Solutions to Problems posed in January 2009

Solution 1.
For any $g \in S$ and any $k > 0$, clearly $gS^k \subset S^{k+1}$ which gives

$$|S| \leq |S^2| \leq |S^3| \leq \cdots\cdots$$

Since G is finite, there is some k so that $|S^k| = |S^{k+1}|$. But then we also have

$$|S^{k+2}| = |S^{k+1}S| = |gS^kS| = |gS^{k+1}| = |S^{k+1}|.$$

Hence, $|S^k| = |S^l|$ for all $l > k$. As $O(G) = n$, cardinality of S^r is $\leq n$ for any r, which implies that $|S^n| = |S^m|$ for all $m > n$. In particular, $|S^n| = |S^{2n}|$ which gives on using the fact that $e \in S^n$, that $S^n \subset S^{2n}$. Thus, $S^n = S^{2n}$ which shows that S^n is closed under the group operation. The other properties required for a subgroup are evidently true.

Solution 2.
(The proof we give is due to M.K.Fort Jr. Much stronger results are known due to Fort as well as A.Norton).
First of all, we clarify what is meant by the slightly more general concept of a k-times (Peano) differentiable function f at a point x. This simply requires that there is a polynomial P_x of degree at most k (the k-th order Taylor polynomial at the point x) such that $(f(x+t) - P_x(t))/t^k \to 0$ as $t \to 0$. For $k = 0$, this is the usual continuity but for $k > 1$, it is more general than the usual k-times differentiability which requires that $f^{(k-1)}$ exist in a neighbourhood of x.
Suppose, if possible, f is a function which is discontinuous at all rationals and differentiable at all irrationals. Consider the set $A = \cap_n A_n$ where

$$A_n = \{p : \exists x, y; |x-p| < \frac{1}{n}, |y-p| < \frac{1}{n}, \frac{f(x)-f(p)}{x-p} - \frac{f(y)-f(p)}{y-p} > 1\}.$$

From the very definition of A, f is not differentiable at any of the points p in A. Thus, A is a subset of the rationals. However, we shall observe that for each n, the interior points of A_n form an everywhere dense set. This would be a contradiction to A being contained in the set of rationals. Start with any open interval I and with some rational number $q \in I$. Choose h, k such that

$$max(f(q), limsup_{t \to q} f(t)) > h > k > min(f(q), liminf_{t \to q} f(t)).$$

If $p \in I \cap (q - \frac{1}{n}, q)$ and $p > q - (h-k)$, then

$$\frac{h - f(p)}{q-p} - \frac{k - f(p)}{q-p} = \frac{h-k}{q-p} > 1.$$

Finally, if we choose x, y very close to q so that $f(x) > h$ and $f(y) < k$ (this is possible because f is discontinuous at q), we get

$$\frac{f(x) - f(p)}{x-p} - \frac{f(y) - f(p)}{y-p} > 1.$$

Hence $p \in A_n$. As the set

$$\{t \in I \cap (q - \frac{1}{n}, q) : t > q - (h-k)\}$$

is open, the above p is an interior point of A_n. Thus, the interior of A_n is everywhere dense.

Solution 3.
This was originally proved by W.Scherrer in 1946. Of course, we are considering here only the regular convex n-gons. For the equilateral triangle, it is simple to see as follows. For a possible lattice equilateral triangle, we must have the length l of any side to be of the form $\sqrt{a^2+b^2}$ for integers a, b. But then the area $\frac{\sqrt{3}l^2}{4}$ cannot be rational (note that the area is rational by using the determinant expression for it). Thus a lattice equilateral triangle does not exist. A similar proof can be carried over to show there are no regular lattice hexagons. Now, suppose $n > 4$ and $n \neq 6$ and suppose there is a regular lattice n-gon with vertices $P_1, \cdots, P_n$. Consider such a polygon of smallest possible area. But, if we reflect its vertices respectively about the vectors $\overrightarrow{P_2P_3}, \overrightarrow{P_3P_4}, \cdots, \overrightarrow{P_1P_2}$, we get a new, regular lattice n-gon which has smaller area !

Solution 4.
(These are due to Papadimitriou and T. Apostol).
There is a typographical error in the problem stated. The correct problem was supposed to be :
Prove that $\sum_{r=1}^{n} cot^2 \frac{r\pi}{2n+1} = n(2n-1)/3.$
IActually, even if we keep the left hand side $\sum_{r=1}^{n} cot^2 \frac{r\pi}{n+1}$ as it appeared originally, it is a similar exercise to prove this equals $n(n-1)/3$. Let us now show

$$\sum_{r=1}^{n} cot^2 \frac{r\pi}{2n+1} = n(2n-1)/3.$$

Start with

$$(cot\theta - i)^n = \frac{(cos\theta - isin\theta)^n}{sin^n\theta} = \frac{cosn\theta - isinn\theta}{sin^n\theta}.$$

Equating the imaginary parts on both sides, we obtain

$$\frac{sinn\theta}{sin\theta} = \sum_s \binom{n}{2s+1}(-1)^s cot^{n-2s-1}\theta.$$

Now, taking $2n+1$ instead of n, we will have

$$sin(2n+1)\theta = (sin^{2n+1}\theta)P_n(cot^2\theta)$$

for $0 < \theta < \pi/2$ where P_n is the polynomial

$$\binom{2n+1}{1}T^n - \binom{2n+1}{3}T^{n-1} + \cdots$$

Noting that the zeroes of P_n are precisely $r\pi/(2n+1)$ for $r = 1, 2, \cdots, n$ we have the first identity from the 'sum of the roots' formula.
Let us now consider the sum $\sum_{r=1}^n cot^{2m}\frac{r\pi}{2n+1}$ for general m. Noting that the inequality $sinx < x < tanx$ implies the inequality

$$cot^{2m}x < 1/x^{2m} < (1 + cot^2 x)^m$$

we have that

$$\sum_{r=1}^n cot^{2m}\frac{r\pi}{2n+1} < \frac{(2n+1)^{2m}}{\pi^{2m}}\sum_{r=1}^n \frac{1}{r^{2m}} < \sum_{r=1}^n (1 + cot^2\frac{r\pi}{2n+1})^m.$$

Therefore,

$$\sum_{r=1}^n (1 + cot^2\frac{r\pi}{2n+1})^m = \sum_{r=1}^n cot^{2m}\frac{r\pi}{2n+1} + O(n^{2m-1}).$$

In other words, to find c_{2m} where $\sum_{r=1}^n cot^{2m}\frac{r\pi}{2n+1} = c_{2m}n^{2m} + O(n^{2m-1})$, it suffices to look at the sum

$$(cot^2\frac{\pi}{2n+1})^m + (cot^2\frac{2\pi}{2n+1})^m + \cdots + (cot^2\frac{n\pi}{2n+1})^m$$

which is the sum s_m of the m-th powers of the roots of the polynomial P_n. By the usual Newton formula, one has

$$-s_r = (-1)^r r\sigma_r + \sum_{k=1}^{r-1}(-1)^{r-k}s_k\sigma_{r-k}$$

where σ_r are the elementary symmetric functions. Now, we note that

$$\sigma_r = \frac{\binom{2n+1}{2r+1}}{\binom{2n+1}{1}} = \frac{2^{2r}}{(2r+1)!} n^{2r} + O(n^{2r-1}).$$

Using this, we can prove without difficulty by induction on m that

$$-s_m = (-1)^m \frac{2^{4m-1} B_{2m}}{(2m)!} n^{2m} + O(n^{2m-1})$$

where B_k's are the Bernoulli numbers. In other words,

$$\sum_{r=1}^{n} cot^{2m} \frac{r\pi}{2n+1} = (-1)^{m-1} \frac{2^{4m-1} B_{2m}}{(2m)!} n^{2m} + O(n^{2m-1}).$$

Solution 5.
(This is due to Sister Beiter).
If n is a power of a prime, say $n = p^k$, then $\Phi_n(X) = \Phi_p(X^{p^{k-1}})$ evidently. Therefore, the cyclotomic polynomial does have all coefficients to be 0 or 1. We claim that for any other n, there is at least one negative coefficient. Indeed, it is another easy exercise to show that when n has at least 2 prime divisors, $\Phi_n(1) = 1$ (ask me if you can't show this). Thus, the sum of all the coefficients is 1. However, the top coefficient is already 1 which means that there must be some negative coefficient because it is clearly impossible that $\Phi_n(X) = X^{\phi(n)}$.

Solution 6.
(This is due to I.Amemiya & K.Masuda).
Call the assertion "whenever $a \in B$ satisfies $a^n \in A$ for all large enough n, it must be in A" as property (P) for A as a subring of B. Suppose A has property as a subring of B, and consider any $f = \sum_{n \geq 0} b_n X^{n+k} \in B[[X]]$ satisfying $f^r \in A[[X]]$ for all large enough r. Now, $b_0^r \in A$ for all large r and, therefore, $b_0 \in A$. The trick is to consider the subring B' of B which consists of all $b \in B$ such that $b_0 b^m \in A$ for all $m \geq 0$. It is clear that it is a subring and that it contains A. Let us show by induction on n that $b_n \in B'$ for all n. Suppose we know $b_0, b_1, \cdots, b_n \in B'$ and we shall show $b_{n+1} \in B'$. Now $b_0(\sum_{i=0}^{n} b_i X^{k+i})^m \in A[[X]]$ for all m. So,

$$b_0 f^r (f - \sum_{i=0}^{n} b_i X^{k+i})^{(r+1)m} = \sum_s a_0 b_0 f^{r+s} (\sum_{i=0}^{n} b_i X^{k+i})^{(r+1)m-s} \in A[[X]]$$

for some $a_0 \in A$. Thus, the corresponding coefficient of $X^{kr+(k+n+1)(r+1)m}$ - which is $b_0^{r+1}b_{n+1}^{(r+1)m}$ - is in A. Hence, by property (P), we have $b_0 b_{n+1}^m \in A$ for all m. Thus, $b_{n+1} \in B'$. So, we have shown that $b_0 f^m \in A[[X]]$ for all m which gives

$$(f - b_0 X^k)^r = f^r + \sum_{s=1}^{r} (const.) b_0^s f^{r-s} X^{ks} \in A[[X]].$$

Since $f - b_0 X^k$ starts with $b_1 X^{k+1}$, we get $b_1 \in A$ again using property (P). In this manner, all the b_i's are in A.
We will indicate how to use this fact to prove Joris's theorem asserting that when $f : \mathbf{R} \to \mathbf{R}$ is so that f^2, f^3 are smooth, then so is f. In fact, this works with a set $n_1, n_2, \cdots, n_r$ of positive integers with GCD 1 instead of $2, 3$. Choose a positive integer p such that every integer $r \geq p$ is a non-negative linear combination of the n_i's. In other words, one could take p to be one more than the corresponding Frobenius number. Thus, it follows that f^r is smooth for all $r \geq p$. The connection with power series is to look, for any smooth function g at a point a, the so-called ∞-jet of g at a which is the power series

$$J_a(g) := \sum_{n \geq 0} \frac{g^{(n)(a)X^n}}{n!} \in \mathbf{R}[[X]].$$

Consider the set D of points a such that $J_a f^p \neq 0$. It is easy to show that D is an open subset and that $J_a f^r = 0$ at each a outside D for any $r \geq p$. Considering the ring B of all continuous functions on D and its subring A which consists of restrictions of continuous functions on $\mathbf{R}$ which vanish outside D. It is clear that A has property (P) as a subring of B. For our smooth functions f^r, $\{J_a f^r : a \in D\}$ can be considered as an element $J(f^r)$ of $A[[X]]$ for each $r \geq p$. As f is smooth on D, the relation $J(f)^r = J(f^r) \in A[[X]]$ for all $r \geq p$ implies, by the above property (P) that $J(f) \in A[[X]]$. From this, it is not difficult to conclude smoothness of f using repeatedly the following observation :
When f, g are continuous on $\mathbf{R}$, vanish outside D, where f is differentiable and $f' = g$ in D, then f is everywhere differentiable and $f' = g$.