SOLUTION 6

1. Solution

Problem 1

Let $gcd(b, m) = 1$ and $p|(b^n + 1)$.

We have that

$$b^n \equiv -1 mod p. \tag{1}$$

We also know from Fermat's Little Theorem that

$$b^{p-1} \equiv 1 mod p \tag{2}$$

Note that p does not divides b since $p|b^n + 1$.

Now let d be $gcd(n-1, p)$.
We do the problem by assuming 2 cases of d.

Case 1: $d < n$
It is possible to write d as linear combination of $(p-1)$ and n since $d = gcd(p-1, n)$.
We then have

$$\begin{aligned} b^d &= b^{u(p-1)+vn} \\ &= (b^{p-1})^u \cdot (b^n)^v \\ &\equiv 1^u \cdot (-1)^v \bmod p. \end{aligned}$$

We conclude that $b^d \equiv \pm 1 \bmod p$.

Date: Friday, November 7, 2008.

However $b^d \equiv 1 \bmod p$ is impossible since this will contradict to (1).
Also from the similar reason n/d have to be odd.
We conclude i) in this case.

Case 2: $d = n$
We have $n|(p-1)$ from the definition of d. This implies $p \equiv 1 \bmod n$.

However from (1) and (2):
$(p^n)^k \equiv 1 \bmod p$ where $nk = p - 1$.
$(-1)^k \equiv 1 \bmod p$.
So k has 2 as a factor.

We conclude that in this case $p \equiv 1 \bmod 2n$.

Note: Richard mentioned to me this problem p needs to be odd.

Problem 2

First part:
Compare to the theorem in problem 1. b is 2 and the exponent is 2^n.

Case i) could not happen since the exponent is 2^n and has no odd factor.
Case ii) $p \equiv 1 \bmod 2(2^n)$.

Second part:
Using *ifactor* command in Maple:

For $n = 5$
$2^{2^5} + 1 = (641)(6700417)$.
We check that 641 and 6700417 are indeed 1 mod 2^6.

For a historical remark, Fermat conjectured that the number in the form $2^{2^n}+1$ are all primes. Today the number in this form is called Fermat number. He showed his assertion for the case when $n = 0, 1, 2, 3, 4$. He could not factor the number when $n = 5$. Euler disproved his conjecture using exactly the same condition in this problem to find the factor when $n = 5$.

For $n = 6$
$2^{2^6} + 1 = (274177)(67280421310721)$.

We check that 274177 and 67280421310721 are indeed 1 mod 2^7.

For $n = 7$
$2^{2^7} + 1 = (59649589127497217)(5704689200685129054721)$.
We check that 59649589127497217 and 5704689200685129054721 are indeed 1 mod 2^8.

Problem 3

Everyone got this problem using Euler's theorem. However we can solve this problem using only the pigeonhole principle.

Let A be the set of the least positive residue of 2^i mod n for i, $1 \leq i \leq n-1$.
If $1 \in A$ then we're done.

Assume for contradiction that 1 is not in A.
It is obvious that 0 is also not in A since n is odd.

Since we have $n-1$ residues of 2^i mod n, $1 \leq i \leq n-1$ but we have only $n-2$ possible least positive residues in A,
there must be a, b with $a > b$ such that $2^a \equiv 2^b \bmod n$.

Hence $2^{a-b} \equiv 1 \bmod n$. Contradict to our assumption at the beginning.

Problem 4

Let n be a pseudoprime to the base b.
Hence n is an odd composite and $b^{n-1} \equiv 1 \bmod n$.

First to show n is a pseudoprime to the base $-b$.
To show $(-b)^{n-1} \equiv 1 \bmod n$.

we start with the left hand side.

$$\begin{aligned}(-b)^{n-1} &\equiv (-1)^{n-1} \cdot b^{n-1} \bmod n \\ &\equiv (-1)^{n-1} \cdot 1 \bmod n \\ &\equiv 1 \bmod n \text{ , since } n \text{ is odd.}\end{aligned}$$

Second to show n is a pseudoprime to the base b^{-1}.
To show $(b^{-1})^{n-1} \equiv 1 \bmod n$.

we start with the left hand side.

$$\begin{aligned}(b^{-1})^{n-1} &\equiv (b^{n-1})^{-1} \bmod n \\ &\equiv 1^{-1} \bmod n \\ &\equiv 1 \bmod n.\end{aligned}$$

Problem 5

Using the program posted on the web site.

Let S be the set of Carmichael numbers ≤ 5000.
$S = \{561, 1105, 1729, 2465, 2821\}$.

Problem 10 page 236 in the book

To show: $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{ab}$ where a and b are relatively prime.

We show
i) $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{a}$.
ii) $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{b}$

i) $a^{\phi(b)} + b^{\phi(a)} \equiv 0 + 1 \equiv 1 \pmod{a}$ by Euler's Theorem.
ii) Similarly $a^{\phi(b)} + b^{\phi(a)} \equiv 1 + 0 \equiv 1 \pmod{b}$. $\square$