T-79.5501 Cryptology
First midterm exam
May 7th, 2007
SOLUTIONS

1. We add 1 to each side of the equation to obtain $(x-5)^2 = 1 \pmod n$. Hence we have to solve equation $y^2 = 1 \pmod n$, where $y = x - 5$. The trivial solutions are $y = \pm 1 \pmod n$ that is $x = 6$ and $x = 4$. A non-trivial solution is given by the system

$$\begin{cases} y = 1 \pmod{17} \\ y = -1 \pmod{19}. \end{cases}$$

We will use the CRT to solve the system. We get $m_1 = 17, m_2 = 19, M_1 = 19, M_2 = 17, y_1 = M_1^{-1} = -8 \pmod{17}$ and $y_2 = M_2^{-1} = 9 \pmod{19}$. The solution is then $y = -19 * 8 - 17 * 9 = 305 \pmod n$ from which we get that $x = 310$. The last solution is $y = n - 305 = 18$ from which $x = 23$.

2. (a) Let us calculate

$$\begin{aligned} \pi_S(w + x^2) &= (w + x^2)^3 = w^3 + w^2x^2 + wx^4 + x^6 \\ &= \pi_S(w) + w^2x^2 + wx(x+1) + (x+1)^2 \\ &= \pi_S(w) + w^2x^2 + w(x^2+x) + x^2 + 1 \end{aligned}$$

and $\pi_S(w + a') + \pi_S(w) = w^2x^2 + w(x^2 + x) + x^2 + 1$ for all w.

(b) From part a) we see that $b' = \pi_S(w) + \pi_S(w + a') = x^2w^2 + (x^2 + x)w + x^2 + 1$. Hence, we get the following table:

w	b'
0	x^2+1
1	x^2+x+1
x	x^2
$x+1$	x^2+x
x^2	x^2+1
x^2+1	x^2+x+1
x^2+x	x^2
x^2+x+1	x^2+x

The row of $N(a', b')$ with $a' = x^2$ is

b'	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
$a' = x^2$	0	0	0	0	2	2	2	2

3. First we calculate $\phi(n) = 4 * 210 = 840$. Then $a = b^{-1} = 611 \pmod{\phi(n)}$ can be calculated by Euclidean Algorithm. Now $611 = 2^9 + 2^6 + 2^5 + 2^1 + 2^0$ and we use Square And Multiply to calculate $x = y^a \pmod n$. We have that $y^2 = 481, y^4 = 316$ etc. The other necessary powers are $y^{512} = 1016, y^{64} = 561$ and $y^{32} = 136$ such that $y^a = 1016 * 561 * 136 * 481 * 314 = 924 = x$.

4. We use Shanks' algorithm with $\alpha = 202$, $G =< \alpha >$ in $\mathbb{Z}_{2005}$, $n = 16$, and $\beta = 133$. Then $m = \lceil \sqrt{16} \rceil = 4$, and $\alpha^m = 202^4 = 381 \pmod{2005}$. The first list L_1 is then as follows:

j	$381^j \bmod 2005$
0	1
1	381
2	801
3	421

To compute the second list we compute first $202^{-1} \bmod 2005 = 268$. Then

i	$133 \cdot 268^i \bmod 2005$
0	133
1	1599
2	772
3	381

from where we see that the solution is $j = 1$ and $i = 3$ from where $x = 1 * 4 + 3 = 7$.