiv 0 \mod p$. Thus the product is $1(p - 1) \equiv -1 \mod p$. For $p = 2, 1$ and $p - 1$ are equal mod $p$. \hfill \Box

For higher powers of the prime $p$, $p^k!$ contains a factor of $p^1+p^2+p^3+\cdots+p^{k-1}$. We introduce the dash notation to indicate that we have skipped all these multiples of $p$: $p^k!' = p^k!/(p^{k-1}!)(p^{k-2}! \cdots p^1!)$.

**Lemma E.0.5.** For $p$ prime and $k \in \mathbb{N}$ we have

$$(p^k - 1)!' \equiv -1 \mod p \quad (p > 2),$$

and $1 \mod p$ for $p = 2$.

More generally, this result holds also mod $p^l$ for powers $k \geq l$, as we shall show below.

**Lemma E.0.6.** For $p$ prime we have:

$$(p^{k-1} - 1)!' \equiv (p - 1)!p^{k-2} \equiv -1 + n_1p^{k-1} \mod p^k \quad (p > 2, k \geq 2),$$

and $1 + p^{kl-1} \mod p^k$ for $p = 2, k \geq 4$.

Here, $n_1 \in \mathbb{Z}_p$ is defined by $(p - 1)! \equiv -1 + n_1p \mod p^2 \quad (p > 2)$.

**Proof.** By induction on $k$. The case $k = 2$ is trivial.

$$(p^{k-1} - 1)!' = [1 \cdot 2 \ldots (p^{k-2} - 1)]' [(p^{k-2} + 1)\ldots (p^{k-2} + p^{k-2} - 1)]' \ldots [((p - 1)p^{k-2} + 1)\ldots (p^{k-1} - 1)]'$$

The first square bracket is $-1 + n_1p^{k-2} \mod p^{k-1}$ by induction; i.e. it is $-1 + n_1p^{k-2} + cp^{k-1} \mod p^k$ (for some integer $c$), a quantity we denote by $a$. The second square bracket is $a + p^{k-2}(p^{k-2} - 1)!S_1(p^{k-2}) \mod p^k$. Since $S_1(p^{k-2}) \equiv 0 \mod p^{k-2}$ by lemma E.0.3 ($p \neq 2$), this is just $a \mod p^k$ if $k > 3$. (For $k = 3$, a trailing $p^2$-const won’t affect the ultimate conclusion). All remaining brackets are also $a \mod p^k$. Hence

$$(p^{k-1} - 1)!' \equiv a^p \equiv (-1 + n_1p^{k-2})^p \equiv -1 + n_1p^{k-1} \equiv (-1 + n_1p)p^{k-2} \mod p^k.$$
For $p = 2$, the anchor is at $k = 4$: $(p^3 - 1)! \equiv 1 \pmod{p^4}$. So the last line reads $a^p \equiv 1 + p^{k-1} \mod p^k$. Since we only have $S_1(p^{k-2}) \equiv 0 \mod p^{k-3}$, there is a trailing $p^{2k-5}$, which is fine for the induction with $k \geq 5$. □

**Corollary E.0.7.**

$$(p^k - 1)! \equiv -1 \mod p^k \quad (p > 2)$$

and $1 \mod p^k$ for $p = 2$.

**Proof.** l.h.s. = $[1 \ldots (p^{k-1} - 1)]' \left[(p^{k-1} + 1) \ldots (p^{k-1} + p^{k-1} - 1)\right]' \ldots [((p - 1)p^{k-1} + 1) \ldots (p - 1)]'$. By the previous lemma, the first square bracket yields $(p - 1)!p^{k-2} (p > 2)$, while the second yields the same plus $p^{k-1}(p - 1)!S_1(p)$ (which is $0 \mod p^k$), and all other square brackets yield the same. In all we have $(p - 1)!p^{k-1} \equiv (-1 + n_1 p + \ldots)p^{k-1} \equiv -1 \mod p^k$ (or $+1$ for $p = 2$). □

The same method of proof easily yields:

**Proposition E.0.8.** For prime $p$ and integers $k \geq 1$ we have

$$(p^k - 1)! \equiv -1 \mod p^l \quad (p > 2)$$

and $1 \mod p^l$ for $p = 2$.

There is no explicit formula for $(p - 1)! \mod p^2$, i.e. the integer $n_1$ in $(p - 1)! \equiv -1 + n_1 p \mod p^2$ is no evident function of $p$. In Hardy and Wright, one will find a formula reducing the factorial to terms involving $p^{k-1}$. Also, for $\mod p^3$, the recent literature exhibits ways to reduce the factorial to complicated terms involving the class number of $p$. 