Primitive Roots in Hensel's *Zahlentheorie* 1913

Steve Kieffer

We review Hensel's treatment of primitive roots in his 1913 book, *Zahlentheorie*. This was the second book in which Hensel chose a portion of known number theory and redeveloped it in the framework of his still new and still underappreciated p-adic numbers. The first book was published in 1908 and treated algebraic number theory. The 1913 book took on elementary number theory.

1 Theory

That all odd prime powers have primitive roots follows in a beautiful way in Chapter 8 of Hensel's *Zahlentheorie*. There are other, more elementary ways to derive the result, but Hensel's fits wonderfully into the p-adic development of elementary number theory that he gives in this treatise.

We can sketch the argument as follows. Hensel proves that in the field $\mathbb{Q}_p$ of p-adic numbers, the equation $x^{p-1} - 1 = 0$ has precisely $p - 1$ distinct roots $w_1, w_2, \ldots, w_{p-1}$, and that in fact for each i the initial term in the p-adic representation of w_i is i itself. Hensel not only proves the mere existence of the w_i, but indicates how they can be computed, to any desired degree of accuracy.

Then, since every equation in $\mathbb{Q}_p$ reduces to a congruence mod p, and since the p-adic $(p-1)^{\text{st}}$ roots of unity $w_1, w_2, \ldots, w_{p-1}$ represent all the nonzero residue classes mod p, results regarding these roots of unity carry over to results on the group $U(p)$ of units mod p. In particular, since the w_i clearly form a cyclic group of order $p - 1$, in which, as is well known, there are exactly $\varphi(d)$ elements of order d for each divisor d of $p - 1$, the same results hold in $U(p)$. Therefore $U(p)$ in fact contains $\varphi(p - 1) > 0$ generators. This proves that each odd prime p has a primitive root.

In order to extend the result to arbitrary powers p^k of an odd prime, Hensel uses the theory of the p-adic exponential and logarithm functions. He shows that if w_{i_0} is a primitive $(p-1)^{\text{st}}$ root of unity, and if w is any p-adic number that differs from w_{i_0} in the first place after the comma (i.e. in the coefficient of p in the p-adic expansion), then w is a primitive root mod p^k, for all k.

Thus, a primitive root γ mod p will in fact be a primitive root mod all powers of p provided the first digit i_1 after the comma in the corresponding p-adic root of unity is nonzero. But i_1 is computed by first reducing i^p mod p^2, then subtracting i, and then dividing by p. Therefore, i_1 is zero if and only if

$i^p \equiv i \bmod p^2$. Furthermore, in the case that $i_1 = 0$, then $\gamma + p$ is a primitive root mod all powers of p. Thus we have proved the:

Lemma 1. *Suppose γ is a primitive root mod p. Then $\gamma + p$ or γ is a primitive root mod p^k for all k, according to whether γ^p is or is not congruent to γ mod p^2, respectively.*

2 Computation

Hensel gives the example of $p = 13$, and computes the first five 13-adic digits of all twelve twelfth roots of unity in $\mathbb{Q}_{13}$.

Let us consider how p-adic representations of roots of unity can be computed, following Hensel's development.

We seek a p-adic number

$$w_i = i_0 + i_1 p + i_2 p^2 + i_3 p^3 + i_4 p^4 + \cdots$$

for which $i_0 = i$, and which is a root of the equation $x^{p-1} - 1 = 0$.

We can think of the process of computing the coefficients i_k of w_i as the process of computing successively better approximations of a number which when raised to the $p-1$ power gives 1. Then since in the p-adics an approximation is increasingly accurate as it holds mod increasing powers of p, the key observation becomes the following. Based on the generalized "little Fermat theorem", we have

$$\begin{array}{rcccl} i^{\varphi(p)} & = & i^{p-1} & \equiv & 1 \bmod p \\ i^{\varphi(p^2)} & = & i^{p(p-1)} & \equiv & 1 \bmod p^2 \\ i^{\varphi(p^3)} & = & i^{p^2(p-1)} & \equiv & 1 \bmod p^3 \\ i^{\varphi(p^4)} & = & i^{p^3(p-1)} & \equiv & 1 \bmod p^4 \\ & \vdots & & \vdots & \end{array}$$

Thus, the numbers $i, i^p, i^{p^2}, i^{p^3}, \ldots$ are increasingly accurate approximations of a number whose $(p-1)^{\text{st}}$ power is 1 in the p-adics. This means that we want

$$\begin{aligned} w_i &\equiv i \bmod p \\ &\equiv i^p \bmod p^2 \\ &\equiv i^{p^2} \bmod p^3 \\ &\equiv i^{p^3} \bmod p^4 \\ &\vdots \end{aligned}$$

For each $k = 0, 1, 2, \ldots$ let us therefore compute the least nonnegative residue

$a_k \bmod p^{k+1}$ such that $i^{p^k} \equiv a_k \bmod p^{k+1}$. Then we want

$$\begin{aligned} w_i &\equiv a_0 \bmod p \\ &\equiv a_1 \bmod p^2 \\ &\equiv a_2 \bmod p^3 \\ &\equiv a_3 \bmod p^4 \\ &\vdots \end{aligned}$$

which means that we should have

$$\begin{array}{rcl} a_0 &=& i_0 \\ a_1 &=& i_0 + i_1 p \qquad\qquad = \quad a_0 + i_1 p \\ a_2 &=& i_0 + i_1 p + i_2 p^2 \qquad = \quad a_1 + i_2 p^2 \\ a_3 &=& i_0 + i_1 p + i_2 p^2 + i_3 p^3 \quad = \quad a_2 + i_3 p^3 \\ & \vdots & \end{array}$$

and thus

$$\begin{aligned} i_1 &= \frac{a_1 - a_0}{p} \\ i_2 &= \frac{a_2 - a_1}{p^2} \\ i_3 &= \frac{a_3 - a_2}{p^3} \\ &\vdots \end{aligned}$$

We therefore obtain the following algorithm to compute the first N of the p-adic digits of w_i.

Algorithm 1 p-adic root of unity congruent to $i \bmod p$

1: $i_0 \leftarrow i$
2: $a_0 \leftarrow i$
3: **for** k **from** 1 **to** $N-1$ **do**
4: $\quad a_k \leftarrow i^{p^k} \bmod p^{k+1}$
5: $\quad i_k \leftarrow \frac{a_k - a_{k-1}}{p^k}$
6:
7: **return** $[i_0, i_1, i_2, \ldots, i_{N-1}]$

As for the examples Hensel gives in Chapter 8 of *Zahlentheorie*, we note that he chose to show examples just for the two primes 7 and 13. As he himself demonstrates on page 157, a primitive 12th root of unity in $\mathbb{Q}_{13}$ can be computed as the root

$$x = \sqrt{\frac{1 + \sqrt{-3}}{2}}$$

of the cyclotomic factor $x^4 - x^2 + 1$ of $x^{12} - 1$. Likewise, for the prime $p = 7$, a primitive sixth root of unity could be computed in $\mathbb{Q}_7$ as

$$x = \frac{1 + \sqrt{-3}}{2}.$$

Hensel has an easy algorithm for extracting square roots in p-adic fields, so in the two cases of $p = 7$ and $p = 13$ he manages to circumvent the general Algorithm 1.

In order to demonstrate the power of the general Algorithm using `POWMOD`, we compute the eighteen eighteenth roots of unity in $\mathbb{Q}_{19}$, where the alternative path through square roots certainly cannot be applied, since the primitive 18th root of unity $e^{i\pi/9}$ is an algebraic number of degree 6.

$$\begin{array}{lll}
w_1 = 1,\ 0\,0\,0\,0 & w_2 = 2,\ 6\,14\,4\,14 & w_3 = 3,\ 16\,7\,8\,16 \\
w_4 = 4,\ 5\,17\,17\,5 & w_5 = 5,\ 3\,3\,13\,11 & w_6 = 6,\ 12\,2\,17\,14 \\
w_7 = 7,\ 15\,7\,0\,1 & w_8 = 8,\ 15\,7\,0\,1 & w_9 = 9,\ 1\,18\,2\,17 \\
w_{10} = 10,\ 17\,0\,16\,1 & w_{11} = 11,\ 3\,11\,18\,17 & w_{12} = 12,\ 3\,11\,18\,17 \\
w_{13} = 13,\ 6\,16\,1\,4 & w_{14} = 14,\ 15\,15\,5\,7 & w_{15} = 15,\ 13\,1\,1\,13 \\
w_{16} = 16,\ 2\,11\,10\,2 & w_{17} = 17,\ 12\,4\,14\,4 & w_{18} = 18,\ 18\,18\,18\,18
\end{array}$$