Key

Math 320 - Dr. Miller - Exam #2, Fall 2015 - **DUE: Weds., Oct. 28, 2015 - Take-Home Portion**

As a take-home, this 25-point portion of the exam will be individualized to protect academic integrity. You are expected not to give nor seek help from any source but your own notes, text, calculator, myself, and the permitted web site below. Each of you will work with your own 4-digit number N for these problems. Here is how to create your value of N:

(*) Write your birth date as a 4-digit code, such as March 15 = 0315, October 27 = 1027.

(*) Add 1000 to your code if your last name starts with A-M; add 2000 otherwise.

(*) Double the number you now have. The result is your value of N.

Write your value of N here: _____.

Prime factor your N; I do not need to see your work - you may choose to use the applet at this web site: http://www.mathwarehouse.com/arithmetic/numbers/prime-number/prime-factorization-calculator.php .

Write your prime factorization here: _____.

smallest

Let p_1 be the ~~largest~~ prime number in your factorization and $P = p_1^{e_1}$ its total contribution to the prime factorization above. For instance, if $N = 2^2 \cdot 3 \cdot 7^3$, then $p_1 \neq 7$ and $P \neq 7^3$; if $N = 5 \cdot 11^4 \cdot 101$, then $P \neq 101$. It will be helpful to write P in standard form if it isn't already: $P = 343$ may be more useful than $P = 7^3$.

Write your values of p_1, P, and N/P in standard form below:

$p_1 =$, $P =$, $N/P =$

Here are the actual exam questions. Staple this question sheet to the front when you hand them in.

1. *[10 pts]* Find the multiplicative inverse of N mod 20011; show clear work and write your answer as a least nonnegative residue.
2. *[5 pts]* Solve the single congruence $Nx + 20011y \equiv 1 \ mod \ 100$. Show clear work and write your answer(s) in least nonnegative residue form.
3. *[10 pts]* Solve the following system of congruences by any meaningful method; show clear work, and write your answer(s) in least nonnegative residue form.

$$\begin{aligned} x &\equiv 2 \ mod \ P \\ x &\equiv 1 \ mod \ N/P \\ x &\equiv 3 \ mod \ 20011 \end{aligned}$$

Math 320 – Sample Solution to Exam #2 Take-Home – W, 10/28/15

I'll use $N = 4442$.

Its prime factorization is $2 \cdot 2221$

$p_1 = 2$, $P = 2$, $N/P = 2221$

1. Find the multiplicative inverse of 4442 mod 20011.

$$\begin{array}{r} 4 \\ 4442\overline{)20011} \\ -17768 \\ \hline 2243 \end{array} \qquad \begin{array}{r} 1 \\ 2243\overline{)4442} \\ -2243 \\ \hline 2199 \end{array} \qquad \begin{array}{r} 1 \\ 2199\overline{)2243} \\ -2199 \\ \hline 44 \end{array}$$

$$\begin{array}{r} 49 \\ 44\overline{)2199} \\ -2156 \\ \hline 43 \end{array} \qquad \begin{array}{r} 1 \\ 43\overline{)44} \\ -43 \\ \hline 1 \end{array}$$

$$\begin{aligned} 20011 &= 4 \cdot 4442 + 2243 \\ 4442 &= 1 \cdot 2243 + 2199 \\ 2243 &= 1 \cdot 2199 + 44 \\ 2199 &= 49 \cdot 44 + 43 \\ 44 &= 1 \cdot 43 + 1 \end{aligned}$$

$$
\begin{aligned}
1 &= 44 - 1\cdot 43 \\
&= 44 - (2199 - 49\cdot 44) \\
&= 50\cdot 44 - 2199 \\
&= 50\cdot(2243 - 1\cdot 2199) - 2199 \\
&= 50\cdot 2243 - 51\cdot 2199 \\
&= 50\cdot 2243 - 51\cdot(4442 - 1\cdot 2243) \\
&= 101\cdot 2243 - 51\cdot 4442 \\
&= 101\cdot(20011 - 4\cdot 4442) - 51\cdot 4442 \\
&= 101\cdot 20011 - 455\cdot 4442
\end{aligned}
$$

So mod 20011, $1 \equiv -455\cdot 4442$,

making $N^{-1} = 4442^{-1} = -455$

$\equiv 19556 \pmod{20011}$

2. Solve $4442x + 20011y \equiv 1 \pmod{100}$.

I already know from above that

$4442\cdot(-455) + 20011\cdot(101) = 1$ outright

so $4442\cdot(-455) + 20011\cdot(101) \equiv 1 \pmod{100}$

$x \equiv -455 \equiv 45 \pmod{100}$

$y \equiv 101 \equiv 1 \pmod{100}$ is the solution generated by this approach.

3. Solve $\begin{cases} x \equiv 2 \mod 2 \\ x \equiv 1 \mod 2221 \\ x \equiv 3 \mod 20011 \end{cases}$

CRT formula solu:

$\boxed{b_1 = 2}$ $m_1 = 2$ $M_1 = 2221 \cdot 20011$ $\boxed{= 44,444,431}$

$M_1 x \equiv 1 \mod 2$

is $1 \cdot x \equiv 1 \mod 2$ so $\boxed{w_1 = 1}$

$\boxed{b_2 = 1}$ $m_2 = 2221$ $M_2 = 2 \cdot 20011 = \boxed{40022}$

$M_2 x \equiv 1 \mod 2221$

is $44x \equiv 1 \mod 2221$

$$\begin{array}{r} 50 \\ 44\overline{)2221} \\ -2200 \\ \hline 21 \end{array} \qquad \begin{array}{r} 2 \\ 21\overline{)44} \\ -42 \\ \hline 2 \end{array} \qquad \begin{array}{r} 10 \\ 2\overline{)21} \\ -20 \\ \hline 1 \end{array}$$

$$\begin{aligned} 1 &= \underline{21} - 10 \cdot \underline{2} \\ &= \underline{21} - 10 \cdot (\underline{44} - 2 \cdot \underline{21}) \\ &= 21 \cdot \underline{21} - 10 \cdot \underline{44} \\ &= 21 \cdot (\underline{2221} - 50 \cdot \underline{44}) - 10 \cdot \underline{44} \\ &= 21 \cdot \underline{2221} - 1060 \cdot \underline{44} \end{aligned}$$

$\Rightarrow \boxed{w_2 = -1060}$

$b_3 = 3$ $\quad m_3 = 20011$ $\quad M_3 = N = 4442$

$w_3 = 19556$ from #1

$$X = b_1 M_1 w_1 + b_2 M_2 w_2 + b_3 M_3 w_3$$
$$= 2 \cdot 44,444,431 \cdot 1 + 1 \cdot 40022 \cdot (-1060) + 3 \cdot 4442 \cdot 19556$$
$$= 307,068,798 \bmod N \cdot 20011$$
$$\equiv 88888862 \bmod N \cdot 20011$$

$$\boxed{X \equiv 40,402,212 \bmod N \cdot 20011}$$

Back-substitution method:

$x = 2 + 2k$ for $k \in \mathbb{Z}$

$2 + 2k \equiv 1 \bmod 2221$

$2k \equiv -1 \bmod 2221$

$\cdot 1110 \quad \cdot 1110$

$-k \equiv -1110 \bmod 2221$

$k \equiv 1110 \bmod 2221$

$k = 1110 + 2221\ell$ for $\ell \in \mathbb{Z}$

$x = 2 + 2(1110 + 2221\ell)$

$= 2222 + 4442\ell$

$$2222 + 4442\ell \equiv 3 \mod 20011$$

$$4442\ell \equiv -2219 \mod 20011$$

from #1 $\times 19556 \quad \times 19556$

$$\ell \equiv -43394764 \mod 20011$$

$$\ell \equiv 9095 \mod 20011$$

$$\ell = 9095 + 20011m \text{ for } m \in \mathbb{Z}$$

$$x = 2222 + 4442(9095 + 20011m)$$

$$= 40402212 + 88888862m$$

$$\boxed{x \equiv 40,402,212 \mod 88888862}$$