

Jerzy Piotr Olszewski

November 25, 2025

The Conjecture We consider the equation

$$X^2 - dY^2 = 1 \tag{1}$$

where d is a square free integer. This is the classical Brahmagupta-Pell equation when considered over \mathbb{Z} where the solutions form a cyclic group and correspond to units in the ring $\mathbb{Z}[\sqrt{d}]$. We treat this equation over the ring $\mathbb{Z}/n\mathbb{Z}$. Perhaps unsurprisingly the solutions still form a group with the usual operations however this group need not a priori be cyclic. This group is of particular interest for $n = 2^P - 1$ with P prime, since the number of points can be related the primality of $n = 2^P - 1$. This was to my knowledge first proposed by Miquel Camprubí-Bonet and Utku Erçetin in their final project for the Security and Codes class in the form

Conjecture 1. (*Camprubí-Erçetin*) Let $n = 2^P - 1$ with P an odd prime and $G = \{(a, b) \in (\mathbb{Z}/n\mathbb{Z})^2 \mid a^2 - 3b^2 = 1 \pmod{n}\}$ then

$$\#G = 2^P \implies 2^P - 1 \text{ is prime.}$$

After some computer calculations they became strongly convinced that it should be true but they had no answer. Subsequently, they posted the problem on Math stack exchange and received an answer which none of us could understand at the time. Utku had recently reminded me of this problem and I had the time to look through this answer and found that i could understand it now. It turned out to be an incomplete argument however it contained some good ideas on approaching the problem and I've managed to rework and complete it. Finally it became apparent that with some modification it shouldn't be too difficult to treat the general case with arbitrary d (given some reasonable assumptions) and this is what is contained in the following pages. Lastly we will talk about the converse implication, which in the original case of $d = 3$ turns out to be true.

1 Setting up the problem

We consider the group

$$G_{n,d} := \{(a, b) \in (\mathbb{Z}/n\mathbb{Z})^2 \mid a^2 - db^2 = 1\}$$

where we assume that: n is odd and $(n, 4d) = 1$ (this ensures that no primes dividing n ramify in $\mathbb{Z}[\sqrt{d}]$ and that the curve is smooth modulo p). We may note that the $G_{n,d}$ can be restated as elements of $\mathbb{Z}[\sqrt{d}]/(n)$ of ‘norm’ 1 with the operation inherited from multiplication in $\mathbb{Z}[\sqrt{d}]/(n)$. Our first result relates the sizes of $G_{n,d}$, $(\mathbb{Z}[\sqrt{d}]/n)^*$ and $(\mathbb{Z}/(n))^*$.

Lemma 1.1. *The sequence*

$$1 \rightarrow G_{n,d} \rightarrow (\mathbb{Z}/n[\sqrt{d}])^* \rightarrow (\mathbb{Z}/n)^* \rightarrow 1$$

is exact, where the last map is the norm map $N : a + \sqrt{d}b \mapsto (a + \sqrt{d}b)(a - \sqrt{d}b) = a^2 - db^2$.

Proof. Note that the norm map sends $a + \sqrt{d}b$ to $a^2 - db^2$ hence our group $G_{n,d}$ is clearly the kernel of this map thus it suffices to show that the norm map is surjective. Let $u \in (\mathbb{Z}/n)^*$ be a unit and consider the equation $X^2 - dY^2 = u$. Note that if this has a solution $(a, b) \in (\mathbb{Z}/n)^2$ then $a + \sqrt{d}b$ is a unit in $\mathbb{Z}/n[\sqrt{d}]$ and our map is surjective. I.e. it suffices to show that $X^2 - dY^2 = u$ has a solution in the ring \mathbb{Z}/n .

Let $p|n$ be prime and denote u_p the reduction of u modulo p and note that this is a unit in \mathbb{F}_p . Then the equation $X^2 - dY^2 = u_p$ has a solution by a pigeonhole principal argument (which we do not write here for due to space). Since the curve is assumed to be smooth, We can apply Hensel’s lemma to lift this to a solution in \mathbb{Z}/p^m for all m (in fact it lifts to a p -adic solution). Thus there exists a solution over the ring $\prod_{p|n} \mathbb{Z}/p^{v_p(n)} \cong \mathbb{Z}/n$. \square

Since all groups are finite this implies that

$$\#G_{n,d} = \frac{\#(\mathbb{Z}/n[\sqrt{d}])^*}{\#(\mathbb{Z}/n)^*}. \quad (2)$$

It is important to note that the main part of solving this problem is computing the exact size of $G_{n,d}$ and we reduce it by the above lemma to computing the size of $(\mathbb{Z}/n)^*$ (which is easy as it is just $\varphi(n)$) and computing the size of $(\mathbb{Z}[\sqrt{d}]/(n))^*$ which is more complicated. The following pages are mainly dedicated to computing the latter.

2 Some Commutative algebra

It should be noted that throughout we assume all primes \mathfrak{p} to be invertible so that the localizations $\mathbb{Z}[\sqrt{d}]_{\mathfrak{p}}$ are DVR-s. This is justified given our problem since 2 is the only possibly singular prime and we exclude it from consideration. In effect we do not need to go to rings of integers. Also m is used to denote an arbitrary positive integer. Our goal here is to come up with a formula for the number of points in $(\mathbb{Z}[\sqrt{d}]/\mathfrak{p})^*$.

Lemma 2.1. *With \mathfrak{p} a prime of $\mathbb{Z}[\sqrt{d}]$ and m as above we have that*

$$x \in (\mathbb{Z}[\sqrt{d}]/\mathfrak{p}^m)^* \iff x \notin \mathfrak{p}.$$

Proof. Firstly, if $x \in \mathfrak{p}$ then it is nilpotent and thus not a unit. As for the converse, note that \mathfrak{p} is maximal in $\mathbb{Z}[\sqrt{d}]/\mathfrak{p}^m$ thus if x is not a unit then $(0) \subseteq (x) \subsetneq \mathbb{Z}[\sqrt{d}]/\mathfrak{p}^m$ and taking radicals we have $\mathfrak{p} = \sqrt{(0)} \subseteq \sqrt{(x)} \subseteq \mathbb{Z}[\sqrt{d}]/\mathfrak{p}^m$ thus by maximality $\mathfrak{p} = \sqrt{(x)} \ni x$. \square

This allows us a useful isomorphism.

Lemma 2.2. *With \mathfrak{p} and m as before, we have the isomorphism*

$$\mathbb{Z}[\sqrt{d}]/\mathfrak{p}^m \cong \mathbb{Z}[\sqrt{d}]_{\mathfrak{p}}/\mathfrak{p}^m$$

Proof. Recall that localization is exact thus $\mathbb{Z}[\sqrt{d}]_{\mathfrak{p}}/\mathfrak{p}^m \cong (\mathbb{Z}[\sqrt{d}]/\mathfrak{p}^m)_{\mathfrak{p}}$ so we have the localization map $\mathbb{Z}[\sqrt{d}]/\mathfrak{p}^m \rightarrow (\mathbb{Z}[\sqrt{d}]/\mathfrak{p}^m)_{\mathfrak{p}}$ sending $a \rightarrow \frac{a}{1}$ and since \mathfrak{p} is prime this map is injective. Now suppose that $\frac{a}{b} \in (\mathbb{Z}[\sqrt{d}]/\mathfrak{p}^m)_{\mathfrak{p}}$ then $b \in (\mathbb{Z}[\sqrt{d}]/\mathfrak{p}^m) \setminus \mathfrak{p}$ and by the previous result we find that $b \in (\mathbb{Z}[\sqrt{d}]/\mathfrak{p}^m)^*$. Hence we can write $\frac{a}{b} = \frac{ab^{-1}}{1}$ with $ab^{-1} \in (\mathbb{Z}[\sqrt{d}]/\mathfrak{p}^m)$ which is clearly in the image of the localization map. \square

This reduces our problem of counting points in $(\mathbb{Z}[\sqrt{d}]/\mathfrak{p})^*$ to counting points in $(\mathbb{Z}[\sqrt{d}]_{\mathfrak{p}}/\mathfrak{p}^m)^*$ which is in some sense easier as $\mathbb{Z}[\sqrt{d}]_{\mathfrak{p}}$ is a DVR. We write $k_{\mathfrak{p}}$ for the field $\mathbb{Z}[\sqrt{d}]/\mathfrak{p} = \mathbb{Z}[\sqrt{d}]_{\mathfrak{p}}/\mathfrak{p}$, now since $\mathbb{Z}[\sqrt{d}]_{\mathfrak{p}}$ is a DVR we have that \mathfrak{p} is principal in $R_{\mathfrak{p}}$ and $\mathfrak{p}/\mathfrak{p}^2$ is a one dimensional $k_{\mathfrak{p}}$ vector space and subsequently $\mathfrak{p}^m/\mathfrak{p}^{m+1}$ is a one dimensional $k_{\mathfrak{p}}$ vector space for all m . Moreover, we have the standard isomorphism (of groups) between U_i/U_{i+1} and $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ where $U_i = 1 + \mathfrak{p}^i$ for $i \geq 0$.

Lemma 2.3. *Let A be a DVR, $\mathfrak{p} = (\pi)$ the maximal ideal and i as above, then the sequence*

$$1 \longrightarrow U_i/U_{i+1} \longrightarrow (A/\mathfrak{p}^{i+1})^* \longrightarrow (A/\mathfrak{p}^i)^* \longrightarrow 1$$

is exact.

Proof. the second map is surjective since it is induced by a surjective ring map hence it suffices to show that it has the appropriate kernel. Suppose then that $a \bmod \pi^{i+1} \mapsto 1 \bmod \pi^i$ this can only occur when $a = 1 + b\pi^i \bmod \pi^{i+1}$. So the kernel is as required and the sequence is exact. \square

If $A = \mathbb{Z}[\sqrt{d}]_{\mathfrak{p}}$, the above groups are finite and $\#U_i/U_{i+1} = \#k_{\mathfrak{p}}$ thus we obtain a first formula

$$\#(\mathbb{Z}[\sqrt{d}]_{\mathfrak{p}}/\mathfrak{p}^{m+1})^* = \#(\mathbb{Z}[\sqrt{d}]_{\mathfrak{p}}/\mathfrak{p}^m)^* \cdot \#k_{\mathfrak{p}}. \quad (3)$$

For $m = 1$ we have $\#(\mathbb{Z}[\sqrt{d}]_{\mathfrak{p}}/\mathfrak{p}^2)^* = \#(\mathbb{Z}[\sqrt{d}]_{\mathfrak{p}}/\mathfrak{p})^* \cdot \#k_{\mathfrak{p}}$ and inductively we get a second formula

$$\#(\mathbb{Z}[\sqrt{d}]_{\mathfrak{p}}/\mathfrak{p}^{m+1})^* = \#(\mathbb{Z}[\sqrt{d}]_{\mathfrak{p}}/\mathfrak{p})^* \cdot (\#(k_{\mathfrak{p}}))^m$$

which simplifies to

$$\#(\mathbb{Z}[\sqrt{d}]_{\mathfrak{p}}/\mathfrak{p}^{m+1})^* = (\#(k_{\mathfrak{p}}) - 1) \cdot (\#(k_{\mathfrak{p}}))^m.$$

Finally lemma 2.2 lets us replace $\mathbb{Z}[\sqrt{d}]_{\mathfrak{p}}$ with $\mathbb{Z}[\sqrt{d}]$. Also note that the above is true also for $m = 0$. In conclusion,

Corollary 2.4. *Let \mathfrak{p} be a prime of $\mathbb{Z}[\sqrt{d}]$ coprime to $4d$ and $m \geq 0$ an integer, then $\#(\mathbb{Z}[\sqrt{d}]/\mathfrak{p}^{m+1})^* = (\#(k_{\mathfrak{p}}) - 1) (\#(k_{\mathfrak{p}}))^m$.*

Proof. □

3 Some Algebraic Number Theory

We consider the extension of rings \mathbb{Z} to $\mathbb{Z}[\sqrt{d}]$. If a prime $p|n$ is inert then $\mathbb{Z}[\sqrt{d}]/p \cong \mathbb{F}_p[\sqrt{d}]$ is a degree two extension of \mathbb{F}_p thus $\#(\mathbb{Z}[\sqrt{d}]/p) = p^2$. On the other hand if p splits as $\mathfrak{p}\mathfrak{q}$ (note that we are assuming it does not ramify) then $\mathbb{Z}/p^m \cong \mathbb{Z}[\sqrt{d}]/\mathfrak{p}^m \times \mathbb{Z}[\sqrt{d}]/\mathfrak{q}^m$ and $\mathbb{Z}[\sqrt{d}]/\mathfrak{p} \cong \mathbb{F}_p$ has p many elements. Note that for $m = 1$ the decompositions of $\mathbb{Z}[\sqrt{d}]/p$ both have the same number of elements, p^2 in the first case and we have two factors with p many elements in the second so it may seem useless to differentiate them if we want to count elements. However the structure of these give different counts when we restrict to units. So we consider the two possible cases (under our assumption of non ramification)

If p is inert then it is still prime in $\mathbb{Z}[\sqrt{d}]$ and by the lemma we have $\#(\mathbb{Z}[\sqrt{d}]/p^m)^* = (\#(k_p) - 1)(\#(k_p))^{m-1} = (p^2 - 1) \cdot p^{2(m-1)}$. In the split case however we have

$$\begin{aligned} \#(\mathbb{Z}[\sqrt{d}]/p^m)^* &= \#(\mathbb{Z}[\sqrt{d}]/\mathfrak{p}^m) \cdot \#(\mathbb{Z}[\sqrt{d}]/\mathfrak{q}^m) \\ &= (\#(\mathbb{Z}[\sqrt{d}]/\mathfrak{p}) - 1)(\#(\mathbb{Z}[\sqrt{d}]/\mathfrak{p}))^{m-1} (\#(\mathbb{Z}[\sqrt{d}]/\mathfrak{q}) - 1)(\#(\mathbb{Z}[\sqrt{d}]/\mathfrak{q}))^{m-1} \\ &= (p - 1)^2 \cdot p^{2(m-1)}. \end{aligned}$$

By the Chinese Remainder Theorem we find that

$$\begin{aligned}
\#(\mathbb{Z}[\sqrt{d}]/n)^* &= \prod_{p|n} \#(\mathbb{Z}[\sqrt{d}]/p^{v_p(n)})^* \\
&= \prod_{p|n, \text{inert}} \#(\mathbb{Z}[\sqrt{d}]/p^{v_p(n)})^* \prod_{p|n, \text{split}} \#(\mathbb{Z}[\sqrt{d}]/p^{v_p(n)})^* \\
&= \prod_{p|n, \text{inert}} (p^2 - 1)p^{2(v_p(n)-1)} \prod_{p|n, \text{split}} (p - 1)^2 p^{2(v_p(n)-1)} \\
&= \prod_{p|n, \text{inert}} (p + 1) \prod_{p|n, \text{split}} (p - 1) \prod_{p|n} (p - 1)p^{2(v_p(n)-1)} \\
&= \varphi(n) \prod_{p|n, \text{inert}} (p + 1) \prod_{p|n, \text{split}} (p - 1) \prod_{p|n} p^{(v_p(n)-1)}.
\end{aligned}$$

Where φ is the Euler totient function. Since $\#(\mathbb{Z}/n)^* = \varphi(n)$, we can apply equation 2 to get the final count of elements of $G_{n,d}$,

$$\#G_{n,d} = \prod_{p|n, \text{inert}} (p + 1) \prod_{p|n, \text{split}} (p - 1) \prod_{p|n} p^{(v_p(n)-1)}. \quad (4)$$

4 The Proof

This, at last, allows us to tackle the problem. Suppose that $n = 2^P - 1$ with P an odd prime and that $\#G_{n,d} = 2^P = n + 1$, equating the last assumption with our count in equation 4 yields that the last factor must be a power of two. Rearranging we get for some A

$$2^A \prod_{p|n} p = \prod_{p|n} p^{v_p(n)} = n$$

but by assumption n is odd thus $A = 0$ and $n = \prod_{p|n} p$ is a product of primes with multiplicity one. This simplifies the count of $G_{n,d}$ as the last factor vanishes and we are left with

$$\#G_{n,d} = \prod_{p|n, \text{inert}} (p + 1) \prod_{p|n, \text{split}} (p - 1).$$

Since this is a power of two, we know that for inert primes $p|n$ it must be true that $p = 2^A - 1$ for some A , similarly split primes must be of the form $p = 2^B + 1$ for some B . Hence n is a product of Mersenne and Fermat primes. We continue by showing that there indeed are no Fermat numbers in the factorization of n (no split primes). Suppose that $p|2^P - 1$, a standard result shows that $p = 1 + 2Pa$ for some integer a . Moreover assume that

p is a Fermat number, $p = 2^B + 1$, then $2^B = 2Pa$ which contradicts the assumption that P is odd. Thus we are reduced to

$$\#G_{n,d} = \prod_{p|ninert} (p+1).$$

It suffices then to show that there can only be one factor. We show that a product of Mersenne primes cannot be a Mersenne number, this is straightforward, although a little messy. Let $n = p_1 \dots p_t$ with $p_i = 2^{A_i} - 1$ and suppose that there are at least two nontrivial factors so we can arrange them such that $P > A_1 > \dots > A_t > 1$ are all odd primes. Then expanding the product gives

$$p_1 \dots p_t = \left(2^{\sum_i A_i} - \sum_i 2^{\sum_{j \neq i} A_j} + \dots + (-1)^{t-1} \sum_i 2^{A_i} + (-1)^t \right).$$

The first component is 2 exponentiated to the sum of all A_i -s, the second is minus the sum of 2 exponentiated to all possible non repeating combinations of $t-1$ exponents, the third of $t-2$ exponents and so on until we reach single exponents and finally 1. The sum alternates due to the -1 -s. Recall that by assumption $P, A_i \neq 2$ so 3 does not divide n . Hence $A_t > 2$, and t must be odd since otherwise the product above is congruent to 1 mod 4 but $n \equiv -1 \pmod{4}$. So we are left with

$$2^P - 1 = \left(2^{\sum_i A_i} - \sum_i 2^{\sum_{j \neq i} A_j} + \dots + \sum_i 2^{A_i} - 1 \right)$$

which cannot be true since modulo $2^{A_{t-1}}$ we have $-1 \equiv 2^{A_t} - 1 \pmod{2^{A_{t-1}}}$ which implies that $2^{A_{t-1}} | 2^{A_t}$ or in other words $A_{t-1} \leq A_t$ which contradicts our ordering of the primes. Therefore, $n = 2^P - 1$ has only one prime divisor with multiplicity one so must itself be a prime. Summing up we have proven our conjecture,

Proposition 4.1. *Let $n = 2^P - 1$ with P an odd prime, $X^2 - dy^2 - 1 \in \mathbb{Z}[X, Y]$ with d a positive square free integer and assume that $(n, 4d) = 1$ then*

$$\#G_{n,d} = 2^P \implies 2^P - 1 \text{ is prime.} \quad (5)$$

Proof. □

The converse: Naturally the next question to ask is whether the converse is true? This is not always so, however we can deduce that in the original statement of the problem, with $d = 3$, it is. Note that our computation of $\#G_{n,d}$ in equation 4 is independent of any assumption on n other than its prime divisors are not ramified. Thus if we assume that $n = 2^P - 1 = p$ is

prime then formula 4 yields either $p+1 = 2^P$ if p is inert or $p-1 = 2^P-2$ if p is split. Moreover the ring $\mathbb{Z}[\sqrt{d}]$ has minimal polynomial X^2-d which splits if and only if d is a square modulo $p = 2^P-1$. Note that $2^P-1 \equiv -1 \pmod{4}$ and $2^P-1 \equiv 1 \pmod{3}$, thus in the special case $d = 3$ quadratic reciprocity lets us conclude that 3 is not a square modulo 2^P-1 thus $\#G_{n,d} = 2^P$.