Ramanujan Nagell in Lean

Barinder S. Banwait

March 12, 2026

Chapter 1

The Ramanujan–Nagell Theorem

The Ramanujan–Nagell equation is the Diophantine equation

$$x^2 + 7 = 2^n$$

where x is an integer and n is a natural number. The theorem, conjectured by Ramanujan and proved by Nagell, states that the only solutions are $(x, n) \in \{(\pm 1, 3),\ (\pm 3, 4),\ (\pm 5, 5),\ (\pm 11, 7),\ (\pm 181, 15)\}$.

The proof splits into two cases depending on the parity of n: the even case uses a factorization argument over $\mathbb{Z}$, while the odd case requires algebraic number theory in the ring of integers of $\mathbb{Q}(\sqrt{-7})$.

1.1 Setup: the ring of integers of $\mathbb{Q}(\sqrt{-7})$

We model $\mathbb{Q}(\sqrt{-7})$ as the quadratic algebra K = `QuadraticAlgebra` $\mathbb{Q}$ (-2) 1, where the generator ω satisfies $\omega^2 = -2 + \omega$, i.e. $\omega = (1 + \sqrt{-7})/2$. We write $R = \mathcal{O}_K$ for the ring of integers, $\theta = \omega \in R$, and $\theta' = 1 - \omega = (1 - \sqrt{-7})/2 \in R$.

Lemma 1 (Integrality of ω)**.** *The element $\omega \in K$ is integral over $\mathbb{Z}$: it satisfies $X^2 - X + 2 = 0$.*

Proof. Exhibit the monic polynomial $X^2 - X + 2$ and verify $\omega^2 - \omega + 2 = 0$. □

Lemma 2 (Integrality of $1 - \omega$)**.** *The element $1 - \omega \in K$ is integral over $\mathbb{Z}$.*

Proof. Exhibit the same monic polynomial $X^2 - X + 2$ and verify $(1 - \omega)^2 - (1 - \omega) + 2 = 0$. □

Lemma 3 (Minimal polynomial)**.** *The minimal polynomial of θ over $\mathbb{Z}$ is $X^2 - X + 2$.*

Proof. Proof in Lean source. □

Lemma 4 (Monogenicity)**.** *The ring of integers R is generated by θ over $\mathbb{Z}$: $\mathbb{Z}[\theta] = R$.*

Proof. Proof in Lean source. □

Lemma 5 (Class number one)**.** *The ring of integers R is a unique factorization domain (equivalently, the class number of $\mathbb{Q}(\sqrt{-7})$ is 1).*

Proof. Proof in Lean source. □

Lemma 6 (Class number one implies PID)**.** *The ring of integers R is a principal ideal ring.*

Proof. Proof in Lean source. □

Lemma 7 (Algebra norm equals quadratic norm)**.** *For any $z \in K$, the Mathlib algebra norm $\mathrm{Norm}_{\mathbb{Q}}(z)$ coincides with the quadratic algebra norm $z \cdot \bar{z}$.*

Proof. Proof in Lean source. □

Lemma 8 (Units are ± 1)**.** *The only units in R are ± 1.*

Proof. Proof in Lean source. □

Lemma 9 (Factorization of 2)**.** *In R, we have $\theta \cdot (1 - \theta) = 2$, i.e. $\frac{1+\sqrt{-7}}{2} \cdot \frac{1-\sqrt{-7}}{2} = 2$.*

Proof. Proof in Lean source. □

Lemma 10 (Exponent of θ)**.** *The exponent of θ (in the sense of Kummer–Dedekind) is 1. This follows immediately from the fact that $\mathbb{Z}[\theta] = R$ (Lemma 4).*

Proof. Rewrite using the characterization of exponent 1 and apply monogenicity. □

Lemma 11 (No prime divides the exponent)**.** *For any prime p, p does not divide the exponent of θ. This is immediate since the exponent equals 1 (Lemma 10).*

Proof. The exponent is 1, so $p \mid 1$ implies $p = 1$, contradicting primality. □

1.2 Parity lemmas

Lemma 12 (Odd square implies odd root)**.** *If x^2 is odd, then x is odd.*

Proof. Contrapositive: if x is even then x^2 is even. □

Lemma 13 (Powers of two are not odd)**.** *For $n \geq 1$, the number 2^n is not odd.*

Proof. 2^n is even for $n \geq 1$. □

Lemma 14 ($2^n - 7$ is odd)**.** *For all $n \neq 0$, the integer $2^n - 7$ is odd.*

Proof. 2^n is even and 7 is odd, so their difference is odd. □

Lemma 15 (x is odd)**.** *If $x^2 + 7 = 2^n$ with $n \neq 0$, then x is odd.*

Proof. $x^2 = 2^n - 7$ is odd, so x is odd. □

1.3 The even case

When n is even, say $n = 2k$, the equation becomes $x^2 + 7 = 2^{2k}$, which factors over $\mathbb{Z}$ as $(2^k + x)(2^k - x) = 7$. Since 7 is prime, this forces $n = 4$ and $x = \pm 3$.

Lemma 16 (Factorization over $\mathbb{Z}$)**.** *If $(2^k + x)(2^k - x) = 7$, then either $2^k - x = 1$ and $2^k + x = 7$, or $2^k - x = 7$ and $2^k + x = 1$.*

Proof. Both factors are positive integers whose product is the prime 7, so one factor is 1 and the other is 7. □

1.4 The odd case

When n is odd and $n \geq 5$, the proof works in the ring of integers of $\mathbb{Q}(\sqrt{-7})$. Setting $m = n-2$, we divide the equation by 4 to obtain $(x^2+7)/4 = 2^m$, which factors in R as $\theta^m \cdot \theta'^m$. The conjugate factors $(x \pm \sqrt{-7})/2$ lie in R (since x is odd) and their product equals $\theta^m \cdot \theta'^m$. Using unique factorization and coprimality, one deduces the key identity $-2\theta + 1 = \theta^m - \theta'^m$.

1.4.1 Exercises: from factorization to sign condition

The proof of the main m-condition is structured as a chain of four lemmas (exercises), followed by a sign-determination step.

Lemma 17 (Conjugate factors in R)**.** *The conjugate factors $(x \pm \sqrt{-7})/2$ lie in R (since x is odd), and their product equals $\theta^m \cdot \theta'^m$. Their difference is $2\theta - 1 = \sqrt{-7}$.*

Proof. Express the factors using θ and θ', verify the product using $\theta \cdot \theta' = 2$, and compute the difference. □

Lemma 18 (Coprimality)**.** *The conjugate factors are coprime in R. The only prime factors of* 2 *in R are θ and θ' (since $2 = \theta \cdot \theta'$). If either divided both factors, it would divide their difference $\sqrt{-7}$, but $N(\sqrt{-7}) = 7$ is not divisible by $N(\theta) = N(\theta') = 2$.*

Proof. Norm argument: any common factor divides $\sqrt{-7}$, whose norm is 7, incompatible with the norm 2 of θ and θ'. □

Lemma 19 (UFD power association)**.** *If $\alpha \cdot \beta = \theta^m \cdot \theta'^m$ and $\gcd(\alpha, \beta) = 1$ in the UFD R, then $\alpha = \pm\theta^m$ or $\alpha = \pm\theta'^m$. This combines unique factorization (`class_number_one`) with the fact that the only units are ± 1 (`units_pm_one`).*

Proof. Proof in Lean source. □

Lemma 20 (Eliminate x)**.** *From $\alpha = \pm\theta^m$ or $\alpha = \pm\theta'^m$, use the product relation to determine β, then take the difference $\alpha - \beta = 2\theta - 1$ to eliminate x and obtain: either $2\theta - 1 = \theta^m - \theta'^m$ or $-2\theta + 1 = \theta^m - \theta'^m$.*

Proof. Case split on the four possibilities for α, determine β from the product, and compute $\alpha - \beta$. □

Lemma 21 (Must have minus sign)**.** *If either $2\theta - 1 = \theta^m - \theta'^m$ or $-2\theta + 1 = \theta^m - \theta'^m$ holds for odd $m \geq 3$, then in fact the minus sign must hold: $-2\theta + 1 = \theta^m - \theta'^m$. This is proved by reducing modulo θ'^2 and checking which sign is consistent.*

Proof. Reduce modulo θ'^2 and verify only the minus sign is consistent. □

1.4.2 Key intermediate result

Lemma 22 (Main m-condition)**.** *For all integers x and odd $m \geq 3$, if $(x^2+7)/4 = 2^m$, then*

$$-2\theta + 1 = \theta^m - \theta'^m.$$

Proof. Chain the exercises: construct the conjugate factors, prove coprimality, apply UFD association, eliminate x, then determine the sign. □

1.4.3 From the m-condition to finitely many solutions

Lemma 23 (Reduction by dividing by 4)**.** *If n is odd with $n \geq 5$ and $x^2 + 7 = 2^n$, then $(x^2 + 7)/4 = 2^{n-2}$.*

Proof. Since $n \geq 5$, we have $4 \mid 2^n$, so divide both sides by 4. □

Lemma 24 (Binomial expansion mod 7)**.** *From $-2\theta + 1 = \theta^m - \theta'^m$, expand via the binomial theorem and reduce modulo 7 to obtain $-2^{m-1} \equiv m \pmod 7$.*

The proof multiplies both sides by 2^m, expands $(1 + \sqrt{-7})^m - (1 - \sqrt{-7})^m$ via the binomial theorem, observes that even-index terms cancel and odd-index terms involve powers of $(\sqrt{-7})^2 = -7$, then reads the result modulo 7.

Proof. Binomial expansion and reduction modulo 7. □

Lemma 25 (Mod 7 constraint)**.** *If n is odd with $n \geq 5$ and $x^2 + 7 = 2^n$, then $(-2)^{n-3} \equiv n - 2 \pmod 7$.*

This follows from the m-condition (Lemma 22) by expanding $\theta^m - \theta'^m$ via the binomial theorem and reducing modulo 7.

Proof. Combine the reduction and binomial expansion lemmas. □

Theorem 26 (Mod 42 constraint)**.** *If n is odd with $n \geq 5$ and $x^2 + 7 = 2^n$, then $(n-2) \bmod 42 \in \{3, 5, 13\}$.*

This follows from $(-2)^{n-3} \equiv n - 2 \pmod 7$ together with Fermat's little theorem $2^6 \equiv 1 \pmod 7$. Checking residues modulo 42 (combining mod 6 and mod 7) yields the three residue classes.

Proof. Exhaustive check of residues modulo 42 using the mod 7 constraint and Fermat's little theorem. □

1.4.4 Uniqueness per residue class

The mod 42 constraint narrows $m = n - 2$ to three residue classes. To show that each class contains at most one solution, we use a 7-adic argument.

Lemma 27 (Corollary C: theta expression is universal)**.** *Any two solutions of the Ramanujan–Nagell equation produce the same theta expression: if $(x_1^2 + 7)/4 = 2^{m_1}$ and $(x_2^2 + 7)/4 = 2^{m_2}$ for odd $m_1, m_2 \geq 3$, then $\theta^{m_1} - \theta'^{m_1} = \theta^{m_2} - \theta'^{m_2}$.*

Proof. Both sides equal $-2\theta + 1$ by the main m-condition. □

Definition 28 (Binomial sum B_d)**.** Define the odd-indexed binomial sum

$$B_d = \sum_{j=0}^{(d-1)/2} \binom{d}{2j+1} \cdot (-7)^j.$$

This arises from expanding $(1 + \sqrt{-7})^d = A_d + \sqrt{-7} \cdot B_d$.

Proof. Proof in Lean source. □

Lemma 29 (7-adic valuation of B_d)**.** *The 7-adic valuation of B_d equals $v_7(d)$: if $7^l \| d$ (i.e. $7^l \mid d$ but $7^{l+1} \nmid d$), then $7^l \mid B_d$ and $7^{l+1} \nmid B_d$.*

This is the core of the 7-adic analysis: the $j = 0$ term of B_d equals d, and all higher terms have strictly larger 7-adic valuation.

Proof. The $j = 0$ term is d with valuation l. Each $j \geq 1$ term has 7-adic valuation $\geq l + 1$, so by the ultrametric property the sum has valuation exactly l. $\square$

Lemma 30 (7-adic valuation of B_d (conjugate))**.** *Same valuation result as Lemma 29, used for the conjugate θ'. Since B_d appears in both $(1 + \sqrt{-7})^d$ and $(1 - \sqrt{-7})^d$ (with only a sign change on $\sqrt{-7}$), the valuation is identical.*

Proof. Identical to Lemma 29. $\square$

Definition 31 (Even-indexed binomial sum A'_d)**.** Define the even-indexed binomial sum

$$A'_d = \sum_{j=0}^{d/2-1} \binom{d}{2(j+1)} \cdot (-7)^j.$$

This arises from the even-index part of the expansion of $(1 + \sqrt{-7})^d$.

Proof. Proof in Lean source. $\square$

Lemma 32 (7-adic valuation of A'_d)**.** *If $7^l \| d$ and $7 \mid d$, then $7^l \mid A'_d$ and $7^{l+1} \nmid A'_d$. The $j = 0$ term $\binom{d}{2} = d(d-1)/2$ has valuation l, and all higher terms have strictly larger 7-adic valuation.*

Proof. Same structure as for B_d: the leading term $\binom{d}{2}$ has valuation l, and higher terms are absorbed. $\square$

Definition 33 (Trace sequence)**.** Define the integer recurrence $a(0) = 2$, $a(1) = 1$, $a(n+2) = a(n+1) - 2\,a(n)$. This is the trace sequence: $a(n) = \theta^n + \theta'^n$ in R.

Proof. Proof in Lean source. $\square$

Lemma 34 (Trace sequence equals $\theta^n + \theta'^n$)**.** *For all n, $\text{trace\_seq}(n) = \theta^n + \theta'^n$ in R.*

Proof. Induction on n using the recurrence, with $\theta + \theta' = 1$ and $\theta \cdot \theta' = 2$. $\square$

Lemma 35 (Trace sequence not divisible by 7)**.** *For all n, $7 \nmid a(n)$. The recurrence has period 3 modulo 7, and the three residues $a(0) \equiv 2$, $a(1) \equiv 1$, $a(2) \equiv -3$ are all nonzero mod 7.*

Proof. Show the recurrence is periodic mod 7 with period 3, then check all three residues. $\square$

Lemma 36 (Even iff not odd)**.** *For natural numbers, n is even if and only if n is not odd.*

Proof. Immediate from `not_odd_iff_even`. $\square$

Lemma 37 (At most one solution per residue class)**.** *If m_1, m_2 are both odd, ≥ 3, satisfy $m_1 \equiv m_2 \pmod{42}$, and both give $-2\theta + 1 = \theta^{m_i} - \theta'^{m_i}$, then $m_1 = m_2$.*

Proof sketch: if $m_1 \neq m_2$, let $d = |m_2 - m_1|$, which is divisible by 42 (hence by 7). The 7-adic analysis of Lemma 29 combined with Corollary C yields a contradiction on the valuation of $\sqrt{-7} \cdot B_d$.

Proof. Contradiction via 7-adic valuation: d is divisible by 42 (hence 7), and the valuation identity forces an impossible parity. $\square$

1.4.5 Verification of known solutions

Lemma 38 (Verification: $m = 3$ (i.e. $n = 5$))**.** $-2\theta + 1 = \theta^3 - \theta'^3$. *Verified via* $x = 5$*:* $(25 + 7)/4 = 8 = 2^3$.

Proof. Direct computation using $\theta^2 = \theta - 2$. □

Lemma 39 (Verification: $m = 5$ (i.e. $n = 7$))**.** $-2\theta + 1 = \theta^5 - \theta'^5$. *Verified via* $x = 11$*:* $(121 + 7)/4 = 32 = 2^5$.

Proof. Direct computation using $\theta^2 = \theta - 2$. □

Lemma 40 (Verification: $m = 13$ (i.e. $n = 15$))**.** $-2\theta + 1 = \theta^{13} - \theta'^{13}$. *Verified via* $x = 181$*:* $(32761 + 7)/4 = 8192 = 2^{13}$.

Proof. Direct computation using $\theta^2 = \theta - 2$. □

1.4.6 Combining

Theorem 41 (Odd case: only three values)**.** *If n is odd with $n \geq 5$ and $x^2 + 7 = 2^n$, then $n \in \{5, 7, 15\}$.*

From the mod 42 constraint, $m = n - 2$ lies in one of three residue classes (3, 5, or 13 mod 42). The verification lemmas show these are actual solutions (at $m = 3, 5, 13$). The uniqueness lemma shows each residue class has at most one solution. Therefore $n \in \{5, 7, 15\}$.

Proof. Combine the mod 42 constraint, uniqueness per class, and verification of the three known solutions. □

1.5 Main theorem

Lemma 42 (Auxiliary: $n \geq 4$ and $n \neq 4$ implies $n \geq 5$)**.** *If $n \geq 4$ and $n \neq 4$, then $n \geq 5$.*

Proof. Immediate by `omega`. □

1.5.1 Direct computation helpers

Once the possible values of n are determined (either by the even-case factorization or the odd-case modular argument), it remains to solve for x by direct computation. Each helper below takes an equation $x^2 = c$ (where $c = 2^n - 7$) and the value of n, then identifies the solution pair (x, n) in the list of solutions.

Lemma 43 (Even case: $n = 4$, $x^2 = 9$)**.** *If $x^2 = 9$ and $n = 4$, then $(x, n) = (\pm 3, 4)$.*

Proof. Solve $x^2 = 9$. □

Lemma 44 (Odd case: $n = 3$, $x^2 = 1$)**.** *If $x^2 = 1$ and $n = 3$, then $(x, n) = (\pm 1, 3)$.*

Proof. Solve $x^2 = 1$. □

Lemma 45 (Odd case: $n = 5$, $x^2 = 25$)**.** *If $x^2 = 25$ and $n = 5$, then $(x, n) = (\pm 5, 5)$.*

Proof. Solve $x^2 = 25$. □

Lemma 46 (Odd case: $n = 7$, $x^2 = 121$)**.** *If $x^2 = 121$ and $n = 7$, then $(x, n) = (\pm 11, 7)$.*

Proof. Solve $x^2 = 121$. ☐

Lemma 47 (Odd case: $n = 15$, $x^2 = 32761$)**.** *If* $x^2 = 32761$ *and* $n = 15$*, then* $(x, n) = (\pm 181, 15)$*.*

Proof. Solve $x^2 = 32761$. ☐

1.5.2 The theorem

Theorem 48 (Ramanujan–Nagell)**.** *The only integer solutions to* $x^2 + 7 = 2^n$ *are*

$$(x, n) \in \{(\pm 1, 3),\ (\pm 3, 4),\ (\pm 5, 5),\ (\pm 11, 7),\ (\pm 181, 15)\}.$$

Proof. First, one shows $n \geq 3$ by bounding $2^n \geq x^2 + 7 \geq 7$. Then x must be odd (Lemma 15).

Case 1: n even. Write $n = 2k$. Then $(2^k + x)(2^k - x) = 7$. By Lemma 16, the only possibility is $2^k = 4$, giving $n = 4$ and $x = \pm 3$ (Lemma 43).

Case 2: n odd, $n = 3$. Direct computation gives $x^2 = 1$, so $x = \pm 1$ (Lemma 44).

Case 3: n odd, $n \geq 5$. By Theorem 41, $n \in \{5, 7, 15\}$, and direct computation gives the remaining solutions (Lemmas 45, 46, 47). ☐

1.6 Additional declarations

Lemma 49 (K_degree_2)**.** *TODO: add description*

Proof. Proof in Lean source. ☐

Lemma 50 (K_discriminant)**.** *TODO: add description*

Proof. Proof in Lean source. ☐

Lemma 51 (K_nrComplexPlaces_2)**.** *TODO: add description*

Proof. Proof in Lean source. ☐

Lemma 52 (K_nrRealPlaces_zero)**.** *TODO: add description*

Proof. Proof in Lean source. ☐

Definition 53 (OK_to_K)**.** TODO: add description

Proof. Proof in Lean source. ☐

Theorem 54 (QuadraticInteger.d_1)**.** *TODO: add description*

Proof. Proof in Lean source. ☐

Lemma 55 (algebraMap_omega_K')**.** *TODO: add description*

Proof. Proof in Lean source. ☐

Lemma 56 (associated_eq_or_neg)**.** *TODO: add description*

Proof. Proof in Lean source. ☐

Lemma 57 (associated_of_theta_pow_dvd)**.** *TODO: add description*

Proof. Proof in Lean source. ☐

Lemma 58 (associated_of_theta_pow_dvd_right). *TODO: add description*

Proof. Proof in Lean source. □

Lemma 59 (factor_not_unit_left). *TODO: add description*

Proof. Proof in Lean source. □

Lemma 60 (factor_not_unit_right). *TODO: add description*

Proof. Proof in Lean source. □

Definition 61 (fieldIso). The -algebra map K' → K sending ' 2 - 1. -/

Proof. Proof in Lean source. □

Lemma 62 (fieldIso_omega). *The -algebra map K' → K sending ' 2 - 1. -/*

Proof. Proof in Lean source. □

Lemma 63 (isIntegralClosure_K). *The -algebra map K' → K sending ' 2 - 1. -/*

Proof. Proof in Lean source. □

Lemma 64 (my_minpoly_theta_prime). *TODO: add description*

Proof. Proof in Lean source. □

Lemma 65 (norm_eq_coeff_zero_minpoly). *TODO: add description*

Proof. Proof in Lean source. □

Lemma 66 (norm_isUnit_iff). *TODO: add description*

Proof. Proof in Lean source. □

Lemma 67 (norm_theta_eq_two). *The minimal polynomial of : X^2 - X + 2.*

Proof. Proof in Lean source. □

Lemma 68 (norm_theta_prime_eq_two). *TODO: add description*

Proof. Proof in Lean source. □

Lemma 69 (quadraticAlgebra_adjoin_omega_eq_top). *The -algebra map K' → K sending ' 2 - 1. -/*

Proof. Proof in Lean source. □

Theorem 70 (ring_of_integers_neg7). *The proof that (1/2) · ('+1) satisfies the relation for QuadraticAlgebra (-2) 1. -/*

Proof. Proof in Lean source. □

Lemma 71 (theta'_irreducible). *TODO: add description*

Proof. Proof in Lean source. □

Lemma 72 (theta'_not_dvd_theta). *TODO: add description*

Proof. Proof in Lean source. ☐

Lemma 73 (theta_irreducible)**.** *TODO: add description*

Proof. Proof in Lean source. ☐

Lemma 74 (theta_not_dvd_theta')**.** *TODO: add description*

Proof. Proof in Lean source. ☐

Lemma 75 (theta_not_unit)**.** *TODO: add description*

Proof. Proof in Lean source. ☐

Lemma 76 (theta_pow_dvd_of_coprime_prod)**.** *TODO: add description*

Proof. Proof in Lean source. ☐

Lemma 77 (theta_prime_not_unit)**.** *TODO: add description*

Proof. Proof in Lean source. ☐

Lemma 78 (theta_theta'_not_associated)**.** *TODO: add description*

Proof. Proof in Lean source. ☐

Definition 79 (toK)**.** The -algebra map K' → K sending ' 2 - 1.

Proof. Proof in Lean source. ☐

Definition 80 (toK')**.** The -algebra map K' → K sending ' 2 - 1. -/

Proof. Proof in Lean source. ☐

Lemma 81 (ufd_associated_dichotomy)**.** *TODO: add description*

Proof. Proof in Lean source. ☐