4. Discussion. By a slightly more complicated argument we could prove that, for some positive constant c,

$$f(x) < x \exp\left\{-c(\log x)^{1/2}\right\};$$

but the true order of $f(x)$ seems to be considerably smaller. As far as I know, the only estimate for $f(x)$ from below is

$$f(x) > C \log x,$$

which is due to Lehmer.

Added later. As far as I know the question of the existence of even numbers satisfying $2^n \equiv 2 \pmod{n}$ has not been considered. Except for the trivial case $n=2$, I have not succeeded in finding any such even numbers.* By the method of this paper it is easy to see that their number $\leqq x$ is certainly less than $x \exp\left\{-\frac{1}{3}(\log x)^{1/4}\right\}$.

References

1. D. H. Lehmer, On the Converse of Fermat's Theorem, I, II, this MONTHLY, vol. 43, 1936, pp. 347–354; vol. 56, 1949, pp. 300–309. These papers contain references to other work on almost primes.

2. P. Erdös, On the Converse of Fermat's Theorem, this MONTHLY, vol. 56, 1949, pp. 623–624.

ANGLES WITH RATIONAL TANGENTS**

T. S. CHU, National Kunming Teachers College

1. Introduction. The purpose of this note is to show that the class of angles having rational tangents, and the class of angles which are rational multiples of π, intersect only in the obvious cases.

2. Theorem. We shall establish the following result.

THEOREM. *If x is a rational multiple of π, and* $\tan x$ *is rational, then x is an integral multiple of $\pi/4$.*

3. Proof. Let $\tan x = q/p$. The theorem is trivially satisfied if $q=0$ or if $|p|=|q|$. Further, without loss of generality, x may be restricted to the first quadrant, so that p and q may be assumed positive, integral, unequal, and coprime.

If $x = m\pi/n$, then $e^{inx} = e^{-inx} = \pm 1$, or

$$(\cos x + i \sin x)^n = (\cos x - i \sin x)^n,$$

and

$$(p + iq)^n/(p^2+q^2)^{n/2} = (p - iq)^n/(p^2+q^2)^{n/2}.$$

---

* Added still later: Lehmer has just informed me that $2^{161038} \equiv 2 \bmod (161038)$, $(161038 = 2 \cdot 73 \cdot 1103)$.

** Revised by J. D. Swift.

Thus

$$(p - iq)^n = (p + iq)^n = (p - iq + 2iq)^n$$
$$= (p - iq)^n + \binom{n}{1}(p - iq)^{n-1}2iq + \cdots$$
$$+ \binom{n}{n-1}(p - iq)(2iq)^{n-1} + (2iq)^n.$$

Therefore $(p-iq)$ divides $(2qi)^n$, and p^2+q^2 divides $(2q)^{2n}$. Similarly, p^2+q^2 divides $(2p)^{2n}$ and therefore divides $(2^{2n}p^{2n}, 2^{2n}q^{2n})=2^{2n}$. Then $p^2+q^2=2^k$; but this is possible in positive coprime integers only when $p=q=k=1$, a contradiction.

4. Corollary. By writing tan nx as a rational function in terms of tan x, the reader may verify the following corollary.

COROLLARY: *The equations*

$$\sum_{k=0}^{a}(-1)^k\binom{n}{2k+1}x^{2k} = 0, \qquad a = \left[\frac{n-1}{2}\right], \qquad n > 2, n \neq 4,$$

and

$$\sum_{k=0}^{b}(-1)^k\binom{n}{2k}x^{2k} = 0, \qquad b = \left[\frac{n}{2}\right], \qquad n > 2,$$

have no rational roots.

A GENERALIZATION OF GAUSS' LEMMA*

ALEXANDER AIGNER, Graz, Austria

1. Introduction. We say that a number *belongs to the first half* modulo a number n if it is congruent mod n to one of the numbers 1, 2, $\cdots$, $[(n-1)/2]$, and that it *belongs to the second half* modulo n if it is congruent mod n to one of the numbers $[n/2]+1$, $[n/2]+2$, $\cdots$, $n-1$. The well-known Gauss' lemma can then be stated as follows:

A number A is a quadratic residue modulo an odd prime p if and only if an even number of the terms

(1) $$A, 2A, 3A, \cdots, (p-1)A/2$$

belongs to the second half mod p.

2. Theorem. In this note we shall prove the following result.

THEOREM: *If p is an odd prime and A is odd, then the number of terms in the sequence* (1) *which belong to the second half* mod p *is equal to the number of terms which belong to the second half* mod $2p$.

* Translated and revised by E. G. Straus.