Using Chebyshev polynomials to find the p-adic square roots of 2 and 3

Peter Bala, Dec 04 2022

Let $p \equiv 1$ or $7 \pmod 8$ be a prime. From elementary number theory we know that 2 is a quadratic residue modulo p, that is, there exists an integer k, $1 < k < p-1$, such that $k^2 \equiv 2 \pmod p$. By Hensel's lemma, k lifts to a p-adic integer $\alpha(k) = k + a_1 p + a_2 p^2 + \cdots$, $0 \le a_i < p-1$, such that $\alpha(k)^2 = 2$ in the ring of p-adic integers $\mathbb{Z}_p$. In these notes we show that $\alpha(k)$ is equal to the p-adic limit as $n \to \infty$ of the integer sequence $\left\{ 2\mathrm{T}_{p^n}\left(\dfrac{k}{2}\right)\right\}$, where $\{\mathrm{T}_n(x)\}$ is the sequence of Chebyshev polynomials of the first kind. We give similar results for the p-adic square roots of 3.

1. Chebyshev polynomials

For information on Chebyshev polynomials see, for example, [Rivlin]. The classical Chebyshev polynomials of the first kind $\mathrm{T}_n(x)$ satisfy the second-order linear recurrence $\mathrm{T}_n(x) = 2x\mathrm{T}_{n-1}(x) - \mathrm{T}_{n-2}(x)$ with the starting values $\mathrm{T}_0(x) = 1$ and $\mathrm{T}_1(x) = x$. We define the scaled Chebyshev polynomials of the first kind by $\widetilde{\mathrm{T}}_n(x) = 2\mathrm{T}_n\left(\dfrac{x}{2}\right)$. Both the Chebyshev polynomials and the scaled Chebyshev polynomials have integer coefficients.

There is an explicit expansion

$$\widetilde{\mathrm{T}}_n(x) = x^n + \sum_{k=1}^{[n/2]} (-1)^k \frac{n}{n-k}\binom{n-k}{k} x^{n-2k} \quad [n \ge 1]. \tag{1}$$

Thus $\widetilde{\mathrm{T}}_n(x), n \ge 1$, is a monic polynomial and for integer k and prime p we have

$$\widetilde{\mathrm{T}}_p(k) \equiv k \pmod p \tag{2}$$

by Fermat's little theorem.

Proposition 1. For integer k and prime p, the sequence $\left\{\widetilde{\mathrm{T}}_n(k) : n \ge 1\right\}$ satisfies the congruences

$$\widetilde{\mathrm{T}}_{p^r}(k) \equiv \widetilde{\mathrm{T}}_{p^{r-1}}(k) \pmod{p^r} \quad [r \ge 1]\,. \tag{3}$$

Proof. Recall that an integer sequence $\{a(n)\}$ satisfies the Gauss congruences if

$$a\left(mp^r\right) \equiv a\left(mp^{r-1}\right) \pmod{p^r} \tag{4}$$

for all primes p and all positive integers m and r. A necessary and sufficient condition for a sequence $\{a(n)\}$ to satisfy the Gauss congruences is that the series expansion of

$$\exp\left(\sum_{n\geq 1} a(n)\frac{t^n}{n}\right)$$

has integer coefficients [Carlitz].

The ordinary generating function for the Chebyshev polynomials T_n is

$$\sum_{n\geq 0} \mathrm{T}_n(x)t^n = \frac{1-tx}{1-2tx+t^2}.$$

Hence

$$\sum_{n\geq 1} \mathrm{T}_n(x)\frac{t^n}{n} = \log\left(\frac{1}{\sqrt{1-2tx+t^2}}\right)$$

and therefore

$$\sum_{n\geq 1} \widetilde{\mathrm{T}}_n(x)\frac{t^n}{n} = \log\left(\frac{1}{1-tx+t^2}\right).$$

Thus, for integer k, the power series expansion with respect to the variable t of

$$\exp\left(\sum_{n\geq 1} \widetilde{\mathrm{T}}_n(k)\frac{t^n}{n}\right) = \frac{1}{1-kt+t^2}$$

has integer coefficients. It follows from Carlitz's result that the Gauss congruences (4) hold for the sequence $\left\{\widetilde{\mathrm{T}}_n(k) : n \geq 1\right\}$. Congruence (3) is simply the particular case $m = 1$. □

An immediate consequence of Proposition 1 is that the integer sequence $\left\{\widetilde{\mathrm{T}}_{p^n}(k) : n \geq 1\right\}$ is a Cauchy sequence in the complete metric space of p-adic integers $\mathbb{Z}_p$. Denote the limit of this Cauchy sequence by $\alpha(k)$ (we suppress the dependence of $\alpha(k)$ on the prime p);

$$\alpha(k) = \text{limit\_}\{n \to \infty\}\ \widetilde{\mathrm{T}}_{p^n}(k).$$

It follows from Proposition 1 that for $n \geq 1$,

$$\begin{aligned}\widetilde{\mathrm{T}}_{p^n}(k) &\equiv \widetilde{\mathrm{T}}_p(k) \pmod p \\ &\equiv k \pmod p\end{aligned}$$

by (2). Letting $n \to \infty$ yields

$$\alpha(k) \equiv k \,(\bmod\, p)\,. \tag{5}$$

Proposition 2. For p an odd prime, the polynomial $\widetilde{\mathrm{T}}_p(x) - x$ of degree p splits into linear factors over $\mathbb{Z}_p$:

$$\widetilde{\mathrm{T}}_p(x) - x = \prod_{k=0}^{p-1} (x - \alpha(k)) . \tag{6}$$

Proof. The Chebyshev polynomials satisfy the composition identity [Rivlin]

$$\mathrm{T}_n(\mathrm{T}_m(x)) = \mathrm{T}_{nm}(x).$$

One easily checks that the scaled Chebyshev polynomials also satisfy the same composition identity

$$\widetilde{\mathrm{T}}_n\left(\widetilde{\mathrm{T}}_m(x)\right) = \widetilde{\mathrm{T}}_{nm}(x).$$

In particular, for odd prime p and integer k,

$$\widetilde{\mathrm{T}}_p\left(\widetilde{\mathrm{T}}_{p^n}(k)\right) = \widetilde{\mathrm{T}}_{p^{n+1}}(k). \tag{7}$$

Let $n \to \infty$ in (7). Since polynomials are continuous functions on $\mathbb{Z}_p$ we obtain

$$\widetilde{\mathrm{T}}_p(\alpha(k)) = \alpha(k) \tag{8}$$

Thus each p-adic integer $\alpha(k)$, $k \in \mathbb{Z}$, is a root of $\widetilde{\mathrm{T}}_p(x) - x$. Now by (5), the p-adic integers $\alpha(0), \alpha(1), \ldots, \alpha(p-1)$ are distinct. We conclude that the polynomial $\widetilde{\mathrm{T}}_p(x) - x$ of degree p splits into linear factors over $\mathbb{Z}_p$ as

$$\widetilde{\mathrm{T}}_p(x) - x = \prod_{k=0}^{p-1} (x - \alpha(k)) . \tag{9}$$

□

Using this result we can use the Chebyshev polynomials to find some p-adic square roots.

p-adic square roots of 2.

Let p be a prime with $p \equiv 1$ or $7 \pmod 8$ (these are precisely the odd primes p such that $x^2 - 2 = 0$ has a solution mod p: see A001132). Then $x^2 - 2$ divides the polynomial $\widetilde{\mathrm{T}}_p(x) - x$ in the ring $\mathbb{Z}[x]$.

Proof. Observe first that $\widetilde{\mathrm{T}}_p\left(\sqrt{2}\right) = \sqrt{2}$. This easily follows from the fact that $\mathrm{T}_n\left(\dfrac{\sqrt{2}}{2}\right) = \mathrm{T}_n\left(\cos\left(\dfrac{\pi}{4}\right)\right) = \cos\left(\dfrac{n\pi}{4}\right)$ by a well-known property of Chebyshev polynomials. Since $\widetilde{\mathrm{T}}_p(x) - x$ is a monic polynomial of degree $p \geq 3$ we can find an integral polynomial $m(x)$ and integers a and b such that $\widetilde{\mathrm{T}}_p(x) - x = m(x)(x^2-2) + ax + b$. Setting $x = \sqrt{2}$ yields $a\sqrt{2} + b = 0$ and hence $a = b = 0$. Thus $x^2 - 2$ is a factor of the polynomial $\mathrm{T}_p(x) - x$ in $\mathbb{Z}\left[x\right]$. □

For example, in the case $p = 7$, the polynomial $\widetilde{\mathrm{T}}_7(x) - x$ factorises in $\mathbb{Z}\left[x\right]$ as $x(x^2-1)(x^2-2)(x^2-4)$ leading to the factorisation of $x^2 - 2$ in the ring $\mathbb{Z}_7\left[x\right]$ as

$$x^2 - 2 = \left(x - \alpha(3)\right)\left(x - \alpha(4)\right),$$

where $\alpha(k) = \text{limit\_}\{n \to \infty\}\ \mathrm{L}_{7^n}\left(k\right)$. The 7-adic integers $\alpha(3)$ and $\alpha(4)$ are recorded in the OEIS as A051277 and A290558.

In addition, we have the factorisations in $\mathbb{Z}_7\left[x\right]$ of the quadratics

$$x^2 - 1 = \left(x - \alpha(1)\right)\left(x - \alpha(6)\right)$$

and

$$x^2 - 4 = \left(x - \alpha(2)\right)\left(x - \alpha(5)\right).$$

from which we find that $\alpha(1) = 1$ and $\alpha(6) = -1$ in the ring of 7-adic integers $\mathbb{Z}_7$ and $\alpha(2) = 2$ and $\alpha(5) = -2$ in $\mathbb{Z}_7$.

p-adic square roots of 3.

Let p be a prime with $p \equiv 1 \,\text{or}\, 11 \bmod (12)$. See A097933. Then $x^2 - 3$ divides the polynomial $\widetilde{\mathrm{T}}_p(x) - x$ in the ring $\mathbb{Z}\left[x\right]$.

Proof. The proof is exactly similar to that given above. In order to show that $\widetilde{\mathrm{T}}_p\left(\sqrt{3}\right) = \sqrt{3}$ we use the fact that $\mathrm{T}_n\left(\dfrac{\sqrt{3}}{2}\right) = \mathrm{T}_n\left(\cos\left(\dfrac{\pi}{6}\right)\right) = \cos\left(\dfrac{n\pi}{6}\right)$. □

Thus, for prime p of the form $12k \pm 1$, the quadratic $x^2 - 3$ factors over $\mathbb{Z}_p$ as $(x - \alpha(k))(x - \alpha(p-k))$, where now $0 \leq k \leq p-1$ satisfies $k^2 - 3 \equiv 0 \pmod{p}$. For example, in the case $p = 13$, the polynomial $x^2 - 3$ factors in the ring $\mathbb{Z}_{13}\left[x\right]$ as

$$x^2 - 3 = \left(x - \alpha(4)\right)\left(x - \alpha(9)\right)$$

where $\alpha(k) = \text{limit\_}\{n \to \infty\}\ \widetilde{\mathrm{T}}_{13^n}\left(k\right)$. The 13-adic integers $\alpha(4)$ and $\alpha(9)$ are recorded in the OEIS as A322087 and A322088.

We finish with a conjecture: for positive integer k, the sequence of polynomials $\left\{\widetilde{\mathrm{T}}_{k^n}(x) - x : n \geq 1\right\}$ is a divisibility sequence; that is, if n divides m then $\widetilde{\mathrm{T}}_{k^n}(x) - x$ divides $\widetilde{\mathrm{T}}_{k^m}(x) - x$ in the polynomial ring $\mathbb{Z}[x]$.

References

Carlitz, Note on a paper of Dieudonné, Proc. Amer. Math. Soc. 9 (1958), 32-33.

Rivlin, T.J., Chebyshev Polynomials: From Approximation Theory to Algebra and Number Theory, (1990). Wiley, New York.