Frobenius and His Density Theorem for Primes

B Sury

Introduction

Our starting point is the following problem which appeared in the recent IMO (International Mathematical Olympiad) :

If p is a prime number, show that there is another prime number q such that $n^p - p$ is not a multiple of q for any natural number n.

Now, this problem can be solved using elementary mathematics (otherwise, it would not be posed in the IMO). However, how does one guess that such a thing ought to be true? Can we produce an abundance of such problems in some systematic manner? We take this problem as a point of reference to discuss some deep number theory (which is already a century old) which not only solves this problem, but also gives us an understanding of why such facts are true and what more one can expect.

B Sury is with the Indian Statistical Institute. He introduces this article by:

A rare sight is seen; yes,
when we spot a genius.
We saw one who made
sense
of prime numbers being
dense.
This was the great George
Frobenius!

Rephrasing and Generalisation

Let us start by rephrasing the above problem. For a prime p, consider the integral polynomial $f(X) = X^p - p$. For any prime q, one may consider f as a polynomial over $\mathbb{Z}/q\mathbb{Z}$, the integers modulo q by reducing the coefficients of f modulo q. Then, the problem asks us to prove that there is some prime q for which f does not have a root in $\mathbb{Z}/q\mathbb{Z}$. So, when is it true that an integral polynomial has roots in $\mathbb{Z}/q\mathbb{Z}$ for every prime p ? Obviously, if the integral polynomial already has an integral root, this happens. Can it also happen when f has no integral root ?

Before answering this, let us note that every nonconstant

Keywords
Density of primes, Frobenius and Chebotarev theorems, Frobenius conjugacy class, Galois group.

The set of odd primes modulo which the polynomial X^2+1 has roots,consists precisely of all primes in the arithmetic progression $4n+1$. In general, every quadratic polynomial has a corresponding arithmetic progression such that the polynomial has roots modulo each prime in this progression, and modulo no other primes.

integral polynomial has a root in $\mathbb{Z}/q\mathbb{Z}$ for infinitely many primes q. Here is the simple argument proving it. See also [3].

Let $P(X) = a_0 + a_1X + \quad + a_nX^n$ be an integral polynomial with $n > 0$ and $a_n \neq 0$. For any integer d, look at the polynomial

$$P(a_0dX) = a_0(1+a_1dX+a_0a_2d^2X^2+\cdot\ \cdot+a_0^{n-1}a_nd^nX^n).$$

Since $Q(X) = 1 + a_1dX + a_0a_2d^2X^2 + \cdot \quad + a_0^{n-1}a_nd^nX^n$ takes the values $0, 1, -1$ at the most for finitely many values of X, it takes a value $Q(m) \neq 0, 1, -1$ which must then be a multiple of some prime p. As $Q(m) \equiv 1$ mod d, p is coprime to d. Therefore, for any d, we have shown that there is some m such that $P(a_0dm)$ is zero modulo p for some prime p coprime to d. Varying d, we have infinitely many such primes p.

The set of odd primes modulo which the polynomial $X^2 + 1$ has roots, consists precisely of all primes in the arithmetic progression $4n + 1$. In general, every quadratic polynomial has a corresponding arithmetic progression such that the polynomial has roots modulo each prime in this progression, and modulo no other primes. This follows from the famous quadratic reciprocity law.

Returning to our case $f(X) = X^p - p$, let us see whether we can explicitly get an infinite set of primes modulo which f does have roots. Consider any prime q and the group $(\mathbb{Z}/q\mathbb{Z})^*$ of nonzero integers modulo q under multiplication modulo q. If the p-th power map $\theta : a \mapsto a^p$ on $(\mathbb{Z}/q\mathbb{Z})^*$ is not $1-1$, then there exists some $a \neq 1$ with $a^p = 1$. Since $a^{q-1} = 1$, we must have $p/(q-1)$. In other words, whenever $q \not\equiv 1$ mod p, our polynomial f has a root modulo q.

Let us now return to the possibility of producing a polynomial which has no integral roots but has roots modulo every integer. Consider the polynomial $g(X) =$

$(X^2 - 13)(X^2 - 17)(X^2 - 221)$. Evidently, its roots $\pm\sqrt{13}, \pm\sqrt{17}, \pm\sqrt{221}$ are not integral (or even rational). We show that it has roots modulo *any* nonzero integer. Recall that the Chinese remainder theorem tells us that whenever $m_1, \quad , m_r$ are pairwise coprime integers and $a_1, \quad , a_r$ are any integers, there is an integer a which is simultaneously $\equiv a_i \bmod m_i$ for $i = 1, \cdot \quad , r$. Therefore, by the Chinese remainder theorem, it suffices to prove that g has roots modulo every prime power. In what follows, for any prime p and a coprime to p, the notation $(\frac{a}{p})$ stands for 1 or -1 according to whether a is a square or not mod p. One also says in the respective cases that a is a quadratic residue modulo p or a is a quadratic nonresidue modulo p.

The Chinese remainder theorem tells us that for natural numbers $m_1, \ldots \; m_r$ which are pairwise relatively prime and for arbitrary integers $a_1, \ldots, a_r$, there is an integer a which leaves the remainder a_i when divided by m_i.

Let us look at g now. If p is an odd prime such that $(\frac{13}{p}) = 1$, then $t^2 \equiv 13 \bmod p$ for some integer t. We show by induction on n that $x^2 \equiv 13 \bmod p^n$ has a solution. Suppose $t^2 \equiv 13 \bmod p^{n-1}$, say $t^2 = 13 + up^{n-1}$. Consider $t_0 = t + p^{n-1}t_1$ where we shall choose t_1 so that $t_0^2 \equiv 13 \bmod p^n$. This requires $u + 2tt_1 \equiv 0 \bmod p$; such a choice of t_1 can be made since $2t$ is coprime to p. Thus, we have shown that if 13 is a quadratic residue modulo an odd prime p, the polynomial g has a root modulo any power p^n. The same argument works if 17 or 221 is a quadratic residue modulo a prime p. For powers of 2 we note that $17 \equiv 3^2 \bmod 2^3$ and work as above but with a minor change; we try $t + 2^{n-2}t_1$ instead of the $(n-1)^{st}$ power. Note that $13 \equiv 8^2 \bmod 17$ and $17 \equiv 2^2 \bmod 13$. Further, for any p, one of $13, 17$ or 221 is a square modulo p. This is because the homomorphism $x \mapsto x^2$ on $(\mathbb{Z}/p\mathbb{Z})^*$ for an odd prime p, has kernel of order 2. Its image, which is the subgroup of squares, is the unique subgroup of index 2. Hence the cosets of 13 and 17 multiply to give the coset of 221. Thus, the above argument goes through for all p and it follows that the polynomial g, indeed, has roots modulo any nonzero integer.

The p-th roots of any prime number p is not a root of an integral polynomial of degree less than p. The Eisenstein criterion is a vast generalisation of such facts.

Now, let us ask ourselves what is different about $X^p - p$ in comparison with the above example. It is immediately evident that g is a reducible polynomial over $\mathbb{Z}$ while the famous Eisenstein criterion (see [3])shows that the polynomial $f(X) = X^p - p$ is irreducible over $\mathbb{Z}$. In fact, irreducibility of f can be proved quite easily even without the Eisenstein criterion.

Ok, but let us look at another obvious irreducible polynomial over $\mathbb{Z}$ the linear polynomial $h(X) = aX + b$ where $(a, b) = 1$. But, if p is any prime not dividing a, then $aX + b$ has a root modulo p. In other words, h does have a root modulo all but finitely many primes even though it is irreducible over $\mathbb{Q}$. Thus, a reasonable guess for us could be :

(*) *An integral polynomial which is irreducible over* $\mathbb{Z}$ *and has degree* > 1 *cannot have roots modulo all but finitely many primes. In other words, for such a polynomial, there are infinitely many primes modulo which the polynomial has no roots.*

Our intention is to show that this is true. In fact, one may wonder whether we have the much stronger result that an irreducible polynomial f over $\mathbb{Z}$ remains irreducible over all but finitely many primes. But, the following example dashes this hope. It was already observed by Hilbert.

Let p, q *be odd prime numbers such that* $(\frac{p}{q}) = (\frac{q}{p}) = 1$ *and* $p \equiv 1 \bmod 8$. *Then, the polynomial* $P(X) = (X^2 - p - q)^2 - 4pq$ *is irreducible whereas it is reducible modulo any integer.*

Now

$$\begin{aligned} P(X) &= X^4 - 2(p+q)X^2 + (p-q)^2 \\ &= (X - \sqrt{p} - \sqrt{q})(X + \sqrt{p} + \sqrt{q}) \\ &\quad (X - \sqrt{p} + \sqrt{q})(X + \sqrt{p} - \sqrt{q}). \end{aligned}$$

Since $\sqrt{p}, \sqrt{q}, \sqrt{p} \pm \sqrt{q}, \sqrt{pq}$ are all irrational, none of

the linear or quadratic factors of $P(X)$ are in $Z[X]$ i.e. $P(X)$ is irreducible over $\mathbb{Z}$. Note, as before, that it is enough to show that a factorisation of P exists modulo any prime power as we can use Chinese reminder theorem to get a factorisation modulo a general integer.

Now, $P(X)$ can be written in the following ways:

$$\begin{aligned} P(X) &= X^4 - 2(p+q)X^2 + (p-q)^2 \\ &= (X^2 + p - q)^2 - 4pX^2 \\ &= (X^2 - p + q)^2 - 4qX^2 \\ &= (X^2 - p - q)^2 - 4pq. \end{aligned}$$

The second and third equalities above show that $P(X)$ is reducible modulo any q^n and any p^n respectively. Also since $p \equiv 1 \bmod 8, p$ is a quadratic residue modulo 2 and, therefore, modulo any 2^n; the second equality above again shows that $P(X)$ is the difference of two squares modulo 2^n, and hence reducible mod 2^n.

If ℓ is a prime $\neq 2, p, q$, at least one of $(\frac{p}{\ell}), (\frac{q}{\ell})$ and $(\frac{pq}{\ell})$ is 1 by the product formula $(\frac{p}{\ell})\cdot(\frac{q}{\ell})\cdot(\frac{pq}{\ell}) = 1$ that we noted earlier. According as $(\frac{p}{\ell}), (\frac{q}{\ell})$ or $(\frac{pq}{\ell}) = 1$, the second, third or fourth equality shows that $P(X)$ is reducible mod ℓ^n for any n.

We mention, in passing, a very simple but important general method of proving the irreducibility of an integral polynomial. This will also set up the notation for our main statement when we address (*). To illustrate it, consider the polynomial $p(X) = X^4 + 3X^2 + 7X + 4$. Modulo 2, we have $p(X) = X(X^3 + X + 1)$ and both factors are irreducible over the field $\mathbb{Z}/2\mathbb{Z}$. We say that the *decomposition type* of $p(X)$ mod 2 is $1, 3$. Therefore, either p is irreducible over $\mathbb{Z}$ or if not, it is a product of a linear factor and an irreducible factor of degree 3 over $\mathbb{Z}$. But, modulo 11, we have $p(X) = (X^2 + 5X - 1)(X^2 - 5X - 4)$ where both factors are irreducible over the field $\mathbb{Z}/11\mathbb{Z}$. That is, the decomposition type of p mod 11 is $2, 2$. Thus, it cannot be that

p has a linear factor over $\mathbb{Z}$. In other words, p must be irreducible over $\mathbb{Z}$.

The Notion of Density of Primes

Let us get back to the guess quoted above as $(*)$. We need some notations. Let f be a monic integral polynomial of degree n. Suppose that f has distinct roots $\alpha_1, \quad , \alpha_n \in \mathbb{C}$; equivalently, the discriminant $disc(f) \neq 0$. Let $K = \mathbb{Q}(\alpha_1, \cdot \quad , \alpha_n)$, the subfield of $\mathbb{C}$ generated by the roots; that is, all rational expressions in the α_i's with coefficients from $\mathbb{Q}$. This is the smallest subfield of $\mathbb{C}$ which contains all the α_i's; it is also known as the splitting field of f for the reason that it is the smallest field over which f splits into the product $\prod_{i=1}^{n}(X - \alpha_i)$. We look at the group G of those permutations of α_i's which give rise to a field automorphism of K. This is known as the Galois group of f and denoted by $\mathrm{Gal}(f)$. For instance, if $f(X) = X^2 - a$ for some nonsquare integer a, then $K = \mathbb{Q}(\sqrt{a})$ where $\sqrt{a}$ denotes a square root of a in $\mathbb{C}$ and G has two elements I, σ where σ interchanges $\sqrt{a}$ and $-\sqrt{a}$. In general, although G is a subgroup of S_n, the permutations which belong to G are rather restricted; for example if f is irreducible over $\mathbb{Q}$, then a permutation in G is necessarily transitive on the α_i's. If $p \not| disc(f)$, then the decomposition type of f modulo p gives a partition of n as we saw above. On the other hand, each element of G has a cycle decomposition as an element of S_n and, thus defines a partition of n as well. Frobenius's wonderful idea is to relate the numbers of such partitions for a particular type. This will be expressed in terms of a notion of density of a set of prime numbers.

A set S of primes is said to have density δ if $\frac{\sum_{p \in S} 1/p}{\sum_{all\ p} 1/p} \to \delta$ *as* $s \to 1^+$ Here 1^+ means the limit when s tends to 1 from the right. For instance, any finite set of primes has density 0. Using this notion of density, we state:

Frobenius Density Theorem

The set of primes p modulo which a monic integral, irreducible polynomial f has a given decomposition type $n_1, n_2, \quad , n_r$, has density equal to $N/O(Gal(f))$ where $N = |\{\sigma \in Gal(f) : \sigma$ has a cycle pattern $n_1, n_2, \quad , n_r\}|$.

It is an elementary exercise that a finite group cannot be the union of conjugates of a proper subgroup.

As we point out now, our guess $(*)$ is vindicated by this theorem and a little bit of group theory; in particular, this also solves the IMO problem.

If f is irreducible, and has roots modulo all but finitely many primes, then the theorem shows that each σ has a cycle pattern of the form $1, n_2, \quad$ This means that each element of $\mathrm{Gal}(f)$ fixes a root. Since the roots of f are transitively moved around by $\mathrm{Gal}(f)$, this group would be the union of the conjugates of its subgroup H consisting of elements which fix a root of f, say α_1. However, it is an elementary exercise that a finite group cannot be the union of conjugates of a proper subgroup. Thus, in our case $H = \mathrm{Gal}(f)$. This means that $\mathrm{Gal}(f)$ fixes each α_i and is therefore trivial. That is, f is linear.

A famous theorem of Dirichlet on primes in arithmetic progressions asserts that the density of the set of primes $p \equiv a \bmod n$ is $1/\phi(n)$ for any $(a, n) = 1$. Dirichlet's theorem implies Frobenius's theorem for the polynomial $f(X) = X^n - 1$. The converse conclusion cannot quite be made. Thus, Frobenius formulated a conjecture which generalises both his theorem and Dirichlet's theorem. This was proved 42 years later by Chebotarev and is known now as the Chebotarev density theorem. This is an extremely useful result and even effective versions are known (see the end of the article for what the word 'effective' means here). Chebotarev's idea of proving this has been described by two prominent mathematicians as " a spark from heaven" In fact, this theorem was proved in 1922 ("while carrying water from the lower part of town to the higher part, or buckets of cabbages

The Galois theory of finite fields amounts to the statement that if g is a polynomial over $\mathbf{F}_p$ with simple roots, then the cycle pattern of $Frob_p$ viewed as a permutation of the roots of g coincides with the decomposition type of g over $\mathbf{F}_p$.

to the market, which my mother sold to feed the entire family") and Emil Artin wrote to Hasse in 1925 : "Did you read Chebotarev's paper? ... If it is correct, then one surely has the general abelian reciprocity laws in one's pocket..." Artin found the proof of the general reciprocity law in 1927 using Chebotarev's technique (he had already boldly published the reciprocity law in 1923 but admitted that he had no proof). Nowadays, Artin's reciprocity law is proved in some other way and Chebotarev's theorem is deduced from it!

To state Chebotarev's theorem, we recall one notion the Frobenius map. The idea is that given a monic integral polynomial f and its splitting field K, we try to associate to any prime $p \not| \, disc(f)$, an element Φ_p of $Gal(f)$ in a natural manner. If we can do this, one may expect that the decomposition type of f modulo p coincides with the cycle pattern of Φ_p. It can almost be done except that a prime p gives rise to a conjugacy class of elements in Gal(f). We do not define the Frobenius conjugacy class here as it is somewhat technical and merely explain some properties it has. For any prime number p, the p-th power map $Frob_p$ is an automorphism of the field $\bar{\mathbf{F}}_p$ which is identity on $\mathbf{F}_p$. Therefore, $Frob_p$ permutes the roots of any polynomial over $\mathbf{F}_p$. Indeed, *the Galois theory of finite fields amounts to the statement that if g is a polynomial over $\mathbf{F}_p$ with simple roots, then the cycle pattern of $Frob_p$ viewed as a permutation of the roots of g coincides with the decomposition type of g over $\mathbf{F}_p$*. In our case, we start with an integral polynomial f and look at it modulo p for various primes p. The basic theory of algebraic numbers shows that whenever $p \not| disc(f)$, the automorphism $Frob_p$ gives rise to a *conjugacy class* in Gal(f), called the Frobenius conjugacy class modulo p.

In Frobenius's density theorem, one cannot distinguish between two primes p, q defining different conjugacy classes $C(x)$ and $C(y)$, where some powers of x and y are

conjugate. For instance, for the polynomial $X^{10}-1$, the decomposition type modulo primes congruent to $1, 3, 7, 9$ mod 10 are, respectively, $1,1,1,1,1,1,1,1,1,1$; $1,1,4,4$; $1,1,4,4$; $1,1,2,2,2,2$.

Frobenius's theorem cannot distinguish between primes which are 3 mod 10 and those which are 7 mod 10; they define different conjugacy classes in $\mathrm{Gal}(X^{10}-1)$. Thus, it would imply that the number of primes $\equiv 3$ or 7 mod 10 is infinite but doesn't say whether each congruence class contains infinitely many primes. This is what Chebotarev's theorem asserts.

Chebotarev's Density Theorem

Let f be monic integral and assume that disc (f) does not vanish. Let C be a conjugacy class of Gal(f). Then, the set of primes p not dividing disc (f) for which $\sigma_p \in C$, has a well-defined density which equals $\frac{|C|}{|G|}$.

We state here two concrete results which can be proved with the aid of Chebotarev's density theorem.

(I) The set of primes which are expressible in the form $3x^2+xy+4y^2$ for integers x, y, has density $1/5$.

(II) The set of primes p for which the decimal expansion of $1/p$ has odd period, has density $1/3$.

Finally, we end with the remark that a recent result due to Berend & Bilu ([1]) gives an 'effective version' of Chebotarev's theorem. This means in simple terms that given a nonconstant integral polynomial, one has a certain number N, explicitly determined in terms of the irreducible factors of f and their coefficients, so that f will have an integral root if, and only if, it has a root modulo N. See also [2] for a nice historical introduction to Frobenius's and Chebotarev's density theorems.

Suggested Reading

[1] D Berend and Y Bilu, Polynomials with roots modulo every integer, *Proc. Amer. Math. Soc.*, Vol. 124, pp. 1663-1671, 1996.

[2] P Stevenhagen and H W Lenstra, Jr., Chebotarev and his density theorem, *Mathematical Intelligencer*, Vol. 18, pp.26-37, 1996.

[3] B Sury, Polynomials with Integer Values, *Resonance*, Vol.6, No.8, pp.46-60, 2001.

Address for Correspondence
B Sury
Stat-Math Unit
Indian Statistical Institute
8th Mile Mysore Road
Bangalore 560 059, India.
Email: sury@isibang.ac.in