Existence of Primitive Roots via p-adic Numbers

LEONARD TOMCZAK

Let $k \geq 1$ be an integer. A *primitive root* mod k is an integer a coprime to k such that a^n mod k runs through the set of all residue classes mod k coprime to k. In group theoretic language, a primitive root is a generator of the multiplicative group $(\mathbb{Z}/k\mathbb{Z})^\times$. The basic result concerning existence of primitive roots is:

Theorem 1 ([IR82, Proposition 4.1.3])**.** *There exists a primitive root mod k, in other words $(\mathbb{Z}/k\mathbb{Z})^\times$ is cyclic, if and only if $k = 2, 4, p^n$ or $2p^n$ for some odd prime p and $n \geq 1$.*

Necessity of this condition is not difficult. However, sufficiency requires a little bit more work. One easily reduces this to the case $k = p^n$ for p an odd prime. Thus, we want to show that for odd primes p, $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is cyclic. Various proofs of this are known. A basic approach is to first prove this in the case $n = 1$ - in which case this is just the fact that a finite subgroup of the multiplicative group of a field is cyclic. Then one proceeds inductively and shows that one can lift primitive roots mod p^n to primitive roots mod p^{n+1}. This method can be found e.g. in [IR82, p. 43, Theorem 2]. Some time ago I learnt about another method of proving this which I want to present in this note. It also provides a somewhat conceptual reason why the claim fails for $p = 2$.

Assume $p > 2$ for now. Our goal is to prove that $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is cyclic, i.e.

$$(\mathbb{Z}/p^n\mathbb{Z})^\times \cong (\mathbb{Z}/(p^{n-1}(p-1))\mathbb{Z}, +).$$

This can be seen as an isomorphism between a multiplicative group and an additive group. We all know of a function which turns addition into multiplication: The exponential function. It gives an isomorphism $\exp : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$ of the additive group of real numbers with the multiplicative group of positive reals. Wouldn't it be nice if we had something similar for $\mathbb{Z}/p^n\mathbb{Z}$? Indeed, there is such a thing, although not over $\mathbb{Z}/p^n\mathbb{Z}$, but over the p-adic numbers $\mathbb{Q}_p$. Just as the reals they form a field, complete with respect to an absolute value. Thus, it makes sense to define the p-adic exponential function by the series

$$\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!},$$

whenever this converges. While over the reals this power series had infinite radius of convergence, this is no longer the case over the p-adics. We have:

Lemma 2. *Let $x \in \mathbb{Q}_p$. Then $\exp(x)$ converges if $|x| < 1$, in particular $\exp$ defines a homomorphism $p\mathbb{Z}_p \to \mathbb{Q}_p^\times$.*

Proof. This requires some basic estimates of $v_p(n!)$, see e.g. [Neu99, Chapter 2, Proposition 5.5] or [Lan94, p. 187]. □

Note that one can analogously define the p-adic logarithm and study its convergence. One then finds that it converges on the open ball of radius 1 centered at 1 and defines an inverse to exp so that analogously to the real case we get an isomorphism of additive and multiplicative groups:

Theorem 3 ([Neu99, Chapter 2, Proposition 5.5])**.** *The exponential function induces isomorphisms* $(p^n\mathbb{Z}_p, +) \cong (1 + p^n\mathbb{Z}_p, \cdot)$ *where* $n \geq 1$.

The final ingredient we need is that we have a splitting $\mathbb{Z}_p^\times \cong (1 + p\mathbb{Z}_p) \times (\mathbb{Z}/p\mathbb{Z})^\times$. This follows from Hensel's lemma, see e.g. [Neu99, Chapter 2, Proposition 5.3]. Under this isomorphism the subgroup $(1 + p^n\mathbb{Z}_p)$ corresponds to $(1 + p^n\mathbb{Z}_p) \times 0$, thus we get

$$(\mathbb{Z}/p^n\mathbb{Z})^\times \cong (\mathbb{Z}_p/p^n\mathbb{Z}_p)^\times \cong \mathbb{Z}_p^\times/(1 + p^n\mathbb{Z}_p) \cong \frac{1 + p\mathbb{Z}_p}{1 + p^n\mathbb{Z}_p} \times (\mathbb{Z}/p\mathbb{Z})^\times.$$

By Theorem 3, there is an isomorphism of $1 + p\mathbb{Z}_p$ with $p\mathbb{Z}_p$ under which $1 + p^n\mathbb{Z}_p$ is carried onto $p^n\mathbb{Z}_p$. Hence, we get get $\frac{1+p\mathbb{Z}_p}{1+p^n\mathbb{Z}_p} \cong \frac{p\mathbb{Z}_p}{p^n\mathbb{Z}_p} \cong \mathbb{Z}_p/p^{n-1}\mathbb{Z}_p \cong \mathbb{Z}/p^{n-1}\mathbb{Z}$. Putting this together, we get

$$(\mathbb{Z}/p^n\mathbb{Z})^\times \cong \mathbb{Z}/p^{n-1}\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^\times.$$

Now note that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic as it is the multiplicative group of a finite field, so $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is cyclic as the product of two cyclic groups of coprime order. This finishes the proof.

Where does this go wrong if $p = 2$? The problem is that the 2-adic exponential series does not converge on $2\mathbb{Z}_2$. It only converges on the smaller disc $2^2\mathbb{Z}_2$ and thus gives isomorphisms $(2^n\mathbb{Z}_2, +) \cong (1+2^n\mathbb{Z}_2, \cdot)$ only for $n \geq 2$. However, we can still use this to determine the structure of $(\mathbb{Z}/2^n\mathbb{Z})^\times$. Indeed, we have a similar splitting of $\mathbb{Z}_2^\times$ as above involving $1 + 2^2\mathbb{Z}_2$, namely $\mathbb{Z}_2^\times \cong (1 + 4\mathbb{Z}_2) \times (\mathbb{Z}/4\mathbb{Z})^\times$. Then proceeding as before gives (assuming $n \geq 2$):

$$(\mathbb{Z}/2^n\mathbb{Z})^\times \cong \mathbb{Z}/2^{n-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Thus, in some sense the non-existence of primitive roots mod 2^n for $n \geq 3$ can be attributed to the phenomenon that the 2-adic exponential series has a smaller radius of convergence than its p-adic counterparts for $p > 2$.

References

[IR82] Kenneth F. Ireland and Michael I. Rosen. *A classical introduction to modern number theory.* Vol. 84. Graduate Texts in Mathematics. Springer-Verlag, New York-Berlin, 1982.

[Lan94] Serge Lang. *Algebraic number theory.* Second. Vol. 110. Graduate Texts in Mathematics. Springer-Verlag, New York, 1994.

[Neu99] Jürgen Neukirch. *Algebraic number theory.* Vol. 322. Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer-Verlag, Berlin, 1999.

Department of Mathematics, Evans Hall, University of California, Berkeley, CA 94720, USA

Email address: `leonard.tomczak@berkeley.edu`