A 2-ADIC APPROACH TO THE RAMANUJAN–NAGELL EQUATION

GERGELY HARCOS

The Ramanujan–Nagell equation is named after Ramanujan (1913) who conjectured and Nagell (1948) who determined its solutions. Unaware of its history, I worked out my own solution that I present below. It is not as elegant as Hasse's treatment [1] that also appears in Mordell's classical book [2], but in a certain sense it is more natural.

Theorem. *The positive integer solutions of the equation* $x^2+7=2^n$ *are* $x=1,3,5,11,181$, *corresponding to* $n=3,4,5,7,15$.

Proof. We can factorize the equation in the ring of integers of $\mathbb{Q}(\sqrt{-7})$ as

$$\frac{x+\sqrt{-7}}{2}\cdot\frac{x-\sqrt{-7}}{2}=a^{n-2}\cdot b^{n-2},$$

where

$$a=\frac{1+\sqrt{-7}}{2}\qquad\text{and}\qquad b=\frac{1-\sqrt{-7}}{2}$$

are the prime factors of 2. Hence

$$\{a^{n-2},b^{n-2}\}=\pm\left\{\frac{x+\sqrt{-7}}{2},\frac{x-\sqrt{-7}}{2}\right\},$$

and we see that n solves the equation if and only if

$$a^{n-2}-b^{n-2}=\pm\sqrt{-7}. \tag{1}$$

We shall show that the $+$ (resp. $-$) sign case is solved by $n=3,4$ (resp. $n=5,7,15$).

The key observation is the following: the exponent of b in $a^{2^k}-1$ equals 1 for $k=0$, and $k+2$ for $k>0$. Indeed, $a-1=-b$ and $a^2-1=b^3$ verify the statement for $k=0$ and $k=1$, and then we can proceed by induction via

$$a^{2^{k+1}}-1=(a^{2^k}-1)(a^{2^k}+1).$$

It follows (e.g. by the binomial theorem), that the exponent of b in a^m-1 equals 1 for m odd, and $k+2$ for m with 2-exponent $k>0$.

Assume now that $n>4$ satisfies the $+$ sign case of (1). Then $a^{n-2}-b^{n-2}=a^2-b^2$, whence $a^{n-2}-a^2$ is divisible by b^2, but not by b^3. That is, the exponent of b in $a^{n-4}-1$ is 2, but this is impossible by the above.

Assume now that $n>15$ satisfies the $-$ sign case of (1). Then $a^{n-2}-b^{n-2}=a^{13}-b^{13}$, whence $a^{n-2}-a^{13}$ is divisible by b^{13}, but not by b^{14}. That is, the exponent of b in $a^{n-15}-1$ is 13, i.e. the 2-exponent of $n-15$ is 11. In other words, $n\equiv 2063 \pmod{4096}$. We infer

$$2^n\equiv 2^{2063}\pmod{2^{4096}-1},$$
$$2^n\equiv 2^{2063}\equiv -2^{15}\pmod{2^{2048}+1},$$
$$x^2=2^n-7\equiv -2^{15}-7\pmod{2^{2048}+1}.$$

To finish the proof, it suffices to show that $-2^{15}-7$ is not a quadratic residue modulo $2^{2048}+1$. Here we cannot do better than to use the fact that the prime $p=319489$ divides $2^{2048}+1$, and $-2^{15}-7$ is not a quadratic residue modulo p. These statements can be checked by hand, or by the simple SAGE command

```
is_prime(319489), mod(2^2048+1,319489), kronecker(-2^15-7,319489)
```

□

REFERENCES

[1] H. Hasse, *Über eine diophantische Gleichung von Ramanujan-Nagell und ihre Verallgemeinerung*, Nagoya Math. J. **27** (1966), 77–102.

[2] L. J. Mordell, *Diophantine equations*, Pure and Applied Mathematics, 30, Academic Press, London-New York, 1969.

ALFRÉD RÉNYI INSTITUTE OF MATHEMATICS, HUNGARIAN ACADEMY OF SCIENCES, POB 127, BUDAPEST H-1364, HUNGARY
E-mail address: gharcos@renyi.hu

CENTRAL EUROPEAN UNIVERSITY, NADOR U. 9, BUDAPEST H-1051, HUNGARY
E-mail address: harcosg@ceu.hu