

1077-11-674

**Carl Pomerance\***, carl.pomerance@dartmouth.edu. *Elliptic Carmichael numbers.*

(This represents joint work with Aaron Ekstrom and Dinesh Thakur.) One hundred years ago, R. D. Carmichael discovered some composite numbers  $n$  that behave like primes with respect to the Fermat congruence; namely,  $a^n \equiv a \pmod{n}$  for every integer  $a$ . The least example is  $n = 561$ , and after joint work with W. R. Alford and A. Granville, we now know that there are infinitely many such  $n$ . In the 1980's, D. M. Gordon defined an analogue where the Fermat congruence is replaced with  $[n+1]P \equiv O \pmod{n}$ , with  $P$  an arbitrary rational point on an arbitrary CM elliptic curve with discriminant coprime to  $n$ . An example is  $n = p(2p+1)(3p+2)$ , where  $p = 468,686,771,783$ . We show, modulo a mild conjecture on the least prime in a residue class, that there are infinitely many of these elliptic Carmichael numbers. (Received September 09, 2011)