SOLUTION 4

1. Solution

Problem 1

Proof by contra positive:
Assume $n \neq 2^k$ for any positive integer k.
To show: $2^n + 1$ is not a prime ≥ 5.

We have that n has an odd factor, say d.
(Or else $n = 2^0$ which gives $2^n + 1 = 2^{2^0} + 1 = 3$ (a prime less than 5)).
Now n can be written as $n = d \cdot n'$.
Let $x = 2^{n'}$.
We can now factor $2^n + 1$ as follow:
$2^n - 1 = 2^{n' \cdot d} + 1 = x^d + 1 = (x + 1)(x^{d-1} - x^{d-2} + ... + 1)$ since d is odd.
$x + 1 > 1$, since $x \geq 1$. We then have $2^n + 1$ is composite.

Problem 2

a) $341 = 11 \cdot 31$
b) $2^{10} - 1 = 1023 \equiv 0 \mod 341$
$\Rightarrow 2^{10} \equiv 1 \mod 341$.
c) $(2^{10})^{34} \equiv 1^{34} \mod 341$
$\Rightarrow 2^{340} \equiv 1 \mod 341$
$\Rightarrow 2^{341} \equiv 2 \mod 341$.

Problem 3

a) $x \equiv y \mod m$
$\Rightarrow 3x \equiv 3y \mod m$
$\Rightarrow 3x + 2 \equiv 3y + 2 \mod m$.

b) $x \equiv y \mod m$
$\Rightarrow x^3 \equiv y^3 \mod m$

Date: Friday, October 10, 2008.

$\Rightarrow x^3 - x \equiv y^3 - y \bmod m$.

c) Assume $P(x) = \sum_{i=0}^{n} a_i x^i$.
$x \equiv y \bmod m$
$\Rightarrow x^i \equiv y^i \bmod m$, for all non-negative integer i
$\Rightarrow a_i x^i \equiv a_i y^i \bmod m$, for all non-negative integer i
$\Rightarrow \sum_{i=0}^{n} a_i x^i \equiv \sum_{i=0}^{n} a_i y^i \bmod m$
$\Rightarrow P(x) \equiv P(y) \bmod m$.

Problem 4

First, we simply the bases.
Since $2222 \equiv 3 \pmod 7$ and $5555 \equiv 4 \pmod 7$, we have
$2222^{5555} + 5555^{2222} \equiv 3^{5555} + 4^{2222} \pmod 7$.

Since $3^6 \equiv 1 \pmod 7$ and $3^5 \equiv 5 \pmod 7$, we have
$3^{5555} = (3^6)^{925}(3^5) \equiv 1^{625}5 \bmod 7 \equiv 5 \pmod 7$.

Similarly $4^3 \equiv 1 \pmod 7$ and $4^2 \equiv 2 \pmod 7$, we have
$4^{2222} = (4^3)^{740}(4^2) \equiv 1^{740}2 \pmod 7 \equiv 2 \pmod 7$.

Therefore $3^{5555} + 4^{2222} \equiv 5 + 2 \pmod 7 \equiv 0 \pmod{7}$.

Problem 5

I was hoping to use the method we learn to solve linear diophantine equation to this problem.

a) Solve $5x \equiv 4 \bmod 3$.
We solve the equation $5x + 3y = 4$.

First find $gcd(5, 3)$ using Euclidean algorithm.

5 = 1(3)+2
3 = 1(2)+1
2 = 2(1).

Second we write 1 as a linear combination of 5 and 3 .

1 = 3 - 1(2).
Then 1 = 3-1(5-3).

$\Rightarrow$ 1 = -(5)+2(3).

Third, we multiply 4 through the whole equation.
4 = -4(5)+8(3).

Therefore $x = -4 + 3k$ for any integer k.

b) Solve $7x \equiv 6 \bmod 5$.
We solve similarly and find $x = -2 + 5k$ for any integer k.

Problem 6

Everyone is doing well in this problem.

$3523 = 271 \cdot 13$.
$2342409 = 780803 \cdot 3$.
$120938091 = 18299 \cdot 6609$.
$32804989 = 36901 \cdot 889$.

Problem 22 page 150

To show: $4^n \equiv 1 + 3n \bmod 9$ for a positive integer n.

Proof by induction:
Base case: $n = 1$.
$4^1 = 4$ and 1+3(1) =4.
so $4^n \equiv 1 + 3(n) \bmod 4$ is true for $n = 1$.

Induction step: assume the statement is true for all k where $1 \leq k \leq n - 1$.
To show: the statement is true for $k = n$.

We start on the left hand side and try to convert it to the right hand side.

$4^n = 4^{n-1}(4) \equiv (1 + 3(n - 1))4 \bmod 4$ by induction hypothesis.
$\equiv 4 + 12n - 4 \bmod 9$
$\equiv 3n \bmod 9$. $\square$.

Problem 8 page 157

8a) The inverse of 2 mod 13 is 7.
8b) The inverse of 3 mod 13 is 9.

Problem 4a) page 164

We use Chinese Remainder Theorem.

$M = 11 \cdot 17 = 187.$
$M_1 = \frac{187}{11} = 17.$
$M_2 = \frac{187}{17} = 11.$
$M_1^{-1} \bmod 11 = 2.$
$M_2^{-1} \bmod 17 = 14.$

$x = a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} \pmod{187}$
$= 4(17)(2)+3(11)(14) \pmod{187}$
$= 598 \pmod{187}$
$= 37.$

Therefore the solutions of these system of equations are $37 + 187k$ for any integer k.