Using Lucas polynomials to find the p-adic square roots of $-1, -2$ and -3

Peter Bala, Dec 01 2022

Let $p \equiv 1 \pmod 4$ be a prime. From elementary number theory we know that -1 is a quadratic residue modulo p, that is, there exists an integer k, $1 < k < p-1$, such that $k^2 \equiv -1 \pmod p$. 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 $\alpha(k)^2 = -1$ 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 $\{\mathrm{L}_{p^n}(k)\}$, where $\{\mathrm{L}_n(x)\}$ is the sequence of Lucas polynomials. We give similar results for the p-adic square roots of -2 and -3.

1. Lucas polynomials

The n-th Lucas polynomial $\mathrm{L}_n(x)$ (see A114525) is defined by

$$\mathrm{L}_n(x) = \left(\frac{x+\sqrt{x^2+4}}{2}\right)^n + \left(\frac{x-\sqrt{x^2+4}}{2}\right)^n. \tag{1}$$

There is an explicit expansion

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

$\mathrm{L}(n,x)$ is a monic polynomial and for prime p and integer k we have

$$\mathrm{L}_p(k) \equiv k \pmod p \tag{3}$$

by Fermat's little theorem.

The Lucas polynomials are related to the Chebyshev polynomials of the first kind at an imaginary argument by

$$\mathrm{L}_n(x) = 2i^n \mathrm{T}_n\left(-\frac{ix}{2}\right). \tag{4}$$

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

$$\mathrm{L}_{p^n}(k) \equiv \mathrm{L}_{p^{n-1}}(k) \pmod{p^n} \quad [n \ge 1]. \tag{5}$$

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

$$a(mp^r) \equiv a\left(mp^{r-1}\right) \pmod{p^r} \tag{6}$$

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. Using the generating function of the Lucas polynomials it is straightforward to show that

$$\exp\left(\sum_{n\geq 1} \mathrm{L}_n(x)\frac{t^n}{n}\right) = \sum_{n\geq 0} \mathrm{F}_{n+1}(x)t^n,$$

where $\mathrm{F}_n(x)$ denotes the n-th Fibonacci polynomial (see A168561);

$$\mathrm{F}_n(x) = \frac{1}{\sqrt{x^2+4}}\left(\left(\frac{x+\sqrt{x^2+4}}{2}\right)^n - \left(\frac{x-\sqrt{x^2+4}}{2}\right)^n\right).$$

Thus the sequence $\{\mathrm{L}_n(k)\}$ satisfies the Gauss congruences (6); congruence (5) is simply the particular case $m = 1$. □

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

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

It follows from (5) that for $n \geq 1$,

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

by (3). Letting $n \to \infty$ yields

$$\alpha(k) \equiv k \pmod{p}\,. \tag{7}$$

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

$$\mathrm{L}_p(x) - x = \prod_{k=0}^{p-1}(x - \alpha(k))\,. \tag{8}$$

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

$$\mathrm{T}_n\left(\mathrm{T}_m(x)\right) = \mathrm{T}_{nm}(x). \tag{9}$$

Using this and (4) we find that the Lucas polynomials satisfy the composition identity

$$\mathrm{L}_n\left(\mathrm{L}_m(x)\right) = \mathrm{L}_{nm}(x) \quad [m \text{ odd}].$$

In particular, for odd prime p and integer k,

$$\mathrm{L}_p\left(\mathrm{L}_{p^n}(k)\right) = \mathrm{L}_{p^{n+1}}(k). \tag{10}$$

Let $n \to \infty$ in (10). Since polynomials are continuous functions on $\mathbb{Z}_p$ we obtain

$$\mathrm{L}_p\left(\alpha(k)\right) = \alpha(k).$$

Thus each p-adic integer $\alpha(k)$, $k \in \mathbb{Z}$, is a root of $\mathrm{L}_p(x) - x$. Now by (7), the p-adic integers $\alpha(0), \alpha(1), \ldots, \alpha(p-1)$ are distinct. We conclude that the polynomial $\mathrm{L}_p(x) - x$ of degree p splits into linear factors over $\mathbb{Z}_p$ as

$$\mathrm{L}_p(x) - x = \prod_{k=0}^{p-1}\left(x - \alpha(k)\right). \tag{11}$$

□

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

p-adic square roots of -1. Let p be a prime with $p \equiv 1 \pmod 4$. See A002144. Then $x^2 + 1$ divides the polynomial $\mathrm{L}_p(x) - x$ in the ring $\mathbb{Z}[x]$.

Proof. Observe first that $\mathrm{L}_p\left(\sqrt{-1}\right) = \sqrt{-1}$. This easily follows from (4) and the fact that $\mathrm{T}_n\left(\frac{1}{2}\right) = \mathrm{T}_n\left(\cos\left(\frac{\pi}{3}\right)\right) = \cos\left(\frac{n\pi}{3}\right)$ by a well-known property of Chebyshev polynomials. Since $\mathrm{L}_p(x) - x$ is a monic polynomial of degree $p \geq 3$ we can find an integral polynomial $m(x)$ and integers a and b such that $\mathrm{L}_p(x) - x = m(x)(x^2+1) + ax + b$. Setting $x = \sqrt{-1}$ yields $a\sqrt{-1} + b = 0$ and hence $a = b = 0$. Thus $x^2 + 1$ is a factor of the polynomial $\mathrm{L}_p(x) - x$ in $\mathbb{Z}[x]$. □

From (11), it must be the case that $x^2 + 1$ splits over the ring of p-adic integers $\mathbb{Z}_p$ as $(x - \alpha(k))(x - \alpha(p-k))$, where $0 \leq k \leq p-1$ satisfies $k^2 + 1 \equiv 0 \pmod p$.

For example, in the case $p = 5$, the polynomial $\mathrm{L}_5(x) - x$ factorises in $\mathbb{Z}[x]$ as $\mathrm{L}_5(x) - x = x(x^2+1)(x^2+4)$ leading to the pair of factorisations in the ring $\mathbb{Z}_5[x]$

$$x^2 + 1 = (x - \alpha(2))(x - \alpha(3))$$

and

$$x^2 + 4 = (x - \alpha(1))(x - \alpha(4))$$

where $\alpha(k) = \text{limit\_}\{n \to \infty\}\ \mathrm{L}_{5^n}(k)$. The 5-adic integers $\alpha(k)$ are in the OEIS as $\alpha(1) =$ A269591, $\alpha(2) =$ A210850, $\alpha(3) =$ A210851 and $\alpha(4) =$ A269592.

Here is Maple code to display the first one hundred 5-adic digits of $\alpha(2)$. The program makes use of the recurrence $a(n) = a(n-1)^5 + 5a(n-1)^3 + 5a(n-1)$, with initial condition $a(1) = k$, which is satisfied by $a(n) = \mathrm{L}_{5^n}(k)$.

```
k:=2:

a := proc (n) option remember; if n = 1 then k else irem(a(n-1)^5 +
5a(n-1)^3 + 5a(n-1), 5^n) end if; end proc:

convert(a(100), base, 5);
```

p-adic square roots of -2. Let p be a prime with $p \equiv 1$ or $3 \pmod 8$ (these are precisely the odd primes p such that $x^2 + 2 = 0$ has a solution mod p: see A033203). Then $x^2 + 2$ divides the polynomial $\mathrm{L}_p(x) - x$ in the ring $\mathbb{Z}[x]$.

Proof. The proof is exacly similar to that just given. In order to show that $\mathrm{L}_p\left(\sqrt{-2}\right) = \sqrt{-2}$ we use (4) and the fact that $\mathrm{T}_n\left(\frac{\sqrt{2}}{2}\right) = \mathrm{T}_n\left(\cos\left(\frac{\pi}{4}\right)\right) = \cos\left(\frac{n\pi}{4}\right)$. $\square$

Thus $x^2 + 2$ is a factor of the polynomial $\mathrm{L}_p(x) - x$ in $\mathbb{Z}[x]$, and from (11) we see that $x^2 + 2$ factors over $\mathbb{Z}_p$ as $(x - \alpha(k))(x - \alpha(p-k))$, where now $0 \le k \le p-1$ satisfies $k^2 + 2 \equiv 0 \pmod p$.

For example, in the case $p = 11$, the polynomial $\mathrm{L}_{11}(x) - x$ factorises in $\mathbb{Z}[x]$ as $x(x^2+2)(x^4+4x^2+1)(x^4+5x^2+5)$ leading to the factorisation of x^2+2 in the ring $\mathbb{Z}_{11}[x]$ as

$$x^2 + 2 = (x - \alpha(3))(x - \alpha(8)),$$

where $\alpha(k) = \text{limit\_}\{n \to \infty\}\ \mathrm{L}_{11^n}(k)$.

In addition, we have the factorisations in $\mathbb{Z}_{11}[x]$ of the quartics

$$x^4 + 4x^2 + 1 = (x - \alpha(2))(x - \alpha(5))(x - \alpha(6))(x - \alpha(9))$$

and

$$x^4 + 5x^2 + 5 = (x - \alpha(1))(x - \alpha(4))(x - \alpha(7))(x - \alpha(10)).$$

p-adic square roots of -3. Let p be a prime with $p \equiv 1\ (6)$. See A002476. Then $x^2 + 3$ divides the polynomial $\mathrm{L}_p(x) - x$ in the ring $\mathbb{Z}[x]$.

Proof. Again, the proof follows that given above. In order to show that $\mathrm{L}_p\left(\sqrt{-3}\right) = \sqrt{-3}$ we use (4) and the fact that $\mathrm{T}_n\left(\frac{\sqrt{3}}{2}\right) = \mathrm{T}_n\left(\cos\left(\frac{\pi}{6}\right)\right) = \cos\left(\frac{n\pi}{6}\right)$. □

Thus, for prime p of the form $6k+1$, the quadratic $x^2 + 3$ factors over $\mathbb{Z}_p$ as $(x - \alpha(k))(x - \alpha(p-k))$, where now $0 \le k \le p-1$ satisfies $k^2 + 3 \equiv 0 \pmod{p}$. For example, in the case $p = 7$, the polynomial $\mathrm{L}_7(x) - x$ factorises in $\mathbb{Z}[x]$ as $x(x^2+3)(x^4+4x^2+2)$ leading to the factorisation of $x^2 + 3$ in the ring $\mathbb{Z}_7[x]$ as

$$x^2 + 3 = (x - \alpha(2))(x - \alpha(5))$$

where $\alpha(k) = \text{limit\_}\{n \to \infty\}\ \mathrm{L}_{7^n}(k)$. The 7-adic integers $\alpha(2)$ and $\alpha(5)$ are recorded in the OEIS as A290796 and A290797.

In addition, we have the factorisation in $\mathbb{Z}_7[x]$ of the quartic

$$x^4 + 4x^2 + 2 = (x - \alpha(1))(x - \alpha(3))(x - \alpha(4))(x - \alpha(6)).$$

We finish with a conjecture: for odd prime p, the sequence of polynomials $\{\mathrm{L}_{p^n}(x) - x : n \ge 1\}$ is a divisibility sequence; that is, if n divides m then $\mathrm{L}_{p^n}(x) - x$ divides $\mathrm{L}_{p^m}(x) - x$ in the polynomial ring $\mathbb{Z}[x]$.

References

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