MATH8510
Lecture 20 Notes

Charlie Conneen

October 9, 2022

Last lecture, we stated the following theorem:

Theorem.[1] *Fix p an odd prime and define $S_{s_0} \coloneqq \{s_0 + m(p-1) \mid m \in \mathbb{Z}_{\geq 0}\}$ for each $s_0 \in \{0, 1, \ldots, p-2\}$. The following are true:*

1. *If $s_0 \neq 0$, then $\frac{B_k}{k} \in \mathbb{Z}_{(p)}$ for all $k \in S_{s_0}$.*
2. *If $s_0 \neq 0$, then $\left(1 - p^{k-1}\right)\frac{B_k}{k} \equiv \left(1 - p^{k'-1}\right)\frac{B_{k'}}{k'} \pmod{p^{n+1}}$ for all $k, k' \in S_{s_0}$ satisfying $k \equiv k' \pmod{p^n}$.*
3. *If $s_0 = 0$, then $pB_k \equiv -1 \pmod{p}$ for all positive $k \in S_{s_0}$.*

Proof. Since $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p-1$, there exists some $\alpha \in \{2, 3, \ldots, p-1\}$ such that $\alpha^{p-1} \equiv 1 \pmod{p}$, but $\alpha^k \not\equiv 1 \pmod{p}$ for all $0 < k < p-1$. Such an α satisfies $\alpha \in \mathbb{Z} \setminus p\mathbb{Z}$, $\alpha \neq 1$, and $\alpha^{\pm k} \equiv 1 \pmod{p\mathbb{Z}_p}$ for all $k \in S_{s_0}$ with $s_0 \neq 0$.

Fix such an α as above and $k \in S_{s_0}$ where $s_0 \neq 0$. Then $\alpha^{-k} - 1 \in \mathbb{Z}_p$, and $p^{k-1} - 1 \in \mathbb{Z}_p^\times$. Therefore:

$$\begin{aligned}\left|\frac{B_k}{k}\right|_p &= \left|\left(p^{k-1} - 1\right)\frac{B_k}{k}\right|_p = \left|\frac{1}{\alpha^{-k} - 1}\int_{\mathbb{Z}_p^\times} x^{k-1}\,\mathrm{d}\mu_{1,\alpha}(x)\right|_p \\ &= \left|\int_{\mathbb{Z}_p^\times} x^{k-1}\,\mathrm{d}\mu_{1,\alpha}(x)\right|_p = \left|\mu_{1,\alpha}\left(\mathbb{Z}_p^\times\right)\right|_p \leq 1.\end{aligned}$$

This proves part (1).

For (2), fix again some α and $s_0 \neq 0$ as before, and suppose $k, k' \in S_{s_0}$ satisfy $k \equiv k' \pmod{p^n\mathbb{Z}}$. Then we have the following:

$$\begin{aligned}\left|\frac{1}{\alpha^{-k} - 1} - \frac{1}{\alpha^{-k'} - 1}\right|_p &= \left|\frac{\alpha^{-k'} - \alpha^{-k}}{(\alpha^{-k} - 1)(\alpha^{-k'} - 1)}\right|_p = \left|\alpha^{-k'} - \alpha^{-k}\right|_p \\ &= \left|\alpha^{-k} - \alpha^{-k'}\right|_p < |k - k'|_p \leq p^{-n}\end{aligned}$$

[1] Parts (1) and (2) of this theorem are due to Kummer. Part (3) is due to Von Staudt and Clausen.

Therefore:

$$\begin{aligned}\left|\int_{\mathbb{Z}_p^\times} x^{k-1}\,\mathrm{d}\mu_{1,\alpha}(x) - \int_{\mathbb{Z}_p^\times} x^{k-1}\,\mathrm{d}\mu_{1,\alpha}(x)\right|_p &= \left|\int_{\mathbb{Z}_p^\times} x^{k'-1}\Big(x^{k-k'}-1\Big)\,\mathrm{d}\mu_{1,\alpha}(x)\right|_p \\ &\le \left|\mu_{1,\alpha}\big(\mathbb{Z}_p^\times\big)\right|_p \cdot \sup_{x\in\mathbb{Z}_p^\times}\left|x^{k-k'}-1\right|_p \\ &< |k-k'|_p \le p^{-n}\end{aligned}$$

Therefore:

$$\begin{aligned}\big(1-p^{k-1}\big)\frac{B_k}{k} &= \frac{-1}{\alpha^{-k}-1}\int_{\mathbb{Z}_p^\times} x^{k-1}\,\mathrm{d}\mu_{1,\alpha}(x) \\ &\equiv \frac{-1}{\alpha^{-k'}-1}\int_{\mathbb{Z}_p^\times} x^{k-1}\,\mathrm{d}\mu_{1,\alpha}(x) \pmod{p^{n+1}\mathbb{Z}_p} \\ &\equiv \frac{-1}{\alpha^{-k'}-1}\int_{\mathbb{Z}_p^\times} x^{k'-1}\,\mathrm{d}\mu_{1,\alpha}(x) \pmod{p^{n+1}\mathbb{Z}_p} \\ &= \Big(1-p^{k'-1}\Big)\frac{B_{k'}}{k'}.\end{aligned}$$

This concludes the proof of (2).

For (3), let $\alpha = 1+p$, and suppose k is a positive multiple of $p-1$. Note that

$$pB_k = \frac{-kp}{1-p^{k-1}}\cdot\zeta_p(1-k) = \frac{-kp}{(\alpha^{-k}-1)(1-p^{k-1})}\int_{\mathbb{Z}_p^\times} x^{k-1}\,\mathrm{d}\mu_{1,\alpha}(x).$$

Since $p>2$ by assumption, $k\ge 2$. Observe that $1+p\mathbb{Z}_p$ is a multiplicative subgroup[2] of $\mathbb{Z}_p^\times$, we have

$$\begin{aligned}\frac{\big(\alpha^{-k}-1\big)\big(1-p^{k-1}\big)}{-kp} &= \alpha^{-k}\cdot\frac{\alpha^k-1}{kp}\cdot\big(1-p^{k-1}\big) \\ &= (1+p)^{-k}\left(1+p\sum_{j=0}^{k-2}\frac{1}{j+2}\binom{k-1}{j+1}p^j\right)\cdot\big(1+p\big(-p^{k-2}\big)\big) \\ &\in 1+p\mathbb{Z}_p.\end{aligned}$$

Hence, $\frac{-kp}{(\alpha^{-k}-1)(1-p^{k-1})} \equiv 1 \pmod{p\mathbb{Z}_p}$. So it now suffices to check that

$$\int_{\mathbb{Z}_p^\times} x^{k-1}\,\mathrm{d}\mu_{1,\alpha}(x) \equiv -1 \pmod{p\mathbb{Z}_p}.$$

To this end, note that $k\equiv m(p-1)$ for some $m>0$, so $\forall x\in\mathbb{Z}_p^\times$,

$$x^{k-1} = \big(x^{p-1}\big)^m\cdot x^{-1} \equiv x^{-1} \pmod{p\mathbb{Z}_p}$$

[2]The only thing to check here is that $1+p\mathbb{Z}_p$ is closed under inversion, which follows by a quick computation using a "geometric series"-like expansion. Left as an exercise.

And therefore:

$$\left|\int_{\mathbb{Z}_p^\times} x^{k-1}\,\mathrm{d}\mu_{1,\alpha}(x) - \int_{\mathbb{Z}_p^\times} x^{-1}\,\mathrm{d}\mu_{1,\alpha}(x)\right|_p \leq \left|\mu_{1,\alpha}\big(\mathbb{Z}_p^\times\big)\right|_p \cdot \sup_{x\in\mathbb{Z}_p^\times}\left|x^{k-1}-x^{-1}\right|_p \leq \frac{1}{p}$$

From this, it follows that

$$\int_{\mathbb{Z}_p^\times} x^{k-1}\,\mathrm{d}\mu_{1,\alpha}(x) \equiv \int_{\mathbb{Z}_p^\times} x^{-1}\,\mathrm{d}\mu_{1,\alpha}(x) \equiv \sum_{d=1}^{p-1}\int_{d+p\mathbb{Z}_p} x^{-1}\,\mathrm{d}\mu_{1,\alpha}(x) \pmod{p\mathbb{Z}_p}.$$

But for each $d \in \{1,2,\ldots,p-1\}$, we have

$$\left|x^{-1}-d^{-1}\right|_p = \frac{|x-d|_p}{|x|_p|d|_p} = |x-d|_p < 1$$

for all $x \in d+p\mathbb{Z}_p$. So each summand satisfies

$$\begin{aligned}
\int_{d+p\mathbb{Z}_p} x^{-1}\,\mathrm{d}\mu_{1,\alpha}(x) &\equiv \int_{d+p\mathbb{Z}_p} d^{-1}\,\mathrm{d}\mu_{1,\alpha}(x) \pmod{p\mathbb{Z}_p} \\
&= d^{-1}\cdot\mu_{1,\alpha}(d+p\mathbb{Z}_p) \\
&= d^{-1}\big(\mu_{B_1}(d+p\mathbb{Z}_p) - (1+p)^{-1}\mu_{B_1}((1+p)(d+p\mathbb{Z}_p))\big) \\
&= d^{-1}\big(\mu_{B_1}(d+p\mathbb{Z}_p) - (1+p)^{-1}\mu_{B_1}(d+p\mathbb{Z}_p)\big) \\
&= d^{-1}\left(1-\frac{1}{1+p}\right)B_1\left(\frac{d}{p}\right) \\
&= d^{-1}\left(\frac{p}{p+1}\right)\left(\frac{d}{p}-\frac{1}{2}\right) \\
&= (1+p)^{-1}\left(1+p\cdot\frac{-1}{d}\right) \\
&\equiv 1 \pmod{p\mathbb{Z}_p}.
\end{aligned}$$

Therefore:

$$\int_{\mathbb{Z}_p^\times} x^{k-1}\,\mathrm{d}\mu_{1,\alpha}(x) \equiv \sum_{d=1}^{p-1} 1 \equiv -1 \pmod{p\mathbb{Z}_p}. \qquad \blacksquare$$

Next time, we will finish up our discussion on Kummer congruences.