Math 445 Homework #2 Solutions

5. $n = pq$, $p<q$ both prime, then $q-1 \nmid n-1$:

Suppose $n-1 = (q-1)x$, then $pq-1 = qx-x$, so $q(p-x) = 1-x$

So $q \mid x-1$, so $|x-1| \geq q$, so $x-1 \geq q$ (we can't have $x<1$, because $x \geq 0$). So $x \geq q+1$, so ~~$x-1 \geq (q-1)(q+1)$~~

$n-1 = (q-1)x \geq (q-1)(q+1) = q^2-1$. So $n = pq \geq q^2$, implying $p \geq q$, a contradiction! So $q-1 \nmid n-1$. ///

6. Find another Carmichael number.

$1105 = 5 \cdot 221 = 5 \cdot 13 \cdot 17$ is a Carmichael number, since

$5-1 = 4 \mid 1105-1 = 1104$ $\quad 1104 = 4 \cdot 276$; also,

$1104 = 12 \cdot 92$ so $13-1 \mid 1105-1$, and

$1104 = 16 \cdot 69$ so $17-1 \mid 1105-1$. Therefore, if $(a, 1105) = 1$, then

$(a,5) = (a,13) = (a,17) = 1$ so $a^4 \underset{5}{\equiv} 1$ so $a^{1104} \underset{5}{\equiv} (1)^{276} = 1$

so $5 \mid a^{1104}-1$. Also $a^{12} \underset{13}{\equiv} 1$ so $a^{1104} \underset{13}{\equiv} (1)^{92} = 1$ so $13 \mid a^{1104}-1$, and

$a^{16} \underset{17}{\equiv} 1$ so $a^{1104} \underset{17}{\equiv} (1)^{69} = 1$ so $17 \mid a^{1104}-1$. Then since $(5,13) = 1$

$5 \cdot 13 \mid a^{1104}-1$, and since $(5 \cdot 13, 17) = 1$, $1105 = 5 \cdot 13 \cdot 17 \mid a^{1104}-1$

so $a^{1104} \underset{1105}{\equiv} 1$ for all a with $(a, 1105) = 1$, so 1105 is a Carmichael number.

[FYI: Other Carmichael numbers are 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, 41041, ... (source: mathworld.wolfram.com)]

7. Find all $a,b,c>0$ with $a \underset{c}{\equiv} b$, $b \underset{a}{\equiv} c$, and $c \underset{b}{\equiv} a$.

Either two (or more) of a,b,c are equal, or they are all distinct; after changing the names (our hypothesis is <u>symmetric</u> in a,b,c) we may assume either $a=b$ or $a<b<c$.
But if $a=b$, then $c \equiv a \pmod b$ <u>really</u> says $c \equiv a \pmod a$, i.e. $c \equiv 0 \pmod a$, i.e. $a \mid c$, so a,b,c <u>really</u> are a, a, ak for some k. But $a \underset{ak}{\equiv} a$, $a \underset{a}{\equiv} ak$, and $ak \underset{a}{\equiv} a$ <u>are</u> all true. So $(a,b,c)=(a,a,ak)$ <u>are</u> solutions.
On the other hand, if $0<a<b<c$, then $0<b-a<c-a<c$ and then $a \equiv b \pmod c$, i.e. $c \mid b-a$ is impossible; no number <u>strictly</u> between 0 and c is a multiple of c. So the <u>only</u> solutions (up to changing names) are a,a,ak; i.e. for any solution, two of the terms are equal, and the third is a multiple of that common value. ///

8. If $x^2 \equiv 1 \pmod n$ and $x \not\equiv \pm 1 \pmod n$ then
$1<(x-1,n)<n$ <u>and</u> $1<(x+1,n)<n$.

We have $n \mid x^2-1=(x-1)(x+1)$ and $n \nmid x-1$ (so $(x-1,n)<n$) and $n \nmid x+1$ (so $(x+1,n)<n$). If $(x-1,n)=1$, then since $n \mid (x-1)(x+1)$ we have $n \mid x+1$, a contradiction. So $1<(x-1,n)<n$. Similarly, if $(x+1,n)=1$, then since $n \mid (x+1)(x-1)$ we have $n \mid x-1$, a contradiction. So $1<(x+1,n)<n$. ///

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

$n-1 = 3276 = 2 \times 1638 = 2^2 \times 819$. So we need to show that

either $2^{819} \equiv 1 \pmod{3277}$ or $2^{819} \equiv -1 \pmod{3277}$ or
$2^{1638} \equiv -1 \pmod{3277}$. So we compute

$2^1 \equiv 2 \pmod{3277}$
$2^2 \equiv 4$
$2^4 \equiv 4^2 \equiv 16$
$2^8 \equiv 16^2 \equiv 256$
$2^{16} \equiv (256)^2 = 65536 \equiv -4 \pmod{3277}$
$2^{32} \equiv (-4)^2 \equiv 16$
$2^{64} \equiv 16^2 \equiv 256$
$2^{128} \equiv (256)^2 \equiv -4$
$2^{256} \equiv (-4)^2 \equiv 16$
$2^{512} \equiv (16)^2 \equiv 256$

$819 - 512 = 307$; $307 - 256 = 51$; $51 - 32 = 19$; $19 - 16 = 3$; $3 - 2 = 1$

So $819 = 1 + 2 + 16 + 32 + 256 + 512$, so $2^{819} = 2 \cdot 2^2 \cdot 2^{16} \cdot 2^{32} \cdot 2^{256} \cdot 2^{512}$

So $2^{819} \underset{3277}{\equiv} 2 \cdot 4 \cdot (-4) \cdot (16) \cdot (16) \cdot (256)$

$\underset{3277}{\equiv} (-32)(256)^2 \underset{3277}{\equiv} (-32)(-4) \underset{3277}{\equiv} 128$ which is $\not\equiv 1$, $\not\equiv -1$.

Then we check

$2^{1638} = (2^{819})^2 \underset{3277}{\equiv} (128)^2 = 16384 = 3277 \times 5 - 1 \underset{3277}{\equiv} -1$.

So $2^{1638} \underset{3277}{\equiv} -1$, so 3277 is a strong pseudoprime to the base 2.