SOLUTION 5

1. Solution

Problem 1

Proof by contrapositive:

Assume n is composite.
To show: $(n-1)!+1$ not congruence to 0 mod n.

We write $n = ab$ where $a > 1$ and $b > 1$.

It is clear that $a|(n-1)!$. Thus a not divide $(n-1)!+1$ since $a > 1$.
As a result n not divide $(n-1)!+1$. $\square$

Problem 2

The Pollard function can factor for $n = 5$ and 6. While the built-in function $ifactor$ can factor for $n = 5, 6$ and 7.
I am a bit disappointed. But this is not the first time Maple beats me.

Problem 12 page 221

$2^{16} \equiv 1 \bmod 17$ by Fermat's Little Theorem.
$(2^{16})^{62500} \equiv 1^{62500} \bmod 17$.
Hence $2^{1000000} \equiv 1 \bmod 17$.
The least positive residue is 1.

Problem 22 page 221

People show me some different ways to do this problem.
I will try to make use of the corollary of Fermat's little theorem.
$a^p \equiv a \bmod p$ for all integer a.

To show: $30|(n^9 - n)$

Date: Tuesday, October 21, 2008.

We show
i) $2|(n^9 - n)$
ii) $3|(n^9 - n)$
iii) $5|(n^9 - n)$.

i) We will repeatedly apply: $n^2 \equiv n \bmod 2$.
We have $n^9 = (n^2)^4(n) \equiv n^4 n \equiv n^2(n) \equiv n(n) \equiv n \bmod 2$.
This shows $2|(n^9 - n)$.

ii) Similarly $n^3 \equiv n \bmod 3$.
We have $n^9 \equiv (n^3)^3 \equiv n^3 \equiv n \bmod 3$.
This shows $3|(n^9 - n)$.

iii) Also $n^5 \equiv n \bmod 5$.
We have $n^9 \equiv (n^5)(n^4) \equiv n(n^4) = n^5 \equiv n \bmod 5$.
This shows $5|(n^9 - n)$. $\square$

Problem 23 page 221

We start from LHS:
$\sum_{k=1}^{p-1} k^{p-1} \equiv \sum_{k=1}^{p-1} 1 \bmod p$ by Fermat's little theorem.

$$\equiv (p-1) \bmod p.$$

$$\equiv -1 \bmod p. \ \square$$