Math 342 Tutorial

July 16, 2025

Question 1. Show the following: **(a)** If n is an Euler pseudo prime to the bases a and b, then n is an Euler pseudoprime to the base ab. **(b)** If n is an Euler pseudoprime to the base b, then n is also an Euler pseudoprime to the base $n-b$. **(c)** If $n \equiv 5 \pmod 8$ and n is an Euler pseudoprime to the base 2, then n is a strong pseudoprime to the base 2. **(d)** If $n \equiv 5 \pmod{12}$ and n is an Euler pseudoprime to the base 3, then n is a strong pseudoprime to the base 3.

- **(a)** We have $(ab)^{(n-1)/2} \equiv a^{(n-1)/2} b^{(n-1)/2} \equiv (a \mid n)(b \mid n) \equiv (ab \mid n) \pmod n$. This shows that n is an Euler pseudoprime to the base ab.
- **(b)** Observe $(n-b)^{(n-1)/2} \equiv (-1)^{(n-1)/2} b^{(n-1)/2} \equiv (-1 \mid n)(b \mid n) \equiv (-b \mid n) \equiv (n-b \mid n) \pmod n$, whereupon n is an Euler pseudoprime to the base $n-b$.
- **(c)** By assumption $2^{(n-1)/2} \equiv (2 \mid n) \equiv -1 \pmod n$. Also by assumption, we have $n-1 = 2^2 t$ with t odd. Thus, $-1 \equiv 2^{(n-1)/2} \equiv 2^{2t} \pmod n$. But this means that n is a strong pseudoprime to the base 2.
- **(d)** By assumption, $3^{(n-1)/2} \equiv (3 \mid n) \equiv -1 \pmod n$. Also by assumption, $n-1 = 12k+4 = 2^2(3k+1)$. Then $-1 \equiv 3^{(n-1)/2} \equiv 3^{2(3k+1)} \pmod n$, and n passes Miller's test.

Question 2. Show that if $n = p_1 \cdots p_k$ is square-free, and if each $(p_i - 1) \mid (n-1)$, then n is a Carmichael number.

Let b be a positive integer with $(b, n) = 1$, Then $b^{p_i - 1} \equiv 1 \pmod{p_i}$ for each p_i. By assumption, there are integers t_i such that $t_i(p_i - 1) = n-1$; but then $b^{n-1} \equiv 1 \pmod{p_i}$ for each p_i. It follows, therefore, that $b^{n-1} \equiv 1 \pmod n$.

Question 3. Show the following: **(a)** Show that if n is a pseudoprime to the bases a and b, then n is a pseudoprime to the base ab. **(b)** Suppose that $(n, a) = 1$. If n is a pseudoprime to the base a, then n is a pseudoprime to the base $\overline{a}$ where $\overline{a}$ is the inverse of a modulo n.

- **(a)** Note $(ab)^{n-1} \equiv a^{n-1} b^{n-1} \equiv 1 \cdot 1 \equiv 1 \pmod n$, hence n is a pseudoprime to the base ab.
- **(b)** Since $\overline{a}$ is the modular inverse of a, we have that $\overline{a^{n-1}} = \overline{a}^{n-1}$ is the modular inverse of a^{n-1}. Then $a^{n-1} \equiv 1 \pmod n$ if and only if $1 \equiv \overline{a}^{n-1} \pmod n$.

Question 4. Show that if $n = (a^{2p} - 1)/(a^2 - 1)$, where $a > 1$ is an integer, and p an odd prime not dividing $a(a^2-1)$, then n is a pseudoprime to the base a. Conclude there are infinitely many pseudoprimes to any any base. [Hint: To establish that $a^{n-1} \equiv 1 \pmod n$, show that $2p \mid n-1$, and demonstrate that $a^{2p} \equiv 1 \pmod n$.]

Note that $n - 1 = a^2(a^{2(p-1)} - 1)/(a^2 - 1)$. Since $a^{2(p-1)} \equiv 1 \pmod p$, we have that $n - 1 \equiv 0 \pmod p$. Next, we write $a^2(a^{2(p-1)} - 1)/(a^2 - 1) = a^2(1 + a^2 + \cdots + a^{2(p-2)})$. Hence, if a is odd then $n - 1 \equiv 0 \pmod 2$. In all cases, then, we have that $n - 1 \equiv 0 \pmod{2p}$. Now, $a^{2p} - 1 \equiv n(a^2 - 1) \equiv 0 \pmod n$, whereupon $a^{n-1} \equiv a^{2pk} \equiv 1^k \equiv 1 \pmod n$ for some integer k.

Question 5. Show that if n is a Carmichael number, then n is square free.

Let n be a Carmichael number. Suppose there is a prime p such that $n = p^t m$ with $(p, m) = 1$ and $t > 1$. Let $b = x$ be a solution to the system of linear congruences $x \equiv p^{t-1} + 1 \pmod{p^t}$ and

$x \equiv 1 \pmod{m}$. Then, since $(b, p) = 1 = (b, m)$, we have that $(b, n) = 1$. If it were the case that $b \equiv 1 \pmod{n}$, then $b \equiv 1 \pmod{p^t}$, a contradiction. Thus, $b \not\equiv 1 \pmod{n}$. Next note that $b^n \equiv (p^{t-1} + 1)^n \equiv 1 \pmod{p^t}$ by the binomial theorem and the fact that $p^t \mid n$. Since also $b \equiv 1 \pmod{m}$, we have that $b^n \equiv 1 \pmod{n}$. But then $b^n \not\equiv b \pmod{n}$ whereupon n is not a Carmichael number. Since this contradicts our original assumption, it follows that n must be square-free whenever n is a Carmichael number.