The Support Problem

Dipramit Majumdar
B.Math.Hons.IIIrd year
I.S.I. Bangalore.

This work is done as a part of the KVPY project under the supervision of Professor B.Sury, I.S.I. Bangalore.

In 1988, Paul Erdös asked the following elementary-looking question :
If $x \neq y$ are different natural numbers, can we find a prime number p such that for some n, p divides exactly one among $x^n - 1$ and $y^n - 1$?
Now, if y is a power of x, then $x^n - 1$ divides $y^n - 1$ for each n. So, one may ask the stronger question whether the assumption, for every n, that each prime divisor of $x^n - 1$ also divides $y^n - 1$ necessarily means that y must be a power of x. This problem came to be known as the 'support problem'. One calls the 'support' of a natural number a to be the set of its prime divisors. It was only as recently as 1997 when Corrales Rodriganez and Rene Schoof answered this in the affirnative. They proved it for general number fields and also generalized the problem to elliptic curves and solved that too. The proof of the answer even to the original question requires from basic algebraic number theory. We discuss the proof for $\mathbb{Q}$ here. We will prove:

Theorem:
Let $x, y \in \mathbb{Q}^*$. If, for all but finitely many primes p and, for all $n \in \mathbb{N}$, one has the implication

$$p \mid (x^n - 1) \Longrightarrow p \mid (y^n - 1),$$

then y is a power of x.
Here p divides a rational number $x = \frac{a}{b}, (a, b) = 1$, means that $p \mid a$.

We start by recalling some standard facts from algebraic number theory.

Let $\Bbbk$ be an algebraic number field i.e., a finite extension field of $\mathbb{Q}$. Now look at the ring of integers of $\Bbbk$. It is, by definition, $O_{\Bbbk} = \{x \in \Bbbk : \min(x, \mathbb{Q})$ is a monic integral polynomial $\}$. Although $O_{\Bbbk}$ is not a principal ideal domain (PID) in general, it is a Dedekind domain. Any nonzero prime ideal in a Dedekind domain is maximal and any ideal in a Dedekind domain is product of prime ideals in a unique manner upto order.

If p is a prime integer, the principal ideal $pO_{\Bbbk}$ need not be a prime ideal in $O_{\Bbbk}$. However, writing

$$pO_{\Bbbk} = P_1^{e_1} \cdots P_g^{e_g}$$

where P_i are prime ideals in $O_{\Bbbk}$, one has a relation of the form $\sum_{i=1}^{g} e_i f_i = [\Bbbk : \mathbb{Q}]$. We say that p splits completely in $\Bbbk$ if $g = n, e_i = 1 = f_i$ for all $i \leq n$; that is, if

$$pO_{\Bbbk} = P_1 P_2 \cdots P_n.$$

Fact 1 (primes splitting in cyclotomic extensions) :
If p is a prime and $p \not| n$ and ζ_n is a primitive n^{th} root of unity, then p splits completely in $\mathbb{Q}(\zeta_n)$ if and only if $p \equiv 1(\text{modn})$.

Fact 2 (primes splitting in a radical extension) :
If q is a prime power, $a \in \mathbb{N}$, p is a prime not dividing a, then p splits completely in $\mathbb{Q}(\zeta_n, a^{\frac{1}{q}})$ if and only if $p \equiv 1(\text{modq})$ and a is a q^{th} power in $\mathbb{Z}/p\mathbb{Z}$.

Fact 3 (split primes determine hierarchy) :
If K, L are finite extensions of $\mathbb{Q}$ and $Spl(K)$ and $Spl(L)$ denote the sets of prime integers which split completely in K and L respectively, then $Spl(K) \subseteq Spl(L)$, then $K \supseteq L$.
This is a deep result whose proof uses the so-called Frobenius Density Theorem.

Fact 4 (Kummer pairing) :
Let q be a prime power. Then there is an injective homomorphism $\theta : \mathbb{Q}(\zeta_q)^*/(\mathbb{Q}(\zeta_q)^*)^q \to Hom(Gal(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_q)), \mu_q)$ where μ_q is the cyclic group of q^{th} roots of unity. This is the Kummer map which takes t to $\theta(t) : \sigma \to \frac{\sigma(t^{\frac{1}{q}})}{t^{\frac{1}{q}}}$.

Fact 5 (Special case of Dirichlet's unit theorem) :
If S is any finite set of prime integers, then the group of units of the ring $\mathbb{Z}[S^{-1}]$ is finitely generated.
This is the Dirichlet unit theorem for a number field, but it is obvious in this case because the concerned group is simply $\pm p_1^{t_1} \cdots p_s^{t_s}$ for $t_i \in \mathbb{Z}$ and where $S = \{p_1, \cdots, p_s\}$.

We will now use these results to prove the theorem.

Proof of theorem.
Assume x, y are as in the theorem, that is, for all n and all but finitely many primes p, one has

$$p \mid (x^n - 1) \Longrightarrow p \mid (y^n - 1).$$

Let S denote the finite set of primes including all those which divide (either the numerators or the denominators of) x, y and, also those where the hypothesis of the theorem does not hold. The proof will depend on the following 2 lemmata.

Lemma 1:
Let q be a power of a prime l and let ζ_q be a primitive q^{th} root of unity. Then $\mathbb{Q}(\zeta_n, x^{\frac{1}{q}}) \supseteq \mathbb{Q}(\zeta_n, y^{\frac{1}{q}})$.
Proof :
Let $p \notin S$ split completely in $\mathbb{Q}(\zeta_n, x^{\frac{1}{q}})$. By Fact 2, $p \equiv 1(\text{modq})$ and x is a q^{th} power in $\mathbb{Z}/p\mathbb{Z}$. Now if $a \in \mathbb{Z}/p\mathbb{Z}$, and $a^{p-1} \equiv 1(\text{modp})$. Since $x = a^q$ in $\mathbb{Z}/p\mathbb{Z}$, $x^{\frac{p-1}{q}} \equiv 1(\text{modp})$. Since $p \equiv 1(\text{modq})$, $\frac{p-1}{q} \in \mathbb{N}$. Thus, by the hypothesis of the theorem, $y^{\frac{p-1}{q}} \equiv 1(\text{modp})$. As $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic, y is a q^{th} power in $\mathbb{Z}/p\mathbb{Z}$. By Fact 2, p splits completely in $\mathbb{Q}(\zeta_n, y^{\frac{1}{q}})$. So $Spl(\mathbb{Q}(\zeta_n, x^{\frac{1}{q}})) \subseteq Spl(\mathbb{Q}(\zeta_n, y^{\frac{1}{q}}))$. Using Fact 3 which is a consequence of the Frobenius density theorem, we have $\mathbb{Q}(\zeta_n, x^{\frac{1}{q}}) \supseteq \mathbb{Q}(\zeta_n, y^{\frac{1}{q}})$.

Lemma 2:
Let q be an odd prime power. Then the natural map $\mathbb{Q}^*/(\mathbb{Q}^*)^q \to \mathbb{Q}(\zeta_q)^*/(\mathbb{Q}(\zeta_q)^*)^q$ is injective.
To prove this lemma we will modify the proof of Hilbert's Theorem 90 slightly. We claim :

Modified Hilbert 90 :
Let q be an odd prime power and let L/K be a Galois extension with cyclic Galois group $G =< \sigma >$. If $\alpha \in L$ is a q^{th} root of unity and $N_{L/K} = 1$, then there is a q^{th} root of unity $\gamma \in L$ with $\alpha = \frac{\sigma(\gamma)}{\gamma}$.
Proof.
Let a be a primitive root modq,that is, a generator of $(\mathbb{Z}/q\mathbb{Z})^*$. Then for a primitive q^{th} root of unity, the extension $\mathbb{Q}(\zeta_q)$ is Galois, and cyclic and is generated by $\sigma : \zeta_q \to \zeta_q^a$. Any integer i can be written as $(a-1)j$ in $\mathbb{Z}/q\mathbb{Z}$, since $(a-1)$ is invertible modq. The elements of $(\mathbb{Z}/q\mathbb{Z})^*$ are elements which are not multiple of p (where $q = p^r, p$ is an odd prime). So if we

can prove that an element of the form $kp+1$ does not generate $(\mathbb{Z}/q\mathbb{Z})^*$, then $a-1 \in (\mathbb{Z}/q\mathbb{Z})^*$. So then $a-1$ is invertible modq. Now let $kp+1$ be a generator of $(\mathbb{Z}/q\mathbb{Z})^*$. So there is an element of the form $k^/p+2$ in the subgroup generated by $kp+1$. But this is not possible, since $(kp+1)^n$ is of the form k_1p+1. So no element of the form $kp+1$ is a generator of $(\mathbb{Z}/q\mathbb{Z})^*$. So if a is a generator of $(\mathbb{Z}/q\mathbb{Z})^*$, then $a-1$ is invertible in $\mathbb{Z}/q\mathbb{Z}$.
For any $i < q$, writing $i = (a-1)j$ in $\mathbb{Z}/q\mathbb{Z}$, we have $\xi^i = \frac{\xi^{aj}}{\xi^j} = \frac{\sigma(\xi^j)}{\xi^j}$. So this modified Hilbert 90 is proved.

Proof of lemma 2:
Let $t \in \mathbb{Q}^*$ be so that $t = s^q$ with $s \in \mathbb{Q}(\zeta_q)^*$. Writing $Gal(\mathbb{Q}(\zeta_q)/\mathbb{Q}) =< \sigma >$, we have $(\frac{\sigma(s)}{s})^q = 1$. Thus $\frac{\sigma(s)}{s}$ is a q^{th} root of unity whose norm over $\mathbb{Q}$ is 1. By the modified version of Hilbert's theorem 90, $\frac{\sigma(s)}{s} = \frac{\sigma(u)}{u}$ for some q^{th} root of unity u. So $su^{-1} = \sigma(su^{-1})$. So su^{-1} is fixed by the galios group G. So $su^{-1} \in \mathbb{Q}$. Now $t = s^q = (su^{-1})^q \in (\mathbb{Q}^*)^q$. So the map is injective.

Proof of theorem continued :
As in Fact 4, consider the Kummer map $\theta : \mathbb{Q}(\zeta_q)^*/(\mathbb{Q}(\zeta_q)^*)^q \to Hom(Gal(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_q)), \mu_q)$ which takes t to $\theta(t) : \sigma \to \frac{\sigma(t^{1/q})}{t^{\frac{1}{q}}}$.
From Fact 1, we have $\mathbb{Q}(\zeta_n, x^{\frac{1}{q}}) \supseteq \mathbb{Q}(\zeta_n, y^{\frac{1}{q}})$. So $\ker\theta(x) \subseteq \ker\theta(y)$. We have the commutative diagram:

$$\begin{array}{ccccccccc} & & & & & \overset{\theta(x)}{} & & & \\ 0 & \longrightarrow & \ker\theta(x) & \longrightarrow & Gal(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_q)) & \longrightarrow & \mathrm{Im}\theta(\mathrm{x}) & \longrightarrow & 0 \\ & & \downarrow \subseteq & & \| & & \downarrow \phi & & \\ & & & & & \overset{\theta(y)}{} & & & \\ 0 & \longrightarrow & \ker\theta(y) & \longrightarrow & Gal(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_q)) & \longrightarrow & \mathrm{Im}\theta(\mathrm{y}) & \longrightarrow & 0. \end{array}$$

As $\mathrm{Im}\theta(\mathrm{x}) \subseteq \mu_q$ is cyclic , the last vertical map ϕ is simply a power map; hence $\theta(y) = \theta(x)^d$ for some $d \in \mathbb{Z}$. As θ is injective from Fact 4, we have then $y = x^d$ in the group $\mathbb{Q}(\zeta_q)^*/(\mathbb{Q}(\zeta_q)^*)^q$. So, by lemma 2, we have $y = x^d$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^q$ also.

Now, we look at the ring $\mathbb{Z}[S^{-1}]$ obtained by inverting all the primes in the finite set S. Let A denote $\mathbb{Z}[S^{-1}]^*/x^{\mathbb{Z}}$ where $\mathbb{Z}[S^{-1}]^*$ is the group of units of $\mathbb{Z}[S^{-1}]$. By Fact 5, we have that the unit group $\mathbb{Z}[S^{-1}]^*$ is finitely generated. Indeed, it consists of all the rational numbers of the form $\pm p_1^{\alpha_1}...p_r^{\alpha_r}$ where $p_i \in S$ and $\alpha_i \in \mathbb{Z}$. In particular, the images of these elements in the quotient

group A generate it.
By Facts 1 and 2, it follows that the image of y in A is already in A^q for each odd prime power q. Now clearly $\cap A^q = \{\pm 1\}$ where the intersection is over all odd prime powers q.
Therefore, $y = \pm x^d$, $d \in \mathbb{Z}$. Suppose, if possible, that $y = -x^d$. This means $p \mid (y^n - 1) \implies p \mid -(x^n + 1)$ and by the assumption, $p \mid (x^n - 1)$. This implies $p = 2$.So we include 2 in S. Note that the proof goes through since $\mathbb{Z}[S^{-1}]^*$ is finitely genrated as long as S is finite. Now since $2 \in S$, $y \neq -x^d$. Hence $y = x^d, d \in \mathbb{Z}$ and this proves the theorem.