

## KUMMER'S LEMMA

KEITH CONRAD

Let  $p$  be an odd prime and  $\zeta = \zeta_p$  be a primitive  $p$ th root of unity. In the ring  $\mathbf{Z}[\zeta]$ , the  $p$ th power of every element is congruent to a rational integer mod  $p$ , since

$$(c_0 + c_1\zeta + \cdots + c_{p-2}\zeta^{p-2})^p \equiv c_0 + c_1 + \cdots + c_{p-2} \pmod{p}.$$

The number  $p$  is not prime in  $\mathbf{Z}[\zeta]$ , as  $(p) = (1 - \zeta)^{p-1}$ , so congruence mod  $p$  is much stronger than congruence mod  $1 - \zeta$ , where all classes have integer representatives.

Of course not every element of  $\mathbf{Z}[\zeta]$  that is congruent to a rational integer mod  $p$  is a  $p$ th power, but Kummer discovered a case when this converse statement is true, for certain primes and certain algebraic integers.

**Theorem 1** (Kummer's lemma). *Let  $p$  be a regular prime and  $u \in \mathbf{Z}[\zeta]^\times$  with  $u \equiv a \pmod{p\mathbf{Z}[\zeta]}$  for some rational integer  $a$ . Then  $u = v^p$  for some  $v \in \mathbf{Z}[\zeta]^\times$ .*

This was used by Kummer to prove Case II of FLT for regular primes.<sup>1</sup> The hypothesis in Kummer's lemma that  $u \pmod{p\mathbf{Z}[\zeta]}$  is congruent to an integer  $a$  is reformulated in the appendix to eliminate the role of  $a$ .

For our purposes, an odd  $p$  will be called *regular* if the Bernoulli numbers  $B_2, B_4, \dots, B_{p-3}$  are all prime to  $p$ . This is not the most conceptual description of regularity, but it is the form in which we will be using the property in the proof. The usual formulation of regularity, in terms of class numbers, allows for other proofs of Kummer's lemma, by class field theory [3, §6, Chap. 13] or by  $p$ -adic  $L$ -functions [4, Theorem 5.36].

We will give here a  $p$ -adic proof of Kummer's lemma, modifying the argument of Faddeev from [1, §6, Chap. 5].

The proof of Kummer's lemma requires knowing something about the unit group of  $\mathbf{Z}[\zeta]$ . Some obvious units in  $\mathbf{Z}[\zeta]$  are

$$\varepsilon_k \stackrel{\text{def}}{=} \frac{\zeta^k - 1}{\zeta - 1} \equiv k \pmod{\zeta - 1}$$

for  $1 \leq k \leq p - 1$ . While  $\varepsilon_1 = 1$ , the units  $\varepsilon_k$  for  $k > 1$  are more interesting.

There is a convenient way to rewrite the  $\varepsilon_k$ . First, since  $\zeta$  has odd order, some power of it is a square root of  $\zeta$ ; indeed,  $\zeta^{(p+1)/2}$  is a square root of  $\zeta$ . However,  $\eta \stackrel{\text{def}}{=} -\zeta^{(p+1)/2}$  turns out to be the more convenient choice of square root, since when  $\zeta = e^{2\pi i/p}$ ,  $\zeta^{(p+1)/2} = -e^{i\pi/p}$  while  $\eta = e^{i\pi/p}$ , the "nicer" square root of  $e^{2\pi i/p}$ . Furthermore, choosing  $\zeta = e^{2\pi i/p}$ ,

$$\varepsilon_k = \frac{\eta^{2k} - 1}{\eta^2 - 1} = \frac{\eta^k}{\eta} \cdot \frac{\eta^k - \eta^{-k}}{\eta - \eta^{-1}} = \eta^{k-1} \frac{\sin(k\pi/p)}{\sin(\pi/p)}.$$

Let  $\delta_k = \sin(k\pi/p)/\sin(\pi/p)$ , so  $\delta_k$  is a real (positive) unit.

The equation  $\varepsilon_k = \eta^{k-1}\delta_k$  can be generalized to any unit of  $\mathbf{Z}[\zeta]$ .

**Lemma 2.** *Every unit  $u$  of  $\mathbf{Z}[\zeta]$  has the form  $u = \zeta^r u'$ , where  $u'$  is a real unit.*

<sup>1</sup>See <https://kconrad.math.uconn.edu/blurbs/gradnumthy/fltreg.pdf>.

*Proof.* Suppose  $u = \zeta^r u'$ . Then  $\bar{u} = \zeta^{-r} u'$ , so we can divide and get  $u/\bar{u} = \zeta^{2r}$ . This suggests the idea of considering the ratio  $u/\bar{u}$  and proving it is a root of unity. Well,  $u/\bar{u}$  and all of its  $\mathbf{Q}$ -conjugates have absolute value 1, so it is a root of unity. Being in  $\mathbf{Q}(\zeta)$ , we must have  $u/\bar{u} = \pm \zeta^a$ . If we can show the plus sign holds, then write  $a \equiv 2b \pmod{p}$  and set  $u' = u/\zeta^b$  to end the proof.

Let's work mod  $(1 - \zeta)$ . Since all powers of  $\zeta$  are congruent to 1,  $u \equiv \bar{u}$ , so  $1 \equiv \pm \zeta^a \equiv \pm 1$ . Since  $1 \not\equiv -1 \pmod{(1 - \zeta)}$ , the plus sign holds.  $\square$

Let  $K = \mathbf{Q}(\zeta)$ ,  $K_p = \mathbf{Q}_p(\zeta)$ ,  $A = \mathbf{Z}[\zeta]$ ,  $A_p = \mathbf{Z}_p[\zeta]$ ,  $\sigma_j(\zeta) = \zeta^j$ ,  $\tau = \sigma_{-1}$  is complex conjugation. Denote the “real” elements of  $A_p$ , i.e. the elements fixed by  $\tau$ , as  $A_p^+$ . (A similar definition can be made for  $K_p^+$ , but we will only be focusing on real elements of  $A_p$ .) The Teichmüller lift of an integer  $k$  to  $\mathbf{Z}_p$  will be written  $\omega(k)$ .

**Lemma 3.** *In  $\mathbf{Q}_p(\zeta)$ ,  $X^{p-1} + p$  splits completely and there is a bijection between roots  $\pi$  of  $X^{p-1} + p$  and nontrivial  $p$ th roots of unity  $\zeta_\pi$ , by*

$$\pi \equiv \zeta_\pi - 1 \pmod{\pi^2}.$$

*Proof.* See [3, Lemma 3.1, Chap. 14].  $\square$

Fix a choice of  $\zeta$ , then fix a root  $\pi$  of  $X^{p-1} + p$  by  $\pi \equiv \zeta - 1 \pmod{\pi^2}$ .

Write  $\tau(\pi) = \theta\pi$ , where  $\theta^{p-1} = 1$ . Since  $\pi = \tau^2(\pi) = \theta^2\pi$ ,  $\theta = \pm 1$ . Since  $\tau(\pi) \neq \pi$ ,  $\tau(\pi) = -\pi$ . Thus  $\pi^2 \in A_p^+$ .

Since  $p$  is odd, the minimal polynomial of  $\pi^2$  over  $\mathbf{Q}_p$  is  $X^{(p-1)/2} + p$  and  $A_p = \mathbf{Z}_p[\pi]$ .

**Lemma 4.**  $A_p^+ = \mathbf{Z}_p[\pi^2]$ .

*Proof.* Left to the reader.  $\square$

Set  $m = (p-1)/2$ , so  $\mathbf{Z}_p[\pi^2]$  has  $\mathbf{Z}_p$ -basis  $\{1, \pi^2, \pi^4, \dots, \pi^{2(m-1)}\}$ .

**Lemma 5.** *For  $x, y \equiv 1 \pmod{\pi}$ ,  $|\log x - \log y| \leq |x - y|$ .*

*Proof.* Since  $\log x - \log y = \log(x/y)$  and  $|x - y| = |x/y - 1|$ , without loss of generality  $y = 1$ . Then  $x \equiv 1 \pmod{\pi} \Rightarrow |\log x| \leq |x - 1|$ . We want to show that for  $k \geq 1$ ,

$$\left| \frac{(x-1)^k}{k} \right| \leq |x-1|,$$

which is equivalent to

$$|x-1| \leq |k|^{1/(k-1)}.$$

Since  $|x-1| \leq |\pi| = (1/p)^{1/(p-1)}$ , we're done.  $\square$

**Corollary 6.** *For  $u \in \mathbf{Z}[\zeta]^\times$  with  $u \equiv a \pmod{p}$  for some rational integer  $a$ ,  $\log(u^{p-1}) \in pA_p^+$ .*

*Proof.* Since  $u^{p-1} \equiv 1 \pmod{p}$ ,  $|\log(u^{p-1})| \leq |u^{p-1} - 1| \leq 1/p$ , so  $\log(u^{p-1}) \in pA_p$ . Writing  $u = \zeta^r u'$  for real  $u'$  by Lemma 2,  $\log(u^{p-1}) = \log((u')^{p-1}) \in A_p^+$ .  $\square$

Given a unit  $u \in \mathbf{Z}[\zeta]^\times$ , write  $\log(u^{p-1}) = \sum_{i=0}^{m-1} b_i \pi^{2i}$ . A trace calculation shows  $b_0 = 0$ : for  $1 \leq k \leq p-1$ ,

$$\mathrm{Tr}_{K_p/\mathbf{Q}_p}(\pi^k) = \sum_{j=1}^{p-1} \sigma_j(\pi^k) = \left( \sum_{j=1}^{p-1} \omega(j)^k \right) \pi^k = 0.$$

So

$$\frac{p-1}{2}b_0 = \text{Tr}_{K_p/\mathbf{Q}_p}(\log(u^{p-1})) = \log(\text{N}_{K_p/\mathbf{Q}_p}(u^{p-1})) = \log(\text{N}_{K/\mathbf{Q}}(u^{p-1})) = \log(1) = 0.$$

For  $2 \leq k \leq m$ , write  $\log(\varepsilon_k^{p-1}) = \sum_{i=1}^{m-1} c_{ik}\pi^{2i}$  for some  $c_{ik} \in \mathbf{Z}_p$ . The subscripts  $i$  and  $k$  both run over sets of size  $m-1$ .

The next theorem is the technical heart of our preparations for Kummer's lemma.

**Theorem 7.** *The numbers  $\{1, \log(\varepsilon_2^{p-1}), \dots, \log(\varepsilon_m^{p-1})\}$  form a  $\mathbf{Z}_p$ -basis of  $A_p^+$  precisely when  $p$  is regular.*

*Proof.* Since  $\{1, \pi^2, \dots, \pi^{2(m-1)}\}$  is a  $\mathbf{Z}_p$ -basis of  $A_p^+$ , we shall check that the  $\mathbf{Z}_p$ -transition matrix  $(c_{ik})$  between  $\{\pi^2, \dots, \pi^{2(m-1)}\}$  and  $\{\log(\varepsilon_2^{p-1}), \dots, \log(\varepsilon_m^{p-1})\}$  has determinant in  $\mathbf{Z}_p^\times$ , or rather than its determinant mod  $p$  is nonzero.

Write

$$\varepsilon_k^{p-1} = \varepsilon_k^p \frac{\zeta - 1}{\zeta^k - 1}.$$

Since  $\varepsilon_k \equiv k \pmod{\pi}$ ,

$$\begin{aligned} \varepsilon_k^p &\equiv k^p \pmod{\pi^p} \\ &\equiv k^p \pmod{\pi^{p-1}} = -p \\ &\equiv k \pmod{p}. \end{aligned}$$

Therefore  $\varepsilon_k^{p-1} \equiv k(\zeta - 1)/(\zeta^k - 1) \pmod{p}$ , so by Lemma 5,

$$\log(\varepsilon_k^{p-1}) \equiv \log(k(\zeta - 1)/(\zeta^k - 1)) \pmod{p}.$$

Let's use the Dwork series  $E(X) = e^{X+X^p/p}$  to express  $\zeta$  in terms of  $\pi$  [3, Theorem 3.2, Chap. 14]:  $E(\pi) = \zeta$  and  $E(\omega(k)\pi) = \zeta^k$ . We will write  $\omega(k)\pi$  as  $\pi_k$ . So

$$\begin{aligned} \varepsilon_k^{p-1} &\equiv k \frac{\zeta - 1}{\zeta^k - 1} \pmod{p} \\ &= k \frac{E(\pi) - 1}{E(\pi_k) - 1} \\ &\equiv \omega(k) \frac{E(\pi) - 1}{E(\pi_k) - 1} \pmod{p} \\ &= \frac{\pi_k}{E(\pi_k) - 1} \cdot \frac{E(\pi) - 1}{\pi}. \end{aligned}$$

Since  $\zeta^k = E(\pi_k) \equiv 1 + \pi_k \pmod{\pi^2}$ , we have

$$(1) \quad \log(\varepsilon_k^{p-1}) \equiv \log\left(\frac{E(\pi) - 1}{\pi}\right) - \log\left(\frac{E(\pi_k) - 1}{\pi_k}\right) \pmod{p}.$$

Writing  $E(X) = \sum a_n X^n$ ,  $(E(\pi) - 1)/\pi = \sum_{n \geq 1} a_n \pi^{n-1}$ . When is  $a_n \pi^{n-1} \equiv 0 \pmod{p}$ ? In [3, p. 322],  $e_n$  denotes  $a_n \pi^n$  and some lower bound estimates on  $\text{ord}_p(e_n)$  are proved that imply  $\text{ord}_p(a_n \pi^{n-1}) \geq 1$  if  $n \geq p^3/(p-1)^2$ . But the lower bound is true for  $n \geq p$ . Rather than work with the lower bound estimates in [3] to squeeze out this more delicate information, we will use [2, Theorem 3.5], which gives a sharper lower bound on  $\text{ord}_p(a_n)$ .

For  $n \geq p^2$ , that bound is

$$\text{ord}_p(a_n) \geq \frac{n}{p^2} \left(2 + \frac{1}{p-1}\right) - \frac{1}{p-1} \geq \left(2 + \frac{1}{p-1}\right) - \frac{1}{p-1} = 2,$$

so  $\text{ord}_p(a_n \pi^{n-1}) \geq 2 + (n-1)/(p-1) \geq 2 + (p^2-1)/(p-1) = p+3 \geq 5$ . If  $p \leq n \leq p^2-1$  then  $a_n$  is a  $p$ -adic integer since  $E(X)$  and the Artin–Hasse series have the same coefficients up through degree  $p^2-1$ , so  $\text{ord}_p(a_n \pi^{n-1}) \geq (n-1)/(p-1) \geq (p-1)/(p-1) = 1$ . Therefore

$$\frac{E(\pi) - 1}{\pi} \equiv \sum_{n=1}^{p-1} a_n \pi^{n-1} \equiv \sum_{n=1}^{p-1} \frac{\pi^{n-1}}{n!} \pmod{p}$$

since  $a_n = 1/n!$  for  $0 \leq n \leq p-1$ . Thus

$$(2) \quad \log \left( \frac{E(\pi) - 1}{\pi} \right) \equiv \log \left( \sum_{n=1}^{p-1} \frac{\pi^{n-1}}{n!} \right) \pmod{p}.$$

The sum  $\sum_{n=1}^{p-1} \pi^{n-1}/n!$  looks like a truncation of the full series  $(e^\pi - 1)/\pi$ . But the latter makes no sense, since  $\pi$  is not in the disc of convergence of  $e^X$ . Nevertheless, progress will come from looking at the formal power series  $\log((e^X - 1)/X)$ .

Since we are computing logarithms only modulo  $p$ , we can truncate log series. To determine how far out we need to go, let's figure out when  $|(x-1)^n/n| \leq |p|$  for  $|x-1| \leq |\pi|$ .

**Lemma 8.** *For  $n \geq p+1$ ,  $|\pi^n/n| \leq |p|$ .*

*Proof.* We need to determine when  $n/(p-1) \geq \text{ord}_p(n) + 1$ . If  $\text{ord}_p(n) = 0$ , this holds when  $n \geq p-1$ . If  $\text{ord}_p(n) = 1$ , this holds as long as  $n \neq p$ . If  $\text{ord}_p(n) \geq 2$ , this always holds.  $\square$

The inequality in the lemma is true for  $n = p-1$ , but we won't need this.

So if  $|x-1| \leq |\pi|$ ,  $\log x \equiv \sum_{n=1}^p (-1)^{n-1} \frac{(x-1)^n}{n} \pmod{p}$ . The last term in the sum is more subtle than the rest since it has a  $p$  in the denominator. So let's isolate the last term.

Let

$$L_{p-1}(1+T) \stackrel{\text{def}}{=} \sum_{n=1}^{p-1} (-1)^{n-1} \frac{T^n}{n} \in \mathbf{Z}_p[T],$$

so  $x \equiv 1 \pmod{\pi} \Rightarrow \log x \equiv L_{p-1}(x) + (x-1)^p/p \pmod{p}$ . Writing  $\alpha = \sum_{n=2}^{p-1} \pi^{n-1}/n!$ , by (2)

$$\log \left( \frac{E(\pi) - 1}{\pi} \right) \equiv \log(1 + \alpha) \equiv L_{p-1}(1 + \alpha) + \frac{\alpha^p}{p} \pmod{p}.$$

Let's compute the last term:

$$\frac{\alpha^p}{p} = \frac{1}{p} \left( \pi \sum_{n=2}^{p-1} \frac{\pi^{n-2}}{n!} \right)^p = -\pi \left( \sum_{n=2}^{p-1} \frac{\pi^{n-2}}{n!} \right)^p.$$

For  $2 \leq n \leq p-1$ ,  $\pi^{n-2}/n! \in A_p$ , so

$$\begin{aligned} \left( \sum_{n=2}^{p-1} \frac{\pi^{n-2}}{n!} \right)^p &\equiv \sum_{n=2}^{p-1} \left( \frac{\pi^{n-2}}{n!} \right)^p \pmod{p} \\ &\equiv \sum_{n=2}^{p-1} \frac{(\pi^p)^{n-2}}{n!} \pmod{p} \\ &\equiv \frac{1}{2} \pmod{p} \quad \text{since } \pi^p \equiv 0 \pmod{p}. \end{aligned}$$

Thus

$$(3) \quad \log \left( \frac{E(\pi) - 1}{\pi} \right) \equiv L_{p-1}(1 + \alpha) - \pi/2 \pmod{p}.$$

Since  $L_{p-1}(1 + T) \in \mathbf{Z}_p[T]$ ,  $L_{p-1}(1 + \alpha) = L_{p-1} \left( \sum_{n=1}^{p-1} \pi^{n-1}/n! \right) \in \mathbf{Z}_p[\pi]$ . We only care about its expression mod  $p = -\pi^{p-1}$ . Let's compute the polynomial  $L_{p-1} \left( \sum_{n=1}^{p-1} T^{n-1}/n! \right)$  in  $\mathbf{Z}_p[T]/T^{p-1}$ . Actually, it turns out to be more convenient to work in  $\mathbf{Q}_p[[T]]/T^{p-1}$ , where we can use the full exponential and logarithm series, whose coefficients are usually not in  $\mathbf{Z}_p$ . Whatever we compute in this larger ring for  $L_{p-1} \left( \sum_{n=1}^{p-1} T^{n-1}/n! \right)$  must be in  $\mathbf{Z}_p[T]/T^{p-1}$ .

For  $f(T) \in 1 + T\mathbf{Q}_p[[T]]$ ,  $L_{p-1}(f(T)) \equiv \log(f(T)) \pmod{T^p}$ , so from  $\sum_{n=1}^{p-1} \frac{T^{n-1}}{n!} \equiv \frac{e^T - 1}{T} \pmod{T^{p-1}}$  we get

$$L_{p-1} \left( \sum_{n=1}^{p-1} \frac{T^{n-1}}{n!} \right) \equiv L_{p-1} \left( \frac{e^T - 1}{T} \right) \equiv \log \left( \frac{e^T - 1}{T} \right) \pmod{T^{p-1}}.$$

This last expression is tractable, and is where Bernoulli numbers enter. To find the expansion for  $\log((e^T - 1)/T)$ , we differentiate the series:

$$\begin{aligned} \frac{d}{dT} \log \left( \frac{e^T - 1}{T} \right) &= \frac{T}{e^T - 1} \cdot \frac{T e^T - (e^T - 1)}{T^2} \\ &= \frac{e^T}{e^T - 1} - \frac{1}{T} \\ &= 1 + \frac{1}{e^T - 1} - \frac{1}{T} \\ &= \frac{1}{T} \left( T + \frac{T}{e^T - 1} - 1 \right) \\ &= \frac{1}{T} \left( T + \sum_{n \geq 1} \frac{B_n}{n!} T^n \right) \\ &= \frac{1}{T} \left( \frac{1}{2} T + \sum_{i \geq 1} \frac{B_{2i}}{(2i)!} T^{2i} \right) \\ &= \frac{1}{2} + \sum_{i \geq 1} \frac{B_{2i}}{(2i)!} T^{2i-1}. \end{aligned}$$

Integrating and noting the constant term must vanish,

$$\log\left(\frac{e^T - 1}{T}\right) = \frac{T}{2} + \sum_{i \geq 1} \frac{B_{2i}}{(2i)!2i} T^{2i} \equiv \frac{T}{2} + \sum_{i=1}^{m-1} \frac{B_{2i}}{(2i)!2i} T^{2i} \pmod{T^{p-1}}.$$

So  $L_{p-1}(\sum_{n=1}^{p-1} T^{n-1}/n!) \equiv T/2 + \sum_{i=1}^{m-1} (B_{2i}/(2i)!2i) T^{2i}$  in  $\mathbf{Z}_p[T]/T^{p-1}$ , and by (3)

$$\log\left(\frac{E(\pi) - 1}{\pi}\right) \equiv \sum_{i=1}^{m-1} \frac{B_{2i}}{(2i)!2i} \pi^{2i} \pmod{p}.$$

Similarly,

$$\log\left(\frac{E(\pi_k) - 1}{\pi_k}\right) \equiv \sum_{i=1}^{m-1} \frac{B_{2i}}{(2i)!2i} k^{2i} \pi^{2i} \pmod{p}$$

since  $\pi_k \equiv k\pi \pmod{p}$ .

Putting these congruences together, we can compute  $\log(\varepsilon_k^{p-1}) \pmod{p}$  by (1):

$$\log(\varepsilon_k^{p-1}) \equiv \sum_{i=1}^{m-1} \frac{B_{2i}}{(2i)!2i} (1 - k^{2i}) \pi^{2i} \pmod{p}.$$

So  $c_{ik} \equiv \frac{B_{2i}}{(2i)!2i} (1 - k^{2i}) \pmod{p}$ . Therefore

$$\det(c_{ik}) \equiv \prod_{i=1}^{m-1} \frac{-B_{2i}}{(2i)!(2i)} \begin{vmatrix} 2^2 - 1 & 3^2 - 1 & \dots & m^2 - 1 \\ 2^4 - 1 & 3^4 - 1 & \dots & m^4 - 1 \\ \vdots & \vdots & \ddots & \vdots \\ 2^{2(m-1)} - 1 & 3^{2(m-1)} - 1 & \dots & m^{2(m-1)} - 1 \end{vmatrix} \pmod{p}.$$

We can rewrite the last determinant in Vandermonde form. It equals

$$\begin{vmatrix} 1 & 0 & \dots & 0 \\ 1 & 2^2 - 1 & \dots & m^2 - 1 \\ 1 & 2^4 - 1 & \dots & m^4 - 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 2^{2(m-1)} - 1 & \dots & m^{2(m-1)} - 1 \end{vmatrix} = \begin{vmatrix} 1 & 1 & \dots & 1 \\ 1 & 2^2 & \dots & m^2 \\ 1 & 2^4 & \dots & m^4 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 2^{2(m-1)} & \dots & m^{2(m-1)} \end{vmatrix} \\ = \prod_{1 \leq i < j \leq m} (j^2 - i^2) \\ \not\equiv 0 \pmod{p}.$$

Therefore  $\det(c_{ik}) \not\equiv 0 \pmod{p}$  precisely when none of  $B_2, B_4, \dots, B_{2(m-1)} = B_{p-3}$  is divisible by  $p$ .  $\square$

We now prove Kummer's lemma.

*Proof.* First let's show  $u$  is real, i.e.  $u$  is fixed by complex conjugation. By Lemma 2,  $u = \zeta^r u'$  for  $u'$  a real unit. So  $u' \in A_p^+ = \mathbf{Z}_p[\pi^2]$ . Thus  $u' \equiv b \pmod{\pi^2}$  for some rational integer  $b$ . Since  $\zeta^r \equiv 1 + r\pi \pmod{\pi^2}$ , we have  $u \equiv b + br\pi \pmod{\pi^2}$ . Since  $u$  is congruent to a rational integer mod  $p$  and  $p = -\pi^{p-1}$ , we must have  $br \equiv 0 \pmod{p}$ , so  $p \mid r$ , hence  $u = u'$ .

Without loss of generality, we may take  $u$  to be positive.

We will work in the group of real positive units of  $A = \mathbf{Z}[\zeta]$ , since that group has no torsion. Recall  $\delta_k$  from before Lemma 2. By Theorem 7, the numbers  $\log(\delta_k^{p-1}) = \log(\varepsilon_k^{p-1})$

are linearly independent over  $\mathbf{Q}_p$  for  $2 \leq k \leq m$ , so the  $m - 1$  units  $\delta_k$  are multiplicatively independent over  $\mathbf{Z}$ . There are  $m - 1$  of them, and  $A^\times$  has rank  $\frac{p-1}{2} - 1 = m - 1$  by the Dirichlet Unit Theorem, so the subgroup generated by the  $\delta_k$ 's has finite index in the group of all units. In particular, for some positive integer  $n$  we have

$$(4) \quad u^n = \prod_{k=2}^m \delta_k^{c_k}$$

for  $c_k \in \mathbf{Z}$ . Since the real positive units have no torsion, we may assume  $\gcd(n, c_2, \dots, c_m) = 1$ . Raising both sides of (4) to the  $(p - 1)$ th power and then taking logarithms, we get

$$n \log(u^{p-1}) = \sum_{k=2}^{m-1} c_k \log(\delta_k^{p-1}).$$

By Corollary 6,  $\log(u^{p-1}) \in pA_p^+$ , so all  $c_k$  lie in  $p\mathbf{Z}_p$ . Since they are rational integers, all  $c_k$  lie in  $p\mathbf{Z}$ , so  $u^n$  is a  $p$ th power of a unit in  $\mathbf{Z}[\zeta]$ . From  $\gcd(n, c_2, \dots, c_m) = 1$  we see  $n$  is prime to  $p$ , so  $u$  is a  $p$ th power of a unit in  $\mathbf{Z}[\zeta]$ .  $\square$

This proof of Kummer's lemma used the units  $\delta_k$  rather than the units  $\varepsilon_k$  only because we needed to work in a group of units where there is no torsion, so the assumption  $\gcd(n, c_2, \dots, c_m) = 1$  could be used. While the assumption that  $p$  is regular implies that the group generated by the units  $\varepsilon_k$  has no torsion (there is only the trivial linear relation among their  $p$ -adic logarithms), it is not clear how to show the group generated by  $u$  and the  $\varepsilon_k$  has no torsion. By working in the group of positive real units (where we proved  $u$  lies) the torsion issue is easily handled.

In Faddeev's proof of Kummer's lemma in [1, §6, Chap. 5], which the proof here is based on, the Dwork series  $E(X) = e^{X+X^p/p}$  is not used. Instead, more systematic use is made of truncations of the series  $e^X$  (while  $E(X)$  is a "truncated" Artin-Hasse series). For instance, since  $\zeta = E(\pi)$ , the congruence

$$\frac{E(\pi) - 1}{\pi} \equiv \sum_{n=1}^{p-1} \frac{\pi^{n-1}}{n!} \pmod{p}$$

that we used is the same as  $\zeta \equiv e_{p-1}(\pi) \pmod{\pi^p}$ , where  $e_{p-1}(T) = \sum_{n=0}^{p-1} T^n/n!$ . This is essentially [1, Lemma 3, p. 372] with  $k = 1$  (and  $e_{p-1}(T)$  is denoted there by  $E(T)$ .)

#### APPENDIX A. REFORMULATION OF HYPOTHESIS IN KUMMER'S LEMMA

Kummer's lemma has an assumption on the unit  $u$ :  $u \equiv a \pmod{p\mathbf{Z}[\zeta]}$  for some  $a \in \mathbf{Z}$ . It is natural to ask how this can be checked in examples. The next theorem expresses the assumption in a way that makes no reference to an integer  $a$ , and it works even if  $u$  is not a unit (only in the *conclusion* of Kummer's lemma is it essential that  $u$  is a unit).

**Theorem 9.** *When  $p$  is prime and  $\alpha \in \mathbf{Z}[\zeta]$ , we have  $\alpha \equiv a \pmod{p\mathbf{Z}[\zeta]}$  for some  $a \in \mathbf{Z}$  if and only if  $\alpha^p \equiv \alpha \pmod{p\mathbf{Z}[\zeta]}$ .*

*Proof.* If  $\alpha \equiv a \pmod{p\mathbf{Z}[\zeta]}$  then  $\alpha^p \equiv a^p \pmod{p\mathbf{Z}[\zeta]}$ . Since  $a^p \equiv a \pmod{p\mathbf{Z}}$  by Fermat's little theorem,  $\alpha^p \equiv a^p \equiv a \equiv \alpha \pmod{p\mathbf{Z}[\zeta]}$ .

To prove the converse, recall that as ideals  $(p) = (\zeta - 1)^{p-1}$  in  $\mathbf{Z}[\zeta]$  and the residue field of  $\mathbf{Z}[\zeta]$  at  $(\zeta - 1)$  is  $\mathbf{F}_p$ . Setting  $\pi = \zeta - 1$ , for each  $k \in \mathbf{Z}^+$  every residue class in  $\mathbf{Z}[\zeta]/(\pi^k)$

has a unique representative

$$(5) \quad a_0 + a_1\pi + \cdots + a_{k-1}\pi^{k-1} \pmod{\pi^k \mathbf{Z}[\zeta]}$$

where  $0 \leq a_i \leq p-1$  for all  $i$ .

Taking  $k = p-1$ , we can write  $\alpha \pmod{p\mathbf{Z}[\zeta]}$  uniquely as

$$\alpha \equiv a_0 + a_1\pi + \cdots + a_{p-2}\pi^{p-2} \pmod{p\mathbf{Z}[\zeta]}$$

where  $0 \leq a_i \leq p-1$  for  $i = 0, 1, \dots, p-2$ . Since  $\mathbf{Z}[\zeta]/(p)$  is a ring with characteristic  $p$ , the  $p$ -th power map is additive on this ring. Since  $a_i^p \equiv a_i \pmod{p\mathbf{Z}}$  and  $\pi^p \equiv 0 \pmod{p\mathbf{Z}[\zeta]}$ ,

$$\alpha^p \equiv a_0^p + a_1^p\pi^p + \cdots + a_{p-2}^p\pi^{p(p-2)} \equiv a_0^p \equiv a_0 \pmod{p\mathbf{Z}[\zeta]}.$$

Thus if  $\alpha^p \equiv \alpha \pmod{p\mathbf{Z}[\zeta]}$  then

$$a_0 \equiv a_0 + a_1\pi + \cdots + a_{p-2}\pi^{p-2} \pmod{p\mathbf{Z}[\zeta]},$$

which is the same as  $a_1\pi + \cdots + a_{p-2}\pi^{p-2} \equiv 0 \pmod{p\mathbf{Z}[\zeta]}$ . That implies  $a_i = 0$  for  $i > 0$ , so  $\alpha \equiv a_0 \pmod{p\mathbf{Z}[\zeta]}$ .  $\square$

How often is an  $\alpha$  in  $\mathbf{Z}[\zeta]$  congruent to an integer modulo  $(\pi^k)$ ? It happens for all  $\alpha$  if  $k = 1$ , since  $\mathbf{Z}[\zeta]/(\pi) \cong \mathbf{F}_p$ , so take  $k \geq 2$ . By (5),  $\mathbf{Z}[\zeta]/(\pi^k)$  has  $p^k$  congruence classes in total, while the condition that  $\alpha \pmod{p\mathbf{Z}[\zeta]}$  is congruent to an integer means  $a_i = 0$  for  $1 \leq i \leq k-1$ , so there are only  $p$  such congruence classes. Thus the proportion of congruence classes mod  $(\pi^k)$  that are represented by an integer is  $p/p^k = 1/p^{k-1} \leq 1/p \leq 1/2$ .

**Corollary 10.** *When  $p$  is prime,  $\zeta_{p^r}$  is a root of unity of order  $p^r$  for some  $r \geq 1$ , and  $\alpha \in \mathbf{Z}[\zeta_{p^r}]$ , we have  $\alpha \equiv a \pmod{p\mathbf{Z}[\zeta_{p^r}]}$  for some  $a \in \mathbf{Z}$  if and only if  $\alpha^p \equiv \alpha \pmod{p\mathbf{Z}[\zeta_{p^r}]}$ .*

*Proof.* In  $\mathbf{Z}[\zeta_{p^r}]$ , which is the ring of integers of  $\mathbf{Q}(\zeta_{p^r})$ ,  $p$  is totally ramified with  $(p) = (\zeta_{p^r} - 1)^{\varphi(p^r)}$ . Run through the proof of Theorem 9 with  $\zeta_{p^r}$  in place of  $\zeta$  and  $\varphi(p^r)$  in place of  $p-1$ , which is  $\varphi(p)$ .  $\square$

Just as the natural map  $\mathbf{Z}/(p^k) \rightarrow \mathbf{Z}_p/(p^k)$  is an isomorphism for all  $k \in \mathbf{Z}^+$ , the natural map  $\mathbf{Z}[\zeta_{p^r}]/(\zeta_{p^r} - 1)^k \rightarrow \mathbf{Z}_p[\zeta_{p^r}]/(\zeta_{p^r} - 1)^k$  is an isomorphism for all  $k \in \mathbf{Z}^+$ , so Corollary 10 is true with  $\mathbf{Z}_p[\zeta_{p^r}]$  in place of  $\mathbf{Z}[\zeta_{p^r}]$ .

## REFERENCES

- [1] Z. I. Borevich and I. R. Shafarevich, “Number Theory,” Academic Press, New York, 1966.
- [2] K. Conrad, Artin–Hasse-type series and roots of unity, <http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/AHrootofunity.pdf>.
- [3] S. Lang, “Cyclotomic Fields I and II,” Springer-Verlag, New York, 1994.
- [4] L. Washington, “An Introduction to Cyclotomic Fields,” Springer-Verlag, New York, 1997.