Math 445 Homework 2 Solutions

6. If $N = p_1 \cdots p_k$ is a product of distinct primes and $(p_i - 1)|(N-1)$, for every i, then N is a pseudoprime to every base a satisfying $(a, N) = 1$.

   We wish to show that if $(a, N) = 1$, then $a^{N-1} \equiv 1 \pmod{N}$. Since $(a, N) = 1$ amd $p_i|N$, $(a, p_i) = 1$ for every i, so $a^{p_i-1} \equiv 1 \pmod{p_i}$ for every i. Since $(p_i - 1)|(N-1)$, $n - 1 = (p_i - 1)q_i$, so $a^{N-1} = (a^{p_i-1})^{q_i} \equiv 1^{q_i} \equiv 1 \pmod{p_i}$ for every i. So $p_i|(a^{N-1} - 1)$ for every i. Since the p_i are distinct primes, they are each relatively prime to one another, so [by an induction argument, using $a|c, b|c$ and $(a, b) = 1 \Rightarrow ab|c$] $N = p_1 \cdots p_k | a^{N-1} - 1$, as desired.

7. If $n = pq$ with $p < q$ and p, q both prime, then it is not possible for $q - 1$ to divide $n - 1$.

   Suppose $q - 1|n - 1$, so $n - 1 = (q - 1)s$; since $n = pq$, we have $pq - 1 = qs - s$, so $q(s-p) = s-1$, so $q|(s-1)$. Note that since $p \geq 2$, $n > q$, so $n - 1 > q - 1$¡ so $s \geq 2$. But $q|(s-1)$ means $|q| \leq |s-1|$, i.e., $s \geq q+1$, but then $n-1 = (q-1)s \geq (q-1)(q+1) = q^2-1$, so $n \geq q^2 > pq = n$, a contradiction. So $q - 1$ cannot divide $n - 1$.

   Another, shorter, approach: If $n - 1 = (q - 1)s$, then since $n - p = (q - 1)p$, we have $p - 1 = (q - 1)(s - p)$, so $(q - 1)|(p - 1)$, so $|q - 1| \leq |p - 1|$, which is impossible, since $p < q$.

8. 2465, 2821, and 6601 are Carmichael numbers.

   We show that the conditions established in Problem # 6 prevail:

   $2465 = 5 \cdot 493 = 5 \cdot 17 \cdot 29$, a product of distinct primes, and

   $2465 - 1 = 2464 = 2 \cdot 1232 = 2^2 \cdot 616 = 2^3 \cdot 308 = 2^4 \cdot 154 = 2^5 \cdot 77 = 2^5 \cdot 7 \cdot 11 = (5-1) \cdot 2^3 \cdot 7 \cdot 11 = (17-1) \cdot 2 \cdot 7 \cdot 11 = (29-1) \cdot 2^3 \cdot 11$.

   $2821 = 7 \cdot 403 = 7 \cdot 13 \cdot 31$, a product of distinct primes, and

   $2821 - 1 = 2820 = 2 \cdot 1410 = 2^2 \cdot 705 = 2^2 \cdot 3 \cdot 235 = 2^2 \cdot 3 \cdot 5 \cdot 47 = (7-1) \cdot 2 \cdot 5 \cdot 47 = (13-1) \cdot 5 \cdot 47 = (31-1) \cdot 2 \cdot 47$.

   $6601 = 7 \cdot 943 = 7 \cdot 23 \cdot 41$, a product of distinct primes, and

   $6601 - 1 = 6600 = 2^2 \cdot 5^2 \cdot 66 = 2^3 \cdot 3 \cdot 5^2 \cdot 11 = (7-1) \cdot 2^2 \cdot 5^2 \cdot 11 = (23-1) \cdot 2^2 \cdot 3 \cdot 5^2 = (41-1) \cdot 3 \cdot 5 \cdot 11$.

9. If $x^2 \equiv 1 \pmod{n}$ and $x \not\equiv \pm 1 \pmod{n}$, then $1 < (x-1, n) < n$ and $1 < (x+1, n) < n$.

   $x^2 \equiv 1 \pmod{n}$ means $n|(x^2 - 1) = (x+1)(x-1)$.
   First note that $(x+1, n) = n$ would mean that $n|x+1$, so $x \equiv -1 \pmod{n}$, a contradiction. So $(x + 1, n) < n$. If $(x + 1, n) = 1$, then this implies that $n|(x - 1)$, so $x \equiv 1 \pmod{n}$, a contradiction. So $(x + 1, n) > 1$. So $1 < (x + 1, n) < n$.

   Similarly, if $(x - 1, n) = n$ then $x \equiv 1 \pmod{n}$, a contradiction. If $(x - 1, n) = 1$ then $n|(x + 1)$, so $x \equiv -1 \pmod{n}$, a contradiction. So $1 < (x - 1, n) < n$.

10. $n = 3277 = 29{\times}113$ is a strong pseudoprime to the base 2.

$n - 1 = 3276 = 2 \cdot 1638 = 2^2 \cdot 819$. So we wish to show that either
$2^{819} \equiv \pm 1 \pmod{3277}$ or $2^{1638} \equiv -1 \pmod{3277}$. We compute:

$819 = 512 + 307 = 512 + 256 + 51 = 512 + 256 + 32 + 16 + 2 + 1$
$= 2^0 + 2^1 + 2^4 + 2^5 + 2^8 + 2^9$. Then, mod 3277,

$2^{2^0} \equiv 2$, $2^{2^1} \equiv 4$, $2^{2^2} \equiv 16$, $2^{2^3} \equiv (16)^2 = 256$,
$2^{2^4} \equiv (256)^2 = 65536 = 3277 * 19 + 3273 \equiv -4$,
$2^{2^5} \equiv (-4)^2 = 16$, $2^{2^6} \equiv (16)^2 = 256$, $2^{2^7} \equiv (256)^2 \equiv -4$, $2^{2^8} \equiv 16$, $2^{2^9} \equiv 256$, so
$2^{819} = 2^{2^0} \cdot 2^{2^1} \cdot 2^{2^4} \cdot 2^{2^5} \cdot 2^{2^8} \cdot 2^{2^9} \equiv 2 \cdot 4 \cdot (-4) \cdot 16 \cdot 16 \cdot 256 = (-32) \cdot (256)^2 \equiv (-32) \cdot (-4)$
$= 128 \not\equiv \pm 1$, but

$2^{1638} \equiv (128)^2 = 16384 = 3277 \cdot 4 + 3276 \equiv 3276 \equiv -1$.

So since $2^{\frac{3277-1}{2}} = -1 \pmod{3277}$, $3277 = 29 \cdot 113$ is a strong pseudoprime to the base 2.