1. INTRODUCTION

In the preceding paper, we gave a history of the Polignac and Sierpinski problems; basically, both problems boil down to a discussion of the values of k for which the numbers $1 + k^2 n$ ($n > 0$) are always composite for all n. For example, if $k = 271,129$, the numbers are always composite (and, indeed, are divisible by a member of the set of primes $P = \{3, 5, 7, 13, 17, 241\}$).

Jacobi half-seriously claimed that in any mathematical problem "one must always invert". In this problem, the situation does seem clearer if we concentrate not on the numbers $1 + k^2 n$ but on the set of primes $P$. Let us ask the question in the inverse fashion: what sets $P$ have the property that there exist integers $k$ such that, for all $n > 0$,

$$1 + k^2 n \equiv 0 \mod P.$$ 

The notation merely means "modulo at least one of the primes in the set $P$". The example in the last paragraph shows that such sets $P$ do exist.

2. DISCUSSION OF SETS OF SMALL CARDINALITY

The fundamental tool in our discussions will be a very easy lemma.

**Lemma 2.1** If $1 + k^2 n \equiv 0 \mod p$ and $1 + k^2 n + a \equiv 0 \mod p$, and if $a$ is minimal, then $p$ divides $2^a - 1$, and $p$ does not divide $2^b - 1$ for $b < a$.

**Proof.** We immediately have

$$k^2 n \equiv -1 \equiv k^2 n + a \mod p.$$ 

Hence $1 \equiv 2^a \mod p$, and $p$ divides $2^a - 1$. Minimality is obvious.

We at once deduce several results.

**Lemma 2.2** $|P| = 1$ is impossible.

**Proof.** $1 + k^2 n \equiv 0 \equiv 1 + k^2 n + 1$ for $|P| = 1$.

But then $p|(2-1)$, and this is impossible.

It is useful at this stage to represent the various congruences by points on a linear graph and label each point by the modulus of the associated congruence.
Basically, Lemma 2.2 shows that adjacent points in the graph cannot possess the same label; so the graph cannot contain a section

Now we prove

Lemma 2.3. $|P| = 2$ is impossible.

Proof. By Lemma 2.2, the system of congruences gives rise to an associated graph of the form

where $P = \{p, q\}$. Then Lemma 2.1 shows that $p | 2^2 - 1$, that is, $p = 3$. Similarly, $q = 3$, and we have a contradiction.

One can proceed onwards solely using graph-theoretic arguments. However, it is useful to employ density arguments as well. We note that the primes

$\{p_2 = 3, p_3 = 7, p_4 = 5, p_5 = 31\}$

belong to exponents 2, 3, 4, 5, respectively, where we say that $p_i$ belongs to $i$ when $p_i | 2^i - 1$ (i being minimal). Clearly, there is at least one $p_i$ for each $i > 1$, except for $i = 6$.

Now if $|P| = 3$, then $P = \{7, 5, 31\}$ can cover at most

$\frac{1}{3} + \frac{1}{4} + \frac{1}{5} = \frac{47}{60}$

of the points of the graph (actually, the number is less). So $P$ must contain the prime 3. The graph thus has the form

Points $A$ and $B$ must be associated with distinct primes; label $A$ by $q$ and $B$ by $r$. Then $C$ must be labelled $q$ (and it follows that $q = 5$). But then any labelling of $D$ leads to a contradiction. This proves

Lemma 2.4. It is impossible to have $|P| = 3$.

For $|P| = 4$, the density argument shortens the graph-theoretic argument quite a lot. Since

$\frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{7} = \frac{389}{720} < 1$, 