A CONGRUENCE PROPERTY OF THE DIVISORS OF n FOR EVERY n

By C. L. Vanden Eynden

If n is any positive integer, n has at least as many positive divisors congruent to 1 as congruent to 3 (mod 4). The purpose of this paper is to characterize those triples of integers a, b and k that can be substituted for 1, 3 and 4 in the preceding sentence. More precisely, denote by $N(n, j, k)$ the number of positive divisors d of n such that $d \equiv j \pmod{k}$. From now on we assume $k > 1$, $a \not\equiv b$, and, for definiteness, $1 \leq a, b \leq k$. Let S be the set of triples $\langle a, b, k \rangle$ such that $N(n, a, k) \geq N(n, b, k)$ for all positive integers n. All congruences will be modulo k unless otherwise specified.

Lemma 1. *Let* $\langle a, b, k \rangle \varepsilon S$ *and* $(a, b, k) = 1$. *Then* $(b, k) = a = 1$.

Proof. First we show $a = 1$. Taking $n = b$ shows $a \mid b$. Since if $n = k + b$, then $(a + k) \nmid n$, we must have $a \mid (k + b)$ and so $a \mid k$. Thus $a \mid (a, b, k)$.

Now let $(b, k) = h$ and set $n = b + kb/h$. Since both $b, n \equiv b$, there must exist another divisor of n congruent to 1 besides 1 itself. Suppose $t(rk + 1) = n = b(k/h + 1)$, $r, t \geq 1$. Clearly $t < b$ unless $h = 1$. But $t \equiv b$, therefore $t = b$. Thus $h = (b, k) = 1$.

Lemma 2. *Let* $\langle a, b, k \rangle \varepsilon S$ *and* $(a, b, k) = 1$. *Then* $c^2 \equiv 1 \pmod{k}$ *whenever* $(c, k) = 1$.

Proof. First we show $b^2 \equiv 1$. Since $a = (b, k) = 1$ by Lemma 1, we can use Dirichlet's theorem to pick distinct primes $p_1, p_2 \equiv b$. Let $n = p_1p_2$. The divisors of n are $1, p_1, p_2, p_1p_2$. Thus $N(n, b, k) \geq 2$ so we must have $p_1p_2 \equiv 1$. Thus $b^2 \equiv 1$.

Now let $(c, k) = 1$. We want to show $c^2 \equiv 1$ and so can assume $c \not\equiv 1$ and $c \not\equiv b$. Choose x such that $cx \equiv b$ and pick primes $p_1, p_2 \equiv c$ and $p \equiv x$. Let $n = pp_1p_2$. Its divisors are $1, p, p_1, p_2, pp_1, pp_2, p_1p_2, pp_1p_2$. Since $pp_1 \equiv pp_2 \equiv b$, n must have at least one divisor $d \equiv 1$ besides 1 itself. If $p \equiv 1$ or $pp_1p_2 \equiv 1$, then $c \equiv b$, contrary to assumption. Also $p_1 \equiv p_2 \equiv c \not\equiv 1$. Only one divisor remains, p_1p_2. Thus $p_1p_2 \equiv c^2 \equiv 1$.

Lemma 3. *A natural number k has the property that* $c^2 \equiv 1 \pmod{k}$ *whenever* $(c, k) = 1$ *if and only if* $k \mid 24$.

Proof. The proof that k has the required property whenever $k \mid 24$ is easy and will be omitted. To see the converse, suppose $k \nmid 24$. Then there exists a divisor m of k such that $(m, k/m) = 1$ and m is either a power of a prime $p \geq 5$,

Received May 22, 1961. The author is a National Science Foundation Fellow. He wishes to thank Professor Ivan Niven for suggesting both the problem and an improvement which shortened the proof.